Department of Digital Systems
School of Information and Communication Technologies
University of Piraeus

Advanced Cyber Security Solutions for Critical Infrastructure and Applications: Smart Grid and Cyber Insurance

Aristeidis Farao

A thesis presented for the degree of
Doctor of Philosophy

Piraeus, Greece
February 2024

Department of Digital Systems
School of Information and Communication Technologies
University of Piraeus

Advanced Cyber Security Solutions for Critical Infrastructure and Applications: Smart Grid and Cyber Insurance

Supervisor:
Prof. Christos Xenakis
Advisors:
Prof. Costas Lambrinoudakis
Assoc. Prof. Christos Doulkeridis

A thesis presented for the degree of
Doctor of Philosophy

Piraeus, Greece
February 2024

APPROVAL SHEET
UNIVERSITY OF PIRAEUS
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
DEPARTMENT OF DIGITAL SYSTEMS

This document hereby attests to the submission of the doctoral thesis authored by Aristeidis Farao, entitled 'Advanced Cyber Security Solutions for Critical Infrastructure and Applications: Smart Grid and Cyber Insurance' as a fulfillment of the stipulated criteria for the Doctor of Philosophy degree. The thesis has been subjected to a comprehensive review to ensure compliance with the guidelines of the University of Piraeus and conformity with established benchmarks for originality.

Christos Xenakis
Professor, University of Piraeus
Supervisor

Costas Lambrinoudakis
Professor, University of Piraeus
Advisor

Christos Doulkeridis
Associated Professor, University of Piraeus
Advisor

Foteini Asderaki
Professor, University of Piraeus
External Examiner

Sokratis Katsikas
Professor, Norwegian University of Science and Technology
External Examiner

Dionysis Xenakis
Assistant Professor, National and Kapodistrian Unviersity of Athens
External Examiner

Evangelos Markakis
Assistant Professor, Hellenic Mediterenian University
External Examiner

Ithaka

As you set out for Ithaka
hope your road is a long one,
full of adventure, full of discovery.
Laistrygonians, Cyclops,
angry Poseidon—don't be afraid of them:
you'll never find things like that on your way
as long as you keep your thoughts raised high,
as long as a rare excitement
stirs your spirit and your body.
Laistrygonians, Cyclops,
wild Poseidon—you won't encounter them
unless you bring them along inside your soul,
unless your soul sets them up in front of you.
Hope your road is a long one.
May there be many summer mornings when,
with what pleasure, what joy,
you enter harbors you're seeing for the first time;
may you stop at Phoenician trading stations
to buy fine things,
mother of pearl and coral, amber and ebony,
sensual perfume of every kind—
as many sensual perfumes as you can;
and may you visit many Egyptian cities
to learn and go on learning from their scholars.
Keep Ithaka always in your mind.
Arriving there is what you're destined for.
But don't hurry the journey at all.
Better if it lasts for years,
so you're old by the time you reach the island,
wealthy with all you've gained on the way,
not expecting Ithaka to make you rich.
Ithaka gave you the marvelous journey.
Without her you wouldn't have set out.
She has nothing left to give you now.
And if you find her poor, Ithaka won't have fooled you.
Wise as you will have become, so full of experience,
you'll have understood by then what these Ithakas mean.

C. P. Cavafy, 'The City' from C.P. Cavafy: Collected Poems.

Acknowledgements

I would like to express my sincere appreciation and gratitude to the individuals who have made significant contributions to this dissertation and have played a crucial role in fostering my scientific growth throughout the preceding years. In the beginning, I would like to sincerely thank my supervisor, Professor Christos Xenakis, for his priceless guidance, unending support, and faith in me and my abilities, as well as, for allowing me to participate in several national and European projects that broadened my horizons to several scientific fields.

I would like to express my gratitude to the advisory committee, Professor Costas Lambrinoudakis, and Assoc. Professor Christos Doulkeridis for their invaluable contributions.

In addition, I would like to extend my thanks to the European Security and Defense College and the Common Security and Defense Policy for their invaluable contributions to my research in the field of cybersecurity dynamics being a fellow since 2022.

Furthermore, I would like to express my gratitude to the members of the Security Systems Laboratory at the University of Piraeus, specifically Panagiotis Bountakas and Vaios Bolgouras for their invaluable cooperation, support and friendship during these years.

Last but not least, I would like to thank my family and BaKon for always believing in me and supporting my decisions. This dissertation could not be possible without you.

Abstract

The rapid digitization of critical infrastructure, coupled with the increasing sophistication of cyber threats, has elevated the importance of robust cybersecurity measures. This dissertation explores the multifaceted realm of cyber defense within the context of critical infrastructure, focusing specifically on the interplay between advanced cyber security solutions, smart grid technology, and the emerging field of cyber insurance. The research begins by dissecting the vulnerabilities inherent in smart grid systems, which form the backbone of modern energy distribution networks. Through a comprehensive analysis of cyber threats targeting smart grids, the study identifies potential attack vectors and assesses the implications of successful breaches on the reliability and resilience of critical energy infrastructure. Subsequently, a range of advanced cyber security solutions is evaluated, encompassing cutting-edge technologies such as artificial intelligence, machine learning, and blockchain, in order to fortify the defenses of smart grid ecosystems. In parallel, the dissertation delves into the evolving landscape of cyber insurance as a risk management strategy for critical infrastructure. Investigating the intricacies of underwriting policies and the quantification of cyber risks, the research elucidates the role of cyber insurance in incentivizing proactive cyber hygiene and fostering a culture of resilience among infrastructure stakeholders. The study also explores the challenges associated with the integration of cyber insurance into existing risk management frameworks and proposes strategies to optimize its efficacy. Furthermore, the dissertation offers a synthesized perspective by examining the synergies between advanced cyber security solutions and cyber insurance. It investigates how a holistic approach, combining technological fortification and financial risk mitigation, can elevate the overall cybersecurity posture of critical infrastructure. Case studies and real-world examples illustrate the practical implementation of these integrated strategies, providing valuable insights for industry practitioners and policymakers alike. In conclusion, this dissertation contributes to the academic discourse on cybersecurity for critical infrastructure by offering a comprehensive examination of advanced solutions tailored to the unique challenges posed by smart grid ecosystems. By exploring the symbiotic relationship between technological fortifications and financial risk mitigation through cyber insurance, this research provides a roadmap for enhancing the cyber resilience of critical infrastructure in the face of evolving cyber threats.

Περίληψη

Η ταχεία ψηφιοποίηση των κρίσιμων υποδομών, σε συνδυασμό με την αυξανόμενη πολυπλοκότητα των απειλών στον κυβερνοχώρο, έχει αυξήσει τη σημασία των ισχυρών μέτρων κυβερνοασφάλειας. Η παρούσα διατριβή διερευνά το πολύπλευρο πεδίο της κυβερνοάμυνας στο πλαίσιο των κρίσιμων υποδομών, εστιάζοντας συγκεκριμένα στην αλληλεπίδραση μεταξύ προηγμένων λύσεων κυβερνοασφάλειας, της τεχνολογίας έξυπνων δικτύων και του αναδυόμενου τομέα της κυβερνοασφάλισης. Η έρευνα ξεκινά με την ανάλυση των τρωτών σημείων που ενυπάρχουν στα συστήματα έξυπνων δικτύων, τα οποία αποτελούν τη ραχοκοκαλιά των σύγχρονων δικτύων διανομής ενέργειας. Μέσω μιας ολοκληρωμένης ανάλυσης των απειλών στον κυβερνοχώρο που στοχεύουν τα έξυπνα δίκτυα, η μελέτη εντοπίζει πιθανούς φορείς επίθεσης και αξιολογεί τις επιπτώσεις των επιτυχημένων παραβιάσεων στην αξιοπιστία και την ανθεκτικότητα των κρίσιμων ενεργειακών υποδομών. Στη συνέχεια, αξιολογείται μια σειρά προηγμένων λύσεων κυβερνοασφάλειας, που περιλαμβάνουν τεχνολογίες αιχμής, όπως η τεχνητή νοημοσύνη, η μηχανική μάθηση και η blockchain, προκειμένου να ενισχυθεί η άμυνα των οικοσυστημάτων έξυπνων δικτύων. Παράλληλα, η διατριβή εμβαθύνει στο εξελισσόμενο τοπίο της ασφάλισης στον κυβερνοχώρο ως στρατηγική διαχείρισης κινδύνων για τις κρίσιμες υποδομές. Διερευνώντας τις περιπλοκές των πολιτικών ανάληψης κινδύνων και την ποσοτικοποίηση των κινδύνων στον κυβερνοχώρο, η έρευνα διευκρινίζει τον ρόλο της ασφάλισης στον κυβερνοχώρο ως κίνητρο για την προληπτική υγιεινή στον κυβερνοχώρο και την προώθηση μιας κουλτούρας ανθεκτικότητας μεταξύ των ενδιαφερομένων για τις υποδομές. Η μελέτη διερευνά επίσης τις προκλήσεις που συνδέονται με την ενσωμάτωση της ασφάλισης στον κυβερνοχώρο στα υφιστάμενα πλαίσια διαχείρισης κινδύνων και προτείνει στρατηγικές για τη βελτιστοποίηση της αποτελεσματικότητάς της. Επιπλέον, η διατριβή προσφέρει μια συνθετική προοπτική εξετάζοντας τις συνέργειες μεταξύ των προηγμένων λύσεων ασφάλειας στον κυβερνοχώρο και της ασφάλισης στον κυβερνοχώρο. Διερευνά τον τρόπο με τον οποίο μια ολιστική προσέγγιση, που συνδυάζει την τεχνολογική ενίσχυση και τον μετριασμό των οικονομικών κινδύνων, μπορεί να ανυψώσει τη συνολική στάση της κυβερνοασφάλειας των υποδομών ζωτικής σημασίας. Μελέτες περιπτώσεων και παραδείγματα από τον πραγματικό κόσμο απεικονίζουν την πρακτική εφαρμογή αυτών των ολοκληρωμένων στρατηγικών, παρέχοντας πολύτιμες γνώσεις τόσο για τους επαγγελματίες του κλάδου όσο και για τους υπεύθυνους χάραξης πολιτικής. Εν κατακλείδι, η παρούσα διατριβή

συμβάλλει στην ακαδημαϊκή συζήτηση για την κυβερνοασφάλεια των υποδομών ζωτικής σημασίας προσφέροντας μια ολοκληρωμένη εξέταση των προηγμένων λύσεων προσαρμοσμένων στις μοναδικές προκλήσεις που θέτουν τα οικοσυστήματα έξυπνων δικτύων. Με τη διερεύνηση της συμβιωτικής σχέσης μεταξύ των τεχνολογικών οχυρώσεων και του μετριασμού του οικονομικού κινδύνου μέσω της ασφάλισης στον κυβερνοχώρο, η παρούσα έρευνα παρέχει έναν οδικό χάρτη για την ενίσχυση της ανθεκτικότητας των υποδομών ζωτικής σημασίας στον κυβερνοχώρο ενόψει των εξελισσόμενων απειλών στον κυβερνοχώρο.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In an era defined by digital evolution and technological progress, the security of critical infrastructure and applications has emerged as a paramount concern. As our world becomes increasingly interconnected, the vulnerabilities of essential systems such as Smart Grids demand robust and sophisticated solutions to ensure resilience against evolving cyber threats. This pressing need for security has given rise to advanced cyber security solutions tailored specifically for safeguarding critical infrastructure and applications.

At the heart of this paradigm shift is the Smart Grid, a dynamic and intelligent energy distribution system that relies heavily on digital communication and data exchange. As we entrust our essential services to these interconnected networks, the potential risks amplify, underscoring the vital importance of advanced cyber security measures. The integration of cutting-edge technologies, such as artificial intelligence, machine learning, and blockchain, into cyber security solutions, paves the way for a fortified defense against cyber threats that could otherwise compromise the integrity of critical infrastructure.

One of the key elements in fortifying critical infrastructure against cyber threats is the deployment of advanced threat detection and prevention systems. These systems are designed to autonomously identify and thwart potential threats in real-time, providing a proactive defense against malicious actors seeking to exploit vulnerabilities. By leveraging artificial intelligence algorithms, these solutions can analyze massive datasets, recognize patterns, and detect anomalies, thereby enhancing the ability to detect even the most sophisticated cyber threats.

Moreover, the advent of machine learning in cyber security solutions of-

fers a dynamic and adaptive defense mechanism. Machine learning algorithms can learn from past incidents, continuously evolving to anticipate and counteract emerging cyber threats. This level of adaptability is crucial in an environment where cyber threats are constantly evolving, demonstrating the necessity of investing in solutions that can evolve in tandem with the threat landscape.

Blockchain technology is another powerful ally in the quest for cyber resilience. By decentralizing data storage and ensuring the immutability of records, blockchain adds an extra layer of security to critical infrastructure. In the context of Smart Grids, where vast amounts of sensitive data are exchanged, blockchain can mitigate the risk of unauthorized access and tampering, thereby enhancing the overall integrity and trustworthiness of the system.

As we embark on the journey to fortify critical infrastructure, collaboration between public and private sectors becomes paramount. Government agencies, utility companies, and cyber security experts must unite to share insights, intelligence, and best practices. A collective effort is essential to stay ahead of cyber threats and create a robust defense ecosystem that can effectively counteract the sophisticated tactics employed by cybercriminals.

However, the evolution of cyber security is not solely reliant on technological advancements. Equally critical is the human factor. Cybersecurity awareness and education play a pivotal role in fortifying the defense against cyber threats. Training programs that empower individuals with the knowledge to identify and respond to potential threats can significantly reduce the risk of successful cyber attacks. By fostering a culture of cyber hygiene, organizations can create a human firewall that complements the technological defenses in place.

In tandem with advanced cyber security solutions, the integration of Smart Grid technologies is pivotal in fortifying critical infrastructure. Smart Grids offer unprecedented efficiency and flexibility in energy distribution, allowing for real-time monitoring, analysis, and adaptive responses. However, with great power comes great responsibility, and the Smart Grid's reliance on digital connectivity demands a robust cyber security framework.

The convergence of advanced cyber security solutions and Smart Grid innovations is not merely a technological integration but a symbiotic relationship that reinforces the resilience of critical infrastructure. A secure Smart Grid not only safeguards the continuous and reliable flow of energy but also ensures the stability of interconnected systems that rely on this vital

resource. It is the linchpin that holds together the intricate web of services and industries that constitute our modern way of life.

Furthermore, the integration of cyber insurance into the equation provides an additional layer of protection. In the face of ever-evolving cyber threats, no system can be deemed entirely invulnerable. Cyber insurance acts as a safety net, offering financial protection against potential damages resulting from cyber attacks. This proactive approach not only mitigates the financial impact of a successful cyber attack but also incentivizes organizations to invest in robust cyber security measures.

The landscape of cyber threats is vast and continually evolving, ranging from ransomware attacks to sophisticated state-sponsored cyber espionage. The importance of a comprehensive and multi-faceted defense strategy cannot be overstated. Cyber insurance, when coupled with advanced cyber security solutions and Smart Grid innovations, forms a formidable trio that enhances the overall resilience of critical infrastructure.

The financial implications of a cyber attack extend far beyond the immediate costs of remediation. Reputational damage, loss of customer trust, and potential legal consequences can have a lasting impact on an organization. Cyber insurance provides a safety net that allows organizations to recover more swiftly from the aftermath of a cyber attack. This, in turn, fosters a proactive approach to cyber security, as organizations recognize the tangible benefits of investing in robust protective measures.

In conclusion, the imperative to fortify critical infrastructure and applications against cyber threats is non-negotiable in our interconnected and digitized world. Advanced cyber security solutions, Smart Grid innovations, and cyber insurance together form a comprehensive defense strategy that not only mitigates risks but also ensures the continuous and secure operation of essential systems. By embracing these advancements, we not only protect our critical infrastructure but also lay the foundation for a resilient and secure future. It is a call to action for collaboration, innovation, and a shared commitment to safeguarding the foundation upon which our modern society is built.

Overall, the scientific publications stemming from this thesis are presented in Table 1.1.

Authors	Title	Venue
Journals		

Farao A, Paparis G, Panda S, Panaousis E, Zarras A, Xenakis C	INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain	IJIS, Springer [IF : 3.2]
Farao A, Veroni E, Ntantogian C, Xenakis C	P4G2Go: A Privacy-Preserving Scheme for Roaming Energy Consumers of the Smart Grid-to-Go [1]	Sensors MDPI [IF : 3.9]
Muñoz A, **Farao A**, Correia JR, Xenakis C	P2ISE: Preserving Project Integrity in CI/CD Based on Secure Element	Information MDPI [IF : 3.1]
Suciu G, **Farao A**, Bernardinetti G, Palamà I, Sachian MA, Vulpe A, Vochin MC, Muresan P, Bampatsikos M, Muñoz A, Xenakis C.	SAMGRID: Security Authorization and Monitoring Module Based on SealedGRID Platform [2]	Sensors MDPI [IF : 3.9]
Suciu G, Sachian MA, Vulpe A, Vochin M, **Farao A**, Koutroumpouchos N, Xenakis C	Sealedgrid: Secure and interoperable platform for smart grid applications	Sensors MDPI [IF : 3.9]
Conferences with Proceedings		
Charalambous M, **Farao A**, Kalantzantonakis G, Kanakakis P, Salamanos N, Kotsifakos E, Froudakis E	Analyzing Coverages of Cyber Insurance Policies Using Ontology [3]	ARES 2023, ACM [$Rank : B$]
Petihakis G, Kiritsis D, **Farao A**, Bountakas P, Panou A, Xenakis C	A Bring Your Own Device security awareness survey among professionals [4]	ARES 2023, ACM [$Rank : B$]

Pantelakis, V., Bountakas, P., Farao, A., Xenakis, C.	Adversarial Machine Learning Attacks on Multiclass Classification of IoT Network Traffic [5]	ARES 2023, ACM $[Rank: B]$
Leonidou, P., Salamanos, N., **Farao, A.**, Aspri, M. and Sirivianos, M.	A qualitative analysis of illicit arms trafficking on darknet marketplaces [5]	ARES 2023, ACM $[Rank: B]$
Karatisoglou M, **Farao A**, Bolgouras V, Xenakis C	BRIDGE: BRIDGing the gap bEtween CTI production and consumption [6]	COMM 2022, IEEE $[Rank: B]$
Kalderemidis I, **Farao A**, Bountakas P, Panda S, Xenakis C	GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments [7]	ARES 2022, ACM $[Rank: B]$
Farao A, Panda S, Menesidou S. A, Veliou E, Episkopos N, Kalatzantonakis G, ... & Xenakis C	SECONDO: A platform for cybersecurity investments and cyber insurance decisions [8]	TrustBus 2020, Springer $[Rank: B]$
Muñoz A, **Farao A**, Correia JR, Xenakis C	ICITPM: integrity validation of software in iterative continuous integration through the use of Trusted Platform Module (TPM) [9]	ESORICS 2020, Springer $[Rank: A]$
Farao A, Rubio JE, Alcaraz C, Ntantogian C, Xenakis C, Lopez J.	Sealedgrid: A secure interconnection of technologies for smart grid applications [10]	CRITIS 2019, Springer $[Rank: C]$

Farao A, Ntantogian C, Istrate C, Suciu G, Xenakis C	SealedGRID: Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID [11]	ICS & CSR 2019, eWiC $[Rank : C]$
Suciu G, Istrate CI, Vulpe A, Sachian MA, Vochin MC, **Farao A**, Xenakis C	Attribute-based access control for secure and resilient smart grids [12]	ICS & CSR 2019, eWiC $[Rank : C]$
Suciu G, Istrate C, Sachian MA, Vulpe A, Vochin M, **Farao A**, Xenakis C	FI-WARE authorization in a Smart Grid scenario [13]	GIoTs 2020, IEEE, $[Rank : C]$
Book Chapter		
Panda S, **Farao A**, Panaousis E, Xenakis C	Cyber-Insurance: Past, Present and Future	Encyclopedia of Cryptography & Security and Privacy 2021 Springer

Table 1.1: List of scientific publications stemming from this thesis.

Chapter 2

Smart Grid Security

2.1 Security and Privacy requirements and challenges of the Smart Grid

The rapid evolution of Information and Communications Technologies (ICT) has revealed the potential for centrally monitoring, controlling, and optimizing power grid networks. In this context, a more intelligent, responsive, and efficient, system has been devised, known as the Smart Grid (SG). As explained in the European Union (EU) Third Energy Package, the SG will support a dynamic two-way information exchange between Utility companies and their customers (energy consumers) and contribute towards a smart and sustainable energy management in Europe. Consumers, on the other hand, may also take advantage of the power grid evolution to establish a Demand Response (DR) energy consumption strategy, which will not only provide them with lower bills, but will also contribute towards building a wiser energy consumption mentality for the new generations. EU regulations require member nations to ensure that 80% of residential households will be fitted with SG nodes, a.k.a Smart Meters (SM) by 2020. However, besides the benefits of such an endeavor, the power grid, which is a vital economic and social infrastructure, will be exposed to security threats inherited from the ICT sector, while privacy issues and new vulnerabilities, related to the specific characteristics of the SG infrastructure, will emerge. The problem is assessed as crucial, if we consider that a potential attack to the SG may lead to cascading failures, ranging from destruction of other interconnected critical infrastructures to loss of human lives. In this sense, several cyber security

threats targeting the SG have been reported in recent years [14], that jeopardize the so-called AIC triangle of security services which have high priority for these critical infrastructures: Availability, Integrity and Confidentiality.

Availability: it means disrupting the electricity supply or causing physical damage to the infrastructure. In this sense, Stuxnet was the first Advanced Persistent Threat (APT) reported, back in 2009 [15]. It was responsible for causing fundamental damage to Iran's nuclear program, using USB flash drive as the primary infection vector. Then, it spread across the network searching for controllers from specific manufacturers, that governed the uranium enriching centrifuges that were finally destroyed. Another example is BlackEnergy, which is the first reported successful cyber attack on a power grid, on December 23 2015 [16]. It managed to disrupt three energy distribution companies in Ukraine and temporarily stop the electricity supply to the end users. In this case, it leveraged spear-phishing emails to obtain the credentials and hijack the Supervisory Control and Data Acquisition (SCADA) systems to ultimately switch off certain substations.

Integrity: it implies keeping the information secure from its alteration or destruction, that may cause problems on the billing operations or affect the power management. Among these threats, we can stress some works that show feasible attacks to modify the price in real-time by compromising the SMs or forging fake energy measurements transmitted through its communication interfaces. As a result, this can lead to incorrect decisions for the DR systems and hence cause disruption on the grid. On the other hand, ransomware also poses a risk for energy companies in terms of data integrity. A widely known attack was ExPetr, which targeted some industrial organizations in Russia and Ukraine in 2017 [17]. In that case, the main infection vector was an altered version of the EternalBlue exploit used by WannaCry. Then, the BlackEnergy propagation mechanisms were leveraged to propagate over the network and activate the ransomware.

Confidentiality: it concerns the unauthorized access to sensitive data. Numerous attacks have affected the confidentiality of information exchanged in the SG. For instance, GreyEnergy is a sophisticated attack believed to be active since 2015 [18], and it is considered the successor of BlackEnergy since it is perpetrated by the same group. In this case, this attack targets energy companies and other critical infrastructures in Central and Eastern Europe. Compared to BlackEnergy, GreyEnergy mainly performs the reconnaissance of the victim network to collect sensitive informatifexpetron. It is also more sophisticated than its predecessor, as the malware is developed as a modular

framework to flexibly adapt to the target organization. On the other hand, attack against confidentiality also includes the disclosure of private customer data: for example, by analyzing the collected consumption usage readings to derive life patterns.

Consequently, studies in the literature, (e.g., [19]), as well as indications/ alerts from real cyber attacks to the SG [20], set the necessity for implementing a security platform tailored to the SG. More specifically, Smart Grid architectures are expected to comply with the following main requirements:

Scalability: Utilities will manage a plethora of SMs, making the Utility side of the SG a highly vulnerable target, since a potential attack may destruct the entire energy distribution system. To guarantee scalability, fully distributed and highly resilient security mechanisms have to be devised, tailored to the processing and power limitations of the SG nodes.

Trust: SG nodes will be accessible by customers creating a fertile field for malicious users that may physically modify hardware or software (SW) to intercept personal information or alter energy measurements and costs. Thus, the SG system should be based on advanced trusted computing solutions.

Interoperability: The evolution towards the SG will be a gradual procedure, involving multiple heterogeneous technologies and potential solutions where multiple network operators or other stakeholders will be involved. Thus, SG protection should cope with inter-domain security issues, i.e., security between nodes that implement different security policies and services.

2.2 SealedGRID Solutions and Architecture

2.2.1 Architecture

In this chapter, the SealedGRID architecture is analyzed focusing the Smart Grid (SG) different components, where SealedGRID is applied to i.e., Smart Meters (SMs), Aggregators, Utility, as well as the different technologies that each component encompasses (see Figure 2.1). Moreover, the fundamental SG operations are briefly elaborated, depicting how the set of requirements discussed in the previous sections are met.

SM: The SealedGRID SM is responsible for generating electricity consumption packets, communicating with other components from the same or different SealedGRID domains and paying the Utility bill. It contains the Federated Login module to communicate with the other components, unlimitedly,

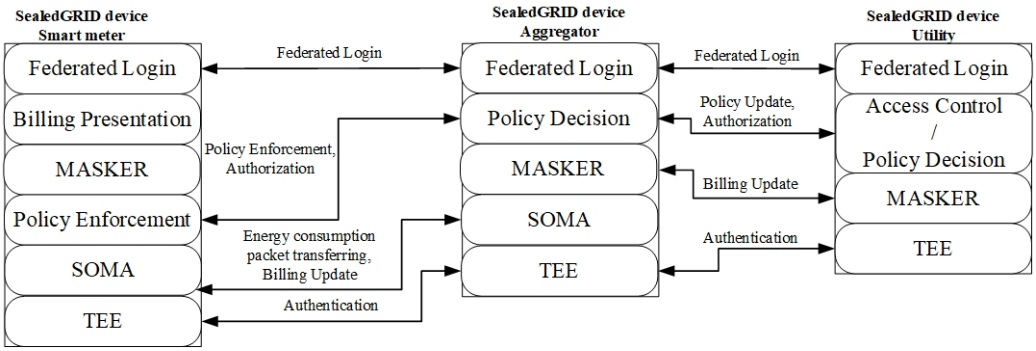


Figure 2.1: Architectural components and integrated modules for SealedGRID

without extra authentication. Regarding authentication, a SealedGRID SM contains the SOMA module, which includes: a) the SOMA client utilized by SMs to request to join in a domain and become part of the SOMA network, and b) the SOMA authenticator used by an already authenticated SM in the SOMA network to handle a new join request; its certificate is issued by the domain's CA and stored within the Trust Execution Environment (TEE). Moreover, it generates the energy consumption readings of the user through a preinstalled application, since these contain confidential information about the end-user's habits, where the construction of the related packets takes place within the MASKER module that provides both security and privacy. To ensure also the integrity of the performed functions, the TEE is involved that executes all the critical operations, like key storage, pseudo-random number generation, digital signing, etc. After the construction of a consumption packet, the SealedGRID SM forwards it to the nearest SealedGRID Aggregator. MASKER also provides to the end-user (customer) periodical reports with billing updates. Regarding authorization, the SealedGRID SM plays the role of a Policy Information Point (PIP) and Policy Enforcement Point (PEP). The PIP determines the severity degree of the area, which can be requested by the Policy Decision Point (PDP) placed in the intermediate nodes of that domain (e.g., the Aggregators of a specific area). The PEP's role is utilized to access data or request the control of another SealedGRID SM from the same domain or from different domains.

Aggregator: A SealedGRID Aggregator authenticates and authorizes new

devices in a specific domain, allowing the system to run smoothly. Moreover, it is accountable for receiving and aggregating individual readings without being able to infer private information from these messages. It includes the SOMA module to authenticate new SMs that request to join its domain. Moreover, it is the CA for its domain; its own certificate is granted from its Utility and is securely stored within the TEE. The SealedGRID certificates contain attributes (e.g., contact expiration) based on the global security policy. Also, it contains the Federated Login module to assist the seamless communication between the components from different domains, and to avoid their repetitive authentication. In addition, it utilizes the MASKER module for collecting and aggregating metering values sent by the SMs. After their aggregation, it forwards the result to the SealedGRID Utility facilitating DR. In this way, the overhead for collecting and aggregating energy consummations is distributed among the SealedGRID nodes, eliminating the burden that is put to the Utility that may become a point of bottleneck. The integrity of the performed operations as well as the security and privacy of the carried data are ensured by the employment of the TEE, which performs crytographic functions and critical operations. As for the authorization, it plays the role of the PEP, since it is responsible for policy enforcement in its domain, according to the policy defined by the Utility. Therefore, it is also considered as an intermediate level PDP, taking access control decisions in a local level, e.g. remove a specific SM.

Utility: The SealedGRID Utility is responsible to maintain steady DR and to calculate the billing by computing the total consumption of customers at the end of a billing period, based on their energy consumption. Moreover, it is liable for issuing the system's policy. It integrates the Federated Login module to provide seamless communication between SealedGRID components from different domains. It also encompasses MASKER to receive high-frequency aggregated values for managing DR as well as low-frequency metering data for calculating customers billing. In the proposed architecture, we deploy many Utilities under the same Energy Distribution Company, which optimizes the management of DR in an area. Finally, a Utility plays the role of the PDP role to issue the system policy. However, it is considered as individual PEP, since it should ensure the enforcement of the security policy in its domain.

The SealedGRID architecture is based on the following main pillars:

- SealedGRID aims at designing, analyzing, and implementing a scalable,

highly trusted and interoperable SG security platform. This platform will be an integrated solution that will be applicable to existing systems, e.g., SCADA.

- The SealedGRID platform is expected to limit the security risks for the expansion of remote energy distribution network management, towards the evolution of SGs.

- The SealedGRID platform will support an optimized key management solution that will provide the cornerstone for data and communication protection.

- Authentication in SealedGRID platform will be based on digital certificates using Web of Trust and Blockchain technologies.

- SealedGRID will design but also implement a trusted computing solution, that will enable any entity, to verify whether the current state of the device is secure and trustworthy, but also gain assurance that, during operation, the execution of application cannot be altered by malicious actor. This way, SealedGRID ensures the assessment of the trusted paths and achieve isolation of misbehaving SG nodes. Also, protection mechanisms for end users' usage and private data will abide by the recommendations of the European Commission. The SealedGRID platform will contain: a) a hardware root-of-trust mechanism based on TEE that can verify and validate any component irrespective of the device's software or hardware; b) a remote attestation mechanism that will allow devices generate proofs that their current state is trustworthy; c) a secure application for execution in TEE and d) a metering data privacy protection mechanism.

- SealedGRID goals is to design and implement authorization and security interoperability mechanisms, aiming at automatically connecting heterogenous SG nodes belonging to different domains. To accomplish this goal, SealedGRID will: a) design and implement a hybrid access control mechanisms based on Attribute based Access Control (ABAC) and Role-based Access Control (RBAC) to achieve flexibility and avoid complexity at the same time; b) construct lightweight protocols that support Single Sign On (SSO) for the interconnection and federation of multiple SG domains using the OpenID Connect protocol and c) design

and implement context-aware mechanisms to account for all the events occurred in the grid in real time.

- The SealedGRID devices implement an Access Control Management Service (ACMS) to control the access to resources and translate the different security policies to achieve security interoperability among various SG data and network objects. The ACMS is designed in a hybrid way to provide both Attribute-Based- Access-Control (ABAC) and Role-Based-Access Control (RBAC). ABAC defines the access rights that are granted to the new SMs using policy that combine attributes together. The policy can use any type of attribute, e.g., expiration of customer's contract. On the other hand, RBAC employs predefined roles that carry a specific set of privileges associated with them. In this regard, the IEC 62351 standard is a reference to provide security in the industry; its RBAC principles stated in part 8 will be applied, since it restricts the access to system resources to authorized users, according to their roles and associated permissions. More specifically, it defines a list of predefined roles (e.g., OPERATOR, ENGINEER, INSTALLER, etc.) and their respective rights (e.g., View, Read, Control, etc.), so that permissions that are assigned to users are only those that are actually needed for their duties, following the principle of least privileges. Altogether, by using this hybrid access control, SealedGRID achieves flexibility and avoids complexity.

- When different domains and devices need to be interconnected each other, the authorization is applied based on Policy Information Points (PIP), Policy Enforcement Points (PEP) and Policy Decision Points (PDP). On the one hand, PIPs associate the set of attribute values to resources (e.g., Smart Meters) based on the context information; therefore, all entities can be considered as PIPs. Through a PEP, the entities (i.e., the smart meters, aggregators or utilities) can request access to the different resources of the system. The PEP intercepts and forwards the request to the PDP so that this latter can manage the authorization policies and determine the access level to the different sections of the system according to a set of factors: the type of entity, the resources and the context. Once the decision is taken by the PDP, the PEP processes it to permit or deny access to the interested entity, thereby protecting the critical resources of the system.

- The context-awareness mechanism will be in charge of retrieving data of the current state of the system in real time, thereby feeding information to the Policy Information Points. This data acquisition includes all the events, components and interactions of the system, which are normalized under a common representation, in order to feed the access control mechanisms with valuable data.

- SealedGRID will protect the confidentiality, integrity, accountability and availability of the system.

2.3 Security Solutions

2.3.1 Background

Beginning with key management, some schemes are based on shared secret keys, which in turn hinder scalability, [21]. Another category of schemes utilizes ID-based cryptography, [22], whose main issue is that Private Key Generator should always be online and available, and can be a single point of failure. In [23], a localization-based key management system is proposed, where data are encrypted by the key associated with the coordinates of the meter and a random key index. However, the encryption keys are managed and distributed by a Trusted Third Party (TTP), which also creates a single point of failure. There have also been efforts to integrate trusted computing on the SG, mainly with the use of the Trusted Platform Module (TPM) [24] and the TEE [25]. In this thesis, we prioritize the use of TEE, since TPM usually imply higher costs, they do not offer protection against runtime attacks and are not suitable for mobile and embedded devices. In turn, TEE does not require a separate hardware module, since it utilizes two virtual processing cores with different privileges: a normal one for applications, and a secure one for security-sensitive code execution. Remote attestation is also important here, as the modification of information in one entity can be detected by a remote one. In this case, TPM is not suitable either, since a malware can exploit an application and operate in the RAM memory of a SM without being detected by the TPM [26].

In [27], a device-to-device authentication framework is presented that is based on a two-layer approach, where SMs are authenticated globally by a PKI, and locally by channel signatures. In [28], an authenticated aggregation protocol is presented based on asymmetric keys; this solution mainly preserves the authenticity of exchanged messages but does not guarantee that only authentic entities are part of the SG. Authentication in the SG has also been recognized as an important issue by the industry as well, leading to standards, like DNP3 Authentication [29] and IEC 62351-5 [30]. The design of secure authorization and interoperability mechanisms is a complex task as specified in [31]. They state that the inter-connection between systems that are not originally envisioned to interoperate may present unanticipated problems, not just in operation, but in data availability, resolution, and format. In [32], a dynamic authorization-based approach is proposed to interconnect systems where each user-role is computed according to the attribute-based hash value. The authorization is maintained so that each user can perform only those actions that are allowed under the access permissions granted to it. Similarly, the work [33] presents the use of smart energy gateways to establish trust relationships between parties using asymmetric key cryptography and cryptographic hash functions; and the work [34] provides a middle-ware architecture based on Role Based Access Control, PEPs and PDPs to collect data streams from multiple sources connected to the Advanced Metering Infrastructure in a standardized format. Last but not least, the work [35], presents a solution based on the use of PEPs and PDPs to interconnect large distributions, containing technologies belonging to different infrastructures, manufactures and vendors.

Regarding privacy, a lot of research has been accomplished comprising solutions to prevent data disclosure, using: i) homomorphic encryption, ii) traditional encryption, and iii) masking. Solutions, like [36], [37] tend to pose high overhead to SG nodes (especially resource-constrained SMs) due to homomorphic encryption. Solutions using traditional encryption include [38]; the use of TTPs and Key Distribution Centres creates a single point of failure. According to standardization organizations CEN/CENELEC/ETSI [39], the efficiency and privacy requirements of a privacy preserving mechanism for the SG can be met using masking. Compared to masking, such methods [40] lack

protection against non-repudiation and adaptability to node joining or leaving.

2.3.2 SealedGRID Solutions

In this chapter the technologies employed in the proposed architecture are the following and are briefly presented: a) Federated Login [41]; b) SOMA [42]; c) MASKER [43]; d) utilization of the TEE [44] and e) Context Awareness Manager [45].

SOMA [42] is a certificate-based authentication infrastructure that creates a secure authentication system for mesh networks without a TTP. SOMA creates a self-organized, efficient and scalable authentication infrastructure, without sacrificing the autonomous characteristics of the nodes. The nodes independently decide with whom to interact, since the SOMA is built on a self-organized, Peer-to-Peer (P2P) and Web-of-Trust (Wot) infrastructure. Not only does it make use of structured P2P as the nodes are mostly static, but also it provides scalability and static resilience, required for an identity management system. SOMA is based on a PGP-like architecture, where the participating nodes create the needed keys. Through certificate exchanges each node builds each keyring and stores it locally, in accordance with PGP WoT. SOMA does not use either a central or a distributed Credential Authority (CA) and avoids completely delegation of trust to a TTP. A node will start a secure communication with another node based on the stored certificated on its keyring. Moreover, SOMA demands the existence of TEE for its secure execution and the secure storage of the generated certificates.

MASKER: [43] provides a privacy-preserving aggregation solution that responds to the following issues: a) it assists the privacy and security of energy consumers and b) it fulfills all requirements needed for the SG. Each SM participating in the architecture shares a series of cryptographically generated pseudo-random values with the Utility. These values act as masks and are used to obfuscate the real consumption readings of the SM. This way, an intermediate Aggregator can provide the Utility with an aggregated consumption by several SMs without knowing the real energy consumption. The Utility subtracts the used masks from the total sum received by the Aggregators, resulting the real combined consumption of all relevant SMs. The only entity that has access to the real energy consumption value is the SM itself. All the performed sensitive computations are protected by utilizing a

TEE, which stores data and executes crucial operations. TEE provides confidentiality and authenticity to the executed code and stored data, integrity to CPU registers, memory and sensitive I/O, while it is able to prove the trustworthiness of SealedGRID nodes, components and modules. By utilizing MASKER in SealedGRID, we achieve a privacy preserving aggregation solution of energy consumption that facilitates DR, which is highly trusted and scalable, imposing low computation overhead.

TEE: As mentioned above the SealedGRID makes use of TEE to protect its components from attackers aiming at manipulating them, as it is proposed by [44]. SealedGRID uses TEE to: a) protect device private keys and its sensitive data through secure storage; b) endorse remote attestation, and c) secure critical procedures like key management. SOMA, which is a key management application is executed within the TEE, where its generated digital certificated are stored. Furthermore, MASKER, which is responsible for the aggregation and protection of energy consumption, performs its cryptographic functions within the TEE. Finally, the Federated Login demands trustworthiness among the participating devices/nodes, which is ensured by the remote attestation mechanism that enables a device to verify that another device operates a trusted SW.

Context Awareness manager: As mentioned above, along with the different security components to be integrated in a SG scenario, it is necessary to implement an Access Control Management Service to control the information flow across the different nodes within the grid, while achieving security interoperability among various network resources. For this task, besides the application of a model capable of defining the different roles, attributes and permissions on the system according to a given access control policy, it becomes crucial to pair this control with the continuous assessment of the network in terms of security, as to permit or deny the use of certain services in cases where some critical resources could be at risk. This is enabled by context-awareness mechanisms, which retrieve data of the production chain in real time (e.g., network events, alarms, raw traffic). As a result, we fully know the current state of the network so we can easily identify the most affected sections of the infrastructure (and the severity of those potential attacks). This way, the system can automatically react to unforeseen situations and hence improve the decision making. Diverse solutions have been traditionally proposed, but the modernization of the industrial systems impose a challenge for the data acquisition due to the heterogeneity and complexity of

those technologies. Here, Opinion Dynamics poses an novel technique [45]. This is a multi-agent collaborative algorithm capable of detecting and tracing APTs during their entire lifecycle, from a holistic perspective. It is designed as a framework to analyze information from external sources (e.g., Intrusion Detection System - IDS) together with Machine Learning techniques in a distributed way: a set of agents are logically spread over the network to gather information about their surroundings. Then, it is correlated with the anomalies measures by their neighbors, which finally creates a fragmentation of the affected zones across the infrastructure. As a result, it has been demonstrated to be effective for tracking sophisticated attacks over long periods of time.

2.4 Fortifying the Common Security and Defence Policy

In fortifying the Common Security and Defence Policy (CSDP), the integration of advanced cybersecurity applications within smart grid technology emerges as a strategic imperative, bolstering the resilience of critical energy infrastructure and enhancing the EU's capacity to respond to contemporary security challenges. Employing sophisticated technologies such as masking, blockchain, secure authorization, secure computing, and programming, and opinion dynamics further amplifies the protective layers around smart grids. Masking technology obscures sensitive information, safeguarding critical data from unauthorized access, while blockchain ensures the immutability and transparency of energy-related data, crucial for verifying information authenticity in defense operations. Secure authorization mechanisms guarantee that only authorized personnel can access and control critical components, aligning with the CSDP's goal of protecting classified data. The incorporation of secure computing and programming practices fortifies smart grids against software vulnerabilities, reducing the risk of disruptions during defense operations. Opinion dynamics technologies offer insights into public sentiments, enabling a more nuanced approach to decision-making that considers societal impact, fostering public acceptance of security measures. This integrated approach establishes a comprehensive security ecosystem within smart grids, facilitating real-time threat detection, cross-sector collaboration, and ultimately reinforcing the CSDP's commitment to collective defense and

Authors	Title	Venue
Farao A, Rubio JE, Alcaraz C, Ntantogian C, Xenakis C, Lopez J.	Sealedgrid: A secure interconnection of technologies for smart grid applications [10]	CRITIS 2019, Springer $[Rank : C]$
Farao A, Ntantogian C, Istrate C, Suciu G, Xenakis C	SealedGRID: Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID	ICS & CSR 2019, eWiC $[Rank : C]$
Suciu G, Sachian MA, Vulpe A, Vochin M, **Farao A**, Koutroumpouchos N, Xenakis C	Sealedgrid: Secure and interoperable platform for smart grid applications	Sensors MDPI $[IF : 3.9$
Suciu G, Istrate CI, Vulpe A, Sachian MA, Vochin MC, **Farao A**, Xenakis C	Attribute-based access control for secure and resilient smart grids	ICS & CSR 2019, eWiC $[Rank : C]$
Suciu G, Istrate C, Sachian MA, Vulpe A, Vochin M, **Farao A**, Xenakis C	FI-WARE authorization in a Smart Grid scenario	GIoTs 2020, IEEE

Table 2.1: List of thesis' publications- Part A

response to emerging security challenges in the dynamic landscape of the 21st century.

Table 2.1 summarizes the scientific publication related to this chapter.

Chapter 3

SAMGRID: Security Authorization and Monitoring Module Based on SealedGRID Platform

IoT devices present an ever-growing domain with multiple applicability. This technology has favored and still favors many areas by creating critical infrastructures that are as profitable as possible. This chapter presents a hierarchical architecture composed of different licensing entities that manage access to different resources within a network infrastructure. They are conducted on the basis of well-drawn policy rules. At the same time, the security side of these resources is also placed through a context awareness module. Together with this technology, IoT is used and Blockchain is enabled (for network consolidation, as well as the transparency with which to monitor the platform). The ultimate goal is to implement a secure and scalable security platform for the Smart Grid. The paper presents the work undertaken in the SealedGRID project and the steps taken for implementing security policies specifically tailored to the Smart Grid, based on advanced concepts such as Opinion Dynamics and Smart Grid-related Attribute-based Access Control.

Table 3.1 summarizes the scientific publication related to this chapter.

Authors	Title	Venue
Suciu G, **Farao A**, Bernardinetti G, Palamà I, Sachian MA, Vulpe A, Vochin MC, Muresan P, Bampatsikos M, Muñoz A, Xenakis C.	SAMGRID: Security Authorization and Monitoring Module Based on SealedGRID Platform [2]	Sensors MDPI [IF : 3.9

Table 3.1: List of thesis' publications- Part B

3.1 Introduction

Traditional power grid models are based on a central system for generating and distributing energy and have undergone significant changes in recent years [46]. The integration of the latest generation of technologies, rare in critical infrastructure such as the Internet of Things (IoT), has facilitated the evolution to a more dynamic and connected power grid model now known as the SG. The SG's contributions result from introducing a mutual flow of information between manufacturers and customers, from which both can benefit. This flow enables fine-grained consumption measurements reported to each energy service provider in near real-time to provide consumers with up-to-date price data or control a utility that contains the grid's energy load in real-time according to actual demand, allowing utilities to perform accurate demand response procedures by anticipating high demand peaks, avoiding and mitigating power outages, and distributing the load on available generators. On the other hand, consumers can take part in programs that reduce electricity consumption in the event of rising energy prices while using homegenerated (renewable) electricity (such as the so-called microgrid).

The above measurement model is called Advanced Metering Infrastructure (AMI) [47]. Technically speaking, this infrastructure consists of several interconnected elements that collect home-measured consumption data, later passed to the power company via an aggregation point. Part of this information is analyzed through Meter Data Management Systems [48]. As a result, further control procedures for the system include industry and information technology equipment (integrated throughout the infrastructure) and correct usage of devices and resources by all involved parties. The architecture for capturing measurement information from IoT devices and consistently con-

trolling power generation contributes to the development of cybersecurity attacks that can compromise resource availability and thus network stability. Access control is essential to manage permissions for all users, processes, and heterogeneous devices that interact continuously within the infrastructure in this complex environment. Therefore, it is imperative to consider the full range of requirements for this scenario to apply the available solutions accurately and propose hybrid access control mechanisms with integrated security monitoring mechanisms.

This uses the approval component to address all these requirements in a modular and flexible way while defining fine-grained guidelines for monitoring the security status of each participating node being an integrated part of a hierarchical authentication framework that spans different devices. The approval framework adheres to integrated industry standards and robust policy rules that always consider the state of the context. In this case, the context awareness manager is used, an authorization component that uses the authentication module in the scope of validating the element's identity requesting access to the resource and signing the token received from the appropriate authorization unit. These components can be put together to make timely access control decisions without impacting the throughput of network assets or ensuring the lowest level of security at all times.

The joining of all these components can certainly help issuing access control decisions in a timely manner without interfering in the throughput of the network assets and ensuring a minimum level of security at all times, as it is envisioned in Figure 3.1 below.

The work makes the following additional contributions with respect to the already obtained project results:

- providing security and privacy requirements for a module dedicated to delivering security authorization and monitoring the security status of the participating nodes;
- proposing SAMGRID, a novel authorization and security monitoring module tailored to SG needs based on well-established security technologies;
- assessing SAMGRID's performance: implementation and evaluation were performed in a simulation environment.

This work is carried out as follows: Section 3.2 presents essential basic information on authorization in the SG, the motivation of our work and the

Related Work/Features	Blockchain	Access Control	Opinion Dynamics	Machine Learning	Data Integrity	Interoperability
Smart Grid Interoperability Standards						✓
Interconnection between heterogeneous cyber-physical systems						✓
Blockchain technology for smart grids	✓				✓	
ML models for Electricity Theft Detection				✓	✓	
Load frequency control of smart grids						
Confidentiality in Smart Grids				✓	✓	
Metering and data access infrastructures in smart grid		✓			✓	
Policy enforcement in smart grid		✓				
Access control for smart grid services based on publish/subscribe		✓				✓
Blockchain-based authorization system	✓				✓	
Proposed work	✓	✓	✓	✓	✓	✓

Figure 3.1: SealedGRID features. ✓the enabled features of the system.

security and functional requirements that we have defined based on the needs of stakeholders. Section 3.3 follows, where the related works are discussed, while Section 3.4 describes the SAMGRID concept. Furthermore, Chapter 3.6 contains an assessment of the measurable performance of SAMGRID Finally, Chapter 3.7 concludes the work.

3.2 Authorization in SG

3.2.1 Definition and Participants

In this work, we focus on the importance of authorizing and monitoring the security status of the participating entities within a SG network. The main SG components are the Utility, the Smart Meter (SM) and the Aggregator. The Utility is responsible for billing by computing the total consumption of a customer at the end of a billing period. The SM is placed within a house or building, and its purpose is to collect the readings of the electricity consumption. The Aggregator represents the binder between the Utility and the SMs. It is responsible to sum all the readings received by SMs and transmit the results to the Utility. In this way, data become available without putting too much load on the Utility. In general, SG's main goal is to provide a dynamic two-way information exchange between Utility companies

and their customers contributing towards a smart and sustainable energy management. However, in such cases, the main challenges that a SG has to exceed are related to scalability [49], trust [43] and interoperability [43]. Thus, divergent information and operational technologies have to cooperate for achieving interconnection of various mechanisms.

There are many ways to cope with the aforementioned challenges including but not limited to policy-based management. Thus, policy specification languages are utilized to communicate the various authorization policies in numerous access control applications with complicated policies. A well-known as well as commonly used language in SG ecosystems is the XACML [1], which is used to construct complex authorization policies [50]. The entities that participate under the policy manner are the following: (i) Policy Enforcement Point (PEP): this is responsible for performing the decision requests, receives policy updates and accordingly translates them, as well as enforces the decisions that stem from each policy. (ii) Policy Decision Point (PDP): this assesses the applicable policy against other relevant policies and attributes providing the decision outcome to PEP. (iii) Policy Information Point (PIP): this acts as a source of attribute values to make a policy decision. (iv) Policy Administration Point (PAP): this provides the authoring and the maintenance of a policy or a set of policies. As we can observe, in the SG ecosystem the participating entities own numerous titles. For instance, a Utility in a domain may also be a PDP. That leads to the fact that the different roles can be allocated to an entity being hardcoded in a device. Figure 3.2 shows the involved entities and the flows between them.

3.2.2 Motivating Examples

In this section, we will showcase the most notorious cyber-attacks in critical infrastructure that occurred in recent decades to gain a better understanding of the presented notions. Our approach aims to emphasize not only the security flaws that enable cyberattacks in critical infrastructures, but also how a malicious actor can take advantage of various vulnerabilities and launch attacks. Moreover, the following examples come from real-life events that shocked involved governments, citizens and stakeholders, also these are explained in brief providing valuable insights.

Stuxnet was a directed cyberwarfare attack against the Iranian nuclear program. It was first uncovered in 2010; however, it has been reported that

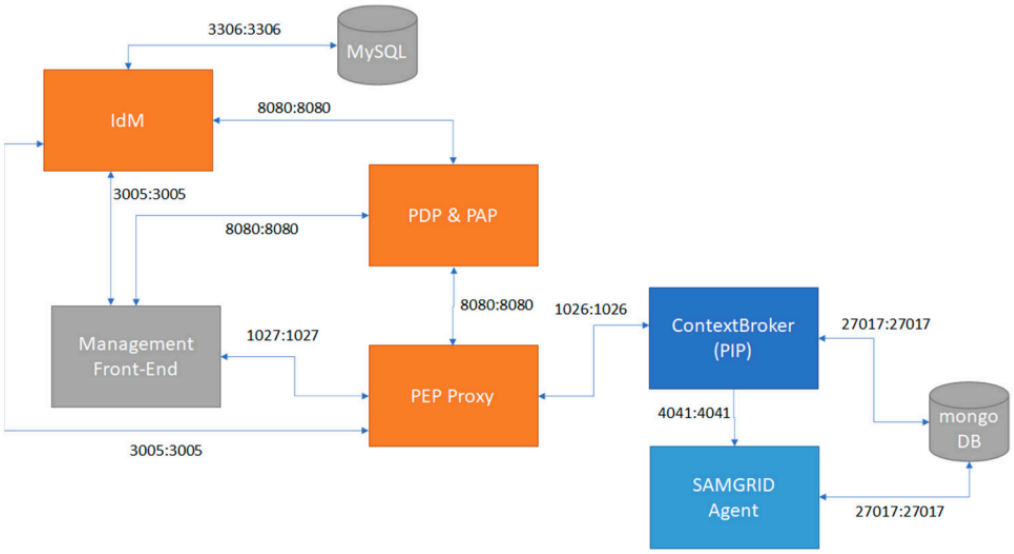


Figure 3.2: Illustration of participants in the authorization component of SAMGRID

it was in development since at least 2005. The attackers' approach relied on delivering the worm via USB sticks and local networks. Stuxnet infected both Windows PCs and also controllers. However, its behavior against the controllers was totally different, picking controllers from a specific manufacturer. Once Stuxnet identified its targeted controller then it went through an intricate process of fingerprinting to make sure that it was the target. When it met the requirements, Stuxnet's dropper loaded rogue code to the controller. The code injection enables Stuxnet to stealthily launch its code, letting legitimate code continue correctly working. The rogue code periodically worked. When the attack time came, the rogue code took control without letting the legitimate controller code understand. Finally, during the attack, the genuine code of the controller was knocked out [13].

Another infamous example is **BlackEnergy**, which is the first reported successful cyberattack on a power grid. On 23 December 2015, the attack occurred, managing to disrupt three energy distribution companies in Ukraine and temporarily stop the electricity supply to the end users. In particular, the attacking group that mounted the attack utilized spear-phishing emails attaching malicious Excel documents with macros infecting computers in a

targeted network. Additionally, it obtained the credentials and hijacked the Supervisory Control and Data Acquisition (SCADA) systems to ultimately switch off certain substations. At the same time, the attackers flood the call centers with automated telephone calls, preventing the affected utilities from receiving outage reports from their customers (end-users) confronting the response effort [15, 51]].

Additionally, a well-known attack is **GreyEnergy** targeting critical infrastructure organizations in Central and East Europe in 2018. It is widely known that the malware used during this attack bears many similarities to the one used in the BlackEnergy attack (see above). The attacking group that was responsible for this cyber-attack used two ways to achieve the intrusion into the organization's network. One the one hand, the first weapon they used was through the GreyEnergy mini, which is a first-stage backdoor that works without the demand of administrative privileges- the attackers searched for public-facing web services running on servers that were connected on the targeted network. Once it was finished, the attackers started mapping and scanning the network, as well as collecting credentials to obtain administrator privilege. Then, they were capable of initiating the main malware. In particular, the attackers targeted servers with high uptime, and workstations used to control industrial and control system environments. Additionally, they utilized command and control services to establish communication among their computers (malicious network) and the compromised machines (targeted network). On the other hand, the second way to end the targeted network was via spear phishing emails that bear with them malicious attachments.

The cyberattacks in industrial control systems (ICS) are not a cybersecurity issue that belongs to the past, in 2020 a ransomware encrypted data in Düsseldorf Hospital and then demanded ransom to unlock it. During this attack, the first death by ransomware was reported. Particularly, the ransomware compromised the digital infrastructure that the hospital relies on to organize its processes forcing the cancellation of many operations and other procedures. The ransomware entered the University Hospital Düsseldorf's network through a widely known vulnerability in a Citrix application. Apart from this attack, in 2021 Colonial Pipeline—the largest fuel pipeline in the U.S.A.—shut down for five days [52]. due to a ransomware attack [53]. In this case, the attackers managed to compromise the targeted network utilizing a VPN account. They found the related credentials inside a batch of leaked passwords on the dark web.

Apart from the aforementioned attacks, it is also mandatory to analyze the different attack stages to complete a cyberattack in ICS. At this point, we will mention the most well-known frameworks that provide the necessary steps for an attack. On the one hand, there is the Cyber Kill Chain framework [8, 54] that provides seven steps that attackers have to fulfill to achieve their objectives, the steps are the following: (i) Reconnaissance; (ii) Weaponize; (iii) Delivery; (iv) Exploitation; (v) Installation; (vi) Command and Control and (vii) Actions on objectives. On the other hand, there is the MITRE ATT&CK framework [54, 55] that provides 14 steps, which the attackers have to follow to accomplish their attack. The steps for this are the following: (i) Reconnaissance; (ii) Resource Development; (iii) Initial Access; (iv) Execution; (v) Persistence; (vi) Privilege Escalation; (vii) Defense Evasion; (viii) Credential Access; (ix) Discovery; (x) Lateral Movement; (xi) Collection; (xii) Command and Control; (xiii) Exfiltration and (xiv) Impact. Both frameworks follow the same pattern. The primary difference between the aforementioned frameworks is that the MITRE ATT&CK framework is a list that consists of tactics and techniques; we have to note that it does not propose a specific order of operation. However, the Cyber kill Chain proposes a well-defined sequence of events.

3.2.3 Security and Functional Requirements

As we can observe, SG is an ecosystem that inherits risks that are directly related not only to the participating SG components (Smart Meter, Aggregator, Utilities), but also to the inadequate security controls implemented by handlers to these. This leads to the conclusion that security and functional requirements need to be declared for a scheme that aims to provide authorization and security monitoring features. Since the functional and security requirements of a SG ecosystem have been extensively expressed by the literature, we aim to shed light on requirements related to security and functionality being dedicated to authorization. In particular, we formulate the requirements intending to meet high demands of SG stakeholders. At the end, we have to note that we express the ensuing requirements adopting a security by design approach.

3.2.3.1 Security Requirements

Since the security among a SG ecosystem depends not only on the devices (e.g., vulnerabilities), but also on the poor security practices that are established for authentication and authorization purposes, we express a kit of standard security requirements applied to it [1, 56, 57, 58, 59, 60].

(**S1**) Data confidentiality: Data exchanged within a SG ecosystem should be available only to SG components with the respective privilege.

(**S2**) Data integrity and authenticity: Data exchanged among the participating SG components should be safeguarded against alteration and replication; thus, these should be capable of verifying the origin of the acquired data.

(**S3**) Accountability: Devices, handlers/employees and end-users should be accountable for their actions.

(**S4**) Non-repudiation: Devices, handlers and end-users should not be able to deny their actions.

(**S5**) Physical protection: All electronic devices that participate in a SG ecosystem should contain protection mechanisms to prevent being tampered by adversaries with physical access.

3.2.3.2 Privacy Requirements

Apart from the security requirements, a SG ecosystem consists of processes that demand specific functionalities to be enabled. Analyzing the current literature, we express the functional requirements applying a security by design approach but understanding the stakeholders demands [56, 57, 58, 59, 60].

(**F1**) Time consuming: As it is well known, the SG concept aims to support real-time services to its end-user. Thus, the implemented application for authentication, authorization, policy updating should not consume much time and deplete the available sources.

(**F2**) Scalability: A SG ecosystem should consist of applications that are capable of handling the numerous fluctuations of grid's size (e.g., nodes can join and leave a grid) without negatively affecting their performance.

(**F3**) Delegated access control: Any application access must be authenticated and authorized by a security policy, and the granting decisions must be made relying on a trusted party.

(**F4**) Authorization: Any access to applications must be authorized according to a security policy.

(**F5**) Authentication: Requesters should be authenticated before accessing any application.

3.3 Related Work

The literature in the field of SAMGRID contains the security authorization and opinion dynamics approaches that have been designed for SG ecosystems and the techniques that are used for monitoring the security status of the participating nodes.

3.3.1 Security Authorization Approaches

Although the literature proposes different authorization methods and mechanisms for the SG ecosystem, to the best of our knowledge, this is the first work that proposes the seamless work of an opinion dynamics approach together with an individual Authorization mechanism. This work is an extension to the paper "FI-WARE authorization in a Smart Grid scenario" written by George Suciu, Cristiana Istrate, Mari-Anais Sachian, Alexandru Vulpe, Marius Vochin, Aristeidis Farao and Christos Xenakis, which has been published in the proceedings of the 4th Global Internet of Things Summit (GioTS) in 2020. Some of the extensions of the work include: (i) an elaborated description of security and functional requirements that should be accomplished by a proposed solution for authorization purposes in SG

ecosystem; (ii) a proposal of an opinion dynamics approach that works together with the initial version of the Authorization element proposed in [13]; (iii) a summary of several performance evaluation experiments performed to analyze different aspects of our module demonstrating the impact that the proposed solution has in terms of performance and efficiency and (iv) an analysis related to the security features of SAMGRID. Parts of the work presented in [13] are reused in the current work.

Security interoperability known as one of the most challenging research areas within the field of critical infrastructures by International Organizations such as the NIST, and IEEE. Therefore, diverse technologies (sensors, meters, actuators, etc.) and various communication systems (WiMAX, Wi-Fi, ZigBee, 3G cellular, etc.) as well as different domains must cooperate in a unified ecosystem to provide the ability of performing critical actions. These actions, involving the control of user's sensitive information (e.g., electrical consumption) performed across the different elements of the SG may be (i) tampered by malicious actors if data are not completely protected, or (ii) disrupted due to missing standardization and interoperability mechanisms. The design of secure authorization and interoperability mechanisms is a complex process as specified in [61, 62]. It is stated that the interconnection between systems that were not originally envisioned to interoperate may pose unanticipated problems, not just in operation, but in data availability, resolution, and format; it may also cause significant delays in the primitive operations.

A solution for providing a decentralized SG in a secure manner using blockchain is presented in [63]. In respect to Electricity Theft Detection, in [64] two solutions based on supervised learning are proposed. The first solution addresses class imbalanced problems solving, perform feature extraction and then use a deep learning-based system to classify electricity consumers. The second solution is a Synthetic Minority Oversampling Technique Edited Nearest Neighbor (SMOTEENN) system. [65] improves the security of existing SCADA systems within smart grids using a cyber-physical digital signature scheme. In [66], Advanced Metering Infrastructure (AMI), which is an important component of an IoT based Smart Grid is analyzed separately and secured based on evolutionary game theory. [67] proposed a middleware architecture based on RBAC, Policy Enforcement Points (PEPs) and Policy DecisionPoints (PDPs) to collect data streams from several sources connected to the AMI in a standardized format. In [68], a solution based on the usage of PEPs and PDPs has been proposed to interconnect large distributions, involving technologies of different infrastructures, manufactur-

ers and vendors. In [69], a data-centric access control framework for smart grids that follow the publish/subscribe model has been analyzed, adopting an Attribute-Based Authorization Policy. In [70], an authorization mechanism for monitoring and reduction in resource consumption by using resource trading contribution, implemented on blockchain technology, has been designed. The proposed system provides secure data access and storage together with controller functions transfers among householders.

The main limitation of the related state of the art is that these solutions are not able to cope with the dynamic environment of SG, since they are based mainly on RBAC. Even more, the above solutions do not offer any implementation details, nor performance evaluations through simulations.

Itron's OpenWay Riva [71] is a commercial communication platform that offers welldefined points of interoperability between customer and utility systems, greatly simplifying and reducing integration costs and issues.

3.3.2 Opinion Dynamics Approaches

Smart Grid is one of the largest applications of the Internet of Things, the revolution of the Internet and machine-to-machine (M2M) communications. While SG offers many wellknown benefits and new opportunities, their distributed nature and two-way information flow between consumer and producer enables a multitude of new attacks against smart grid infrastructure. Given the potentially extremely severe consequences that these attacks could have (e.g., environmental hazards/pollution, rendering hospitals or security defenses inoperable, suspension of economic activities) it is important to note that these attacks are likely to have a significant impact on the environment. Therefore, it is evident that it is imperative to develop anomaly/intrusion detection techniques and systems.

Traditional Intrusion Detection Systems (IDS) are only a first line of defense in attempting to identify anomalous behavior at very specific points in the infrastructure and are tailored to specific types of communication standards or data types, which is not sufficient to track the wide range of attack vectors that could be used against an SG environment. One of the most interesting and innovative cybersecurity innovations in the SG scenario is the usage of the Opinion Dynamics as a distributed detection technology to evaluate the security status of the SG environment. The Opinion Dynamics method proposes to aggregate the coverage of multiple detection sys-

tems strategically deployed on the infrastructure under a common distributed framework, which permanently correlates all detected malicious patterns and anomalies and learns from them.

The study and modeling of opinion propagation in a network through the interactions of its agents originated a few decades ago. French in 1956 was one of the first researchers who focused on opinion dynamics [72]. Subsequently, De Groot formalized one of the simplest and most famous dynamic models of opinions in 1974 [73]. Since then, the interest of the research community has gradually increased and according to the nature of the context under consideration the format of the different opinions expressed by the agent and the purpose of interaction, the dynamics of opinions have taken different forms [74, 75, 76].

Opinion Dynamics can be used in the SG cybersecurity context to design a multi-agent advanced detection system [58, 45, 60, 77], which is one of the main defense threats in the field of SG cybersecurity [78]. In [56], an intrusion detection scheme Opinion Dynamics-based was initially proposed under a theoretical perspective. From a practical point of view, in [45] its ability to detect and monitor attacks in an industrial testbed was demonstrated; in [78], it also showed its contributions to the Smart Grid scenario, and in [60] to the Industrial IoT, also known as IIoT, scenario. This is possible because the opinion dynamics can include anomalous indicators (i.e., equipment and communication link compromises) as the main indicators (opinions), which also include the integration of external IDS.

3.4 SAMGRID Concept

In this section, we present an archetype of the proposed module along with the processes that take place for their consistent integration as shown in Figure 2 with any SG application. In SAMGRID, apart from the standard entities and roles that participate in SG authorization process (see Section 3.3) we introduce an opinion dynamics (ODyn) mechanism (see Table 3.2), an additional mechanism that we consider as the pedestal of our module. ODyn is a mechanism that in a continuous basis monitors a specific domain of the grid, enforcing the participating entities to exchange security information among them. ODyn is also utilized to guarantee the integrity and availabil-

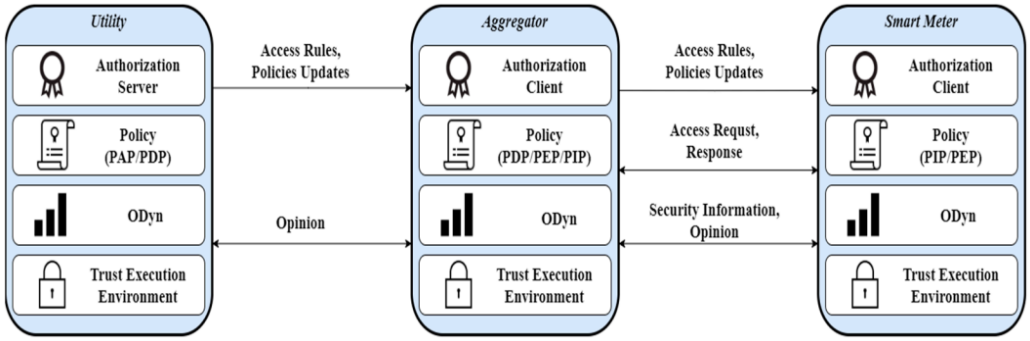


Figure 3.3: SAMGRID architectural components

Table 3.2: Main entities and roles participating in SAMGRID

Entity	**Description**
Smart Meter (SM)	Collect the readings of the electricity consumption.
Aggregator	Sum all the SMs' readings and transmit the result to the Utility.
Role	**Description**
PAP	Authors and maintains a set of policies.
PDP	Assesses a policy against other relevant policies and attributes.
PIP	Is a source of attribute values.
PEP	Performs decision requests, receives policy updates and accordingly translates them, and enforces policies' decisions.

ity of each active entity. We have to note, that the proposed authorization process as well as the ODyn utilize TEE [50] that is the anchor for integrity and validation proofs constructing a robust foundation for any application to be on top; however, we will avoid analyzing the TEE and its performance because TEE is out of scope of this work.

3.4.1 SAMGRID

SAMGRID consists of two individual sub-modules. The first one is the Authorization that handles issues related to issuing and enforcing policies within a SG domain. The second sub-module is ODyn, which is responsible for monitoring the security status of each participating node, understanding if a node is compromised or not.

In the case where a new node is introduced into a SG domain, the first ex-

ecuted process will be part of the Authorization sub-module so that it can get updated regarding the latest policies (e.g., security policies). Once the processes of the Authorization submodule are successfully completed, the ODyn then starts working since the new node shall start exchanging the respective information. The same pattern is followed also when the Authorization submodule will issue and demand the spread of a brand-new policy. To perform the SAMGRID operations, we assume that SMs, Aggregators and Utilities are the participating parties and have at least one of the available roles (PAP, PDP, PEP and PIP) (see also Table 3.2). For instance, a Utility may be at the same time a PAP and a PDP.

3.4.2 SAMGRID Authorization

First, we need to properly define the mechanism behind the Authorization module. As established previously the Authorization module is the one responsible (and that holds the authority) to accept or deny requests within the SG, be that a reallocation of resources or the integration of a new device. What this essentially means is that the state of the SG is continuously changing due to its nature (varying loads within the grid for example), and it is readjusting itself to be as optimal as possible. Therefore, we have a set of factors that change the state of the SG due to the needs that it serves, and we have a set of local components that try to change the state of the SG in order to properly adapt it. The actions of the latter need to be properly analyzed before they are accepted in order to ensure that the new SG state that they will create, will not be a vulnerable one or even become damaged either intentionally (malicious intent) or unintentionally (accidental). In order to accomplish that SAMGRID proposes a hierarchical authorization framework, composed of the previously defined roles (PAP, PDP, PIP, PEP).

In order to know the new state of the SG that accepting a request will create previous states must be known. This is conducted using entities that hold the PIP role. These are located essentially everywhere in the Smart Grid and their role is to gather as much information as possible. This is conducted using the embedded context-awareness module, present in all devices within the grid. The data gathered are normalized in order to keep only relevant information, the rest being dismissed as noise. This information can consist for example of the number of energy usage readings, the set of households controlled by an aggregator and their energy demands, updates regarding

utility systems, databases, contractual arrangements, and network related aspects. Security assessments are also being conducted at this level in order to enable a fast response in the case of a potential threat. This is mainly accomplished by the Opinion Dynamics module that will be discussed in the next section.

With the current state, which is essentially a digital twin, of the Smart Grid known, the next state created by a request can be predicted. In order to assess if the new state is desirable (does not contain security threats, for example), strict policies are defined. The entities that tackle the control-access policies are the ones that have a PDP role.

3.4.3 SAMGRID Opinion Dynamics (ODyn)

In this section, we will analyze ODyn's goals and technical approach. ODyn relies on numerous internal processes and only their combination can lead to its final target.

SAMGRID adopts and integrates an opinion dynamics approach that aims to seamlessly work together with the SAMGRID authorization mechanism intending to address and maintain a secure ecosystem with a low cybersecurity risk. In particular, ODyn transforms the nodes, which participate in a domain, from being passive without being involved with security actions, to active agents. The latter, due to the new activated mode, are enforced to communicate among them security related information to detect anomalies. As previously clarified, PDP, a role mainly given to a Utility, is capable to authorize access to the grid resources based on policies or on the security status of the controlled domain as well as various attributes (e.g., usage of computational resources) that affect the assets that request access. The latter information is provided at all times by the ODyn module that is hardcoded in each participating node of a domain. Overall, ODyn acts as a framework that gathers and combines input from various sources (due to heterogeneity of a domain). The combination is crucial for monitoring a domain and confronting security threats in it, during its whole lifecycle. ODyn is capable of it through its correlation algorithm that analyzes and traces numerous threats.

In particular, our module, ODyn, follows pre-existing models [56, 59] perceives a domain as a graph $G(V, E)$, where V is the set of nodes $v_i, ..., v_n$ and E is the set of edges $e_i, ..., e_m$ that represent the connection (v_i, v_j) among

the nodes. Moreover, there is the set $A = a_1, ..., a_n$ that mirrors the agents. As we described above, each node due to the ODyn has been transformed to an agent; this leads to fact that $|V| = |A|$. ODyn aims to compute the opinion of an agent ai in the t-th iteration, we defined it as $o_i(t)$. It receives values from 0 to 1, where 0 means the absence of anomaly while 1 shows the paramount anomaly. To compute this value, every agent a_i nominates a value—its opinion—to its neighbor j to consider or not its opinion that is denoted as w_{ij}. We have to note that the sum of weights coming from every agent is 1, regarding its own opinion. Based on the aforementioned assumptions, ODyn calculates the opinion of agent ai in the iteration $t + 1$ based on the following function $o_i(t + 1) = w_{i1}o(t) + w_{i2}o(t) + ... + w_{in}o(t)$. We can observe that the influence on a specific agent comes from a weighted average of the opinions that stem from its neighbors.

3.5 Performance Evaluation

This chapter analyzes the performance evaluation of the sub modules that assemble the SAMGRID component to scrutinize the feasibility and efficiency of the proposed module.

3.5.1 Authorization

We analyzed the performance of the Authorization component of SAMGRID in order to gather insight on its feasibility and scalability. We have tested the response time of the authorization API (as a crucial parameter that might otherwise render the component unusable) as well as the RAM and CPU consumption. In our proof-of-concept implementation, the participating SMs and Aggregator are simulated on ARM devices and used as operating system Raspbian Jessie. The Utility, which is the owner of the domain, is a server with Intel(R) Core (TM) i5-65000 processor. The testbed is summarized in Table 3.3.

To assess the authorization component, we subjected it to a stress test, using a series of scripts written in bash, as well as two tools: percentile (https://github.com/yuya-takeyama/percentile (accessed on 17 March 2022)) and ntimes (https://github.com/yuya-takeyama/ntimes (accessed on 17 March 2022)).

We defined a series of tests by varying the number of clients that call

Entity	Setup
Smart Meter	ARM Device, 4-core CPU at 1–1.2 GHz, 512 MB RAM
Aggregator	ARM Device, 4-core CPU at 1.2–1.4 GHz, 1 GB RAM
Utility	Intel Core i5-6500 CPU at 2 GHz 8 cores, 8 GB RAM

Table 3.3: SAMGRID testbed parameters for Authorization.

# of Nodes	Average CPU Utilization (Percentage)			Average Memory Consumption (MB)			API Response Time (ms)		
	Smart Meter	Aggregator	Utility	Smart Meter	Aggregator	Utility	Smart Meter	Aggregator	Utility
10	6.86	1.39	0.8	154.57	315.69	1455.42	162.85	71	38.62
50	6.68	6.87	3.43	154.71	327.29	1464.28	868.83	357.41	137.96
100	6.58	12.82	6.59	132.28	261.78	1481.81	4041.98	460.3	189.1
500	7.86	19.3	34.3	137.40	304.12	2033.95	6670.35	2529	1545.4

Figure 3.4: Authorization component performance

the REST API interface of the component. We considered as evaluation results the measured API response time as well as CPU and RAM variation according to the number of clients.

Figure 3.4 shows the performance of the authorization component as deployed on the three types of the SAMGRID devices. We can observe from the results that the CPU utilization is relatively low with a few percentages for all device types, especially for a small number of clients making requests. We noticed an increase in CPU utilization especially for the Aggregator and Utility. The memory consumption of the SAMGRID devices does not vary significantly with the number of connected clients. For the SM and Aggregator, it is relatively constant at approx. 30% of RAM consumed. For the utility, it drops to 18–25% of RAM.

The most significant difference is noticed in API response time. The more powerful resources of the Utility enable a faster response time, ranging from 38 ms to 1.54 s. For the SM, these numbers are considerably worse (starting from 162 ms to 6.6 s), as well as for the Aggregator (from 71 ms to 2.5 s).

3.5.2 ODyn

Regarding the ODyn, we analyzed the performance of this sub-module of

Entity	Setup
Smart Meter, Aggregator	ARM Device single-core CPU at 700 MHz, 512 MB RAM (Download: 9.6 Mbps; Upload: 9 Mbps)
Utility	Intel Core i5-6500 CPU at 3.2 GHz 4 cores, 8 GB RAM (Download: 98 Mbps; Upload: 92 Mbps)

Table 3.4: SAMGRID testbed parameters for ODyn

SAMGRID to investigate its feasibility and effectiveness. We focused on the execution time of the core source code of ODyn regarding the time needed to detect a cyber-attack within a specific domain, identify the malicious node as well as to spread the opinion of the latter node to the whole domain. For our proof-of-concept implementation, the participating SMs and Aggregator bearing the responsibility of executing the ODyn are simulated on ARM devices with a 700 MHz single-core CPU, a 512 MB RAM and used as operating system Raspbian Jessie. The Utility, which is the owner of the domain, is a server with Intel(R) Core (TM) i5-65000 at 3.2 GHz with four cores, an 8GB RAM and used as the operating system Debian GNU/Linux 10. The testbed is summarized in Table 3.4.

For the ODyn prototype, we developed and utilized our own implementation of ODyn in Python language and forced one iteration per second; it is a custom implementation and can be configured to match the various cases. Moreover, to simulate the ransomware and crypto mining attacks, we used our own scripts in Pythons to deplete the sources of the infected nodes; the latter were randomly chosen by a Python script and the malicious code was then integrated to their OS.

To assess the performance of ODyn, we calculated the average CPU utilization, memory consumption and network usage during every iteration of the ODyn algorithm as shown in Figure 3.5 . We evaluated the behavior of ODyn in three different cases where the domain had a different length including 100, 500 and 1000 SMs and Aggregators. To calculate the aforementioned values, we executed the experiments 10 times. We have to note that we do not consider the Utility as an extra domain participant since it participates in every experiment as the owner. Regarding the CPU consumption of the participating SMs and Aggregator it is constant at 1.44% regardless of the domain length. However, the CPU utilization for the Utility, which is the owner of the domain, fluctuated based on the domain length. As it is presented in

# of Nodes	CPU Utilization (Percentage)		Memory Consumption (Percentage)		Network Usage	
	Smart Meter, Aggregator	Utility	Smart Meter, Aggregator	Utility	Smart Meter, Aggregator	Utility
100		1.47		0.26		51 MB
500		18.07		0.9		255 MB
1000	1.44	25	0.1	1.1	514 Kb	500 MB

Figure 3.5: ODyn overhead

Table 4, when the domain included 100 nodes, then the CPU utilization was at 1.47%, with 500 nodes was 18.07%, while when within the domain, there were 1000 nodes the CPU utilization reached the 25 of the CPU (one core out of four available cores). Furthermore, the memory consumption for the participating nodes of the domain was consistent disregarding the length of the domain. In addition, the memory consumption at the Utility's side is at 0.26%, 0.9% and 1.1% for a domain including 100, 500 and 1000 nodes, respectively. Additionally, the network usage of SMs and Aggregator regards their number was steady at 514 Kb per node. While the network usage at the Utility's side escalated based on the domain's length. In particular, it was 51 MB, 255 MB and 500 MB for a domain including 100, 500 and 1000 nodes correspondingly. Overall, based on our experiments, we can observe that the ODyn as an individual component of SAMGRID does not deplete the resources of the participating entities, even for constrained devices such as SMs and Aggregators. Additionally, based on the results we can assume that the ODyn does not impede the rest of the SG application that may work on top of the SAMGRID enabling their seamless cooperation.

Finally, we assessed the effectiveness of the ODyn algorithm against ransomware and crypto mining attacks, developing Python scripts, to investigate if our implementation can identify the attack and detect the malicious node in time. To complete the aforementioned experiment, we created a domain with one Utility that is the owner of the domain, and 100 nodes from SMs and Aggregators. In both simulated cyber-attacks (ransomware and crypto mining), we randomly infected 10 and 55 nodes to examine how responsive the ODyn is. We have to note that, in this evaluation, to calculate the corresponding values, we executed the experiments 10 times, as we did for the previous experiments (see previous paragraph). In particular, we targeted

to scrutinize if the final opinion that is generated, for a specific node due to a cyber-attack, by the algorithm is unbiased or not by its neighbors. We have to note that the graph used in both cyber-attacks is a fully connected graph. We decided to follow this approach to provoke ODyn to follow a false opinion; it could lead to a silent cyber-attack with numerous aftermaths. On the one hand, during the first experiment, the 10 out 100 nodes are detected as infected nodes since their opinion starts with value being from 0.8 to 1, the rest nodes are healthy having low values as opinions. In Figure 3.6 3a, we can observe that in the first iterations (Time—x axis) the opinion is different and quickly we understand that the domain is under attack. However, while the iterations pass the opinion dramatically changes creating the opinion that the domain is healthy and not under attack, the opinion was near to 0.5 (see Figure 3.6). On the other hand, when the infected nodes were 55 out of the 100 nodes the situation was totally different. In the first iterations the opinion was steady high. However, this opinion was followed even after the 100 iterations. Then, the total opinion was near to 0.9 suggesting that the domain is under attack (see Figure 3.7). Overall, studying the results we can observe that the final opinion of a domain depends on the connectivity among the participating nodes, the number of the infected nodes and the approach being encapsulated by each Utility regarding the value of each opinion (extreme; high; medium; low). It is discernible that the more the connections among the nodes, the more accurate the opinion. However, the most important is that ODyn can detect that a domain is under attack when the number of infected devices is more than half of the total participating. Finally, we have to note the final opinion in the question "Is the domain under attack or not?" depends on the approach that is followed by each Utility against the ODyn. The stricter the used approach is the more agile the opinion will change.

3.6 Security Analysis

In this chapter,the SAMGRID is evaluated in relation with the security requirements presented in Chapter 3.2. Argued that SAMGRID meets all security requirements presented in Chapter 3.2, except for physical protection (S5 requirement as presented in Chapter 3.2), as hardware security [79] can be considered out of the scope of this work. First, the SAMGRID integrating the Authorization sub-module achieves maintenance within a domain specific

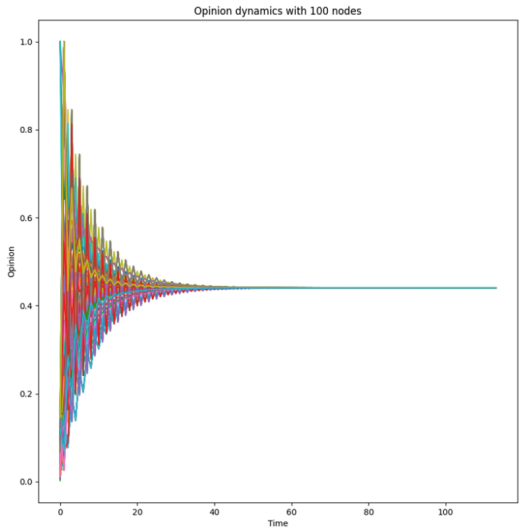


Figure 3.6: 10 out of 100 nodes are infected

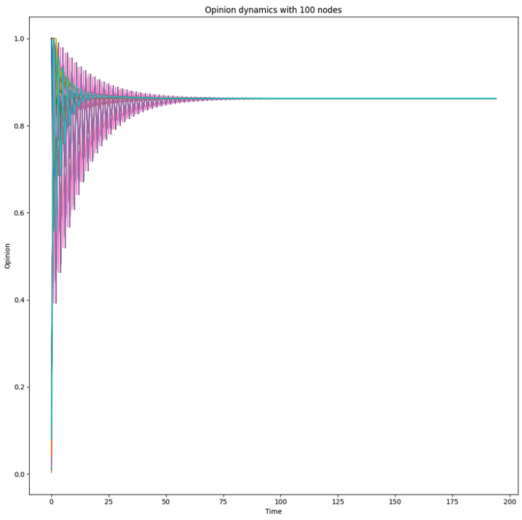


Figure 3.7: 55 out of 100 nodes are infected

entity that follow the security policies being issued by their corresponding PDPs and PAPs. Apart from this, SAMGRID, having numerous nodes with the PIP in a network topology, can gather data and through the ODyn can evaluate the behavior of each participating node based on specific policies. We can observe that the collaboration of the two SAMGRID sub-modules is capable of safeguard the data confidentiality in a domain.

Moreover, the Authorization sub-module that is based on FI-WARE (see Sectio 3.5) is responsible for monitoring the various events, issue policies (e.g., security policies) and audit the actions of the participating nodes within a domain. In particular, our implementation utilizes cloud as we have already clarified in Section 3.5 and all events and logs are stored there. Through the audit of the various events, SAMGRID is based on the issued security policies and identifies malicious events and actors who tried to violate any policy. Thus, SAMGRID can practically maintain the accountability and nonrepudiation features that are crucial in a SG domain. Additionally, ODyn utilizes TEE for its main processes. Its integration effectively enriches the integrity and authenticity features. TEE, due to its characteristics, safeguards against alteration and replication attacks. However, we do not analyze here the TEE since we have analyzed its capabilities and performance in our previous published work [50].

Finally, a hypothesis indirectly related to the security characteristics of the SAMGRID is that instead of designing new protocols from scratch, we have appointed a solution that includes a long-established technology. More specifically, SAMGRID's pillars are technologies that have been broadly analyzed and reviewed, and up to now, there are no imminent threats that can break its security properties. This makes SAMGRID not only provably secure, but also easier to be absorbed by industrial environments.

3.7 Conclusions

This work introduces, for the first time, the SAMGRID module that combines an authorization mechanism and an opinion dynamics approach (ODyn) to maintain and spread a standard cybersecurity risk level in a SG domain. The security status of a SG domain depends not only on the security risk inherited by the components but also on the inadequate security controls implemented by handlers to these. The crux of the SAMGRID is the ODyn that monitors on a continuous basis the security status of all participating components

of a SG domain. Having designed and implemented the SAMGRID, we quantitatively evaluated its performance and effectiveness. One the one hand, regarding its performance we proved that it could cope with various domains regardless of their length (continuous join and leave actions of components). On the other hand, we assess SAMGRID and especially ODyn's effectiveness against attacks that simulated ransomware and crypto mining attacks. We believe that this work will pave the way for numerous upcoming schemes and frameworks for enhancing the security features of the SG ecosystem, as we did with the recent introduction of SAMGRID.

The outcomes of this work can be extended in various ways as a future work. For this proof-of-concept implementation of SAMGRID, we designed and developed a prototype; ODyn was evaluated in simulation environments, while the authorization module was evaluated in a virtualized environment. Next, we plan to integrate SAMGRID as a whole in physical devices assessing its behavior. Moreover, we aim to utilize self-sovereign-identity technologies to assess SAMGRID's applicability in the SG ecosystem. This will help us to identify supplementary case studies for SAMGRID to advance its current features and extend its functionalities with new ones.

Chapter 4

P2ISE: Preserving Project Integrity in CI/CD based on Secure Elements

During the past decade, software development has evolved from a rigid, linear process to a highly automated and flexible one, thanks to the emergence of continuous integration and delivery environments. Nowadays, more and more development teams rely on such environments to build their complex projects, as the advantages they offer are numerous. On the security side however, most environments seem to focus on the authentication part, neglecting other critical aspects such as the integrity of the source code and the compiled binaries. To ensure the soundness of a software project, its source code must be secured from malicious modifications. Yet, no method can accurately verify that the integrity of the project's source code has not been breached. This chapter presents P2ISE, a novel integrity preserving tool that provides strong security assertions for developers against attackers. At the heart of P2ISE lies the TPM trusted computing technology which is leveraged to ensure integrity preservation. We have implemented the P2ISE and quantitatively assessed its performance and efficiency.

Table 4.1 summarizes the scientific publications related to this chapter.

Authors	Title	Venue
Muñoz A, **Farao A**, Correia JR, Xenakis C	ICITPM: integrity validation of software in iterative continuous integration through the use of Trusted Platform Module (TPM)	ESORICS 2020, Springer [$Rank : A$]
Muñoz A, **Farao A**, Correia JR, Xenakis C	P2ISE: Preserving Project Integrity in CI/CD Based on Secure Element	Information MDPI [$IF : 3.1$

Table 4.1: List of thesis' publications- Part C

4.1 Introduction

Lately, the programming community has been witnessing a rapid increase in the adoption of development methods like Development and Operations (*DevOps*), *Agile* and Continuous Integration, and Continuous Delivery (*CI/CD*) by developers across the world. Automation is a key aspect of the aforementioned methods, used to build, deliver, and test high-frequent increments of features [80],[81],[82]. *DevOps* has been defined as a set of practices intended to optimize the time required between committing a change to the system and for said change to be incorporated into production code. *Agile* practices are focusing on eliminating the aforementioned processes and accelerating product delivery, by quickening the development life cycle. The *CI/CD* pipeline is considered to be among the best practices for delivering code changes more frequently and reliably during code implementation. On one hand, Continuous Integration (*CI*) can be described as the guided practices that enable continuous surveillance in code repositories allowing development teams to implement changes in code and their check-in. To achieve this, relevant mechanisms are required for the integration and validation of code changes derived from multi-platform features from contemporary applications. Technically, we can define *CI*'s primary goal as providing a set of tools to build, package and test applications in an automated and consistent way. This consistency allows the teams to increase the frequency of committing code changes, improving both collaboration and software quality. On the other hand, the Continuous Delivery (*CD*) technique which picks up at the end

of *CI*, performs automation in application delivery to particular infrastructures. The use of different environments for code production, development, and testing where multiple code changes are submitted at the same time has recently become a widely popular practice. *CD* provides an automated way to perform those changes, keeping stored packaging parameters bound to every delivery.

Due to its features, *CI/CD* is one of the most popular practices used by software developers to deliver code changes in the most reliable way. According to a survey by DigitalOcean [83] on developer trends released in 2017, it has been revealed that 42% of the survey respondents and members of the DigitalOcean developer community use a *CI/CD* solution and they believe that its most beneficial aspect is that it allows developers to quickly review and deploy code. The *CI/CD* pipeline consists of specific components; however, it inherits the security considerations which are related to the traditional IT system but also connected to human behavior. Establishing mechanisms that protect the integrity of a software project against cyber-attacks that threaten to compromise it is of paramount importance for ensuring the robustness of the final product. Despite the increasing popularity of *CI/CD* tools among the developers community and the all attention they have been getting, to the best of our knowledge, there is no work in the literature proposing a way to guarantee the integrity of software projects as part of the *CI/CD* pipelines. This work identifies and analyzes the security gap that exists in the *CI/CD* pipeline regarding a software project's integrity. To this end, we propose the *P2ISE*, a novel tool that is tailored to the *CI/CD* concept and employs trusted computing technologies, such as secure elements, to ensure the integrity of software projects. More specifically, at the heart of *P2ISE* lies the *TPM* trusted computing technology that enables secure storage of critical data (e.g., cryptographic keys), as well as secure execution of sensitive operations. The proposed *P2ISE* has been designed taking into account the existing, traditional architecture of the *CI/CD* pipelines, which extends by introducing a new entity responsible for ensuring the integrity of each software project. To assess the performance of *P2ISE*, we have fully implemented and deployed a prototype utilizing a real *TPM* which was used to evaluate the median duration time, CPU utilization, and memory consumption of the *P2ISE* processes against various software projects. Numerical results show that *P2ISE* can efficiently operate without depleting developers' resources. In summary, the paper makes the following contributions:

- Define security and functional requirements of a tool that is meant to provide developers with *CI/CD* features following a security by design approach.
- Propose *P2ISE*, a solution for integrity preservation for software projects within *CI/CD* environments based on the use of secure elements, in particular the *TPM* chipset. To the best of our knowledge, this is the first paper that proposes a tool to bridge the identified security gap.
- Assess the proposed *P2ISE*'s performance and qualitatively reason about its security properties. For this purpose, we have implemented and evaluated it against various projects.

The work unfolds as follows: Section 4.2 presents essential background information on *CI/CD*, the motivation of our work, the threat analysis we have performed on the *CI/CD* pipeline, and finally the security and functional requirements we have identified based on the developers' needs. Next, Section 4.3 discusses the related work, whereas Section 4.4 elaborates on the processes of the *P2ISE* describing in detail all the required steps. Section 4.5 includes a quantitative performance evaluation of *P2ISE*, and Section 4.6 discusses its security properties. Lastly, Section 4.7 concludes the paper.

4.2 The CI/CD Concept

4.2.1 Definition and participants

The *CI/CD* objective is to enable developers to deliver code changes as frequently as needed, in the most reliable manner. For this reason, *CI/CD* foresees continuous testing, which typically is offered as performance, regression, and another set of tests done within a *CI/CD* pipeline. Developers submit their code for commitment into the version control repository. Also, it is common practice to establish a minimal rate of daily code commitments per team to facilitate the identification of defects and bugs on smaller delta pieces of code rather than large-scale developments. Moreover, working on smaller commit cycles reduces parallel working on the same code by multiple developer teams. Many teams that implement continuous integration start with version control configuration and practice definitions. Even though checking in code is frequently performed, features and fixes are implemented in both short and longer time frames.

Different techniques are used to control and filter code for production in *CI*. Among the most common practices requires from the developers to run regression tests in their environments, which implies that only code that passed regression tests was committed. We notice that commonplace for development teams is to have at least one development and testing environment, which allows for reviewing and testing application changes. A *CI/CD* tool such as Jenkins [1], CircleCI [2], AWS CodeBuild [3], Azure DevOps [4], Atlassian Bamboo [5], or Travis CI [6] is used to automate the steps and provide reporting. A typical *CD* pipeline [81] includes the following stages: (i) build; (ii) test; and (iii) deploy. Nonetheless, improved pipelines include also the following stages: (i) picking code from version control and executing a build; (ii) allowing any automated action such as restarting or shutting down both cloud infrastructure, services, or service endpoints; (iii) moving code to the target computing environment; (iv) setting up and managing environment variables; (v) enabling services as API services, database services or web servers to be pushed to application components; (vi) allowing rollback environments and the execution of continuous tests and (vii) alerting on delivery state and data log are provided. A *CI/CD* environment consists of (i) the *Source Code Control Server* which is responsible to manage changes to the project's documents (ii) the *Assembly Server* which receives the changes and assembles them; (iii) the *Testing Server and Deployment Server* that validates the project work and then publishes the latest version. Conceptually each previously mentioned server is located on different premises.

4.2.2 Motivation

Software development has radically evolved in the last years, from classical rigid models like the waterfall to Agile methodologies providing less docking among member functions developments and more oriented towards impending automation demanded by Industry 4.0 [84]. However, the related security requirements elicited from the procedures followed in recent models

[1] `https://jenkins.io/` Online
[2] `https://circleci.com/` Online
[3] `https://aws.amazon.com/es/codebuild/` Online
[4] `https://docs.microsoft.com/en-us/azure/devops/?view=azure-devops` Online
[5] `https://www.atlassian.com/software/bamboo` Online)
[6] `https://travis-ci.com/` Online

have not been carefully addressed. DigitalOcean [85] published as part of a *CI/CD* best practices tutorial that the proper way to ensure a *CI/CD* environment for a company devoted to virtual server deployment under premises is the isolation from external access. Protecting the *CI/CD* server is crucial, and for that purpose several solutions exist, such as the use of secure shell (SSH) or private keys for APIs connecting through services like GitHub (`https://github.com/` Online; accessed on 3 September 2021) or GitLab (`https://about.gitlab.com/` Online; accessed on 3 September 2021) to the *CI/CD* environment. Moreover, the use of a strong password and a 2-factor authentication solution is also widely recommended [86]. However, Milka [87] revealed that less than 10% of Google users make use of a 2-factor authentication solution. A fail in securing those keys could lead to source code filtering or code modifications as a result of impersonation attacks.

Furthermore, *CI/CD* solutions provide an intermediate interface to manage *Assembly and Test Server* (i.e., Jenkins or GitLab) through a web interface. In the case of Jenkins, it is enabled as credential-based access, and thus, the security of this interface is another issue to consider. We notice that many providers ignore recommendations about *CI/CD* server isolation. Also, Paul et. al in [88] revealed that developers who work with *CD* pipeline are only familiar with the general security attributes and lack in-depth security knowledge. As described in [85], failures in a *CI/CD* pipeline are immediately visible and could halt the advancement of the affected release to the later stages of the cycle.

Nowadays, dockerization and virtualization are used to protect against unexpected events. However, currently deployed software is not considered trustworthy because, on most occasions, software security measures are not carefully considered. Deployment tends to be isolated in host machines, restricting privileges and hardware access as much as possible; however, it is controversial whether developers can rely on these measures or not. The underlying software that controls these virtual machines acting as an intermediary layer between every virtual machine and the hardware is the *Hypervisor*. Dedicated to handling virtual machines, *Hypervisor* can become a single-point-of-failure. For instance, an attacker who gained control of *Hypervisor* can handle every virtual machine without leaving any trace that could reveal the source of the attack. This technique is known as *hyperjacking* [89], and its most common implementation is to insert a malicious *Hypervisor* to replace the original one. The above is an example of a deployment pipeline attack scenario; however, there are many possible attack scenarios. Figure

4.1 depicts how this attack could be implemented in four steps: (i) *Developer* implements a new feature and this is uploaded to *Source Code Control Server* (*Git*-based server in most cases); (ii) changes finished in *Source Code Control Server* are sent to *Assembly and Test Server;* (iii) *Assembly and Test Server* assembles a new software version and conducts unit test and linkage prepared for this software and (iv) once recommended tests are passed, a new version of the software is made public (deployment).

However, assuming that every communication between the participants is secure, we have identified that the most vulnerable participant is the *Assembly and Test Server*. In most cases, it is considered trusted because its interaction is restricted to insert source code. Notwithstanding, we have identified a security gap in a process that is described below. For example, we assume the existence of a malicious agent that has been granted access to *Assembly and Test Server* and inserts a piece of code for detecting every time source code is generated and files are modified. Then it replaces a piece of a key source code file opening a backdoor. The changes will be deployed since at this point the source code is considered as checked and valid. Once the deployment is done, then attacker can complete his attack.

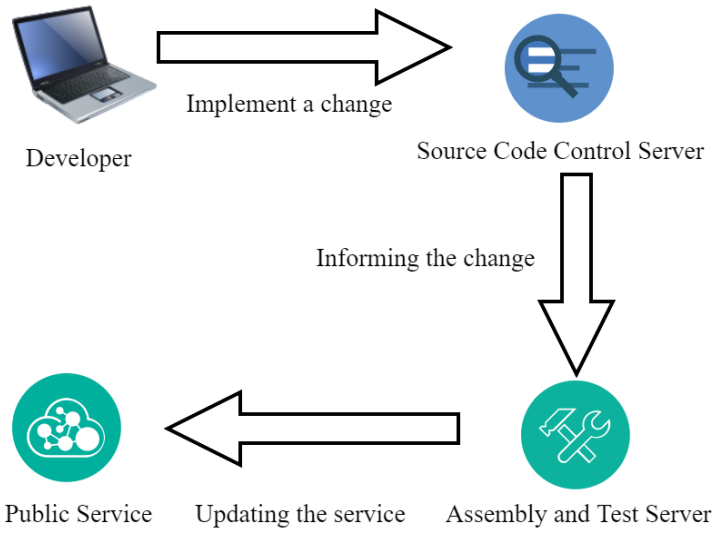


Figure 4.1: Identified Risk in Continuous Integration Process

Threat Analysis

To identify all possible threats for a *CI/CD* pipeline (see Figure 4.1) we

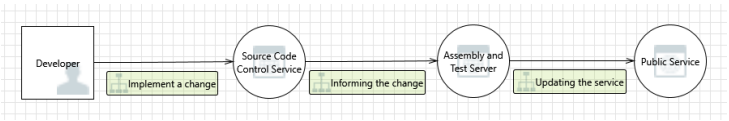


Figure 4.2: CI/CD process scenario in Microsoft Threat Modeling Tool

Table 4.2: CI/CD assets

Information assets	**Physical assets**
User credential	Server
Authorization mechanism	Computer (Developer's PC)
Log information	
Project code	
Product (*Public Service*)	

utilize Microsoft's threat modeling tool that supports the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege) methodology. The scenario that we draw contains the basic entities that participate in a *CI/CD* pipeline, which are the following: (i) *Developer*; (ii) *Source Code Control Service*; (iii) *Assembly and Test Server* and (iv) *Public Service*. We assumed that the *Developer* is a human and does not authenticate himself. Moreover, the *Source Code Control Service* uses both authentication and authorization mechanisms. While the *Assembly and Test Server* utilizes only an authorization mechanism. Finally, the *Public Service* is represented as a Web Service and presents the relevant updates. Defining this architecture, we can observe that the assets in this scenario are distinguished in Information and Physical assets; these are summarized in Table 4.2. However, at this point we have to mention that the identified threats (see below) are related with the specific architecture (see Figure 4.2). By this, we mean that a different use case may generate different threats applicable to our scenario.

By applying the STRIDE methodology to the aforementioned scenario, we identified the threats that are presented below.

T1. *Elevation Using Impersonation*: *Source Code Control Service* may be able to impersonate the context of a Developer in order to gain additional privilege.

T2. *Elevation Using Impersonation*: *Assembly and Test Server* may be able

to impersonate the context of *Source Code Control Service* in order to gain additional privilege.

T3. *Weak Authentication Scheme*: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system.

T4. *Source Code Control Service Process Memory Tampered*: If *Source Code Control Service* is given access to memory, such as shared memory or pointers, or is given the ability to control what *Assembly and Test Server* executes (for example, passing back a function pointer), then *Source Code Control Service* can tamper with *Assembly and Test Server*. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copying data provided, and then validate it.

T5. *Collision Attacks*: Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1.

T6. *Assembly and Test Server Process Memory Tampered*: If *Assembly and Test Server* is given access to memory, such as shared memory or pointers, or is given the ability to control what *Public Service* executes (for example, passing back a function pointer.), then *Assembly and Test Server* can tamper with *Public Service*. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.

T7. *Replay Attacks*: Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity.

T8. *Elevation Using Impersonation*: *Public Service* may be able to impersonate the context of *Assembly and Test Server* in order to gain additional privilege.

T9. *Cross Site Scripting*: The web server *Public Service* could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.

4.2.3 Security and Functional Requirements

As previously mentioned, the *CI/CD* is a concept that provides many advantages to developers but also attracts the attackers' attention. Moreover, a *CI/CD* ecosystem inherits the risks (see Figure 4.1) of traditional IT systems as well as the risks posed by the developers' poor security practices. This leads to the conclusion that security and functional requirements need to be clarified. Since the functional requirements of *CI/CD* ecosystems have been well-established by the literature, lately the focus appears to be shifting towards the security-related conditions that must be met by every proposed solution. For solutions designed to address the needs of developers who employ the *CI/CD* pipeline, we define the following security and functional requirements after considering the *CI/CD* components, users' security and functional demands, and the related research. We have to notice that we redefine functional requirements following security by design approach.

4.2.3.1 Security Requirements

Since a *CI/CD* ecosystem involves risks inherited from both traditional IT system and developers' poor security practices, we re-establish the set of standard security requirements applied to it [90], [91], [92], [93], [94]. In addition, in "Who is Using Jenkins" ((`https://wiki.jenkins.io/pages/viewpage.action?pageId=58001258` Online; accessed on 3 September 2021) there are projects as KDE (`https://kde.org/` Online; accessed on 3 September 2021), Apache (`https://www.apache.org/` Online; accessed on 3 September 2021), AngularJS (`https://angularjs.org/` Online; accessed on 3 September 2021) and Ubuntu (`https://ubuntu.com/` Online; accessed on 3 September 2021) that are publicly accessible and may offer significant help in the integration of general security requirements.

S1. *Data confidentiality*: Code of a project within the *CI/CD* environment should be available only to responsible developers. No adversaries should be able to read and edit the code of the software project.

S2. *Data integrity*: All code transactions (e.g., *push* commands) among the engaging entities (developers) should be protected against malicious alternations. Each process should be monitored and verified.

S3. *Non-repudiation*: Once a developer completes an action (e.g., code changes) then he should not by able to deny it; each actor should be responsible for his actions. This lead to the fact that each action should be monitored and securely recorded.

S4. *Accountability*: A developer should be held accountable for his actions.

4.2.3.2 Functional Requirements

Apart from the security requirements, a *CI/CD* pipeline has processes that require specific functionalities to be enabled. Analyzing the literature [91], [94], we redefine the established requirements following the developing norms and a security by design approach.

F1. *Passive storage with no shared access*: Data that should be accessed only by entities that have been authorized by the owner for specific actions needs to be protected against access attempts by unauthorized entities or to unauthorized actions, while maintaining availability for authorized users.

F2. *Privileged activity tracking*: All modification attempts should be monitored.

F3. *Integrity verification*: Each modification attempt should be verified via hash function before being deployed for avoiding malicious activities.

F4. *Key utilization*: The keys that are used for modifications should have been created and stored only inside the *TPM* preventing possible hardware attacks and data leakage.

F5. *Time consuming*: Since the deployment of project modifications depends on the project's size, the time added due to the extra verification should not negatively affect the *CI/CD* performance.

4.3 Related Work

The literature in the field of *P2ISE* contains the security approaches in *CI/CD* environments and the technology of Secure Element.

4.3.1 Security approach in CI/CD environment

While there is a plethora of works that highlight the importance of security in *CI/CD* pipelines, to the best our knowledge, this is the first paper that proposes the incorporation of an integrity-preserving method in the *CI/CD* pipeline, leveraging for this purpose trusted computing technologies. This work is an extended version of the paper entitled "ICITPM: Integrity Validation of Software in Iterative Continuous Integration Through the Use of Trusted Platform Module (TPM)" by Muñoz et al., that has been published in the proceedings of the 1st Workshop on Dependability and Safety Emerging Cloud & Fog Systems (DeSECSys 2020) [9]. In particular, this extended version includes: (i) a detailed model of possible threats in the study architecture; a precise justification of the need to use a secure element as a trust anchor; (ii) a summary of different benchmarking tests that have been carried out to analyze different projects that exhibit a variety in terms of size and conditions, which demonstrate with real figures the impact that the proposed solution has in terms of performance; and (iii) a discussion related to the security features of *P2ISE*. Parts of the work in [9] are reused in the present paper.

As mentioned above, the use of *CI/CD* has become a prominent practice within the software development community. There are different works such as [95] that review some of the most commonly used practices for *CI/CD* with a specific provider (Azure Kubernetes), while others focus on the use of proprietary tools such as GitOps for a Kubernetes *CI/CD* pipeline. Other works propose ways for organizations to incorporate security practices in the CD process [96] and the separation of duties with the consequent division of development, security and operations roles (*DevSecOps*), by introducing automation mechanisms that reduce the need for a human interface, or by using a development framework for Trusted Execution Environments (TEE) on top of deployment artifacts for their protection [90]. Moreover, authors in [85] proposed a gatekeeping mechanism that safeguards the most important environments from untrusted code through a physical separation between

the *Testing Server* and *Assembly Server*. This, nevertheless, produces a false sense of security since the integrity of the source code is not guaranteed.

We have to note that *P2ISE* is not the first work that utilizes secure elements to reinforce the security of the *CI/CD* pipeline. The integration of secure elements has also been suggested in previous works. Despite the effort for different TEE implementations, such as ARM TrustZone, Intel SGX and recently AMD SEV, to be introduced and leveraged in the software development process, TEEs have so far been more prominent on mobile devices [97]. The proposal from Asylo [90] achieves a breakthrough in improving the *CI/CD* process by integrating an additional step so that artifacts are protected against untrusted administrators, achieving high level of protection even from cloud service providers. Yet, it does not provide a solution to the gap identified and solved in this work. Also, Bass et al. [92] proposes an engineering process within trusted components embedded in parts of the pipeline, which is intimately related to our approach although the use of trusted hardware is not foreseen. Moreover, in [93] different security tactics have been applied between *CD* components communications with encouraging results, whereas Rimba et al. [94] have presented an approach based on the use of composing patterns to address security issues in *CD* pipeline.

Moreover, there are approaches as Nomad [98], Mood et al. present a defense system against known and future side channels and Deepa et al. [99] deal with securing web applications from injection and logic vulnerabilities or approaches based on static analysis and run-time protection and mitigation of vulnerability impact based on security testing techniques [100]. Lipke [101] studies threats in *CD* pipeline using the *STRIDE* methodology implementing a proof of concept based on Docker. Schneider [102] proposes a four-staged dynamic security scanning methodology (pre-authentication scanning, post-authentication scanning, back-end scanning and scanning workflows specific to the targeted application). Also, the same author introduces the *SecDevOps* Maturity Model (SDOMM). This can be considered as instructions for automatically achieving particular security aspects in *CI* pipeline.

In summary, the related work on the security issues of the *CI/CD* pipeline copes with various emerged challenges. However, the preservation of integrity is a requirement that has not been met yet. Therefore, a new scheme dedicated to the integrity preservation is required. The proposed *P2ISE* aims to bridge the gap and enhance the security level of the *CI/CD* pipeline in general.

4.3.2 Secure Element as Trust Anchor

The technological pillar of the proposed solution that provides indisputable security properties is a secure element (SE) with the role of trust anchor. Our concept of secure element is a by design protected from unauthorized access microchip with features as data storing and secure running of applications inside itself. SE can typically be found as a dedicated chip installed on the motherboard of a device (i.e. a smartphone), in an external element such as a flash memory card, in the circuitry of devices such as the SIM card itself used in mobile phones, or as a cloud service in Host Card Emulation technology. A new family of embedded environments known as Trusted Execution Environments (TEE) [103, 104] has emerged. A TEE is a hardware environment with a secure operating system that is isolated and completely separated from the mobile platform. The concept behind a TEE implementation is to provide an independent execution environment that runs alongside the operating system [105]. This environment provides certain security services to the native operation system [1]. Over the last few years, work has been ongoing to standardize the TEE architecture itself as well as the interfaces to interact with environments such as secure environments and SE led by GlobalPlatform (`https://globalplatform.org/` Online; accessed on 3 September 2021). The main objective of this standardization is to provide a hardware and software environment for securing applications such as banking or corporate applications. Moreover, Matetic et al. [106] propose a flexible delegation system with a TEE-based implementation on any browser-based device (smartphone, laptop, desktop, tablet, etc.) that can be also considered SE. In the case of TEE, two implementations have been taken as reference, the proposal of Intel SGX and the proposal of TrustZone and the Global Platform TEE implementation. These two implementations have been taken as references, since the range of TEE capabilities is very wide and each alternative offers different sets of features, but these are widely used and representative of different approaches.

Since specific requirements have been extracted (see Section 4.2), we have decided to integrate the implementation of Infineon's TPM as a technology of the Trusted Computing standard. The Trusted Platform Module (*TPM*) is useful for data protection, as well as for the generation of platform integrity tests, which for our case is a basic feature. However, *TPM* devices are known to come with certain restrictions. Among them, the most significant one is the investment required for this device. For these reasons we have include a

detailed comparison among this *TPM* and TEE implementations to support our decision.

Vasudevan et al. [107] describe the following TEE objectives: (i) Isolated Execution; (ii) Secure Storage; (iii) Integrity, Confidentiality; (iv) Freshness; (v) Remote Attestation; (vi) Secure Provisioning, and (vii)Path of Trust. Among these required properties for any TEE we have to assume that it is difficult to find all of them in the same TEE implementation. Another *TPM*'s advantage is that its specification is open with all that this entails in terms of transparency and evolution, while the Intel SGX implementation is a closed one.

Regarding the functional requirements described above (see Section 4.2), passive storage with no shared access can be achieved using both *TPM* and TEE. However, we have to consider the number of vulnerabilities found in TEE implementations as those focus on the isolation between worlds [108, 109], the wide attack surface [110, 111] and memory side-channel attacks [112, 113, 114, 115, 116, 117, 118, 119]. Moreover, there are side-channel attacks focusing on the TEE's covert channel communication Prime+Probe [112], Evict+Time [112], Flush(Evict)+Reload [113]and Flush+Flush [114]. Therefore, we can safely deduce that *TPM* is a more robust alternative than the TEE.

Furthermore, the activity tracking requirement can be addressed using both *TPM* and TEE. However, the integrity verification related to that required tamper-proof resistant feature to avoid possible attacks as meltdown [120] and spectre [121] is provided only from *TPM*. As keys are issued and stored within the *TPM*, this feature contributes on building the integrity required. The last functional requirement to be considered is the time consumption. However, in terms of efficiency, *TPM* is less efficient since it only has a slow communication bus with the CPU. while in TEE the code is executed directly on a more powerful main CPU, giving a higher level of efficiency, being faster as well as having access to all the RAM available to the OS at the time of execution.

In terms of functionality, the design of the *TPM* states that the processor of the module itself remains isolated from the CPU. For this reason, the *TPM* can only operate with what is provided to it, i.e., it is a passive device that must be accompanied by certain software to make use of its functionality. Indeed, an additional software is needed but some implementations as tpm2 (`https://github.com/tpm2-software` Online; accessed on 3 September 2021) and xaptum (`https://github.com/xaptum` Online; accessed on 3

September 2021) follow the recommendations set out by Trusted Computing Group (`https://trustedcomputinggroup.org/` Online; accessed on 3 September 2021) . Among the different TEE alternatives, TrustZone only allows an isolated section. In the case of Intel SGX, there is a strong linkage to the CPU that allows it to control the management of virtual memory, context switches, as well as high-speed communications. On its part, *TPM* functionality is fully integrated into the hardware and although its design is aimed at providing flexibility. Also, flashing allows arbitrary code to be executed, but has no access to the operating system or drivers. Therefore, only computation and very simple I/O is possible.

Finally, protection against physical attacks is a mandatory requirement; however, TEE does not provide protection against physical attacks. SGX solution provides a protection mechanism against this category of attacks. However, certain weaknesses have appeared, such as the interface to the CPU which is not protected at all, the trusted zone keys may be in unencrypted flash memory or the SGX keys may be in the CPU, which should not be trivial to extract. In contrast, the *TPM* guarantees the physical protection of the keys, the model is much more robust and secure and in spite of the additional cost and other mentioned restrictions we consider the suitable choice to our proposed tool to bridge the integrity gap previously described (see Section 4.2).

4.4 The P2ISE Concept

In this section, we present a blueprint of the proposed tool's architecture along with the process that takes place for its seamless integration with a *CI/CD* platform as shown in Figure 4.3. In *P2ISE*, apart from the standard entities that participate in a *CI/CD* pipeline (see Section 4.2) we introduce the *Trusted Integrity Platform* (*TIP*) (see also Table 4.3), an additional entity that we consider the pillar of our scheme. *TIP* is a server equipped with a *TPM* and a trust software stack for testing the software project integrity. The *TPM* is used as the anchor for integrity and validation proofs as it provides guarantees for building a robust *TIP* server with a controlled software stack that *P2ISE* leverages so it can assure that no malicious code can alter the project. The integrity of the *TIP* server is secured by the *TPM* public key, since its trusted boot process is bound to the corresponding *TPM* sealed key.

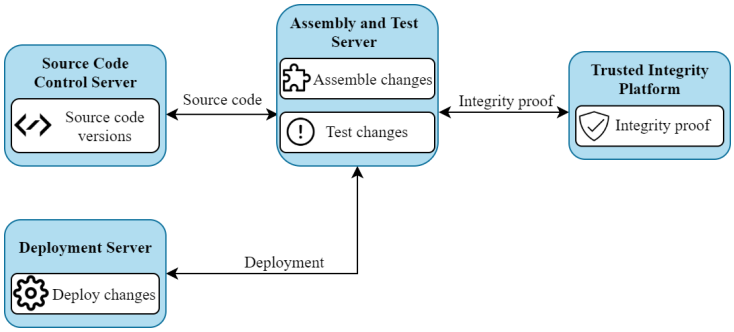


Figure 4.3: Architectural components

Table 4.3: Main entities participating in *P2ISE*

Entity	Description
Developer	A developer who initiates commands.
Source Code Control Server	Track changes in source code.
Assembly and Test Server	Receives changes and assembles them.
Deployment Server	Deploy changes.
Trusted Integrity Platform	Proves software project's integrity.

4.4.1 P2ISE

P2ISE consists of three individual integrity proofs. The first one is taken before installing all the required software dependencies and guarantees integrity between code instances from the *Assembly and Test Server* and *Source Code Control Server*. The second integrity check guarantees that source code under *Assembly and Test Server* remains unchanged from external agents. The third validation checks that the whole process was successfully completed and the code remains unchanged after the assembling.

Regarding the high-level design of the proposed solution, the underpinning idea is that the *TIP* will safeguard the integrity of a *CI/CD* pipeline establishing a secure and trustworthy code integrity control when an assembly code computer is not trusted, utilizing the *TPM* technology. One of the novelties of *P2ISE* lies in the fact that we propose a 3-factor security check. In particular, the third security check provides strong security assertions, since it utilizes the *TPM* keys that are safely stored in the module. *P2ISE* provides a set of functionalities related to software integrity where trust is by default ensured thanks to the use of the *TPM* trusted technology. More-

over, *P2ISE* follows an user-centric approach. Developers are responsible for submitting their code for commitment to a corresponding *Source Code Control Server* and assumed to be trustworthy by the owner of a specific software project. However, *Developers* have always been susceptible to different kind of attacks or bad security practices, making them the weakest link in a *CI/CD* ecosystem.

We consider that a 3-factor integrity proof [122, 123] is the most appropriate for the *CI/CD* pipeline. A comprehensive description of the complete process is described below:

- **First integrity proof measure**: is taken before installing all dependencies required for the project; this guarantees that the source code from the *Assembly and Test Server* is identical to the *Source Code Control Server*.
- **Second integrity proof measure**: it guarantees that source code under assembly remains unchanged from external agents in *Assembly and Test Servers*.
- **Third integrity proof measure**: it guarantees that the whole process was successfully completed without undesired modifications after the project was assembled.

Figure 4.4 shows a sequence diagram with *TIP* process communications in the *CI/CD* pipeline. This shows the 3-factor verification described above, as well as the check point of every integrity proof. The algorithm that enables communication with the *TIP* server actually implements project integrity validation. This script is based on PowerShell and it is tested on Jenkins. The procedure script is included as part of *CI/CD* pipeline testing batches. Also, we have included the *TIP* server script communication from Jenkins in PowerShell.

Every integrity proof is taken following particular steps, which we have categorized in the following phases (see also Figure 4.4):

- **Suspicious code reception**: *Assembly and Test Server* forwards to *TIP* server a compressed file with the *suspicious* source code. If the *uncompressing* phase is not successful, this file is discarded and the integrity proof is considered invalid.
- **Trust code reception**: *TIP* server retrieves source code from the Git repository that is considered as trusted.

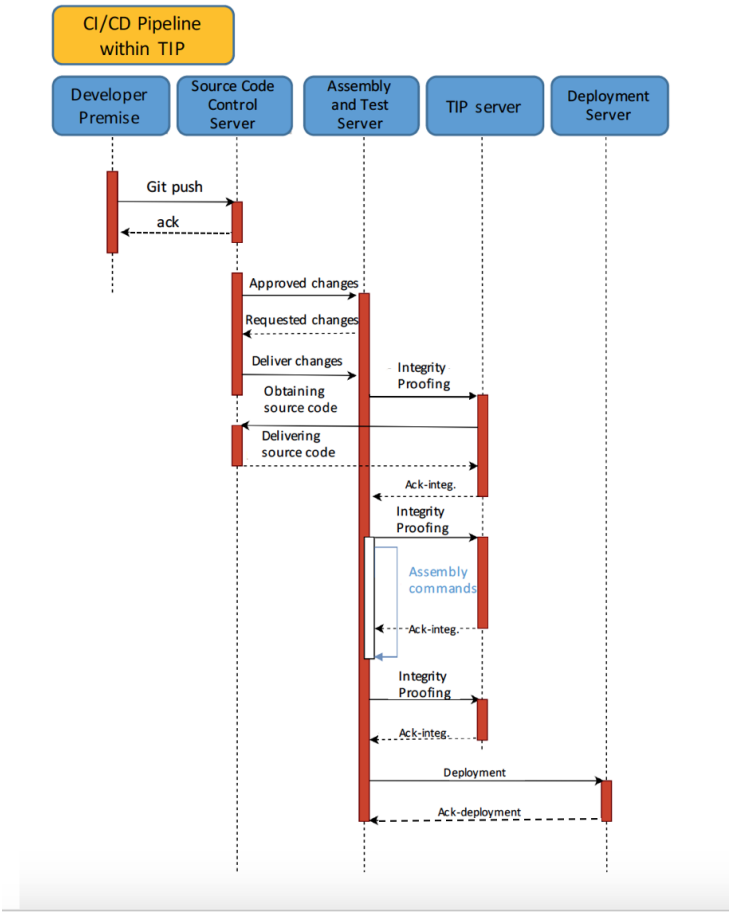


Figure 4.4: Sequence diagram *CI/CD* pipeline within TIP server

- **BigHashes proofs**: *TIP* server verifies, using the respective *TPM* functionalities, that the content of the compress file and the corresponding source code from the repository are identical. This is conducted consulting every hash file from the Git server. These Git registered metadata are linked as a unique chain named bigHash and the *TPM* hash functions are used to verify bigHash values. Therefore, when both bigHash values (project bigHash and compressed file's bigHash) are identical, integrity proof is considered successful.

4.4.2 Technical Approach and Methodology

In this section we analyze how *P2ISE* internally relies on the aforementioned processes to achieve the 3-factor integrity validation proof.

4.4.2.1 First Integrity Validation Check

For the first integrity check, we assume that the *Developer* has already executed Git commands to the *Source Code Control Server*. The latter forwards the changes to the *TIP*. Hence, a temporary folder within the *TIP* Server is created to contain every Jenkins work-space file. Next, all files from Jenkins work-space are compressed into a file (e.g., ZIP file), and the first security check is initiated. Once the compression is completed, the files from the selected folder are taken and filtered, and those included in the *ToExclude* list are removed preserving work-space. Once the file is sent to the *TIP* server, we have a variable $tipServer as a script input parameter. *TIP* server is implemented in PHP and it contains the *gateway.php* file which is the main responsible for the TIP server and includes the configurable variables. Most of those variables are HTTP control headers to allow remote deployment of the *TIP* server. Once all settings are done, then the *TIP* server tries to decompress it. If the decompression process is successfully completed, then the first integrity validation check has been concluded. Moreover, the file is uncompressed in a folder labeled as *suspect*. We have to note that the communication among the *Source Code Control Server* repository and the *TIP* server are performed through *POST* requests.

4.4.2.2 Second Integrity Validation Check

During the second integrity check, the trustworthy repository cloning takes place. Once it is successfully cloned, the BigHash values are computed using a PowerShell script and then *TPM* hashes are retrieved from the trusted repository. After the BigHash value of *suspicious* repository has been also computed, the two bigHash values are compared and the result of validity is obtained.

In our scheme, to compute the hash values, we use the SHA-256 function taking into account both the level of security provided (SHA-256 is considered

secure, while for SHA-1 several vulnerabilities have been identified [124]), as well as the length of the output. Specifically, the *P2ISE* solution takes advantage of the available *TPM* functions to compute the hash values, so the size of the hash would not exceed the *TPM* input buffer limit, which is 32 bytes [125]. Moreover, to compute a complete Git folder hash, every file has to be accessed to link every hash value to a file.

4.4.2.3 Third Integrity Validation Check

The third integrity validation check completely relies on the intrinsic functionality of the *TPM*. *TPM* equipped computers can use the *TPM* functions for issuing and using keys that never leave the chip. These keys are used by internal functions within the chip and can only be accessed by authorized interfaces, but keys are never accessible. This fact enables the protection of created key from disclosure. *TPM* works with a particular key hierarchy that starts with an endorsement root key that is unique for each *TPM* chipset and is assigned while manufacturing. We highlight that the private part of the endorsement key will not be exposed as we have used it in the TIP server.

This step consists of each change being submitted to the Git server carrying a complete copy of the project being signed using the *Developer's* private key. This key is considered as *trusted* since it is created and stored within the *TPM*. To this end, the TIP server stores the project copy when integrity proof is required; it can be decrypted using *Developer's* public key (see Figure 4.5). Therefore, three copies are taken as input integration proofs, these versions should be identical. Creating a private key inside the *TPM* is a trivial process while extracting this key to a hard disk is not. At this point, we have to mention that we have taken into consideration the fact that *CI/CD* ecosystems include users with different privileges. This, however, does not create any problems to the proposed *P2ISE* solution, as the user who uploads the code can also upload updates without corrupting any step imposed by the *CI/CD* process.

4.4.3 Security Appraisal

In this Section, we evaluate *P2ISE* against the nine threats that have been identified (see Section 4.2) using the STRIDE methodology. The proposed tool effectively addresses all threats.

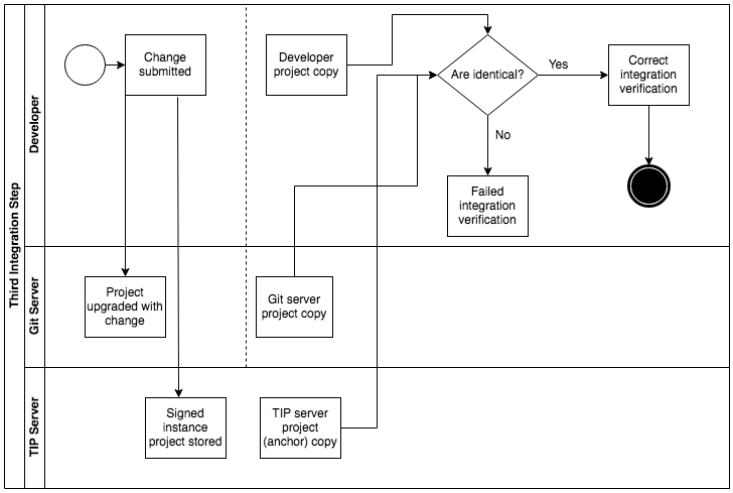


Figure 4.5: Third Integration Verification Step - Developer Verification

First, Elevation using impersonation, from *Source Code Control Service* ($T1$), *Assembly and Test Server* ($T2$) as well as from *Public Service* ($T8$) can be prevented by *P2ISE* since it takes advantage of the TIP approach. The TIP server is equipped with a controlled server stack that guarantees that there is no possibility of containing malicious code, which leads to the fact that the software project is protected against any possible threat of impersonation. Moreover, *P2ISE* can successfully avert threats related to memory tampering of *Source Code Control Service* ($T4$) and *Assembly and Test Server* ($T6$). Again, this is achieved thanks to the use of *TPM* that it is a tamper-proof device. This valuable feature has been extensively presented in Section 4.3 and it is the main reason for choosing to integrate the *TPM* in *P2ISE* instead of a TEE. Last but not least, the design of the proposed solution can avert attacks related to the implementation of a weak authentication scheme ($T3$). As we have already mentioned in the above paragraphs, *P2ISE* utilizes the sealed bind keys of the *TPM* device. Finally, as mentioned in the description of the protocol, communications among the participated entities are designed to avoid possible collusion ($T5$), replay ($T7$), and cross-site scripting attacks ($T9$). Concluding, we can observe that the presence of a *TPM* and a trusted boot system that guarantees each of the boot and execution steps is necessary.

4.5 Performance Evaluation

In this section, we analyze the performance of the proposed tool investigating its feasibility and efficiency. We specifically focus on the added overhead as a result of the newly introduced *TIP* to different *CI/CD* processes. Due to the nature of the integrity checking process, the results vary from project to project and are also highly depended on hardware performance. For this reason, several different tests have been performed and the results offer, in conclusion, a baseline reference for the evaluation of the proposed scheme using relatively modern and fast x86 hardware.

For the prototype implementation, we developed *P2ISE* in C# language utilizing the *TPM* library that is also written in C# [126]. Also, the *TIP* server has been implemented using PowerShell scripts and receives a PHP script as input. Moreover, Powershell 7.2 was chosen as the CLI to be used for the communication among Jenkins and the *TIP* server. For the prototype evaluation, we have employed a desktop PC equipped with an AMD Ryzen 2700 CPU at 3.7 GHz, 32GB RAM, and an AMD *TPM* v3.6.0.3 (compliant with the *TPM* 2.0 specification) integrated into the ASUS ROG B450-F motherboard. Regarding the software that was used to perform these benchmarks, the PC's OS was Microsoft Windows 10 Pro 20H2, and Jenkins was the *CI/CD* environment of choice. The reason behind designing and developing *P2ISE* for Windows OS is that many large organizations have been utilizing Windows Servers to run their services. Besides, Microsoft Server was the market leader with a 48% share of the total server OS shipments in 2018 [127]. *P2ISE* is a tool, which can be integrated into day-to-day processes by these organizations that rely on the code integrity of their projects providing strong integrity guarantees.

To assess the performance of *P2ISE*, we calculated the median duration time of each process individually: (i) Integrity check; (ii) *CI/CD* build process, and (iii) Dependency tree resolution. For evaluation purposes, we decided to assess the performance of our tool against three well-known and open-source projects: (i) the Caddy Server v2 project [128] which has been developed in Go language and is approximately 32k lines of code (LoC); (ii) the Nuxt.js+Vuetify project [129], developed in JavaScript with around 1427k LoC; (iii) the Svelte project [130] developed primarily in JavaScript with only 318 LoC. In all the above cases, the LoC is counted using scc (scc. Sloc, Cloc and Code on GitHub. Retrieved March 29, 2021, from

`https://github.com/boyter/scc/` Online; accessed on 3 September 2021). These three projects with different LoC were selected to highlight how *P2ISE* affects the deployment of projects based on their LoC. While large software projects are more common to come across compared to small ones like Svelte, through these tests we aimed to assess the proposed solution's performance against both types of projects. To calculate the median duration of each process we executed each experiment 5 times and only the necessary processes were being executed at the same time. Jenkins and the TIP server were managed through a web browser application software and only one Jenkins job ran at a time to prevent possible hardware bottleneck. The duration of each process was measured via the Jenkins timestamp plugin. The results are as follows (see also Figure 4.6):

Caddy Server v2: Measuring the performance of our tool against this project, we noticed that the integrity check overhead does not exceed the project's compiling time. The integrity check overhead was found to be stable between the different tests performed and the results show that *P2ISE* adds a small delay compared to the advantages it bears by ensuring the software integrity.

Nuxt.js+Vuetify project: Assessing the performance of our tool against this project, we highlight that the integrity check overhead has been consistent throughout the testing process and practically negligible.

Svelte project: For Svelte, we observe that the integrity check overhead is on par with the build time, which we consider a reasonable addition to this project since the overall time spent on each *CI/CD* cycle is very low. Finally, it is interesting to mention here that the Svelte project is compiled even faster than other projects with similar LoC, because it is acting as a compiler itself.

From the numerical results we can deduce that the overhead caused by our tool is little and well within reason. Overall, it is beyond any doubt that the development community will greatly benefit from adopting the proposed technique since it creates a much safer *CI/CD* pipeline.

Figure 4.7 depicts the summarized results of the performance evaluation for each process. The obtained results have been compared in terms of total lines of code of each project, establishing homogenization between them. As expected, the heaviest process is the build process while the time required for the integrity check, regardless of the number of lines, remains low and stable. We consider this as an indisputable advantage of our tool, since the newly introduced integrity check process does not severely affect the overall

Process Duration (in Seconds)	Caddy Server v2	Nuxt + Vuetify Server	Svelte Server
Integrity check	5.5	2.2	1.9
CI/CD build process	7.1	36.6	1.7
Dependency tree resolution	n/a	13.6	2.6
Baseline	1.1	39.12	2.1

Figure 4.6: meidam duration per process

developer routine.

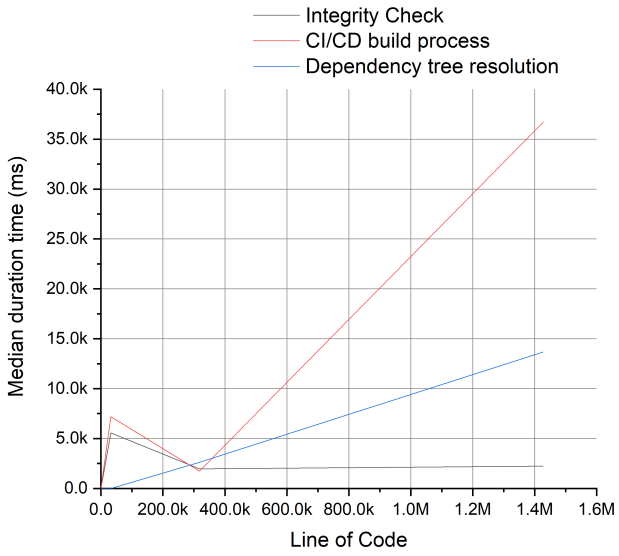


Figure 4.7: Performance evaluation results

Additionally, we measured the average CPU utilization and memory consumption of the processes (Integrity check, *CI/CD* build process and the dependency tree resolution) as shown in Table 4.4. Regarding the *Caddy Server v2*, we observed that the CPU utilization for the integrity check is 10.6% while for the *CI/CD* build process is 38.3%; the memory consumption is 26.4% for both of said processes. As we mentioned above, we did not evaluate the process of dependency tree resolution since it is supported by this project. However, for the Nuxt+Vuetify and Svelte Server projects, we computed the CPU utilization and memory consumption for all processes. The integrity check process for the Nuxt+Vuetify Server project was 6.5% and the memory consumption was 23.2%; the *CI/CD* building process used

the 10.2% of the CPU and the 26.1% of the memory, while the dependency tree resolution process utilized the 26.6% of CPU and the 23.6% of memory. Also, the CPU utilization for the Svelte Server during the integrity check, *CI/CD* build process and the dependency tree resolution was 14.8%, 14.2%, and 25% respectively, while the memory consumption for the aforementioned processes was 25.7%, 26%, and 25.9%. Overall, the most resource-consuming process is apparently the *CI/CD* build while the integrity check that is introduced by *P2ISE* is usually well below the consumption percentages recorded for the build process, regardless of the project and its size (LoC). Last but not least, we can observe that the introduction of a *TPM* chip does not entail a high additional cost. Finally, the results of our experiments have confirmed that the *P2ISE* processes do not deplete developers' resources neither delay the total deployment time, while they guarantee that the final product maintains the integrity of the source code.

Table 4.4: P2ISE overhead.

Software Project	P2ISE Process	CPU Utilization	Memory Consumption
Caddy Server v2	Integrity Check	10.6%	26.4%
	CI/CD build process	38.3%	26.4%
	Dependency tree resolution	n/a	n/a
Nuxt+Vuetify Server	Integrity Check	6.5%	23.2%
	CI/CD build process	10.2%	26.1%
	Dependency tree resolution	26.6%	23.6%
Svelte Server	Integrity Check	14.8%	25.7%
	CI/CD build process	14.2%	26%
	Dependency tree resolution	25%	25.9%

4.6 Security Analysis

In this section, we evaluate the security level provided by *P2ISE* in relation with the security requirements presented in Section 4.2. The results show that the proposed tool meets all the objectives, a conclusion that can be

further corroborated in different cases. First, even an adversary who managed to steal the credentials of a legitimate developer is not in position to manipulate the source code, since he cannot verify his identity because the keys used for this purpose (see Section 4.4) safely reside in the *TPM*. This way, both confidentiality and integrity are achieved.

Moreover, all modern *CI/CD* environments keep records of developers' actions, using them as evidence also in cases where an abnormal or malicious behavior is detected. *P2ISE* ensures the accountability and non-repudiation for each one of these actions (i.e., commit command) by having them signed with the developer's secret key which is securely stored in the *TPM*. This way, no participants can deny their actions since they can be uniquely identified through the use of their key.

Critical processes such as the generation and storage of cryptographic keys, and the execution of other important cryptographic functions (i.e., hush functions) take place within the *TPM* chip. Moreover, in our scheme, each developer authenticates himself by utilizing the *TPM*'s unique key, that is hardcoded into itself. Due to the above, adding a layer of physical protection becomes essential, as all security critical procedures are bound to the hardware. By leveraging the *TPM* technology which provides multiple physical security mechanisms, the *P2ISE* operations are also proofed against physical attacks. Overall, *P2ISE* takes advantage of the features that are provided by the *TPM* to improve the *CI/CD* security.

Finally, an assertion indirectly related to the security characteristics of the proposed scheme is that instead of designing new protocols from scratch, we have opted for a solution that includes a long-established technology. More specifically, *P2ISE* is based on a solution that has been extensively analyzed and reviewed, and up to now, there are no imminent threats that can break its security properties. This makes *P2ISE* not only provably secure but also easier to be incorporated into industrial development environments.

4.7 Conclusions

This work is the first to introduce an integrity preserving tool, specifically designed for developers that use *CI/CD* pipelines to manage their software projects. As the security status of a project depends not only on the underlying IT infrastructure, but also on the personal security habits of the *Developers*, it inherits the security considerations of both. Based on this ob-

servation, in this work it is proposed, designed, and implemented the *P2ISE*, a novel integrity preserving tool for *CI/CD* pipelines based on the use of secure elements. The crux of *P2ISE* is the *TPM* trusted technology, which offers undeniable integrity assertions in the project and helps prevent unauthorized actions. Having designed and implemented the *P2ISE*, we quantitatively evaluated its performance and showed that it can cope with highly demanding projects without depleting developers' resources. As the number of *Developers* who leverage the *CI/CD* pipelines in their software delivery routine is expected to increase over time, new security challenges will emerge. We hope that the research outcomes of this work become a precursor for designing schemes, frameworks, and tools for enhancing the security features of the *CI/CD* pipelines, as we did with the newly introduced *P2ISE*.

The research outcomes of this work can be extended as future work in many ways. For this proof-of-concept implementation of *P2ISE*, we designed and developed a prototype for Windows environments. Next, we plan to implement *P2ISE* for Linux and Unix-based servers, use it alongside different *Assembly and Test Servers* environments besides Jenkins and GitLab, and finally test its performance against large-scale software projects and distributed development environments. This will help us identify additional use-cases for our tool, optimize its existing features, and extend its functionality with new ones.

Chapter 5

P4G2Go: A Privacy-Preserving Scheme for Roaming Energy Consumers of the Smart Grid-to-Go

Due to its flexibility in terms of charging and billing, the smart grid is an enabler of many innovative energy consumption scenarios. One such example is when a landlord rents their property for a specific period to tenants. Then the electricity bill could be redirected from the landlord's utility to the tenant's utility. This novel scenario of the smart grid ecosystem, defined in this paper as Gridto-Go (G2Go), promotes a green economy and can drive rent reductions. However, it also creates critical privacy issues, since utilities may be able to track the tenant's activities. This paper presents P4G2Go, a novel privacy-preserving scheme that provides strong security and privacy assertions for roaming consumers against honest but curious entities of the smart grid. At the heart of P4G2Go lies the Idemix cryptographic protocol suite, which utilizes anonymous credentials and provides unlinkability of the consumer activities. The scheme is complemented by the MASKER protocol, used to protect the consumption readings, and the FIDO2 protocol for strong and passwordless authentication. We have implemented the main components of P4G2Go, to quantitatively assess its performance. Finally, we reason about its security and privacy properties, proving that P4G2Go achieves to fulfill the relevant objectives.

Table 5.1 summarizes the scientific publications related to this chapter.

Authors	Title	Venue
Farao A, Veroni E, Ntantogian C, Xenakis C	P4G2Go: A Privacy-Preserving Scheme for Roaming Energy Consumers of the Smart Grid-to-Go [1]	Sensors MDPI $[IF: 3.9]$

Table 5.1: List of thesis' publications- Part D

5.1 Introduction

The smart grid [131] is becoming the next-generation power grid supporting bi-directional power and communication flows between utility companies and energy consumers. It delivers electricity from utilities to consumers while reducing costs and increasing reliability and transparency. The SG enables better pricing policy and can increase the potential of energy markets due to its flexible model. A new energy market has recently emerged through the vehicle-to-grid (V2G) networks, promoting the use of renewable energy resources and the concept of green energy. V2G has lately gained a lot of attention from the research community, since electric vehicles are expected to play a key role in the forthcoming years in the global effort for transportation to become environmentally sustainable.

Due to its flexibility in terms of charging and billing, the SG is an enabler of many interesting new application scenarios of power consumption and usage. One such use case is the following one. Consider a scenario where landlords rent their properties to tenants for a specific period for business or leisure purposes (Airbnb is an example of an online marketplace for renting houses [132]). According to the current metering and billing system, landlords must pay for their tenants' energy consumption. However, tenants seem to expect unrestricted consumption leading to excessive charges (e.g., charging of electric vehicles by tenants) [133, 134, 135]. In such scenarios, the adoption of smart grid effectively can solve this issue by billing the actual consumer instead of the landlord [10]. SMs can be programmed to charge the tenant through routing consumption measurements from the landlord's utility to the tenant's utility. Nowadays, the Grid-to-Go (G2Go) concept seems to be more relevant than ever. Due to the unprecedented mobility restric-

tions enforced by the COVID-19 pandemic, the "work from home" model has gained significant traction, making professionals realize that they can provide their services from anywhere in the world. These professionals have now the opportunity to embrace the location-independent working lifestyle of digital nomads that allows them to travel and work remotely from anywhere in the Internet-connected world. A recent report reveals that the number of digital nomads in the United States has soared by nearly 50% since 2019 [136]. Even after the mobility restrictions are lifted, the new digital nomads are expected to retain their flexible workspaces [137, 138], since many corporations are shifting towards permanent remote working.

Enabling the G2Go concept improves the efficiency and flexibility of the smart grid, but it also raises great privacy issues and challenges. As G2Go leverages the main architectural components of the location-fixed smart grid networks, it inherits the smart grid privacy considerations which are related to the fact that the smallest detail of household energy consumption can be revealed, including energy consumer habits or detection of the residents' absence from the property [139, 43]. On top of that, G2Go also shares most of the privacy-related concerns encountered in V2G, as both networks permit roaming and consumer mobility, a feature that could be exploited to track location patterns and disclose habits [140]. Therefore, the G2Go requires a new approach in order to cover the privacy and security requirements of smart grids and V2G networks simultaneously. This paper proposes P4G2Go, a privacy-preserving scheme designed to address the needs defined by the roaming consumer scenario. P4G2Go utilizes well established, secure cryptographic protocols and assembles them into a novel scheme that provides strong security and privacy assertions for roaming energy consumers against honest but curious utilities, as well as adversaries who may monitor the smart grid. More specifically, at the heart of P4G2Go lies the Idemix anonymous credential system that enables selective disclosure of attributes that prove that an energy consumer (i.e., the tenant) is legitimate without however disclosing their real identity to untrusted utilities. Idemix provides unlinkability of charging sessions and energy consumption by roaming consumers [141, 142], regardless of the number of times the same credential has been used for verification. This is of paramount importance as colluding utilities can try to track the trajectory of roaming consumers as they move from one place to another. P4G2Go also integrates the Fast Identity Online 2 (FIDO2) [143] to achieve passwordless authentication and enable the mobile device that consumers habitually carry to be the secure container

of the Idemix credentials. Finally, in order to establish a trustworthy environment in the smart grid ecosystem, P4G2Go incorporates the MASKER protocol (developed and evaluated in our previous paper [43]), which aims at providing a privacy-preserving data aggregation solution to protect the energy consumption readings from internal and external adversaries who may monitor the smart grid network. To assess the performance of P4G2Go, we have implemented the incorporated technologies including Idemix. Numerical results show that P4G2Go can efficiently operate a significant number of verification requests. Finally, we evaluate the security and privacy properties of P4G2Go to prove its effectiveness against a set of privacy breach attempts. In summary, the paper makes the following contributions:

1. Define the G2Go concept and present its functional, security and privacy requirements. To the best of our knowledge, this is the first time a scenario for roaming energy consumers is being proposed by the literature.

2. Propose P4G2Go, a privacy-preserving scheme designed for the G2Go concept based on well-established security and privacy-preserving technologies.

3. Assess P4G2Go's performance and qualitatively reason about its security and privacy properties. For this purpose, we have implemented the main components of P4G2Go including the Idemix anonymous credential system.

The work unfolds as follows: Section 5.2 discusses the related work, while Section 5.3 presents the characteristics of the G2Go concept as well as its security and privacy requirements. Next, Section 5.4 investigates the technologies leveraged in P4G2Go and provides a high-level description of the architecture. Section 5.5 elaborates on P4G2Go operations describing in detail all the required steps. Section 5.6 includes the performance evaluation of our scheme, while Section 5.7 discusses its security and privacy properties. Finally, Section 5.8 concludes the paper.

Also, it inherits the SG privacy considerations which are related to the fact that the smallest detail of household energy consumption can be revealed, including energy consumer habits or detection of the residents' absence from the property [139, 43]. On top of that, it also shares most of the privacy-related concerns encountered in V2G, as both networks permit roaming and

consumer mobility, a feature that could be exploited to track location patterns and disclose habits [140]. Therefore, it requires a new approach in order to cover the privacy and security requirements of smart grids and V2G networks simultaneously.

5.2 Related Work

While this paper is the first work that defines the G2Go scenario for traveling consumers who occasionally reside in places other than their home, incorporating for this purpose technologies for anonymous authentication and billing to protect the consumer's data security and privacy, such technologies have been previously combined in the context of electric mobility (e-Mobility) and vehicle-to-grid (V2G) networks. More specifically, there is a plethora of works aiming at addressing the many privacy-related challenges that networks which foresee consumer mobility (e.g., V2G) face. Electronic Vehicle (EV) require frequent stops for charging, a procedure that starts with the authentication of both EV's and owner's identities and usually concludes with the billing process, raising numerous security and privacy concerns [144, 145]. Since several similarities can be identified in the security and privacy concerns described for the roaming EV charging scenario and the proposed application scenario, we have considered previous research on privacy-preserving charging schemes for roaming EVs as related work for this paper, focusing on the technologies used and the level of privacy protection they offer. There is a vast literature concerned with finding solutions to the most prominent privacy-related problems in the V2G ecosystem. A large part of it is dedicated to proposing anonymous authentication and authorization mechanisms for EVs, considering also the identity of their users [146, 147, 148, 149, 150]. Another common problem that has received significant attention from researchers is the billing and payment processes [140, 151, 152, 153, 154, 155, 156]. Research works that deliver solutions to the aforementioned critical topics but do not specifically consider the roaming charging scenario, are out of the scope of this thesis.

In both V2G and G2Go, the challenge lies in building a robust and computationally efficient scheme following the privacy-by-design approach. More specifically, the proposed solutions should satisfy the security and privacy requirements, and at the same time allow critical information to reach the operators to be able to effectively monitor the grid and ensure the account-

ability and non-repudiation in the system. Up to this day, only few privacy-preserving charging schemes for roaming ECs have been published, each exhibiting one or more limitations according to the existing literature [144, 157].

The first study that proposed a privacy-preserving protocol for e-Mobility charging was [153]. Höfer et al., after identifying by means of a Privacy Impact Assessment the privacy gap in the draft ISO/IEC 15118 standard which specifies the V2G communication interface for EV charging, designed and implemented its privacy-enhanced version called POPCORN. Similar to the this thesis, POPCORN leverages anonymous credentials to enable selective disclosure of attributes using the Idemix cryptographic protocol suite, whereas it employs group signatures for ECs to sign the meter readings during charging for protection against cheating vehicles. The authors had to introduce additional actors in the ecosystem defined by the ISO/IEC 15118 standard for handling the payments between providers and resolving possible disputes. While some of its privacy properties have been formally verified, several shortcomings have also been identified, such as the fact that no strong unlinkability properties have been formally proven for the presented scheme [158].

Another privacy-preserving charging protocol for roaming ECs has been proposed in [154], considering the hosts' renewable energy sources as potential electricity suppliers other than the grid. To this end, the authors introduced in their scheme a fair billing functionality, all the while maintaining the EV user's identity and location privacy, as well as session unlinkability through the use of different pseudonyms. Moreover, designed back in 2014, the scheme foresees the utilization of the now outdated smart cards for users to store their sensitive data (i.e., cryptographic keys) for authentication purposes. According to [155] however, the roaming user's privacy can yet be compromised, since the home and host suppliers have direct communication, disclosing both the home and visiting area of the consumer based on the location of the host supplier's charging stations.

Saxena et al. [159] proposed a mutual authentication scheme based on a bilinear pairing technique to preserve the privacy of an EV's information from different entities participating in the grid (e.g., aggregators), both in the home and the visiting V2G networks. While the scheme has shown through comprehensive security analysis to provide resistance against various attacks, it has been identified that it bears significant additional overhead due to the use of computationally inefficient cryptographic primitives [160, 161, 162]. A charging protocol extended to support payment transactions

in line with the principles of the Secure Electronic Transaction protocol, was proposed in [155]. This work provides anonymous authorization and payment simultaneously through the use of dual signatures and pseudonym IDs, protecting user's privacy from both home and host suppliers. To do so, apart from a certificate authority, a broker entity was also added in the system in order to act as a mediator between suppliers. Both the security and the efficiency of the proposed protocol were not verified by the authors.

Finally, the work carried out in [156] has revealed the shortcomings of existing and upcoming Plug-and-Charge standards (ISO 15188, Open Charge Point Protocol, and Open Interchange Protocol) where, based on the authors' analysis, no measures have been defined for protecting the privacy-sensitive charging and billing user data, and avert the generation of movement profiles. The authors have in turn proposed extensions to the aforementioned protocols to address these flaws, leveraging group signatures and a Direct Anonymous Attestation technique that employs a Trusted Platform Module installed in the vehicle, introducing only minimal overhead to the original Plug-and-Charge process.

In summary, the related work on V2G networks copes with various privacy and security challenges, including charging session linkability, security attacks at the level of vehicle software/firmware, vehicle ID tracking, obtaining location related information and extracting driving preferences of users. However, the security and privacy requirements of G2Go extend well beyond the basic requirements of V2G. As G2Go is a hybrid concept, combining features from V2G and location-fixed smart grid networks, G2Go inherits also the security and privacy requirements of the latter, where determining personal behavior patterns and the use of specific appliances is possible, allowing the real time surveillance of the household by adversaries, who are in position to detect residents' absence from the property and launch targeted home invasions (elderly, children), or having third parties use consumption data for profiling and marketing purposes. Therefore, a new privacypreserving scheme is required that will fulfil not only the security and privacy requirements of V2G, but also of the traditional smart grid networks.

5.3 The Grid-to-Go concept application of Smart Grid ecosystem

5.3.1 Definition and Participants

The G2Go allows roaming consumers to have full control over their energy consumption and billing in every property they visit or rent, even in cross-border cases, as long as the related smart grid technology is supported. The basic scenario of G2Go unfolds as follows 5.1. A roaming Consumer is a subscriber to their Home Utility company (denoted as U_H hereafter). At some point, the Consumer travels and becomes a tenant for a specific period of time in a different place, which is served by a different utility company defined as Roaming Utility (denoted as U_R). G2Go enables landlords to avoid being charged for the consumed energy by their tenants. Instead, the tenants will be charged for their exact consumption by their UH. Evidently, a Service Level Agreement (SLA) between the U_H and the U_R should define the way the UR will be reimbursed for the energy consumption of the tenant. For example, small payments may be mutually discarded.

A notable advantage of G2Go is the disincentivization of tenants to needlessly consume energy when they reside in a rented property for a short period (such as in cases of short-term rental agreements through Airbnb). Thus, G2Go contributes towards building a wiser energy consumption mentality promoting environmental awareness. On the other hand, landlords' profit is indirectly increased, since the energy consumption and the related bill is decoupled from the landlord's. Therefore, the property owners can reduce the cost of renting their apartments (i.e., positive externalities), making them more affordable for tenants and thus, more attractive. One can draw parallels between the G2Go scenario and the roaming scenario in mobile networks. In the latter case, a mobile user wants to access the roaming network and get charged by their home operator. However, in contrast to G2Go, mobile operators have long established trust relationships between home and roaming networks. For the G2Go concept to be realized, in a similar manner to the mobile operators, roaming agreements must be put in place between energy suppliers to facilitate flexible charging for consumers traveling domestically or abroad [153].

The G2Go enables interesting business cases and new actors. In particular, we identify three primary stakeholders: (i) the end-users, (ii) the

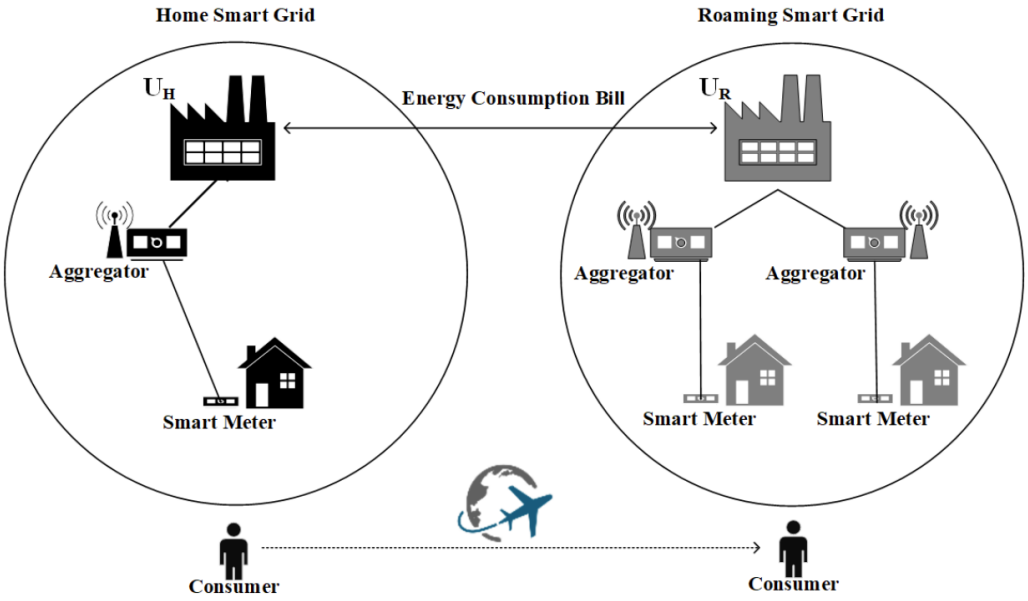


Figure 5.1: Relation between the P4G2Go entities

property owners (landlords), and (iii) the utility companies. A fourth stakeholder is the secondary market that may emerge, in order to address the need for new specialized software for renting, marketing and advertising, etc. On a technical level, the entities that participate in the G2Go scenario are defined as follows (see also Table 5.2): (i) The Utilities are responsible for supplying electric energy and billing the Consumers for their consumption. In G2Go, two different types of Utilities have been distinguished: the U_H that supplies the Consumer's home with electricity and the U_R that supplies the rented property, (ii) The SMs are responsible for collecting energy consumption packets. Each property (e.g., apartment, workplace) is bound to one SM, (iii) The aggregator, which acts as an intermediate node between the Utility and the SM, collects the consumption packets sent by SMs and calculates the consumed energy in each property, (iv) The Consumer who is a person who has an official contract with their U_H, and, (v) The Consumer's Device, which is a mobile device that Consumers habitually carry along (denoted as D_C), such as a smartphone or a tablet. Note that the DC is not part of the G2Go architecture, but it plays a significant role in the

Table 5.2: Main entities participating in G2Go

Entity	**Description**
Consumer	A roaming energy consumer
U_H	Is under contract to supply the Consumer with energy. Issues P4G2Go credentials to its customers.
U_R	Is under contract to supply the rented property with energy. Verifies roaming consumers' P4G2Go credentials.
D_C	Consumer's mobile device
SM	Is bound with a property and measures the occupants' energy consumption. Conveys the consumption readings to its corresponding aggregator.
Aggregator	Aggregates the consumption readings received by SMss. Sends valid and accurate energy consumption data to its corresponding Utility

architecture of P4G2Go it will be analyzed below.

5.3.2 Security Model

Taking into account the aforementioned participating entities and their relations, now this section will draw the respective security model for the proposed solution, relying on the following assumptions:

1. SMs convey consumption readings and they are trustful. However, a malicious software injected after the proper deployment of the SM may try to obtain the readings or convey false information to aggregators.

2. Aggregators follow the honest-but-curious model, which is what most related works on privacy-preserving aggregation depend on. According to this model, aggregators securely send valid and accurate energy consumption data without discarding or tampering the transmitted messages, but they may try to deduce information from the received messages.

3. U_R also follows the honest-but-curious model in the sense that they properly execute the involved protocols, but they are curious and may try to read the data received from other nodes in order to gain information. We assume that different UR may collude and combine

legitimately acquired information in order to link the activities of the Consumer.

4. The U_H follows strict protocol procedures and is trusted by both U_R and the Consumer.

5.3.3 Security and Privacy Requirements

As previously mentioned, the G2Go is a hybrid concept combining features from V2G and location-fixed SG networks and as such, it inherits the security and privacy requirements of both. Since the security requirements of the SG ecosystem have been well-established by the literature, lately the focus appears to be shifting towards the privacy-related conditions that must be met by every proposed solution [163]. For solutions designed to address the needs of roaming consumers who reside in temporary accommodation and wish to be billed fairly for the energy they consume, we define the following security and privacy requirements after considering the smart grid's architectural components, users' security and privacy demands and the related research.

5.3.3.1 Security Requirements

Since the SG involves network operations inherited from both traditional IT and electricity systems, this thesis redefines the following set of standard security requirements applied to the former category within the G2Go concept [145, 164, 165], with the addition of the physical protection requirement, which has been elicited based on the known weaknesses of the smart grid components to physical attacks [11,39].

(**S1**) *Data confidentiality*: Consumption data must be available only to the responsible Utility and the Consumer. No entities may collude to gain information in order to track a Consumer's activity.

(**S2**) *Data integrity and authenticity*: All data exchanged between the participating entities should be protected against alteration and replication. Each entity should be in a position to verify the source of the data received.

(**S3**) *Non-repudiation*: No Consumer should be able to deny their actions. item *Authorization and access control*: Access to the roaming service

is granted only to legitimate Consumers registered at the Utilities that participate in the scenario.

(**S4**) *Accountability*: A Consumer should be held accountable for their actions.

(**S5**) *Physical protection*: SG components should incorporate protection mechanisms to prevent being tampered with by adversaries with physical access

5.3.3.2 Privacy Requirements

The privacy requirements set for G2Go are mainly mobility-related and for this purpose, previous work considering the roaming electric vehicle charging scenario has been used as a basis for their definition [144, 154, 156]. The only exception to the above is the privacy preserving data aggregation requirement, an objective of great significance for the users to be able to maintain their privacy, that was usually encountered in fixed-location smart grid networks[43, 166, 167] until recently [168]:

(**P1**) *Identity privacy*: Consumer's true identity should only be known to their U_H. U_R authenticates Consumers only by their pseudonyms, and it should not be possible for adversaries to identify a Consumer by monitoring the grid.

(**P2**) *Location privacy*: There should be no way for colluding UR entities to track the trajectory of Consumers.

(**P3**) *Unlinkability*: Guarantees that different charging sessions from the same Consumer cannot be linked to each other.

(**P4**) *Minimum data disclosure*: Guarantees that suppliers should access Consumer's data limited to the minimum required to bill them.

(**P5**) *Privacy-preserving data aggregation*: Aggregation of consumption data should happen in a secure and privacy-preserving manner that protects Consumer's individual consumption from being disclosed or modified by unauthorized parties, and prohibits the linkage of a property with a specific energy usage. Also, the end result of the consumption data aggregation should be computed correctly in order to charge the Consumer.

5.4 Technologies and Architectural Overview

5.4.1 Technologies

Now this section briefly presents the technological pillars of the P4G2Go scheme that jointly provide a privacy-by-design solution for the G2Go. We have designed P4G2Go on the grounds of well-established technologies with proven security and privacy properties: (i) Idemix, (ii) Trusted Execution Environment (TEE) and (iii) MASKER and (iv) FIDO2.

5.4.1.1 Idemix

Idemix [169] is an anonymous credential system for selective disclosure of attributes to minimize revealing personal data in digital communications. Moreover, it provides privacy-preserving features such as anonymity, the ability to transact without revealing the identity of the transactor, and unlinkability, the ability of a single subject to send multiple transactions without revealing that these were completed by the same subject. Idemix is the crux of our proposed scheme; it will allow roaming Consumers to hide their real identity from UR, to prevent leakage of their private information. Generally speaking, the involved participants in Idemix are the user, an issuer and a verifier. The Idemix protocol consists of two basic functionalities. The first is the credential issuance, where the user (acting as a receiver) obtains credentials by the issuer. This credential consists of a set of attribute values, as well as cryptographic information that allows the credential's owner (i.e., the user) to create a proof of possession. Each credential is issued on a pseudonym of the user. The user can generate an arbitrary number of pseudonyms using a private key called Idemix master secret. These pseudonyms are unlinkable in the sense that an entity cannot tell whether two pseudonyms originated from the same master secret. Moreover, revealing a pseudonym does not provide any information about the master secret. The use of pseudonyms generated by a secret key is analogous to traditional public key cryptography, where a public key is the identity of the user (e.g., as in Bitcoin), but unlike public key cryptography, in Idemix the user can generate as many public keys (i.e., pseudonyms) as they want from their private key (i.e., master secret). The second functionality of Idemix is credential proving, where a user (acting as a prover) must prove the possession of certain attributes to a verifier without necessarily revealing the values contained within them using zero-knowledge

proofs. When showing a credential, the user can choose which of the credential's attributes shall be revealed and which will be hidden. The user also generates a pseudonym (different from the one used to issue the credential) that will be used as a user reference by the verifier. In this way, both issuers and verifiers identify users only by (different) pseudonyms which cannot be linked.

An extended functionality of Idemix is the cryptographic primitive called verifiable encryption. The latter allows an Idemix credential owner to prove that their credential contains a special attribute which is in essence an encrypted value using the public key of an entity (a trusted third party or the credential issuer itself). This can be very helpful for cases where, for example, a verifier allows access to a service only if the received credential includes the (encrypted) ID card of the user. Thus, although the verifier cannot decrypt the ID card, it can validate the fact that the encrypted value of the ID card is indeed present in the credential (hence the term verifiable encryption). If de-anonymization is required, the verifier will convey the encrypted ID card to the owner of the public key (a trusted third party or the issuer) in order to decrypt (using the related private key) and reveal the real identity of the user. In P4G2Go we take advantage of a verifiable encryption attribute, in order to de-anonymize the Consumer and charge them when needed as we analyze below.

5.4.1.2 Trusted Execution Environment (TEE)

The TEE [103] can be considered a sandbox capable of executing applications (named Trusted Applications). The isolation of the normal operating system from the TEE entails a secure environment, where applications of the normal world including malicious software are out of reach of sensitive data either stored in TEE or utilized by trusted applications. ARM TrustZone is an implementation of a TEE, which has gained particular attention, because ARM processors are omnipresent in the mobile market. Originally, the ARM TrustZone was introduced only for the Cortex-A processors (found in mobile devices), but more recently it has been extended to Cortex-M processors specially designed for embedded platforms, such as SMs. In P4G2Go, the DC that supports an ARM TrustZone will be utilized for storing the Idemix anonymous credentials and the Idemix master secret, while SMs and aggregators will also utilize ARM TrustZone to enhance the security properties of the MASKER protocol.

5.4.1.3 MASKER

A vital part of P4G2Go's architecture is the MASKER [43] protocol, which provides a lightweight privacy-preserving aggregation of consumption data. In MASKER, each participating SM shares with the Utility a series of securely generated pseudorandom values called masks. These mask values are used to hide the SM readings without loss of accuracy. The obfuscation is achieved by simply adding the random mask values to the consumption data. This way, an intermediate aggregator receives from the SM only masked consumption readings and cannot obtain the real consumption values. The aggregator sums all the masked data and provides the Utility with an aggregated value (which is the masked total consumption). The Utility simply performs a subtraction of the used masks from the aggregated value received by the aggregators, resulting in the real total consumption of the relevant SM. In other words, MASKER provides an additive homomorphic solution in a scalable and efficient manner, suitable for low capability devices such as SMs. Only the SM can read the real energy consumption values. In this way, MASKER protects the consumers' privacy by concealing the energy consumption and withstands against adversaries who may attempt to monitor the consumers' activities and habits. Furthermore, MASKER achieves an accurate consumption data mechanism leading to a correct and fair billing method.

At the level of SMs and aggregators, the performed sensitive computations in MASKER are protected by utilizing a TEE, which stores data and executes crucial operations. In particular, MASKER utilizes a TEE in aggregators and SMs for: (i) key generation and storage; (ii) performing secure computations (i.e., additions) for deriving the readings in a masked form. In essence, TEE can provide an extra layer of security, safeguarding SMs and aggregators from malware that may attempt to tamper the randomness of the generated keys. The inner working of MASKER and its technicalities can be found in [43].

5.4.1.4 Fast Identity Online 2 (FIDO2)

The FIDO2 protocol [143, 170, 171] enables users to leverage common devices such as smartphones (also known as FIDO2 devices) to provide a passwordless authentication [41] to services. First, the user must register their mobile device to a FIDO2 server, using authentication mechanisms supported by the device such as fingerprints (or any other biometric modality or authenti-

cation mechanism, such as a pin). The exact authentication mechanism can be imposed by the security policies of the FIDO2 server. At this point, the FIDO2 server attests the user's device and then the latter, acting as a FIDO2 authenticator, generates a public/private key pair. The private key will be stored in the TEE of the device while the public key will be transferred to the FIDO2 server. After the registration of the device, the FIDO2 server can authenticate the user of that specific device. This is performed with public key cryptography using a challenge-response protocol. That is, the FIDO2 server sends a challenge to the device, and the latter requires the authentication of the user in order to release the private key. In case of successful authentication, the device signs the challenge and sends it back to FIDO2 server for verification. Evidently, the device of the user must be secure from attacks that could attempt to retrieve the private key.

FIDO2 includes several advantageous characteristics compared to standard authentication procedures. First, it provides strong authentication based on the use of biometric authentication while the overall user experience is frictionless since the user neither needs to type passwords in such small devices, nor has to remember passwords in the first place. In P4G2Go, FIDO2 is primarily used for the authentication of the Consumer with the UH (i.e., the Idemix issuer).

5.5 P4G2Go Architecture

In this section, a blueprint of the P4G2Go architecture is presented along with the protocol stack of each entity participating in G2Go as shown in Figure 5.2:

D_C: The mobile device of the user is the gist of our architecture. P4G2Go takes advantage of the FIDO2 protocol to utilize the mobile device of the user as a gateway for accessing the service offered by our solution. In particular, the D_C allows users to request the issuance of cryptographic credentials from the U_H and is responsible for revealing issued credentials to U_R. The DC incorporates also a TEE to store Idemix credentials along with the Idemix master secret key. In this way, a Consumer can access and use their Idemix anonymous credentials using their mobile device eliminating the need for smart cards or other cumbersome solutions that would undermine the overall user experience.

U_H: This entity is an Idemix issuer allowing users to issue cryptographic credentials, from their verified identity attribute, directly to their mobile device and then use them to access U_R. U_H has an identity repository that stores its customers' profiles and issued credentials. It also encapsulates a FIDO2 server for undertaking FIDO2 authentication. Finally, the UH will also receive the payment of the energy consumption bill from the Consumer.

U_R: This entity is an Idemix verifier. It will validate the received anonymous credentials of the Consumer, checking whether they are eligible to use the service or not. Moreover, the U_R is responsible for unmasking the masked aggregated values to calculate the total consumption bill using the MASKER protocol.

SMs and aggregators: These two entities run the MASKER protocol for privacy-preserving aggregation of consumption data. Additionally, both entities include an ARM TrustZone TEE to further safeguard MASKER's critical operations.

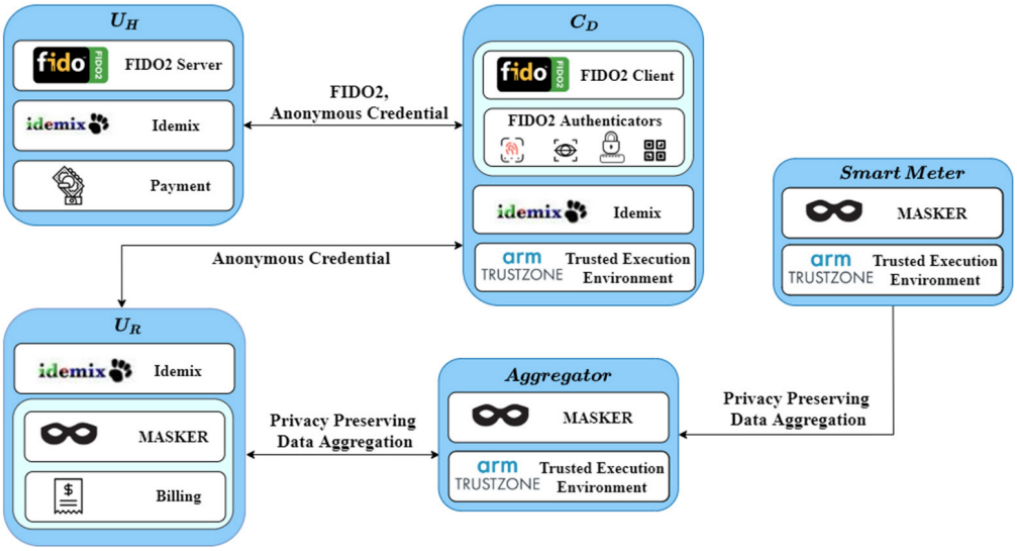


Figure 5.2: P4G2Go architectural components.

5.5.1 P4G2Go Operations

P4G2Go consists of the following individual operations: (i) The Credential issuance in which the Consumer is authenticated to their UH using FIDO2 and subsequently requests the issuance of credentials; (ii) Credential verification and privacy-preserving data aggregation where, as its name implies, the user shows their credentials to the UR and in case of a successful verification, the Consumer can start using electrical appliances or charge their devices. The MASKER protocol enables privacy-preserving data aggregation of consumption measurements which are conveyed to the UR for billing; (iii) Finally, the Billing and payment procedure which involves the de-anonymization of the Consumer by the UH in order to provide the electricity bill to Consumer. To perform the P4G2Go operations, we assume that the DC has installed a mobile application that implements the required functionality of P4G2Go. We also assume that the smart meter includes a local interface (such as a touch/display screen) that allows user interaction with smart meter functionalities (e.g., showing energy usage). The work in [172] analyzes several value-added services specifically based on the local interface of such smart meters.

5.5.1.1 Credential Issuance

For the credential issuance, we assume that the Consumer has already performed a FIDO2 registration with the U_H. We also assume that the Consumer has generated a pseudonym N_H using the Idemix master secret stored in the TEE of the D_C. This pseudonym is permanent and registered in the U_H (note that such pseudonyms are called domain pseudonyms in Idemix terminology). At the beginning of the credential issuance procedure, the Consumer performs a FIDO2 authentication as shown in 5.3 3 (steps 1–6). After the Consumer is successfully authenticated, the UH verifies that the Consumer does not have unsettled debts with the UH and they are eligible to use the roaming service. If this verification is successful, the UH signs the attributes and issues an anonymous credential for this specific Consumer (steps 7–9). We assume that the latter stores the credentials inside a TEE in the DC (step 10). An example of a P4G2Go credential that includes a set of attributes is shown in Table 5.3.

The most important attribute of the P4G2Go credential is $PK_{U_H}(N_H)$, which is the encryption of the Consumer's pseudonym N_H using the public

Attributes	Description
PK_{U_H}	The public key of U_H.
$PK_{U_H}(N_H)$	The N_H encrypted with the public key of the U_H.
Consumer details	Various requirements depending on access control policies.
Type of consumer	Individual, corporate.
Type of appliances	Need for high energy consumption equipment, charging electric vehicles, etc.
Discounts	Special offers for the Consumer.
U_H	The U_H of the Consumer.
Lifetime	The expiration date of the credential.

Table 5.3: P4G2Go credential attributes

key of the U_H. Note that the attribute $PK_{U_H}(N_H)$ will be used by the U_H for billing the Consumer.

This attribute is a verifiable encryption of the pseudonym N_H as discussed previously. Other attributes in the credential are the Consumer details, which include various identity attributes for the Consumer (e.g., age), the type of Consumer (e.g., whether the user represents a corporate company and is eligible for a special offer), type of appliances that will be used (e.g., whether the Consumer can charge their electric vehicle), special offers and discounts, etc

5.5.1.2 Credential Verification and Privacy-Preserving Data Aggregation

When the Consumer rents a property and wants to be charged for the energy consumption, they must provide their P4G2Go credential to the UR for validation as shown in Figure 5.4. To initiate the procedure, the Consumer interacts with the display screen of the smart meter (step 0). The latter forwards the request to the U_R, which generates and sends a QR-code to the particular smart meter, which is presented on its display screen. The QR-code contains the UR URL along with a nonce value (steps 1–2). On QR-code scanning, the P4G2Go application in the D_C prompts for fingerprint (or another biometric modality) authentication to unlock the P4G2Go credential stored on the TEE of the D_C. On successful authentication of the

Consumer, the D_C generates on the fly a pseudonym N_R using the Idemix master secret. The Consumer can generate as many pseudonyms as they want, which cannot be linked by the U_R or any other entity. The D_C sends N_R along with the nonce value (of the QR-code) to the U_R (steps 3–4). The latter can identify from the nonce value the smart meter used by the specific Consumer. At this point, the Idemix Proving Protocol is initiated between the U_R (which is the verifier) and the D_C (which is the prover). The proving protocol requires the D_C and the U_R to agree on which attribute will be revealed and which attributes will be revealed partially (for instance, the D_C can prove that an attribute value is larger or smaller than a specified constant, but the real value will remain hidden from the U_R). Based on the attributes of the Consumer, the U_R checks that the specific Consumer conforms to the policies of the U_R regarding the use of G2Go (e.g., the Consumer is over 18). Moreover, during the verification process, the Consumer proves that the provided pseudonym N_R and the N_H (which is encrypted in the P4G2Go credential—see Table 5.3 2) is generated by the same master secret (step 5). After successful credential verification, the U_R forwards to the corresponding smart meter, the Consumer's pseudonym N_R informing that the Consumer is a valid customer and is eligible to consume energy at the rented property (step 6). From this point, the energy consumption will be charged to the Consumer under the pseudonym N_R. Consumption data are obfuscated thanks to the MASKER protocol which guarantees an anonymous aggregation of the smart meter readings. In particular, the smart meter masks the energy consumption readings with the addition of randomly generated values before conveying them to its corresponding aggregator (step 7). The latter aggregates the masked consumption readings for the corresponding smart meter, and periodically sends them to the UR (step 8). Finally, the latter unmasks the aggregated consumption data and calculates the electricity bill for the Consumer which can be presented on the smart meter display screen (steps 9–11).

5.5.1.3 Billing and Payment

The identity of the Consumer must be revealed to the U_H in order to charge them for their energy consumption. To this end, the U_R sends to the U_H the electricity bill along with $PK_{U_H}(N_H)$, which was included in the P4G2Go credential of the Consumer. Upon receiving this information, the UH decrypts the permanent pseudonym NH using its private key and matches it

Entity	Setup
U_H, U_R	-Intel Core i5-4590 CPU at 3.30 GHz, 8 GB RAM (Download: 90.44 Mbps; Upload: 93.32 Mbps)
D_C	-Xiaomi Redmi Note 5, Octa-core, 2000 MHz, ARM Cortex-A53, 64-bit, Android 9 (Download: 12.9 Mbps; Upload: 1.1 Mbps)
Smart meter, Aggregator	-Raspberry Pi v1 (a single-core 700 MHz CPU, and 512 MB–400 MHz RAM) (Download: 6.9 Mbps; Upload: 0.5 Mbps)

Table 5.4: P4G2Go testbed parameters.

with the corresponding Consumer identity. After successfully retrieving the Consumer's true identity.

5.6 Performance Evaluation

In this section, the performance analysis of the core components of P4G2Go is presented investigating the feasibility and efficiency of the proposed scheme. The evaluation focused on the execution time of (i) issuing an Idemix credential; (ii) verifying an Idemix credential; (iii) authentication through the FIDO2; (iv) registration via the FIDO2; (v) MASKER execution time in smart meters and (vi) MASKER execution time in aggregators. For the proof-of-concept implementation, the U_H and U_R are implemented on a desktop PC equipped with an Intel Core i5–4590 CPU at 3.30 GHz, 8 GB RAM. The D_C is a Xiaomi Redmi Note 5 Qualcomm Snapdragon 6258953, Octa-core, 2000 MHz, ARM Cortex-A53, 64-bit with Android 9. The smart meters and aggregators bearing the responsibility to execute the MASKER are implemented on a Raspberry Pi v1 with a 700 MHz single-core CPU and 512 MB RAM. The P4G2Go testbed is summarized in Table 5.4.

For the P4G2Go prototype, an own implementation of Idemix in Python language has been developed and used, along with the open-source implementation of FIDO2 protocol provided by StrongKey [173], and our previous implementation of the MASKER protocol [174]. To evaluate MASKER, real world consumption values are required. To this end, during the evaluation the utilized publicly available datasets of energy consumption taken from the European Network of Transmission System Operators for Electricity

Table 5.5: Average duration of P4G2Go processes

P4G2Go Processes	Average Duration (in Seconds)
Issuing a P4G2Go credential	1.2
Verifying a P4G2Go credential	1.65
FIDO2 Authentication	3.08
MASKER execution on smart meter	0.05
MASKER execution on aggregator	0.17

(ENTSO-E) [175] has been used.

To assess the performance of P4G2Go, the average execution time of each process individually has been calculated: (i) issuing a P4G2Go credential; (ii) verifying a P4G2Go credential; (iii) FIDO2 authentication; (iv) MASKER execution in smart meters and (v) MASKER execution in aggregators. To calculate the average duration of each process we executed it 10 times. The results are as follows (see also Table 5.5).

Issuing a P4G2Go credential: We calculate the performance of this process by generating an Idemix anonymous credential, containing two attributes to represent the Consumer. The time that is required to issue an Idemix credential fluctuates from 0.9 s to 1.5 s, with an average time of 1.2 s.

Verifying a P4G2Go credential: We calculate the performance of this process by verifying an Idemix anonymous credential that contains two attributes to represent the Consumer. The time that is required to verify an Idemix credential varies from 1.4 s to 1.9 s, with an average time of 1.65 s.

FIDO2 Authentication: We calculate the performance of this process by authenticating the Consumer on the FIDO2 Authentication Server of the U_H, using their fingerprint. The time that is required authenticate a Consumer through the FIDO2 is 3.08 s.

MASKER execution on smart meter: We measure the time that it takes for a smart meter to compute the masked readings and send them to its corresponding aggregator. The time that is required to complete this procedure is 0.05 s.

MASKER execution on aggregator: We measure the time that it takes for an aggregator to accumulate the received masked readings by the corresponding smart meter. The time that is required to complete this procedure is 0.17 s.

Overall, from the numerical results we can deduce that the overhead of the

P4G2Go functions is not substantial and can be executed by the smart grid entities participating in the scheme. The most time-consuming operation is the FIDO2 authentication, which takes on average 3.08 s to execute mainly due to the fingerprint authentication that requires user intervention, which causes delays in the overall authentication process.

Moreover, we measured the average CPU utilization and memory consumption of the utilized protocols (i.e., MASKER, FIDO2 and Idemix) as shown in Table 5. Regarding MASKER, we observed that the CPU utilization in the smart meter is 5.1%, while for the aggregator is 6.6%; the memory consumption is 4.8 MB and 5 MB in the smart meter and aggregator respectively. The results for UR are negligible and are not shown. Therefore, we can observe that MASKER is indeed lightweight and efficient even for devices with limited resources. For the FIDO2 protocol, the CPU utilization in the D_C is 10% and 27% for registration and authentication, respectively. On the other hand, the memory consumption was around 60 MB for both registration and authentication. Additionally, for the U_H that undertakes the responsibility to execute the FIDO2 processes for the server side, the CPU utilization is 5% and 2.6% for the authentication and registration respectively; the memory consumption is accordingly 1148 MB and 1158 MB. The reason behind the higher memory consumption is due to the full-fledged FIDO2 server (i.e., StrongKey server) that was utilized in the experiments. Additionally, the CPU utilization for issuing an Idemix credential containing two attributes is 17% and 26% for D_C and U_H respectively, and for verifying the same credential the CPU utilization reaches 28% in U_H. The memory consumption during the issuance process is at 4.61 MB and 4.76 MB for D_C and U_R respectively. Moreover, the verification process demands 4.78 MB of memory in U_R; the CPU utilization of the verification process taking place in D_C is not shown, since it is negligible (the D_C does not participate in the Idemix verification). Overall, based on our experiments, we argue that the individual components of P4G2Go do not deplete the resources of the participating entities, even for constrained devices such as smart meters.

Finally, we assess the performance of the proposed P4G2Go credential verification against the performance of the vanilla FIDO2 authentication. The aim of this experiment is to assess the overheads imposed by the use of anonymous credentials instead of anonanonymous authentication solution such as FIDO2. The experiments were carried out by sending multiple authentication requests per second (from 1 to 2000 requests). The aim here was to measure the response time (average) to complete the authentication

Entity	**Technology**	**Process**	**CPU Utilization**	**Memory Consumption**
U_H	FIDO2	Authentication	2.6%	1158MB
		Registration	5%	1148 MB
	Idemix	Issuance	26%	4.76MB
U_R	Idemix	Verification	28%	4.78 MB
D_C	FIDO2	Authentication	27%	61.7MB
		Registration	10%	60 MB
	Idemix	Issuance	17%	4.61MB
Smart meter	MASKER	Masking readings	5.1%	4.8 MB
Aggregator	MASKER	Aggregating masked readings	6.6%	5MB

Table 5.6: P4G2Go overhead

process. We used a desktop PC to emulate the DC and we simulated concurrent authentication requests using different software threads. To conduct the experiments, we utilized the Locust tool [176], a Python load testing tool, to generate valid traffic load towards our server that provided us with the average response time for each request of the processes under examination. The results were obtained for both Idemix verification and FIDO2 server authentication as shown in Figure 5.5. The juxtaposition of the two graphs suggests that the Idemix verification presents a non-negligible overhead compared to the vanilla FIDO2 authentication. This is a sheer showcase of usability-security trade-off as authentication does not provide anonymity. However, we observe that the P4G2Go scheme can efficiently operate a significant number of parallel credential verification requests (up to 500 requests per second). The impact on the average response time is increased critically when going above 500 authentication requests per second, suggesting that the server requires more resources (scale up) or replication (scale out) to handle efficiently the workload. Note that concurrent authentication requests higher than 500 can be considered unrealistic for our scenario.

5.7 Security and Privacy Analysis

In this section, the security and privacy analysis of the proposed scheme is presented. It is argued that P4G2Go meets all privacy and security requirements presented in Section 5.3, except for physical protection (S6 requirement as presented in Section 5.3) as hardware security can be considered out of scope of this work. P4G2Go delivers a privacy-preserving solution that can assure that the U_R will not be able to identify the identity of the specific roaming Consumer, who is away from their home and not being served by the UH (P1-Identity privacy) they have a contract with. This observation can be further extrapolated in two different cases. First, the U_R cannot link the Consumer even if the same roaming Consumer is visiting the same property multiple times with the same P4G2Go credential (P3-Unlikability). This is a direct result of the Idemix, which allows multi-showing of credentials (in contrast to another popular anonymous credential called U-Prove [177] which breaks the unlinkability property if the same credential is shown twice). Moreover, using Idemix anonymous credentials we achieve to reveal only specific attributes of the Consumer (P4-Minimum data disclosure). The second case is that our solution guarantees that no colluding parties (i.e., two or more U_R) can join efforts to enhance their linking capabilities. In other words, any attempt by two or more U_R to collaborate and exchange information for tracking a specific Consumer's movement activities and disclose their private information will fail (P2-Location privacy). Again, this is a direct outcome of Idemix as well as the use of different pseudonyms for each different UR. Finally, the use of credentials and specific attributes allows only legitimate consumers to use the service made available through G2Go (S4-Authorization and access control).

Another important aspect of the proposed framework is related to the fact that it achieves balance between anonymity and accountability. This feature is inherited by Idemix since the latter is capable of handling potential abuses of anonymity. Accountability in smart grids is of utmost importance. This happens due to the criticality of the underlying operations of the smart grids and a potential malign Consumer who may cause power disruptions in extreme cases. Accountability of the P4G2Go credential can be easily achieved by the UH as it is the entity that can identify all consumers when the UR sends the $PK_{U_H}(N_H)$ value for billing purposes (S5-Accountability).

On the other hand, it should be noted that the U_R learns the U_H of the

Consumer and their total energy consumption. The U_H can be considered a private information, but in order to charge the Consumer, the specific U_H should be revealed to the U_R. One evident solution to this problem is the addition of a third party, which will act as a payment broker between the U_H and the U_R. However, we have opted for a solution which is free of third parties, since it introduces additional layers of trust, single point of failure and deployment issues.

A usual approach proposed in the literature for storing Idemix credentials is smart cards [178], an unwieldy solution that undermines the overall user experience. P4G2Go resolves this issue by using mobile devices which users habitually carry. The positive effects of utilizing mobile devices are not limited only to usability improvements, but also to security fortifications. The omnipresence of TEE in mobile devices [179] guarantees that sensitive information is security stored. In particular, the Idemix anonymous credentials, and more importantly the Idemix master secret, are stored securely in the TEE of the D_C. As the Idemix master secret is the equivalent of a private key, adversaries may target it through malicious software. If the master secret is revealed, then the security of Idemix may be compromised. However, the use of TEE hinders malware from executing arbitrary code and accessing the stored secret since TEE has the highest privileges in the OS. As a result, malware must also find an exploit to break TEE in order to read private information stored in the secure world [103]. On the other hand, the Idemix master secret being the equivalent of a private key, can be considered as a solution for non-repudiation (S3-Non-repudiation). The use of a mobile device as a credential wallet has another positive side-effect; it allows P4G2Go to take advantage of FIDO2 to promote passwordless authentication using strong authentication modalities, such as biometrics. Coupling FIDO2 and Idemix seems to be a promising approach allowing Consumers to issue Idemix credentials and store them in the TEE of a mobile device.

As U_R and aggregators are considered honest but curious (see Section 2.3.2), one source of concern is that patterns of consumption may reveal more information regarding a customer and their movements. However, this is not possible in P4G2Go, since the exact goal of MASKER is to prevent such privacy breach attempts. In particular, the obfuscation of consumption values by adding randomly generated values (called masks) entails data confidentiality and integrity against honest-but-curious entities which is the most widely used model in the related literature (S1-Data confidentiality and S2-Data integrity). Note that if an aggregator forwards the received masked

values without aggregating them, then it does not follow the model of honest-but-curious entities, because the proper execution of the involved protocol is violated. Even if the aggregator is not trustful and misbehaves, the latter cannot obtain the readings values. Important to note also that it has been proven that the protocol does not leak information that could lead to data eavesdropping [43]. In other words, an adversary cannot deduce readings just by observing the transmitted data. MASKER preserves also the accuracy of the consumption values, because the utility can reverse the process of masking and recover the aggregated measurements exactly (P5- Privacy-preserving data aggregation). Moreover, MASKER utilizes a TEE not only for secure storage of keys, but also for executing sensitive operations from a security point of view including generation of masks, addition of masked values with readings, etc.). On the contrary, a TPM would not be able to perform arbitrary operations like MASKER requires, since a TPM is able to execute only a limited set of standard cryptographic operations. In this way, malicious software injected at the level of smart devices cannot penetrate and obtain sensitive cryptographic information. It is worth mentioning that the feasibility of implementing MASKER as a trusted application has been analyzed in [44]. In contrast to software attacks, hardware attacks are possible to smart meters in P4G2Go, since generally TEEs are not designed to withstand hardware attacks. There is a movement from the European Union [180] to provide available techniques for enhancing cybersecurity and privacy in Smart Metering Systems. Besides, ENISA [181] has mentioned the importance of smart grid hardware security. The literature includes works that propose the use of a TPM [103] to enhance the hardware security of smart meters, while smart cards [154] and PUFs [148] have been proposed for V2G networks.

5.8 Conclusions

The research outcomes of this paper can be extended in many ways as a future work. First, this work introduced for the first time the G2Go concept, which can be further analyzed from a functionality and architectural point of view. Use cases and scenarios that showcase the beneficial aspects of the proposed G2Go can be analyzed in-depth to underscore the novelty and its relevance to digital nomads. Another future direction could be towards decentralizing the architecture of the P4G2Go. This can be achieved using the notion of

decentralized identifiers (DIDs). According to the W3C [182], a decentralized identifier, or DID, is "a globally unique identifier that does not require a centralized registration authority because it is registered with distributed ledger technology or other form of decentralized network". Therefore, blockchain technology can be utilized to achieve a decentralization of the P4G2Go, in order to avoid placing trust in specific entities. Moreover, except for Idemix, other anonymous credential solutions can be utilized such as Anoncreds 2.0 that use the lightweight BSS+ signature [183] instead of the CL signature of Idemix. Finally, anonymous payments can be also considered by utilizing cryptocurrencies.

This paper is the first to introduce G2Go, which is a new concept realized over the smart grid, designed for traveling energy consumers who occasionally stay in places other than their home, within or outside the borders of their country of permanent residence. As the G2Go stands between the fixed-location smart grids and the mobility-enabled V2G networks, it inherits the security and privacy considerations of both. Based on this observation, this paper proposed, designed and implemented P4G2Go, a novel privacy-preserving scheme that provides strong security and privacy assertions for roaming consumers against honest but curious utilities. P4G2Go is composed of cryptographic solutions and protocols that have been analyzed, and up to now, no security flaws have been identified that could undermine their security and privacy assurances. The crux of P4G2Go is the Idemix cryptographic protocol suite, which allows roaming consumers to hide their real identity from roaming Utilities and also provide unlinkability between different showings of the consumer credentials. In P4G2Go, smart meter readings are hidden by simply adding masking values to preserve confidentiality in a lightweight manner. This is achieved by the MASKER protocol which is another critical component of our solution. We have evaluated the performance of P4G2Go and showed that it can cope with high demand as it scales well without affecting the average response time. Finally, we performed a security and privacy analysis of P4G2Go to prove that it fulfils the requirements of G2Go.

As the number traveling consumers is expected to increase over time, new privacy and security challenges will emerge. Digital nomads are becoming the standard way of remote working and may soon become the prime target of adversaries that seek to find their way to access corporate sensitive information. We hope that the research outcomes of this work become a precursor for designing privacy-preserving schemes for the newly introduced

G2Go scenario.

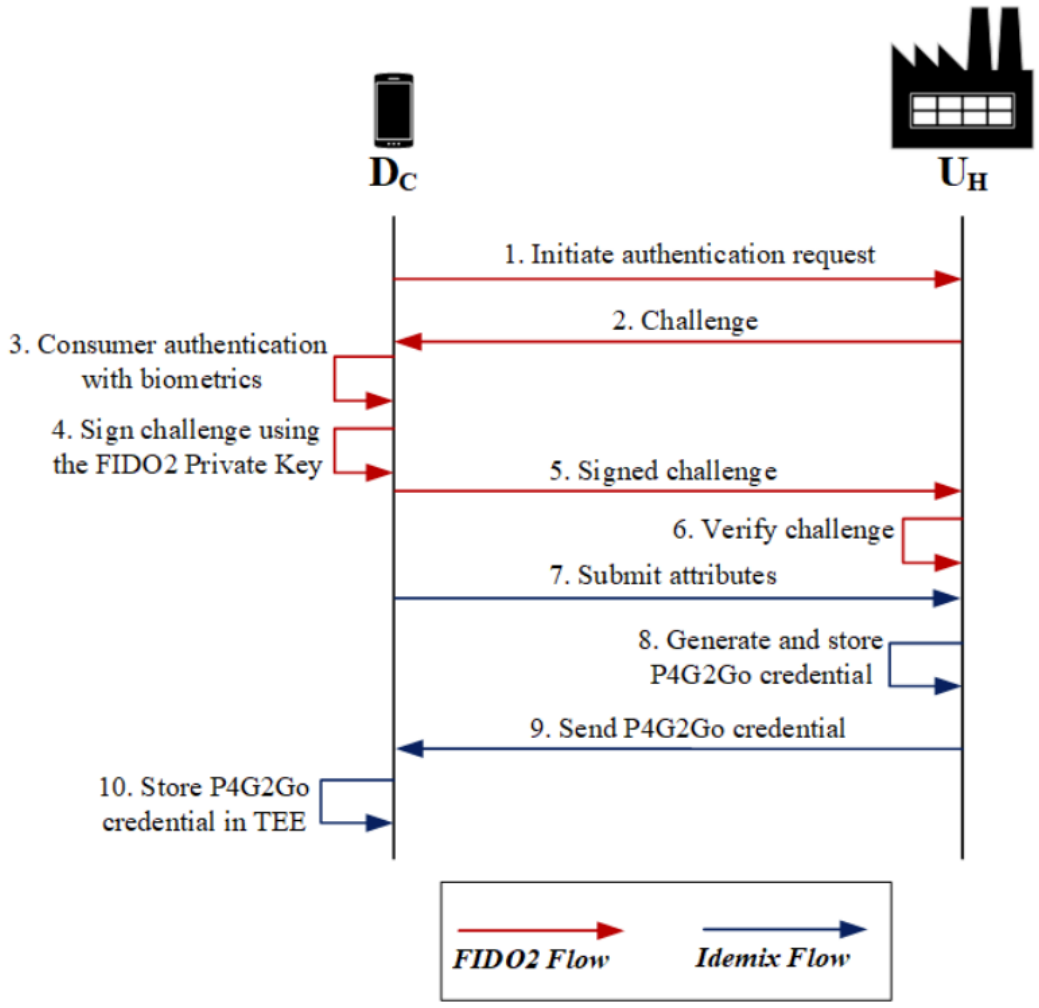


Figure 5.3: P4G2Go credential issuance.

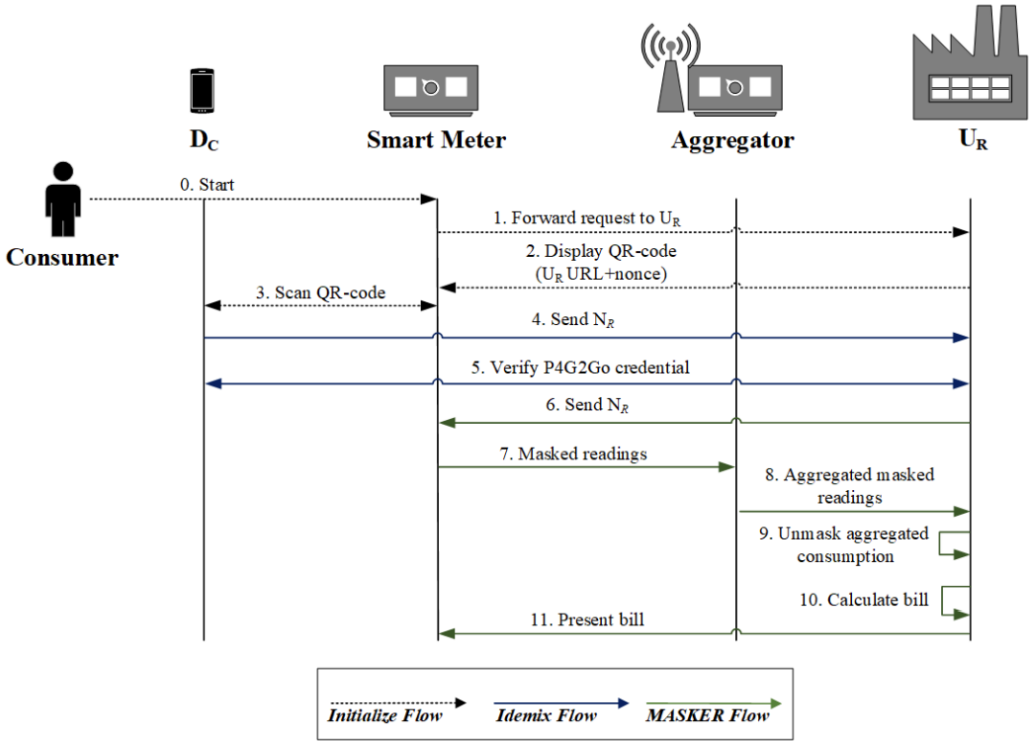
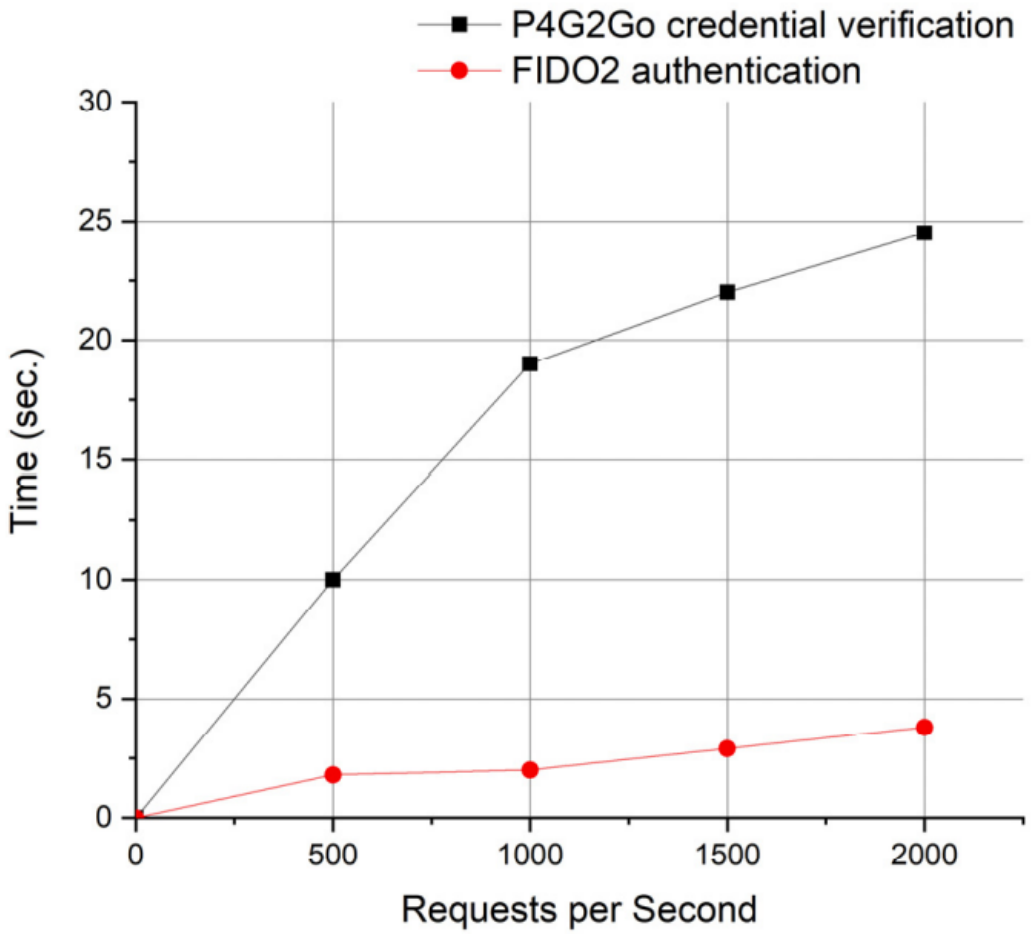


Figure 5.4: P4G2Go credential verification and energy consumption.

Figure 5.5: Average Response Time of P4G2Go credential verification vs. FIDO2 authentication.



Chapter 6

Cyber Insurance

6.1 Cyber-insurance:Past, Present and Future

6.1.1 Outline

Insurance, in general, is a financial contract between the one buying the insurance (also known as the *policyholder* or *insured*) and the one providing insurance (known as *insurance carrier* or *insurer*). The contract, known as the insurance policy, typically states that the policyholder will pay a regular insurance premium in exchange for a financial compensation, also known as *indemnification*, in the event of a loss defined in the *insurance policy*. Insurance is used to manage risks by transferring them to the insurer and cyber-insurance in particular deals with cyber risks covering direct and indirect damages caused by cyber attacks. The cyber-insurance market is still growing and have been receiving broader interest from research communities and government bodies over the years. This paper provides an overview of cyber-insurance, novel models proposed throughout the years and future challenges to be addressed for cyber-insurance to become a key component of an organisation's and household's cyber risk management approach.

Table 6.1 summarizes the scientific publication related to this.

6.1.2 Background

Today, computer networks play a critical role in defining the economic success of most organisations and are essential for providing critical services and

Table 6.1: List of thesis' publications- Part E

Authors	Title	Venue
Panda S, **Farao A**, Panaousis E, Xenakis C	Cyber-Insurance: Past, Present and Future	Encyclopedia of Cryptography & Security and Privacy 2021 Springer

managing sensitive data. Due to the importance of these network systems, they have become preferable targets for adversaries and keeping these connected networks protected from adversaries is a priority. Many organisations have started considering cyber security as a critical business risk and, as a result, are seeking methods to ensure the continuity of their business. Despite the wide application of security measures, a challenging task for cyber security decision-makers is to assign limited resources across a range of possible security countermeasures to prevent or mitigate the effects of a breach. Although security countermeasures and practices are important, decision-makers should also consider other options to deal with residual risks as no amount of investment in cyber security can assure complete protection. One of the alternatives to deal with residual risks is risk transfer where organisations besides implementing countermeasures transfer a portion of their cyber risk (residual risk) by purchasing cyber-insurance.

Insurance is a financial contract between the insured (the policyholder or the one buying insurance) and the insurer (one who insures). The contract, known as the insurance policy, typically states that the insured party will pay a regular insurance premium in exchange for financial compensation, also known as indemnification, in the event of a loss defined in the insurance policy. One of the first work in cyber-insurance was published in the late 1970s discussing specialised insurance coverage against computer crime. Early works in 1990s focused on the general merits of cyber-insurance [184]. As firms became increasingly dependent on network systems and technology, traditional insurance policies fell short in providing the required coverage. To address this, insurance companies started offering standalone cyber-insurance policies. These policies offered coverage for a specific set of cyber risks. Table 6.2 presents the most common coverage and risks that the policy provide liability for, adopted from [185].

The most prominent researcher who brought cyber-insurance into academic research was [186] and from there on it has drawn heightened interest

Coverage	**Risks Covered**
First-Party Coverage	Coverage for the cost of replacing or restoring lost data. Excludes intellectual property.
Data Privacy and Network Security Liability	Coverage for liability claims of a third party (e.g. a data breach or unintentional transmission of a computer virus).
Business Interruption	Covers revenues lost as a result of network down time.
Cyber-Extortion	Cover for investigation costs, sometime the extortion demand.
Public Relations	Fees for public relations firm to manage reputation in the event of a breach.
Multi-Media Liability	Costs relating to the content of a firm's website like copyright infringement.
Professional Services	Liability relating to a service offer such as web hosting or internet service.

Table 6.2: The range of available cyber-insurance coverage.

in the research community. [187] have presented a framework supporting cyber-insurance modelling decisions. While modelling cyber-insurance, the attitude of the agents towards risks plays a critical role. Insurance, in general, requires agents to be risk averse and seek to reduce cyber risks posed to their assets. [187] examine modelling decisions based on five key components: i) Network environment, ii) Demand side, iii) Supply side, iv) Information structure, and v) Organisational environment. The proposed framework offers models and methods to deal with interdependent security risks (or correlated risk) which, along with information asymmetry, are considered as the main obstacles to the development of the cyber-insurance market. The interdependent security risks express the effect (known as externality) of an organisation's security investment decisions on other organisations. Based on the nature of the effect, the externality can either be positive or negative. In the case of positive externalities, the decisions of an organisation have positive effects on itself and others, e.g., increased endpoint security may decrease aggregated losses due to network attacks. On the other hand,

negative externalities have negative impact on the organisation and others , e.g, lack of anti-malware system may negatively impact neighboured PCs, which is under a malware attack, since a number of neighboured PCs may be unintentionally infected. On the other hand, information asymmetry refers to the situation where there is insufficient information about the market and participants. Lack of adequate information leads to two challenging problems: i) *Adverse selection* where the insurer cannot distinguish organisations based on their risk profiles before the insurance contract is in place. ii) *Moral hazard* where insured organisations could undertake risky actions that affect the probability of loss during the contract period. A recent survey on the existing cyber-insurance market and scientific advancements is presented in [188].

Besides modelling, another stream of research develops analytical models to determine the cyber-insurance premiums based on the risk profile of the organisations. [189] introduce models assisting organisations to decide on the utility of cyber-insurance products and to what extent they can integrate them into their procedures. The authors introduced an assessment algorithm based on Copula-aided Bayesian Belief Network for cyber vulnerability assessment to price insurance products incorporating the risk profile and the wealth of the insured organisation. The model took a directed acyclic graph containing the nodes that could lead to a security breach as input and provided a vulnerability assessment report detailing the expected cyber risk value at each node of the graph. They derived the cyber-insurance premium based on the computed expected cyber risk of the nodes. Finally, they introduce a model for assisting organisation to decide whether to transfer the cyber risk or to manage it in-house. [190] took an alternative way by investigating cyber loss cases from an operational risk database to gain statistical insights between loss and cyber-insurance. A key finding was that organisations integrating cyber-insurance achieve to become more aware of risk-appropriate behaviours and protect themselves from cyber risks. The authors have also identified randomness of loss occurrence, information asymmetries, and cover limits as vital obstacles that hinder the development of the insurance market.

Growing cyber-insurance market has encouraged researchers to study various regulatory mechanisms including fines and rebates, liability coverage, and competitive markets ensuring better investments in self-protection and acceptable cyber-insurance contracts. Despite the willingness in considering the cyber-insurance due to increase in number of cyber incidents, a gap exists between the current cyber-insurance assessment process and established

security practices [185]. This gaps can be bridged by coordination among the stakeholders belonging to both government and private sector. To develop cyber-insurance market further, insurers should not only ask organisations to individually invest in cyber security in exchange for lower premium but also should take a proactive role in improving the overall security of their clients. However, such incentivising schemes might bring additional challenges for cyber-insurers as organisations might be inclined to misreport their actual security standards to gain lower premium. To counter such adverse scenarios, [191] introduced a game-theoretic model to study optimal auditing strategies against fraudulent claims in post-incident scenarios to prevent collapse of the cyber-insurance market when policyholders can fraudulently report their security levels.

6.1.3 Advantages

Apart from the primary advantage of transferring cyber risks, insurance in general and cyber-insurance, in particular, has additional benefits. First, cyber-insurance can be used to provoke organisations in increasing their investments in protection to reduce their insurance premium. Secondly, cyber-insurance is believed to improve the social optimum by increasing the level of cyber protection for each participant. Third, cyber-insurance can serve as an indicator of the level of protection of an organisation. Last but not least, cyber-insurance may lead to new and improved standards in cyber security. The growing market of cyber-insurance have encouraged researchers to studies various regulatory mechanisms including fines and rebates, liability coverage, and competitive markets ensuring better investments in self-protection and acceptable cyber-insurance contracts.

6.2 Challenges

Technological inventions and developments have started to become an integral part of any company's lifecycle. However, despite conferring significant advantages, they bring with them an enhanced cyber-physical risk of cyber incidents, and a subsequent growth in products and services aimed at combating the cyber-physical risks. In turn, the proposed solutions (products or services) come with a cost making cybersecurity investment which is a key problem for Chief Information Security Officers (CISOs) to tackle. Impor-

tantly, the GDPR brings into force strengthened requirements for organizations, whihc process or store data as to build data protection and privacy into their organization and design, to notify the authorities of all data breaches that put individuals at cyber-physical risk. With high fines for GDPR violations (up to 20 € million or 4% of annual turnover), cyber-crime can no longer be considered an acceptable running cost of business. It provides a major impetus for organizations to proceed with optimal investments in cybersecurity solutions and procedures to minimize their cyber-physical risk exposure while transferring the residual cyber-physical risk to cyber insurance.

Cyber insurance is a hybrid ecosystem combining features from classic insurance and information technology and inherits challenges from both sectors. The existing literature analysis has identified numerous challenges the cyber insurance ecosystem faces, which we present below.

CH1 – Lack of Data. The cyber insurance ecosystem requires plenty of data to perform an accurate cybersecurity risk assessment and a fair premium calculation. In particular, the data needed is the following. The *historical data* for their potential Policyholders (PHs) to identify future cyberattacks [192]. The *data from the PH's industry* (e.g., healthcare, information, finance) that can reveal a set of asset vulnerabilities and the frequency of a cybersecurity incident occurrence. The *general cybersecurity data* related to information systems (i.e., network, operating systems, information security management system), processes, and human resources for the specific PH. Sadly, Insurance Companies (ICs) do not share their collected data with others due to technical and legal obstacles, as well lack of trust in such a competitive market.

CH2 – Lack of Automated Tasks. All processes between ICs and their PHs require manual operations and labor, which are highly time-consuming [193, 8]. The most critical processes, the claim's submission and validation, are the most time-consuming and drawn-out ones; ICs have to process the claim, verify the cybersecurity incident, and decide whether the PH qualifies for reimbursement.

CH3 – Fraudulent Claims. The most important risk of an insurance agency is the fraudulent actions by PHs [191, 194], which insure their cyber assets at many ICs. This approach allows a dishonest PH to make multiple claims to different ICs for the same cybersecurity incident or split the claims and over-represent losses from the same one [195].

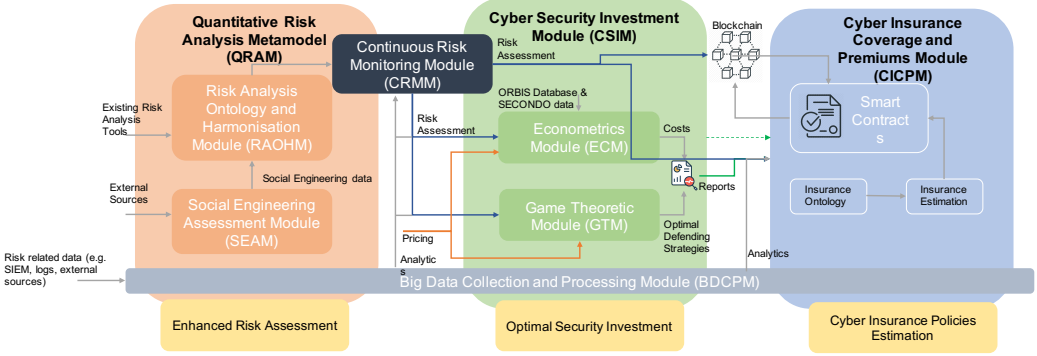
CH4 – Identity Theft. Attackers submit false claims masquerading eligible PHs to an IC utilizing various social engineering techniques, including but not limited to phishing attacks and stealing the personal information of PHs [196, 2, 197]. Remarkably, this challenge originated from ineligible PHs.

CH5 – Loss of Sensitive Data. ICs store the gathered data becoming vulnerable to cybersecurity attacks that aim to copy, alter, or delete them [198, 199]. These are personal data, including the PH's revenue, its assets inventory, its answers to risk assessment questionnaires that prove vulnerability existence, and a set of scanned paper credentials. Data breaches in ICs can expose PHs' personal data that can be used for various cybersecurity attacks (i.e., masquerade). Therefore, rigid data storing methods by ICs inhibit the expansion of the cyber insurance market. Apart from that, PHs may also be targeted by malevolent attacking groups that pretend to be legal ICs to steal their sensitive data and perform illegal actions.

CH6 – Know Your Customer. This challenge includes the actions that ICs follow to verify the identity of PHs and monitor their behavior before and during the life of the cyber insurance contract. ICs request that PHs provide detailed and updated information about their businesses. The existing verification methods are costly and time-consuming. In addition, the quality of the collected data may be inaccurate, leading ICs to draw the wrong conclusions for them [200, 201].

CH7 – Information Asymmetry: It refers to a market situation in which one party has insufficient information about the other party, leading to market failure [202]. Information asymmetry is directly connected to moral hazard and adverse selection. On the one hand, moral hazard occurs when the PH gets involved in a risky event knowing its protection against the risk and the IC will pay the cost [187, 188, 203]. That means one of the parties (usually the PH) accepts a deal to change its behavior after a deal is made. This happens when it believes it will not have to face the negative consequences of its actions. On the other hand, adverse selection occurs when the PH conceals its high-risk exposure from the IC before the cyber insurance contract [187, 204, 188]. That means one of the two parties has more accurate or different information than the other before they reach an agreement. This puts the less knowledgeable party at a disadvantage because it is more difficult for it to assess the risk of the deal. Overall, this ultimately leads to an inefficient outcome and a lower quality of goods and services in the market.

Figure 6.1: Architectural components and integrated modules for SECONDO



Apart from the challenges above, others, such as *Interdependent and Correlated Risks*, and *Premium Calculation*, have been studied and addressed. Regarding the Interdependent and Correlated Risks, they are created during the cybersecurity risk assessment due to the connectivity of information assets of a PH with other assets on an external network [205, 206]. As for the Premium Calculation, their existing formulas are static and unable to adopt technological changes to reduce the overpricing of cyber insurance [207]. On the contrary, the present work avoids getting involved with the aforementioned cyber insurance challenges (i.e., Interdependent and Correlated Risks, and Premium Calculation) since these cannot be addressed with the existing characteristics of Blockchain, Smart Contracts, and Self-Sovereign Identity (SSI).

6.3 SECONDO: A Security ECONomics service platform for smart security investments and cyber insurance pricing in the beyonD 2020 netwOrking era

In this chapter, the SECONDO architecture (see Fig 6.1) along with its components and modules is presented.

6.3.1 Quantitative risk assessment and data analytics

Information security management must start with a risk analysis [208]. The goal of SECONDO risks assessment is to identify: (i) relevant *threats* targeting the assets of an organization; (ii) *vulnerabilities*, both internal and external that these assets exhibit; (iii) *value-at-risk* of the organization that is equivalent to the value of assets (both tangible and intangible) being endangered by adversaries; and (iv) the likelihood that an attack will be launched against the assets. The risk represents the expected losses of an organization should one or more attacks compromise the asset affecting the confidentiality, integrity and availability of business critical services.

Asset pricing - The SECONDO platform will adopt a combination of methods for pricing *tangible* and *intangible* digital assets from a cybersecurity perspective. The objective is to provide precise point estimates on valuations of assets considering both the tangible and intangible aspects such that they can be used to directly value insurance claims in a standard actuary framework.

The outcome of the valuation methods will contribute to the Econometrics Module (ECM) which provides estimates on all kinds of costs of potential attacks.

Risk modeling - Utilizing a Quantitative Risk Analysis Metamodel (QRAM), SECONDO determine quantitative estimates of the exposed risk of an organization. It achieves this by defining methodologies for asset identification and valuation, and utilizing security metrics to quantitatively estimate risk exposure of an organization. QRAM is composed of two modules. The first, Social Engineering Assessment Module (SEAM) which is used to experimentally determine the likelihood of being exploited by social engineering attacks on different employee roles of an organization. Table 6.3 illustrates the results from our experimental study. The second, Risk Analysis Ontology and Harmonization Module (RAOHM) communicates with SEAM and existing risk analysis tools such as OLISTIC[1] to gather their output and harmonize through its unique vocabulary. It uses entity-relationship diagrams between threats, vulnerabilities, security controls, assets, and identified risks with an aim to identify assets to be used in the risk analysis process. Moreover, utilizing the risk analysis ontology will assist in gathering the heterogeneous information from all business areas to support the decisions of an

[1] `http://www.olistic.io/`.

Table 6.3: Overall Likelihood results

Actions	**Contributor**	**Management**	**Upper Management**	**Executives**
Report Email	0	0	0	0
Email Opened	0.33	0.2	0.25	0.33
Email Sent	0.11	0	0.38	0.33
Link Clicked	0.11	0.3	0	0
Submitted Data	0.44	0.5	0.38	0.33
Attack Likelihood	0.55	0.8	0.38	0.33

organization regarding its cyber governance strategy. Currently, SECONDO is implementing this module.

Big data collection and Processing Module (BDCPM) - This module of SECONDO acquires risk related data either from internal organizational sources such as network infrastructure, Security Information and Event Management, log files, users' interactions, or external sources such as social media and other internet-based sources including Darknet with specialized crawlers.

The collected and processed data would be specified and quantified within a meta-model, and utilizing set of data mining and learning algorithms to perform sophisticated analysis.

6.3.2 Cyber Security Investments and Blockchain

This segment of SECONDO will build up on the above discussed modules to compute optimal cybersecurity investment strategies and deploy blockchain technology for secure storage, access and notification of security and privacy information of organisations. This segment consists of two modules:

Continuous risk monitoring and blockchain (CRMM) - This module will continuously assess the risk levels, including the performance of the implemented cybersecurity controls.

It will update the private blockchain with information regarding the security and privacy risk of cyber-insurance clients through smart contracts. Moreover, these will notify the involved parties (insurer and insured) when the insurance terms have violated or when an event has happened to activate the insurance. These are embedded in the distributed ledger and cannot be modified due to its immutability feature providing verifiable records.

Decision-making for cyber investments - Security investment decisions with a limited budget is always a challenging task, even more in the presence of uncertainty, with massive business implications. There have been several studies [209] proposing cost-benefit approaches for selecting an optimal set of controls against cyber attacks. Along this line of work, the Cyber Security Investment Module (CSIM) aims at computing optimal cybersecurity investment plans utilizing the Econometrics Module (ECM) and the Game Theoretic Module (GTM). ECM will provide estimates about the costs of potential attacks as well as the costs of each possible security control using a set of existing econometric models. Utilizing the asset pricing method (detailed in the previous section), ECM will also determine the impact value of an asset. On the other hand, GTM will derive strategically optimal defending strategies expressed in the form of controls to be implemented by the organization. The interaction between players is modeled as a non-cooperative game in GTM where players compete against each other. Following the widely-cited work [210], the corresponding Nash Equilibria (NE), the solution of the game, for each available cybersecurity control will be computed and sent to CSIM to compute an optimal investment solution subjected to a budget while considering the financial cost of each NE.

6.3.3 Cyber Insurance and Smart Contracts

The core component of this segment is the *Cyber Insurance Coverage and Premiums Module* (CICPM). This module will provide insurance exposure assessment and estimates for insurance coverage and premiums based on the insurance policies of the underlying insurer. The insurance policies will be modeled using a common vocabulary and language of cyber-insurance policies by utilizing a cyber-insurance ontology. The ontology will empower the SECONDO platform to automatically incorporate policies. Moreover, the ontology will be based on a comprehensive survey and analysis of the cyber-insurance market and well-known insurance policies as discussed in [187, 185, 188, 204].

CICPM will not only enable underwriters to incorporate their own strategy, as required by a competitive market, but also aim at minimizing the information asymmetry between insurer and insured by applying a verifiable and shared methodology that includes standard and enhanced procedures such as quantitative risk analysis using security metrics and optimal security investments for managing cyber-physical risk. In reconciliation with

CRMM, CICPM will monitor conditions leading to non-compliance of the cyber-insurance contract agreements and assist with resolving claim disputes.

6.3.4 Use case of SECONDO platform in Cyber-physical Risk Transfer in Maritime

The Maritime Cyber Risk Management guidelines [211] highlights the importance of cybersecurity technologies in facilitating critical business functions and secure operation of the maritime industry. Regardless of the increasing cyber incidents, there has been no holistic approach to manage maritime cyber-risks [212]. Further, security procedures and policies are still being defined and determined to be practiced in maritime which further results to an increasing dependency on the insurance industry.

On the other hand, the insurance industry has particularly investigated the *affirmative risks* and *silent* cyber-physical risk [213] to facilitate suitable coverage. With regards to the affirmative cyber-physical risk, the Insurance Property and Casualty Policy [214] states that the insurer shall cover the costs of impact, either physical or digital, in case of data breach and/or network failure or attack.

Coverage capacity, cyber-physical risk estimation and appropriate solutions are difficult for insurers to manage, leading to a margin of the so called silent (unintended) cyber coverage. In this section, we summarize the applicability of the SECONDO platform in the maritime sector to achieve optimal cyber-insurance premium acknowledging both the insured's and insurer's perspective. In the recent past, physical attacks, such as piracy, was a common threat to the maritime sector.

6.3.4.1 Cyber-insurance in maritime

After the adoption of electronic systems such as sonar and IoT systems in both onshore and on-board environments, new cyber and cyber-physical vulnerabilities have emerged increasing the threat exposure of the sector. According to Alliance[2] more than 1,000 vessels have been hacked in the last five years. However, cyber losses quite often are excluded from an insurance coverage as the expected impact of cyber attacks may be considered too uncertain to be included in policy terms. Damages caused by cyber attacks or

[2]https://maritimecyberadvisors.com/_files/200000086-a389ca4859/MaritimeCyberInsurnace052019.pdf

errors (e.g., damage to the vessel due to navigation system malfunctioning after being hacked) are not covered by non-cyber-insurance policies, due to a specific cyber attack exclusion clause ([10/11/2003] also known as Cl.380). According to this clause, insurers do not cover for damages caused by a cyber attack whether it includes physical harm, business interruption or property damage. Other exceptions may include terrorism-related attacks and the NMA2914 electronic data exclusion[3] creating a "cyber-insurance gap" which becomes an impediment for the maritime sector given the drastic increase of cyber incidents [215].

Although cybersecurity incidents in the maritime field increase, only few are being reported. Only major cyber attacks are made public and well-documented, such as the Maersk attack in 2017[4]. The lack of data regarding cyber attacks in maritime creates a "false sense of security" to maritime companies, making them to underestimate the expected cyber-physical risk inflicted by cyber attacks.

6.3.4.2 SECONDO Application

In this use case, the applicability of SECONDO in assisting a shipping company to effectively transfer its *cyber-physical risks* to an insurer provider is presented. The risk transfer process is detailed in three different phases: (1) Cyber-physical Risk assessment; (2) Cyber-physical Risk management; and (3) Insurance exposure estimation, coverage and premium calculation.

Phase 1: The critical assets of a shipping company, as identified in [211], are vulnerable to cyber attacks inflicting cyber-physical impact and endangering the company's financial situation, reputation, property, crew's life, and the environment. This phase deals with undertake the cyber-physical risk assessment on a vessel's infrastructure and systems. It will utilize the CORAS language[5] to formalize threat models and cyber-physical risk scenarios. It will further involve in identifying assets, vulnerabilities and threats to compute the overall risk scores using the RAOHM.

The output will be a quantitative estimation of the cyber-physical risks of the shipping company's infrastructure, assuming known cyber and cyber-physical maritime threats.

[3] https://www.lmalloyds.com/LMA/Wordings/NMA2914A_C.aspx.

[4] https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/.

[5] http://coras.sourceforge.net/coras_language.html.

Phase 2: This phase deals with the cyber-physical risk management utilizing the risk assessment results from Phase 1 and data gathered by BD-CPM. The payoff functions and the optimal controls selection strategies are determined using the GTM and ECM.

The defending strategies will reveal a mapping between the Critical Internet Security (CIS) controls[6] and various threats of the shipping company. For each CIS control, a game will be defined and solved to obtain an optimal solution. The solution of each game will determine the optimal distribution of control implementation levels (Low, Medium, High) over all targets of this use case. The payoff functions will capture both the reduction of cyber-physical risk and the indirect costs of implementing each of the controls.

CSIM will use the results of all these modules to derive optimal ways to invest in cybersecurity controls.

At the end, a smart contract will be set up between the insurance provider and the shipping company indicating the premium as well as the coverage derived from the optimal strategy.

Phase 3: In this phase, CICPM will be used to collect the results of the aforementioned modules to produce an optimal insurance premium and coverage protection. After the premium is set by the insurer, the broker communicates with the shipping company in order to analyze the contract. Along with the proposed contract terms, the shipping company must demonstrate its compliance with various information security guidelines such as BIMCO cybersecurity guidelines[7], the International Maritime Organization's Resolution on IT and OT systems [211], best practices and cyber-physical risk management, and ISO cybersecurity standards compliance. If the shipping company accepts the contract and exhibits compliance to industry and governance guidelines, then all three main actors (the shipping company, the broker and the insurer) strike an optimal deal with policies of the agreement being stored as a smart contract on a blockchain. During the smart contract lifetime, CRMM is used to continuously monitor for possible violation of the agreed policies and to convey any discrepancies on behalf of the insurance provider and the insured shipping company.

[6] `https://www.cisecurity.org/controls/`

[7] `https://iumi.com/news/news/bimco-the-guidelines-on-cyber-security-onboard-ships`.

6.3.4.3 Attack scenario

In this section, a cyber attack scenario illustrating the usefulness of SECONDO platform in effective post-incident management is presented.

Malware infection -

Let us assume that the shipping company is under attack by a ransomware called CryptoMarine.

Its payload encrypted the files of all hard disks and the back-up files. Moreover, the collected data from the sensors about tank levels, nitrogen oxide concentration, temperature, and other on-board parameters [216] are encrypted. Without these values, it is extremly challenging to detect potential failures which could lead to catastrophic accidents. Further, the navigation system and telecommunications including network communications have collapsed, not permitting the vessel to successfully communicate with the onshore infrastructure of the company. As a result, this attack affects the shipping company in several different ways, since its property, crew, and reputation are jeopardized, and its share price is in a downward trend while the attackers demand ransom in crypto-currency to unlock the encrypted devices.

Company's response team - When an employee of the shipping company identifies the incident -the ransomware infection- and, according to the shipping company's *disaster recovery policy*, the responsible officers, e.g., the Cyber Security Operation Team, as well as the Insurance Company are contacted immediately. At the same time, the *business continuity plan* is activated. The Emergency Response Team is called to action, which then assembles: (i) a Disaster Recovery Team (DRT), which is responsible for key services restoration and business continuity; (ii) a Business Recovery Team (BRT) consisting of senior members of the main departments and the management team, who are responsible for the company's operation's prompt recovery; and (iii) a Media Team, to be in contact with the media.

Insurer's role - Besides, the insurer closely cooperating with the shipping company ensuring that immediate incident response actions are taken, the recovery plan has been initiated, and a dedicated team has been assign to assist the company with the cyber defense efforts. In parallel, Personal Relations assistance is also deployed to manage the communication with the shipping company's clients that have either been affected by the attack or information regarding them has been compromised in order to be compliant with regulations such as GDPR.

Response actions - According to the Insurance Company's approach, paying the ransomware is the last option, given that alternative approaches have been planned beforehand. DRT and BRT, in collaboration with insurer's experts will work on the systems' restoration and attempt to disinfect them. First, the existing recovery plan must be applied. Existing back-up countermeasures, adopted by the shipping company prior to the incident (suggested by SECONDO), will be implemented to countermeasure the impact.

Smart contract updates - Since there is an active incident, the insurance provider initiates an immediate forensic investigation. The results of the investigation are input to the SECONDO smart contract, which automatically initiates its process to assess the damage and decide which actions will be executed. The actions will be recommended by cross-evaluating the security practices and postures recorded by CRMM and the insurance policies.

6.4 Strengthening the Common Security and Defence Policy

In the continuous evolution of cybersecurity, the seamless integration of advanced cybersecurity applications within the framework of cyber insurance emerges as a strategic imperative to fortify the Common Security and Defence Policy (CSDP) of the European Union. In response to an increasingly complex threat landscape, the synergy between these two realms offers multifaceted advantages. Proactive cybersecurity measures incentivized by cyber insurance policies, encompassing robust firewalls, intrusion detection systems, and regular security audits, not only prevent cyber threats but also align with the CSDP's overarching goal of preemptively addressing security challenges. Furthermore, the incorporation of cybersecurity applications facilitates swift incident response and crisis management, enhancing the EU's ability to navigate and mitigate the impact of cyber incidents in line with the CSDP's mission of effective crisis management. The intersection of cybersecurity and cyber insurance also promotes data protection and privacy compliance, aligning with regulatory frameworks like the General Data Protection Regulation (GDPR) and reinforcing the CSDP's commitment to safeguarding the privacy of EU citizens. By leveraging threat intelligence

Authors	Title	Venue
Farao A, Panda S, Menesidou S. A, Veliou E, Episkopos N, Kalatzantonakis G, ... & Xenakis C	SECONDO: A platform for cybersecurity investments and cyber insurance decisions	TrustBus 2020, Springer $[Rank : B]$

Table 6.4: List of thesis' publications- Part F

and encouraging information sharing, cybersecurity applications contribute to collaborative defense mechanisms, fostering a collective approach in line with the CSDP's emphasis on collaboration and information exchange. Additionally, the integration of cybersecurity applications within cyber insurance frameworks supports capacity building and skill development, promoting a robust cybersecurity workforce to counter sophisticated threats—an integral aspect of the CSDP's capacity-building objectives. Moreover, the focus on resilience and redundancy planning, facilitated by cybersecurity measures, aligns seamlessly with the CSDP's mission of ensuring the resilience of EU member states in the face of diverse security challenges. By extending its influence on the global stage, the EU can shape international norms for cyber behavior through the alignment of cyber insurance requirements with globally accepted cybersecurity standards. In navigating the dynamic landscape of modern security threats, the incorporation of cybersecurity applications within cyber insurance not only ensures a proactive defense but also underscores the EU's commitment to comprehensive, collaborative, and internationally informed strategies, solidifying the CSDP's role as a bulwark against emerging cyber challenges.

Table 6.4 summarizes the scientific publication related to this chapter.

Chapter 7

INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain

Despite the rapid growth of the cyber insurance market in recent years, insurance companies in this area face several challenges, such as a lack of data, a shortage of automated tasks, increased fraudulent claims from legal policyholders, attackers masquerading as legal policyholders, and insurance companies becoming targets of cybersecurity attacks due to the abundance of data they store. On top of that, there is a lack of Know Your Customer procedures. To address these challenges, in this chapter, INCHAIN, an innovative architecture that utilizes Blockchain technology to provide data transparency and traceability. The backbone of the architecture is complemented by Smart Contracts, which automate cyber insurance processes, and Self-Sovereign Identity for robust identification. The effectiveness of INCHAIN's architecture is compared with the literature against the challenges the cyber insurance industry faces. In a nutshell, our approach presents a significant advancement in the field of cyber insurance, as it effectively combats the issue of fraudulent claims and ensures proper customer identification and authentication. Overall, this research demonstrates a novel and effective solution to the complex problem of managing cyber insurance, providing a solid foundation for future developments in the field. Table 7.1 summarizes the scientific publication related to this chapter.

Authors	Title	Venue
Farao A, Paparis G, Panda S, Panaousis E, Zarras A, Xenakis C	INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain	IJIS, Springer [IF : 3.2]

Table 7.1: List of thesis' publications- Part G

7.1 Introduction

The increasing shift towards the digital realm raises concerns about cybersecurity attacks, which can lead to substantial financial losses for corporations, amounting to millions or even hundreds of millions of dollars. However, the consequences of these attacks go beyond finances, posing risks to critical infrastructure, social cohesion, and mental health. Therefore, prioritizing effective cybersecurity measures is crucial to mitigate such risks. Recently, large-scale cybersecurity attacks rank third on the list of global threats [217]. Cyber insurance is the primary method for transferring insured financial risks and losses associated to networks and computers caused by cybersecurity incidents to a third party [187, 218]. As a product, cyber insurance can aid PHs, encompassing both organizations and individuals, in mitigating the risks associated with cybersecurity threats. Nonetheless, the market for cyber insurance is currently at a pivotal moment, with significant implications for both ICs and PHs.

ICs, on the one hand, are having trouble making a profit due to the growing number of claims and increasing expenses. First and foremost, this relates to the cyber insurance *Fraudulent Claims* and *Identity Theft* challenges. While the former occurs when dishonest PHs submit many claims for the same cybersecurity incident with several ICs, the latter happens when attackers masquerade as eligible PHs to submit false claims and steal the identity of others. Moreover, ICs have only a few years' worth of data to operate without having access to reliable data on their PHs' assets and security measures [219]. That rises from the *Lack of Data* (i.e., ICs do not have access to accurate data regarding PHs' assets, revenue amount, type of processed data, security controls, and frequency of cybersecurity incidents) and *Lack of*

Know Your Customer (i.e., ICs lack methods to gather PHs' accurate data and monitor their behavior) challenges. In addition, ICs become a natural target for cyber attacks as they possess substantial amounts of confidential PH data. That is directly related to the *Loss of Sensitive Data* challenge.

On the other hand, PHs have raised concerns not only from existing ICs but also from prominent ones. According to SOPHOS' 2022 report, 47% of the respondents noted that current policies are more complicated, which is attributed to the challenge of *Information Asymmetry* [220]. This occurs when there is an imbalance between two negotiating parties in their knowledge of relevant factors and details. Additionally, 37% of the respondents claimed that cyber insurance procedures take an extended period, which is linked to the *Lack of Automated Tasks* challenge. This happens because cyber insurance processes are often performed manually and are outdated, making them time-consuming.

The problems and challenges mentioned earlier have been encountered in numerous cybersecurity attacks. In 2017, Merck was hit by the NotPetya malware, resulting in a loss of more than $1.4B. Merck had $1.75B in property insurance and believed it would cover the costs caused by NotPetya. However, their IC rejected the claim because NotPetya was considered an act of war, and the insurance policy did not cover it [221, 222]. This indicates a misunderstanding regarding the coverage provided by the purchased insurance. Furthermore, LLOYD'S report presented the Shen attack scenario [223]. It is a hypothetical cyber attack on ports across the Asia Pacific, targeting the maritime supply chain, infecting 15 ports, and resulting in estimated losses of $110B. The report demonstrates that the global economy is unprepared for such an attack, with 92% of the total economic costs being uninsured.

Based on the above statements and established facts, our research aims to address the following questions:

RQ1: *Which are the main insurability challenges?*

RQ2: *Which are the primary stakeholders and processes of cyber insurance, and how do they interact to accomplish the goal of cyber insurance?*

RQ3: *How does the literature address existing cyber insurance challenges with Blockchain and Smart Contracts?*

In general, a thriving cyber insurance market should benefit all parties

involved. Consequently, as the market for cyber insurance becomes increasingly complex, it becomes imperative to revise and adapt cyber insurance products to meet evolving demands and ensure that all stakeholders reap maximum benefits [224]. Rather than treating cyber insurance as a mere commodity in a soft market, it should be viewed as a means of protecting the balance sheet. In this respect, cyber insurance should be regarded as the last resort to mitigate losses in the event of a catastrophic cybersecurity incident.

Now, we will summarize the challenges in cyber insurance and introduce our innovative architecture, `INCHAIN`, which addresses these issues and ensures security, fairness, trust, and interoperability among all participating entities. Our work is built on well-established technologies that are assembled into a novel architecture. The backbone of our proposed architecture is Blockchain, providing data transparency, traceability, and fostering applications for the evolution of cyber insurance. `INCHAIN` includes two applications: *Smart Contracts* and *SSI*. Smart Contracts equip `INCHAIN` with automated tasks and requirements that bind participating entities, while SSI enables data minimization, robust identification, data interoperability, portability, controllability, decentralization, and transaction transparency. Our proposed architecture provides a viable solution to the rigid cyber insurance ecosystem by proving the benefits and demonstrating how it can address these challenges.

The remainder is structured as follows. Section 7.2 presents related work, summarizes cyber insurance challenges, and analyzes candidate technologies used in the proposed architecture. Section 7.3 elaborates on cyber insurance stakeholders, applied processes, and the proposed `INCHAIN` architecture, including involved operations. Next, Section 7.4 examines how `INCHAIN` meets cyber insurance processes, holistically addresses identified challenges, and compares `INCHAIN` with other works. Section 7.5 discusses the limitations of this paper and proposes directions for future work. Finally, Section 7.6 concludes the paper.

Table 7.2: Table of acronyms

Acronym	Definition
CIB	Cyber Insurance Broker
DID	Decentralized Identifier
IC	Insurance Company
NCSA	National Cyber Security Authority
PH	Policyholder
PHI	Protected Health Information
PII	Personal Identifiable Information
SSI	Self-Sovereign Identity
VC	Verifiable Credential

7.2 Background

7.2.1 Acronyms

This paper employs several acronyms to refer to specific terms and concepts. We have included a table of acronyms to ensure clarity and avoid confusion. Table 7.2 offers a comprehensive list of all the acronyms used, along with their corresponding definitions. We encourage readers to consult this table whenever encountering an unfamiliar acronym in the text, as it will provide a quick reference to its meaning. By using acronyms judiciously and including a table for easy reference, we aim to make our paper more accessible and comprehensible to readers while maintaining the requisite technical terminology for our research.

7.2.2 Related Works

Franco et al. [225] introduced `SaCI`, a Blockchain-based approach that enhances trust and automation in the interaction between the PH and its IC. Their approach utilizes Smart Contracts to handle multiple aspects of the cyber insurance process. These contracts facilitate premium payments, contract updates, damage coverage requests, dispute resolutions, and contract information and integrity verification. The authors evaluated the effectiveness of `SaCI` through a proof of concept in dispute cases. `SaCI` is implemented on the Ethereum network, where each Smart Contract function incurs a gas fee.

To further support this endeavor, Lepoint et al. [226] proposed `BlockCIS`, a dynamic cyber insurance system that collects data on the PH's information technology and computer infrastructure. This data is used for tailored risk assessment and attack surface identification. Third parties and auditors can access the collected data for analyses and actions. `BlockCIS` is developed on top of the Hyperledger Fabric, eliminating fees for executing Smart Contract functions.

Vakilinia et al. [227] presented a Blockchain-based cyber insurance crowdfunding framework on the Ethereum network. This framework involves four participants: Vendor, Customer, Auditor, and Insurance Company. The insurance process begins with the vendor requesting insurance services. Interested insurers then participate in a sealed-bid auction, submitting their preferred premium for the insurance service. The auction winners are selected to provide insurance coverage. In case of an indemnity request, an auditor verifies its validity. The authors implemented the proposed system on the Ethereum Blockchain, resulting in gas fees. The developed Smart Contract handles crowdfunding initialization, bidding, wrapping, and reimbursement.

Xu et al. [197] enhanced the time efficiency of crowd-sourcing tasks in Blockchain applications. The proposed framework reveals its robustness through three different time-relative tasks: (*i*) time-sensitive, (*ii*) slightly time-sensitive, and (*iii*) time-insensitive. Automation of tasks in reimbursement issues is achieved within this framework. The authors developed the framework on the Ethereum network, where each Smart Contract function incurs a gas fee. The Smart Contract handles various actions, including bidding, cyber insurance creation, and reimbursement.

The `SECONDO` project [8] introduces a dedicated platform for the assessment and effective management of cyber risks, adopting a quantitative approach that considers both technical and non-technical parameters, such as user behavior, which influence cyber exposure. It aims to address information asymmetry between the insured and the insurer while providing analysis for efficient risk management by recommending optimal investments in cybersecurity controls [7]. The project determines residual risks, estimates cyber insurance premiums based on the IC's business strategy, and eliminates information asymmetry between the PH and the IC [3]. To securely store data on the effectiveness of implemented cybersecurity controls, `SECONDO` integrates the Blockchain technology and utilizes Smart Contracts embedded in the distributed ledger. These Smart Contracts automate agreement processing, notify the ICs and PHs when an agreement is bound, and facilitate premium

and commission payments.

Blockchain has been employed in various insurance-related business cases. Loukil et al. [228] proposed CioSy, a collaborative blockchain-based insurance system that monitors and processes insurance transactions. It utilizes smart contracts for claims handling, payments, and validation, and is built on top of the Ethereum, resulting in gas fees for its operations. Kumar et al. [229] presented FLAME, a trusted fire brigade service and insurance claim framework that utilizes blockchain to offer immediate fire brigade services and prevent insurance fraud. The authors provided the architecture and functionality of FLAME, where smart contracts automate the processes related to fire brigade services and insurance claims. The prototype has been implemented on the Hyperledger Besu Blockchain, using the Istanbul Byzantine Fault Tolerance 2.0 consensus protocol.

Yadav et al. [230] proposed a blockchain framework for vehicle insurance to streamline the reporting of accidents and filing of insurance claims. The framework is developed on top of the Hyperledger Fabric to store information about vehicles, owners, and insurance. Efficient querying of this blockchain requires specific participants, assets, and transactions. The consensus algorithm identifies invalid claims if a transaction request contains an error. Karmakar et al. [231] proposed ChainSure, an Ethereum blockchain-based framework empowered with TOPSIS and smart contracts, which provides an automated, tamper-proof, transparent, and scalable system fulfilling the major functional blocks in a medical insurance environment. ChainSure using the TOPSIS method allows users to find an insurance policy that best suits their needs. ChainSure has also gas fees.

7.2.3 Candidate Technologies

At this point, we present the technological pillars of the proposed cyber insurance architecture. These jointly provide a robust solution for the cyber insurance ecosystem and analyze why the proposed architecture integrates them. Also, the proposed architecture has been designed on the grounds of well-established technologies (i.e., Blockchain, Smart Contracts, and SSI) with proven security properties.

7.2.3.1 Blockchain

Blockchain lies in the concept of distributed ledgers that assist in making a log of any asset's history that cannot be altered and is transparent for all involved entities to check [232]. Blockchain is the crux of the proposed architecture, not as a stakeholder but as a network. It will not only enable trust, security, transparency, and the traceability of data shared across a business network, but it will also create a fertile surface for applications that will support the cyber insurance processes. The proposed cyber insurance architecture takes advantage of the following Blockchain features [233]: (*i*) immutability, (*ii*) distribution, (*iii*) decentralization, (*iv*) secure records, (*v*) consensus, and (*vi*) unanimity.

7.2.3.2 Smart Contracts

A Smart Contract is a contract between two or more Blockchain nodes [234]. They are programs stored within a Blockchain that respond to certain events encoded within the contract. In essence, they are responsible for automating the execution of an agreement so that its participants remain assured of the outcome without any intermediary's intervention. Smart Contracts follow the ``if/when ... then ...'' statements and can automate a workflow by triggering an upcoming action when predetermined conditions are met. When these conditions are met and verified, the Blockchain nodes execute the actions and update the Blockchain. Therefore, the transaction is immutable. Thus, only nodes with the right permissions can see the results. The proposed cyber insurance architecture takes advantage of the following Smart Contracts features [235]: (*i*) agreement, (*ii*) speed, (*iii*) automation, (*iv*) security, and (*v*) records management.

7.2.3.3 Self-Sovereign Identity

Self-Sovereign Identity [236, 237], also known as SSI, is a decentralised identity management system. It allows individuals or organizations to own and manage their digital identities. In addition, SSI facilitates the practice of selective attribute disclosure as a means of reducing the disclosure of personal data. Furthermore, it offers privacy-preserving characteristics such as *anonymity* and *unlinkability*. With SSI, no central authority maintains possession of users' data, eliminating the need to pass it on to others upon

request. The user carries its data, and due to the underlying cryptography and distributed ledger technology, it can make claims about its identity, which others can verify with cryptographic certainty.

By utilizing SSI, cyber insurance stakeholders can exchange verifiable data in an automated and privacy-preserving manner. This approach helps prevent the leakage of private information and saves time by eliminating the need for manual data verification processes. At the heart of SSI lie the Verifiable Credentials (VCs). W3C published a formal recommendation of VCs and defined them as tamper-evident credentials with authorship that can be cryptographically verified [238]. VCs are interoperable and support selective disclosure of its user's information. In general, the engaged participants in SSI are an issuer, a user (the one who owns the VCs), and a verifier. The SSI is comprised of two basic functionalities: (*i*) *VC Issuance* and (*ii*) *VC Verification*.

The first functionality is the VC Issuance, where the user (acting as the holder) acquires a VC from the issuer. VC consists of tamper-evident claims and metadata that cryptographically prove its issuer [238]. Claims represent a holder's statements (e.g., the number of past data breaches). Each VC is issued on its holder's and issuer's Decentralized Identifiers (DIDs) and has the role of a public key. A DID is a globally unique persistent identifier that consists of a string of letters and numbers and is directly correlated with a pair of public and secret keys. The private key allows the user to access and manage its data. The user should be the only one who knows the private key, which should never be shared with anyone else. Regarding DIDs, the private key allows users to prove ownership and grant permission to share specific data. On the other side, Blockchain stores the public key associated with the DID of the VC's issuer public key and is safely shared with anyone to send and receive data. A digital identity wallet securely stores the issued VCs [239]; it is the place (e.g., a mobile app) where holders keep their VCs [1]. These cannot be hosted only within smartphones; some implementations support their host within trusted computers [9, 79, 240].

The second functionality is the VC Verification, in which the user (acting as the prover) must demonstrate possession of accurate attributes to the verifier without necessarily revealing the values contained within them. This is accomplished using zero-knowledge proofs and establishing that the corresponding user is, in fact, in control of the presented identity. To verify the authenticity of the VC, the verifier shall check the Blockchain to see its issuer (i.e., DID of the VC's issuer) without having to contact the issuer. When

presenting a VC, the user can select which claims to disclose and which to conceal. In addition, SSI achieves unlinkability as the user employs a distinct DID for each presentation.

SSI is built on top of Blockchain and equips the proposed cyber insurance ecosystem with trust among the participants, instant exchanged data verification, robust identification, data minimization, interoperability, portability, controllability, decentralization, and transaction transparency. The proposed cyber insurance architecture integrates the SSI due to its following features [236]: (*i*) less personal data management, (*ii*) transparency, (*iii*) interoperability, (*iv*) decentralized identity management, and (*v*) instant verification.

In this work, we introduce our innovative architecture, `INCHAIN`, which addresses these issues and ensures security, fairness, trust, and interoperability among all participating entities. Our work is built on well-established technologies that are assembled into a novel architecture. The backbone of our proposed architecture is Blockchain, providing data transparency, traceability, and fostering applications for the evolution of cyber insurance. `INCHAIN` includes two applications: *Smart Contracts* and *SSI*. Smart Contracts equip `INCHAIN` with automated tasks and requirements that bind participating entities, while SSI enables data minimization, robust identification, data interoperability, portability, controllability, decentralization, and transaction transparency. Our proposed architecture provides a viable solution to the rigid cyber insurance ecosystem by proving the benefits and demonstrating how it can address these challenges.

7.3 The Cyber Insurance Concept

This section outlines the fundamental stakeholders and processes that constitute the existing cyber insurance ecosystem while analyzing the participants and operations of the proposed architecture, called `INCHAIN`, designed to tackle cyber insurance challenges.

7.3.1 Definition, Stakeholders, and Processes

Here, we address the third research question (*RQ3 – Which are the basic stakeholders, processes of cyber insurance, and how do they interact to accomplish the goal of cyber insurance?*). The essential stakeholders in cyber

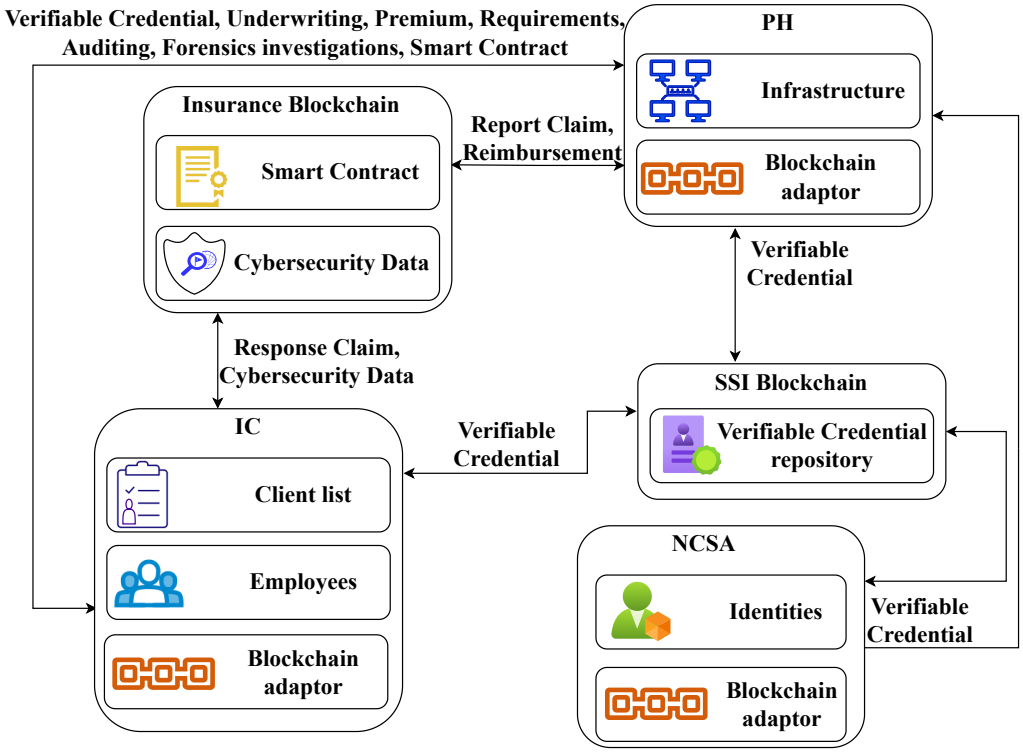


Figure 7.1: `INCHAIN` architecture

insurance are further elaborated below [241, 188, 242]. In a nutshell, a PH is a holder of cyber insurance and a customer to an IC. The latter is a stakeholder responsible for selling cyber insurance policies to potential PHs, investigating a cybersecurity incident, and auditing whether the PHs comply with the cyber insurance policies and have implemented the indicated cybersecurity countermeasures [191]. Additionally, Cyber Insurance Brokers (CIBs) performi market research and bring the most suitable contracts to their PHs. We analyze the identified cyber insurance processes below:

CIP1 – Market Research: A CIB aims to find advantageous cyber insurance contracts for its PHs [242]. The latter knows its cybersecurity exposure and has already identified the cybersecurity risks; technical measurements will address some of them [243, 7, 79] and cyber insurance contracts will cover them in a cybersecurity incident. During this phase, the CIB thoroughly explains the available cyber insurance policies to its PHs, analyzing

its definitions, liabilities, coverages, and exclusions. The latter is written in a boilerplate language and comes with many disadvantages, including but not limited to a misunderstanding about what is insured, what perils and risks are covered, and how losses are assessed [244, 3, 245]. This process is performed between a CIB and a potential PH. The *Market Research* process is performed between a CIB and a PH, and it is directly related to the *Information Asymmetry* (*CH7*) since a PH has to understand what each cyber insurance contract can offer to meet PH's requirements. However, in this process the IC is not involved and the candidate technologies (see Section 7.2.3) cannot address it. Thus, its optimization is outside the scope of this work.

CIP2 – Client Registration and Validation: On the one hand, the potential PH gathers the required documents to register and apply for a cyber insurance contract with its IC. These include but are not limited to identification documents, IT security certifications, and any other compliance documents [246, 247]. On the other hand, the IC verifies the validity of the applied documents [8, 247]. It also verifies their accuracy. Once the validation is complete, the PH can carry on safely, knowing that it is fully insured. This process is performed between an IC and a potential PH. It is well known that processes responsible for validating and registering a PH lack unmanned actions (`CH2`). Currently, the existing actions are time-consuming and require human labor. Dishonest PHs also deceive ICs by submitting outdated documentation (`CH6`) regarding their status (e.g., updated security controls). Finally, ICs store data related to PHs becoming vulnerable to cybersecurity attacks (e.g., data breaches) and being at risk of losing personal data (`CH5`).

CIP3 – Underwriting: It is the most crucial process for the IC and is based on assessing the cybersecurity risk of the PH [188, 248]. First, the IC identifies the main parameters of risk considering valuable assets, possible threats, and existing vulnerabilities of the PH. Then, the IC determines an incident's likelihood and possible impact, considering the combined probability of events happening. A blend of self-assessment questionnaires, checklists, business documentation, meetings, as well as interviews perform this assessment [7, 249, 250, 251]. Their main goal is to pinpoint the installed software and deployed security measures, and verify the existence of sensitive data and how it is accumulated and handled. It undoubtedly aims to detect any other information that can affect the global security posture of the firm under investigation [252]. A deeper analysis can be carried out by installing moni-

toring software that produces security logs and telemetry devices. The results of this process contain analysis and advice of the PH, emphasizing deficiencies and precautions to comply with the well-known and top-notch security practices [253]. Also, the IC may suggest and demand the implementation of security countermeasures [6], which will affect the premiums [254, 255, 256]. This process is performed between an IC and a potential PH. The weakness of this process is the lack of automated tasks (CH2) to validate if PHs have fulfilled the IC's requirements and propositions (CH6). Currently, the compliance of PHs with IC's requirements is validated through questionnaires and audits. PHs can exploit that backdoor by submitting inaccurate data (CH7).

CIP4 – Pricing Premium: An IC is in charge of calculating the price of the PH's premium using existing econometric and statistical models [207, 248, 204]. This process is performed between an IC and a potential PH. It is observed that the lack of historical cybersecurity data is of utmost importance [207]. Data can influence the premium calculation with parameters that may be a barometer for the final price; however, lack of data leads to unfair premiums (CH1). This process is outside the scope of this work. Thus, we do not design and deliver an algorithm to optimize this process.

CIP5 – Periodic Risk Assessment: Risk assessment is highly recommended and conducted by the IC during a cyber insurance lifetime [188]. It allows ICs and PHs to collect updated information about new threats, vulnerabilities, and evolving cyber risks. Overall, it is required to perform a continuous risk assessment to reduce the amount of PHs' impassable information, with the ultimate goal being to mitigate unfair behaviors such as negligence and fraud. An IC and a PH perform this process. Until now, this process has been mainly conducted through questionnaires. Thus, the absence of automated methods (CH2) to collect accurate cybersecurity data makes this process vulnerable to cybersecurity attacks performed by legal PHs that aim to fool it by answering spuriously in questionnaires (CH6). As a result, IC has an inaccurate view of PHs' cybersecurity exposure (CH7).

CIP6 – Claims Submission: As soon as a PH realizes a cybersecurity incident occurrence, it informs its IC to request reimbursement [248]. This step aims to get a refund to cover damages from the cybersecurity incident. Generally speaking, cyber insurance protects a PH through three distinct insuring agreements: (*i*) *Network Security and Privacy Liability*, (*ii*) *Media Liability*, and (*iii*) *Errors and Omissions* [257]. The PH has to fill out documents describing the cybersecurity incident in detail, including but

not limited to information related to the location, hour, infected systems, networks, software, damaged hardware, downtime of systems, the type of compromised data (personal or not), as well as the estimation of potential economic losses [258]. This process is performed by a PH. Currently, the claim submission process is time-consuming and requires human labor (e.g., sending documents through email and filling out questionnaires). When this procedure is done, a significant amount of time will have been wasted in addressing the problem on the PH's side. Automated claim submission processes can solve this issue. Also, the lack of a robust identification system within the cyber insurance ecosystem leads ICs to face dishonest PHs that seek reimbursement without any incident and malevolent actors that masquerade as eligible PHs to steal their reimbursement (`CH2`, `CH3`, and `CH4`).

CIP7 – Claims Validation and Auditing: IT security experts from the IC start verifying the claim's submission and performing a forensic investigation [248, 259, 260]. Notably, most policies in a cyber insurance contract cover the cost of incident response and forensic investigations, including identifying stolen or compromised data and the extent to which third parties have to be informed according to the current regulations. Audits performed by the IC aim at revealing a PH's fraudulent claim or a PH that does not follow the reported security procedures. In this case the IC can refuse to indemnify the PH [191]. This process is performed between an IC and a PH, and requires human involvement. Validation and auditing are time-consuming due to a lack of automated methods for gathering accurate and real-time cybersecurity data (`CH2` and `CH6`). Audits last for an extended time. Hence, until its completion, the victim (PH) may have already lost money and reputation. In certain cases, the responsibility for incident response does not lie with the IC, but rather, the PH opts to engage an external firm to detect, mitigate, and recover from the cybersecurity incident. This proactive measure aims to minimize the impact and losses resulting from such incidents. The expenses incurred for incident response services provided by external firms are referred to as *transaction costs* and are ultimately covered by the PH [261].

CIP8 – Claims Payment: It is the final stage of the cyber insurance life cycle, and reimburses the PH due to the cybersecurity incident [262]. The refund reimburses the PH's business not only due to interruption caused by a cybersecurity incident but also due to loss of reputation whenever the cyber incident is publicly disclosed [263]. This process is performed between an IC and a PH. It is well-known that the lack of automated payments transforms

Table 7.3: Correlation between cyber insurance challenges and processes

Challenges	**Processes**							
	CIP1	**CIP2**	**CIP3**	**CIP4**	**CIP5**	**CIP6**	**CIP7**	**CIP8**
CH1 - Lack of Data	×	×	×	✓	×	×	×	×
CH2 - Lack of Automated Tasks	×	✓	✓	×	✓	✓	✓	✓
CH3 - Fraudulent Claims	×	×	×	×	×	✓	×	×
CH4 - Identity Theft	×	×	×	×	×	✓	×	×
CH5 - Loss of Sensitive Data	×	✓	×	×	×	×	×	×
CH6 - Know Your Customer	×	✓	✓	×	✓	×	✓	×
CH7 - Information Asymmetry	✓	×	✓	×	✓	×	×	×

this process into a stiff one (CH2).

In summary, based on the analysis above, the following observations are raised. First and foremost, the *Market Research* process is influenced only by *CH7* challenge. The process named *Client Registration and Validation* is affected by the CH2, CH5, and CH6 challenges. Next, the *Underwriting* process is influenced by the CH2, CH6, and CH7 challenges. Moreover, the *Pricing Premium* process is affected by the CH1 challenge. Furthermore, the *Periodic Risk Assessment* process is afflicted by CH2, CH6, and CH7 challenges. The *Claims Submission* process is affected by the CH2, CH3, and CH4 challenges. The *Claims Validation and Auditing* process is directly related to CH2 and CH6 challenges. Finally, the *Claims Payment* process is influenced by CH2 challenge. Table 7.3 depicts the aforementioned observations.

7.3.2 INCHAIN

We introduce here the cyber insurance architecture of INCHAIN, including the operational layer of every participant (see Figure 7.1). The engaged participants are analyzed in detail:

NCSA: This entity is newly introduced as a pillar of the proposed cyber insurance architecture. It constitutes an SSI issuer, allowing potential PHs to issue VCs (see Section 7.2.3.3) from their verified identity attributes and then use them to access cyber insurance services. A National Cyber Security Authority (NCSA) coordinates activities with all ministries, government agencies, and bodies, ensuring interoperability at all levels and and has the ability to issue VCs with accurate data for each possible PHs. Furthermore, it has a Blockchain adaptor to upload the issued VCs to the Blockchain. NCSA communicates only with potential PHs and the SSI Blockchain network. In

addition, NCSA maintains all data pertaining to recent cybersecurity events with PHs, which is mandadory for generating accurate VCs. In essence, adding a new entity responsible for issuing VCs is inevitable; none of the existing stakeholders is confident enough to issue VCs with accurate claims, in contrast to NCSA, which accomplishes this with high confidence.

PH: Apart from the characteristics reported in Section 7.3.1, the PHs of `INCHAIN` is equipped with the following capabilities. The PH makes a request to the NCSA to issue VCs based on its attributes. Hereafter, the PH submits the VCs to the IC to purchase cyber insurance to safeguard its infrastructure that satisfies IC's criteria. Moreover, it is geared with a Blockchain adaptor to create a Smart Contract together with the IC—describing in a digital format the agreed cyber insurance contract—as well as to report a cybersecurity incident.

IC: Apart from the characteristics defined in Section 7.3.1, the IC of `INCHAIN` is also equipped with the following attributes. The IC is a VC verifier verifying the received credential of a potential PHs, checking the latter's eligibility to use the service (cyber insurance). Furthermore, it is equipped with a Blockchain adaptor to create Smart Contracts together with PHs to handle cybersecurity claims and store cybersecurity data to monitor its behavior via the Smart Contract.

SSI Blockchain: This Blockchain network belongs to the NCSA. It is responsible for storing VCs and performing operations related to their issuance and verification (see Section 7.2.3.3).

Insurance Blockchain: This Blockchain consists of pre-selected ICs, which are responsible for validating transactions and have banded together to share information to improve existing workflows, transparency, and accountability. It is responsible for storing Smart Contracts and processing claims.

`INCHAIN` allows a PH to completely control its cyber insurance contract. The basic scenario of `INCHAIN` unfolds as follows. A possible PHs is a legitimate business and is exposed to cybersecurity threats. At some point, the PH aims to buy a cyber insurance contract from its desirable IC. The latter has specific requirements to sell its cyber insurance contracts. Thus, based on them, IC will calculate the premium of PH's cyber insurance contract and perform a continuous risk assessment to prevent naive behaviors and fraud. The requirements are the following:

1. ***Business Information:*** It includes information related to the legal business name, its principal address, business nature (e.g., SME), number of employees, and annual audited revenue.

2. ***Type of Collected Data***: It includes information related to the type of data that the business processes and stores (e.g., Personal Identifiable Information (PII), Protected Health Information (PHI), intellectual property).

3. ***Security Controls***: These include information related to compliance with cybersecurity certifications (e.g., ISO27001, GDPR), utilization of *Payment Card Industry Data Security Standards*, and integration of cybersecurity controls (e.g., IDS, firewall, IPS).

4. ***Information Loss***: It includes the number of past data breaches (e.g., the PH has totally faced seven data breaches).

`INCHAIN` is an architecture that benefits both ICs and PHs. A notable advantage of `INCHAIN` is the automated verification process of attributes and claims handling for the cyber insurance ecosystem. In essence, PHs get reimbursed immediately since the Smart Contracts transfer money from one account to another without the involvement of third parties. Therefore, the PHs can immediately focus on recovering from the incident. Finally, Smart Contracts are also responsible for monitoring PHs' behavior (e.g., contract violation) via the collection of cybersecurity data (e.g., audits).

7.3.3 INCHAIN Operations

`INCHAIN` consists of the following individual operations: (*i*) *Verifiable Credential Issuance*, (*ii*) *Verifiable Credential Verification and Cyber Insurance Issuance*, and (*iii*) *Cybersecurity Incident Report and Reimbursement*. The `INCHAIN` architecture does not include actions involving the selection of a cyber insurance contract between a potential PH and CIB and the premium pricing. These operations are inextricably linked in the cyber insurance backbone; however, they are outside the scope of this work. Below, each `INCHAIN` operation is examined together with its purpose, its relationship to existing cyber insurance processes (see Section 7.3.1), and how it addresses specific cyber insurance challenges (see Section 6.2). The `INCHAIN` operations are analyzed based on IC's requirements for selling cyber insurance contracts and a PH's attributes; Table 7.4 represents both of them.

Table 7.4: Cyber insurance contract requirements and claims

Attribute	PH (Attribute)	IC (Requirements)
Business Information		
Name	INCHAIN Tech	Official Name
Address	Milky Way 21	Existing Address
Business Nature	Information Technology	ALL types
Number of Employees	50	<50, 50-100, 100+
Annual Audited Revenue	210K €	<250K, 240K-500K, 500K+
Type of Collected Cata		
Type of Stored Data	PII	ALL
Type of Processed Data	PII	ALL
Security Controls		
Certifications Compliance	ISO27001, GDPR	At least one
Security Controls	IDS, firewall, backup	Last update < today
Information Loss		
Number of Past Data Breaches	7	<10
Total Fines	7K €	<1M €

7.3.3.1 Verifiable Credential Issuance

As its name implies, this operation is responsible for issuing VCs to a PH based on its verified attributes. It is executed between a PH and a NCSA. It aims to create a robust identification method for supplying the IC with the PH's accurate data. In particular, this operation enriches the traditional cyber insurance process entitled *Client Registration and Validation* with automated mechanisms. These are responsible for equipping PHs with verified data by NCSA that do not demand human intervention for their validation by ICs.

For the credential issuance (see `Steps 1 - 7` depicted in Figure 7.2), let us assume that the potential PH uses a secure identity wallet on its trusted device (see Section 7.2.3.3). At the beginning of the VC issuance procedure, PH generates a public/private key pair, stores the private key within its trusted device, and publishes the public key to the Blockchain, generating and storing its DID for the public key in its data store (`Step 1`). Then, the PH navigates to the NCSA website and requests from it to issue the VCs (`Steps 2 - 3`). PH requests the issuance of the following four VCs:

- ***Business-Information-VC*** that includes PH's official name, address, business nature, number of employees, and its latest annual audited revenue, along with their legitimacy proofs.

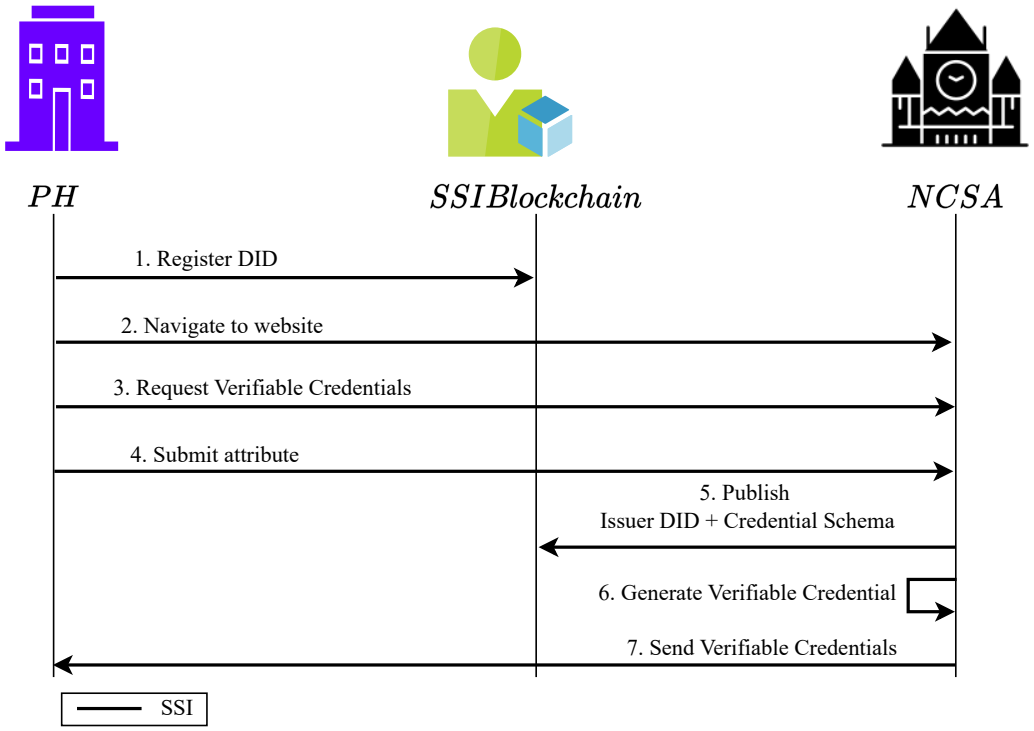


Figure 7.2: INCHAIN Verifiable Credentials issuance

- ***Type-of-Collected-Data-VC***, which proves that the PH stores and processes only PII data.
- ***Security-Controls-VC***, which proves that the PH complies with ISO27001 and GDPR, and has installed all required security controls (i.e., IDS, firewall, backup policy routine).
- ***Information-Loss-VC*** that proves the PH has already been a victim of a cybersecurity attack at least seven times, and its total fine is 7K €.

The aforementioned four `INCHAIN`'s VCs follow a specific format and include the subsequent attributes:

➢ ***ID*** that is a unique verifiable identifier characterizing the credential (e.g., *https://ncsa.gr/credentials/1872*).

➢ ***Credential Type*** that represents that the current credential is a verifiable one (e.g., *Business-Information-VC*).

➢ ***Issuer*** that represents the issuer who issued it (e.g., NCSA). It is a type of PH that explains PH's status, whether it is an individual or an enterprise (e.g., *Large Enterprise, SME*).

➢ ***Issuance Date*** that represents the VC's issuance date (e.g., `2022 - 31 - 12T00: 00:00Z`).

➢ ***Lifetime*** that represents VC's expiration date (e.g., `2023 - 31 - 12T00: 00:00Z`).

➢ ***Proof*** that represents the public key signatures of the PH's and NCSA's DID. This information will be used later by the IC to verify the authenticity of the identity and claim by verifying the PH and NCSA's DID signatures (contained in the claim) against the verifiable data registry. The Proof contains the following fields:

- ***Type:*** The specific type of the proof's signature (e.g., Ed25 519 Signature 2020)
- ***Created Date:*** The day of the proof's creation (e.g., `2022 - 31 - 12 T00: 00: 00Z`)
- ***Verification Method:*** The method that should be used for verification by the verifier (e.g., *selective disclosure*)
- ***Proof Purpose:*** The purpose for the proof (e.g., *assertionMethod*)
- ***Proof Value:*** The value of the specific proof (e.g., *z58D AdFf a9Sk qZMU J*)

➢ ***Claim*** that includes identity attributes for the PH (e.g., number of past data breaches). The Claim includes the following fields:

- ***Identifier:*** The unique attribute identifier of the VC: (e.g., did: ebfe b1f7 12eb c6f1 c276 e12e c21)
- ***Attribute:*** The owner's identity attribute (e.g., number of past data breaches: 7)

NCSA, as part of the public sector, collects the verified data from other ministries, government agencies, and bodies and issues the *Business - Information - VC* and the *Information-Loss-VC*. However, for issuing the *Type-of-Collected-Data-VC* and *Security-Controls-VC* the PH submits its attributes to the NCSA for verification (`Step 4`). The submitted attributes are certifications proving that the PH complies with the `ISO27001` and `GDPR` and the latest security update occurrence issued by known organizations (e.g., the service provider). Upon successful verification, the NCSA publishes its DID and the credential schemas[1] of VCs to the SSI Blockchain and then issues VCs that are signed by its DID (`Steps 5 - 6`). Ultimately, NCSA sends the generated VCs to the potential PH. The latter stores them within its secure digital identity wallet and fully controls them (`Step 7`).

It is observable that this operation addresses the challenges `CH2` and `CH6`. SSI facilitates the *Know Your Customer* operations. Its usual responsibilities are performed automatically when a PH uses a SSI login (e.g., digital evidence of identification or other attributes are sought and delivered as part of the login process). Therefore, telephone verification and the provision of scanned papers are rarely required. Overall the multiple-step and time-consuming *Know Your Customer* processes are replaced with a SSI single, seconds-long procedure, which benefits both the IC and the PH.

7.3.3.2 Verifiable credential verification and cyber insurance issuance

In this operation, the PH presents its VCs to the IC, and if the verification is successful, the PH can start using the cyber insurance services provided by the IC. A Smart Contract is used to translate the classic cyber insurance contract into a digital format, which binds the PH and the IC under specific requirements. This operation affects the traditional cyber insurance processes entitled `CIP2` and `CIP3`. On the one hand, the `CIP2` process on the IC side becomes fully automated due to the utilization of SSI and VCs. Hence, the PH will submit to IC only verified attributes minimizing the time needed for their verification since these will come from trusted entities (e.g., NCSA) and encapsulated within VCs. On the other hand, the `CIP3` process is strengthened by using VCs, as the IC's underwriters can gather verified

[1]The Credential Schema is a document that is used to guarantee the structure, and by extension the semantics, of the set of claims comprising a VC. A shared Credential Schema allows all parties to reference data in a known way [264].

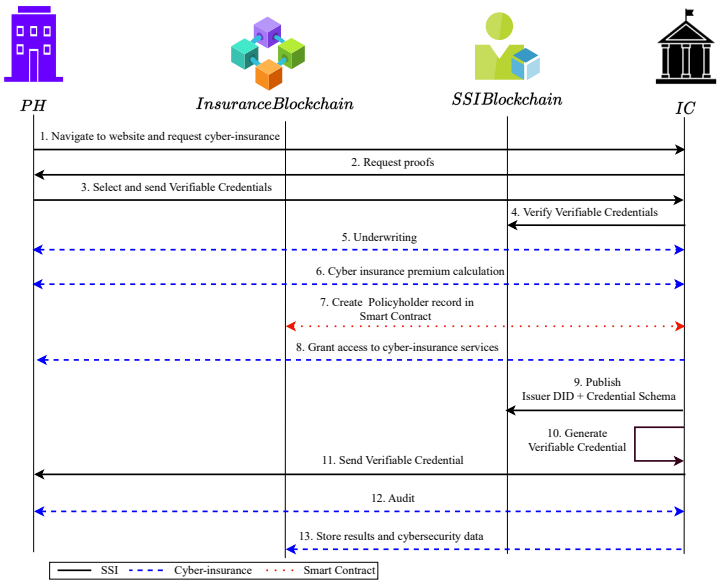


Figure 7.3: Verifiable Credential verification and Cyber-insurance issuance

information about the PH's cybersecurity awareness, behavior (e.g., number of past data breaches), and infrastructure. This leads to the identification of new cybersecurity risks that may not have been previously considered and could potentially affect the PH.

When the potential PH aims to buy a cyber insurance contract from a specific IC, it has to provide the VCs to the latter for validation (see `Steps 1 - 13` depicted in Figure 7.3). To initiate the operation, the potential PH interacts with its chosen IC by visiting the latter's website and requesting to buy cyber insurance (`Step 1`). The latter requests proofs (`Step 2`) based on specific requirements (see Table 7.4) from the potential PH proving that: (*i*) PH is a legitimate business, (*ii*) PH processes and stores data, (*iii*) PH complies with cybersecurity certificates and standards, (*iv*) PH has updated cybersecurity controls, (*v*) PH's total past data breaches are less than or equal to 7, and (*vi*) PH's total fine is less than 1M €.

Next, the PH selects and sends the whole claim or only a subset of it, ensuring minimal disclosure of data (`Step 3`). The proving function requires the participating entities to agree on which attributes will be disclosed (e.g., number of past data breaches) and which attributes will be partially revealed (selective disclosure) [265]. For more information see Table 7.4. For

instance, apart from its annual audited revenue, the PH reveals the general information related to its business, the type of data stored and processed, and the information related to its implemented security controls. Regarding the annual audited revenues, the VC, instead of revealing the accurate value, responds with a `YES` as a positive answer, proving the PH's latest annual audited revenue is less than 250K €. Moreover, the PH hides information related to the number of past data breaches and the total fines; the VC, instead of revealing the accurate number of data breaches, responds with a `YES` as a positive answer, proving that the PH meets the requirement of having fewer than 10 data breaches and that its fine is less than 1M €. Based on the submitted VCs of the PH, the IC can verify that the PH conforms to its policies regarding the purchase of cyber insurance; the IC validates the authenticity of the received VC by verifying the signatures of the PH's and NCSA's DID stored within the SSI Blockchain (`Step 4`).

Upon the successful verification, the IC, together with the PH, starts the processes related to underwriting and pricing the premium (`Steps 5 { 6`); the results of the previous actions lead to the cyber insurance contract agreement. Assuming that the cyber insurance premium is equal to 1080 €, the limit of liability[2] is at 591K € and the deductible[3] is 4K €. The cyber insurance purchased by the PH covers the incidents summarized in Table 7.5. In particular, PH is covered against business email compromise, lost device, malware/virus, phishing attacks, and ransomware cybersecurity attacks, with maximum reimbursement at 123K €, 57K €, 160K €, 72K €, and 179K € correspondingly (see Table 7.5). Then it is translated into a digital format as a Smart Contract binding them with specific requirements. Apart from the reimbursement information, the cyber insurance contract includes obligations that should be met by the PH (e.g., penetration tests every three months, daily vulnerability scanning and patching, and finally, two security awareness campaigns for its employees in a year). Moreover, the Smart Contract checks if the PH is consistent with its obligations during the coverage period. If the obligations above are not met by the PH, then the Smart Contract will be terminated, and in case of an incident, the PH will receive no reimbursement.

A record within the `INCHAIN` Smart Contract will include the following attributes:

[2]The limit of liability determines the maximum amount of money an IC will pay for a covered claim.

[3]A deductible is the amount of money a PH must pay on its own before cyber insurance can cover the damages.

Table 7.5: INCHAIN covered cybersecurity incidents and maximum reimbursement

Incident Name	Maximum Reimbursement (€)
Business email compromise	123K
Lost device	57K
Malware/Virus	160K
Phishing	72K
Ransomware	179K

- ***PH_{id}:*** A unique identifier characterizing the PH (e.g., `1531435435`).
- ***IC_{id}:*** A unique identifier characterizing the IC (e.g., `58567696`).
- ***Premium:*** The amount of cyber insurance contract (e.g., *1080 €*).
- ***Limit of Liability:*** The maximum amount an IC will pay for claims during the contract period (e.g., *500K €*).
- ***Deductible:*** The amount of money a PH must pay on its own before IC can cover the damages (e.g., *4K €*).
- ***Obligations:*** PH's obligations against the contract (e.g., *penetration tests every 3 months*).
- ***Reputation:*** A score characterizing the PH based on compliant behavior in obligations against the contract. Its initial value is equal to 100. If the PH violates the contract, its reputation decreases. The lower the value is, the worse the reputation is.
- ***$Incident_{id}$:*** A unique identifier of the incident and is correlated to specific incident evidence (e.g., firewall, IDS, IPG, and SOC logs) that are submitted by the PH and investigated by the IC.
- ***Incident:*** The name of the incident for which PH is requesting compensation (e.g., *phishing*).
- ***Reimbursement:*** The amount paid to cover expenses that have been spent due to the incident (see Table 7.5).

- ***Start Date:*** The contract's issuance date (e.g., `2022-31-12T00:00:00Z`).
- ***End Date:*** The contract's expiration date (e.g., `2023-31-12T00:00:00Z`).
- ***Coverages:*** The set of what cyber incidents PH is covered for (e.g *ransomware, business interruption, data breaches*).
- ***Controls:*** The set of installed PH's cybersecurity controls (e.g., staff cyber security training every six months).
- ***ExternalFirm$_{id}$:*** A unique identifier of the external firm that is responsible for handling the incident.

The `INCHAIN` Smart Contract consists of the following functions:

➢ ***PH Creation:*** It creates the PH record into the IC's Smart Contract within the Insurance Blockchain network. Its input is the values of PH_{id}, IC_{id}, *Premium*, *Limit of Liability*, *Deductible*, *Start Date*, and *End Date*. Its output is a new record that includes the data above.

➢ ***PH Reading:*** It returns the PH's cyber insurance contract stored in the Insurance Blockchain. Its input is the values of PH_{id} and IC_{id}. As output, it returns the value of PH_{id}, IC_{id}, *Premium*, *Limit of Liability*, *Deductible*, *Start Date*, and *End Date*.

➢ ***Incident Report:*** It is executed by the PH to report a cybersecurity incident. Its input is the value of PH_{id}, IC_{id}, $Incident_{id}$, and *Incident*. As output, it notifies the PH for the corresponding incident.

➢ ***Incident Response***: It is executed by the IC to accept or reject a reimbursement of a cybersecurity incident. Its input is the values of PH_{id} and IC_{id}. As output, it updates the value of *Limit of liability*.

➢ ***PH Obligation Checks:*** It is executed by the IC to check whether the PH meets its *Obligations* (e.g., penetration test every three months) comparing with *Controls*. Its input is the values of PH_{id} and IC_{id}. Its output is the value of *Obligations* together with a `YES/NO` that declares if the PH meets them or not.

➢ ***Asset Transfer:*** It can be called by the Incident Response function and transfers funds from IC to the PH. Its input is the values of PH_{id}, IC_{id},

and *Reimbursement*. As output, it notifies the PH that the asset has been successfully transferred to its account.

➢ ***Violation:*** It is triggered by the PH Obligation Check function, and it is responsible for decreasing the reputation of PH when the PH does not meet its obligations. Its output is the updated *Reputation* value.

➢ ***Contract Analysis***: It is triggered by both a PH and IC to present the incidents for which the PH is covered and its obligations with respect to those coverages. Its input is the values of PH_{id} and IC_{id}. Its output is the values of *Coverages* and *Obligations*.

➢ ***HandleIncident***: The Incident Response outsourcing occurs when the IC delegates the incident coordination to an external firm rather than handling it internally. The function takes inputs, including the values of IC_{id}, $Incident_{id}$, and $ExternalFirm_{id}$. The output of this function is an amount representing the transaction costs incurred, which will be factored into the final compensation calculation.

The IC creates a record within the Smart Contract for its new PH that is stored in the Insurance Blockchain (`Step 7`), and then, the PH can utilize cyber insurance services (`Step 8`). Moreover, the IC issues a VC to the PH to control the access to the *Insurance Blockchain* that consists of Smart Contracts and security information related to its PHs and handles all cyber insurance related (`Steps 9 { 11`). The VC issued by the IC verifies that the corresponding PH is the legitimate owner of the cyber insurance contract issued by it. Through this credential, the PH can access the Smart Contract stored within the Insurance Blockchain to perform actions regarding the cyber insurance contract, including but not limited to cybersecurity incident reports. Finally, the IC starts performing unexpected audits to the PH to identify Smart Contract violations and improve the data regarding this PHs that are stored within the Blockchain, achieving a continuous risk monitoring system (`Steps 12 - 13`).

Through this operation, `INCHAIN` addresses the cyber insurance challenges entitled `CH1`, `CH2`, `CH5`, and `CH6`. This `INCHAIN` operation is responsible for verifying PH's data against IC requirements to check its eligibility for buying a cyber insurance contract. `INCHAIN` substitutes the rigid verification processes that occur on IC's side with automated processes provided by the SSI (`CH2`). Hence, the IC will not allot resources to validate attributes submitted by potential PHs. In addition, it is directly connected with the `CH6`; `INCHAIN` with the SSI integration achieves to equip ICs with a collection of methods

Algorithm 1 INCHAIN's Smart Contract Pseudocode

1: **function** IncidentReport($Policyholder_{id}$, $InsuranceCompany_{id}$, $Incident_{id}$, incident, reimbursement)
2: **if** exists PH record with $PH_{id} = Policyholder_{id}$ **and** $IC_{id} = InsuranceCompany_{id}$ **then**
3: store $Incident_{id}$ and incident and reimbursement into PH record
4: **end if**
5: **end function**
6:
7: **function** IncidentResponse($Policyholder_{id}$, $InsuranceCompany_{id}$)
8: reimbursement = 0
9: **if** exists PH record with $PH_{id} = Policyholder_{id}$ **and** $ICid = InsuranceCompany_{id}$ **then**
10: **if** reimbursement of PH record > deductible of PH record **then**
11: reimbursement = reimbursement of PH record - deductible of PH record
12: **else**
13: reimbursement = 0
14: **end if**
15: **if** reimbursement > 0 **and** Limit of liability of PH record ≥ reimbursement **then**
16: call AssetTransfer($Policyholder_{id}$, $Insurancecompany_{id}$, reimbursement)
17: **end if**
18: **end if**
19: **end function**
20:
21: **function** AssetTransfer($Policyholder_{id}$, $InsuranceCompany_{id}$, reimbursement)
22: **if** exists PH record with $PH_{id} = Policyholder_{id}$ **and** $ICid = InsuranceCompany_{id}$ **then**
23: limit of liability of PH record = limit of liability of PH record - reimbursement
24: **end if**
25: **end function**

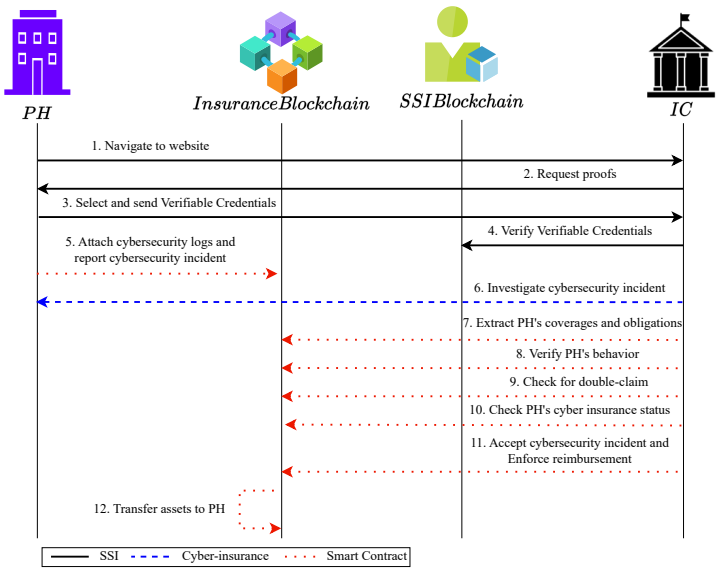


Figure 7.4: Incident report and reimbursement

that allows them to confirm the identification of their PHs and verify they are acting legally. Moreover, it is well-known that ICs have to store data regarding their PHs becoming targets of cybersecurity attacks (e.g., hackers perform data breaches on ICs to steal PHs' sensitive information). However, with SSI, data is stored on the PHs' side, eliminating many threats related to centralized storage. The information stays in the hands of the PHs, giving the IC permission to view the necessary data. It means that hackers can no longer break into large databases held by ICs to view sensitive data, eliminating many threats for ICs (`CH5`). Also, the gathering of PHs' data eliminates the `CH1` as long as the IC can know important information about its cybersecurity exposure (e.g., security controls, cybersecurity behavior, frequency of cybersecurity incidents). Finally, the collected data during the audits stored within the Insurance Blockchain can be used in the future for underwriting and pricing premium processes for these PHs or future ones.

7.3.3.3 Incident Report and Reimbursement

During a cyber insurance lifetime, a PH may need to report to its IC

a cybersecurity incident having as its ultimate goal to receive reimbursement following their agreement as part of the agreed cyber insurance and the Smart Contract rules. Figure 7.4 depicts this operation, which is responsible for handling the report of a cybersecurity incident by the PH, the investigation of it by the IC, and the payment order by the latter. It also influences the classic cyber insurance processes entitled *Claims Submission*, *Claims Validation and Auditing*, and *Claims Payment*. First, the process of *Claims Submission* is performed by the PH, which is becoming an automated process due to the Smart Contract functions entitled `IncidentReport`, and `IncidentResponse` (see Sections 7.2.3 and 7.3.3.2). Moreover, it substitutes the bureaucracy that characterizes the rigid way of reporting a cybersecurity incident (e.g., email and questionnaires). The same applies to the process named *Claims Payment*. Once an IC accepts the PH's reimbursement, it calls a Smart Contract function and automatically reimburses the PH. In addition, `INCHAIN` enhances the *Claims Validation and Auditing* process with accurate cybersecurity data from the VCs. This data includes new information that has not been considered yet by the existing methods (e.g., employee behavior against phishing attacks). In addition, it becomes more agile since the Smart Contract function *Check PH Obligations* assists auditors by returning if the PH meets its obligation during the incident period. This opinion comes from the VC's extracted data. It is directly related to the investigation of a cybersecurity incident since the results can be more precise due to the exploitation of the accuracy that characterizes the collected historical data.

For the declaration of a cybersecurity incident (see `Steps 1 - 12` depicted in Figure 7.4), the PH has to prove its identity to the IC. The IC will request proof from the PH to confirm that it is a legitimate PH with a cyber insurance contract issued by the IC. Let us assume that the PH is the victim of a ransomware attack, with the attackers demanding a ransom of 100K €. While the PH looks within its wallet at the VCs it holds, it can choose to send the entire claim or only a subset of it, ensuring minimal disclosure of its data and proving that it is the legitimate holder of the VCs. Then the IC validates the authenticity of the received VCs by verifying the signatures of the PH's and IC's DID stored within the SSI Blockchain (`Steps 1-4`). Once the identification is completed, the PH notifies its IC about the cybersecurity incident (`Step 5`).

The PH provides detailed reports and data that describe the incident (e.g., firewall, IDS, IPS, SOC logs). As a result, the IC performs an incident investigation and, based on the results, decides whether to accept or

reject the reimbursement request (`Step 6`). Also, the IC calls Smart Contact functions to extract the PH's obligations that must be met based on its contract and verify that the PH indeed meets them (`Steps 7 - 8`). Last but not least, the IC searches within the Insurance Blockchain to verify that the PH has not submitted the same claim (e.g., recovery expenses from the same ransomware attack) to a different IC (`Step 9`). Then, the IC checks PH's limit of liability and deductible (`Step 10`). The IC checks if the PH has remaining money for its coverages. If the amount is equal to zero, the process is terminated. Otherwise, IC accepts and forces automatic payment to the PH's wallet (`Steps 11 - 12`).IC compensates the PH with 96K €. Then, the limit of liability is automatically reduced to 404K € for the next incident following the reimbursement. However, in the event of a request rejection or identification of double-claim[4], the operation is terminated in `Step 7` or `Step 8` correspondingly. Moreover, in case of Smart Contract's rules violation, the IC triggers a Smart Contract function to decrease PH's reputation.

This operation can address the cyber insurance challenges entitled `CH1`, `CH2`, `CH3`, and `CH4`. `INCHAIN` uses Smart Contracts and aims to simplify interactions between a PH and its IC regarding the cybersecurity incident report (`CH2`). In the event of a cybersecurity incident, a PH triggers a Smart Contract function (i.e., the function `IncidentReport`), and automatically its IC gets notified of it. In terms of response, IC can immediately begin incident and forensic investigation. In the end, the IC reimburse the PH by triggering the proper Smart Contract function. Moreover, all incidents with their IDs and attributes stored in the Insurance Blockchain prevent dishonest PHs from reporting the same incident multiple times (`CH3`).

Finally, the use of SSI and VCs deters hackers from stealing PHs' identities by performing masquerade attacks (`CH4`). The VC's claims can be verified only by its owner, which securely stores the correlated private key (see Section 7.2.3.3). Finally, the IC collects all the cybersecurity data related to the incident and stores it within its Insurance Blockchain to access it later, addressing the challenge `CH1`.

[4]When a business has insurance cover in respect of the same risk and subject matter from more than one insurer and submits a claim for the same incident to them.

Table 7.6: Cyber insurance processes and INCHAIN operations

Cyber Insurance Processes	INCHAIN Operations		
	Verifiable Credential Issuance	Verifiable Credential Verification and Cyber Insurance Issuance	Incident Report and Reimbursement
Client Registration & Validation	✓	✓	✗
Underwriting	✗	✓	✗
Claims Submission	✗	✗	✓
Claims Validation & Auditing	✗	✗	✓
Claims Payment	✗	✗	✓

7.4 Exploring the Value of INCHAIN

This section demonstrates how INCHAIN aligns with the established cyber insurance processes outlined in Section 7.3.1. Furthermore, it effectively addresses the challenges that the cyber insurance landscape poses, as discussed in Section 6.2. Finally, a comparative analysis is conducted with related works, as presented in Section 7.2.2, to illustrate the uniqueness and effectiveness of INCHAIN.

7.4.1 INCHAIN Capabilities Against Cyber Insurance Processes and Challenges

The INCHAIN architecture fulfills all cyber insurance processes outlined in Table 7.6, with the exception of *Market Research* and *Pricing Premium* (as discussed in Section 7.3.1). *Market Research* primarily involves communication between a PH and its CIB, and thus falls outside the scope of this work. Similarly, INCHAIN does not provide a pricing formula for determining the premium, as this is also beyond the scope of this work.

First and foremost, the INCHAIN operation named *Verifiable Credential Issuance* (see Section 7.3.3.1) as its name implies, is responsible for issuing VCs to a PH. It can be observed that the INCHAIN architecture fulfills the cyber insurance process of *Client Registration and Validation* (as discussed in Section 7.3.1), as the PH is equipped with credentials that contain verified data from a trustworthy entity (i.e., NCSA). Next, the INCHAIN operation *Verifiable Credential Verification and Cyber Insurance Issuance* as its name implies, includes the verification of a PH's VCs by its IC and upon successful verification the cyber insurance issuance. In particular, VCs automate the *Client Registration and Validation* process. Also, a PH and its IC exchange only accurate data among them, used within the underwriting

process. Finally, the *Incident Report and Reimbursement* operation, as its name implies, is responsible for handling claims and includes the *Claims Submission*, *Claims Validation and Auditing*, and *Claims Payment* processes. Its main pillar is the *Smart Contract* functions. On the one hand, the PH triggers the `IncidentReport` function to submit a claim (i.e., *Claims Submission*). On the other hand, other functions (i.e., `IncidentResponse`, `PHObligationChecks`, as well as `AssetTransfer`) are triggered by the IC to initiate investigations and to force the reimbursement.

Table 7.6 depicts the aforementioned correspondence between the cyber insurance processes (see Section 7.3.1) and `INCHAIN` operations (see Section 7.3.3). The correspondence between cyber insurance processes and the `INCHAIN`'s operations is indicated using the symbols ✓ and ✗. The ✓ symbol signifies that there is a correspondence between a cyber insurance process and an `INCHAIN`'s operation, while the ✗ symbol indicates that there is no such correspondence.

However, `INCHAIN` can be characterized by the following drawbacks. First, it does not include a formula to calculate the premium of a cyber insurance contract; this process occurs offline at IC's side. Moreover, `INCHAIN` does not perform an automated incident investigation to decide whether to reimburse an incident; this process also occurs offline. It requires seamless communication between the PH and its IC, including interviews and exchange of logs that need to be analyzed offline by the latter.

In general, it is strongly arguable that `INCHAIN` can address all cyber insurance challenges mentioned above. This observation is further extrapolated below.

CH1 – Lack of Data. `INCHAIN` utilizes the Blockchain network as a repository to securely store cybersecurity data related to its PHs. As mentioned above (see Section 7.2.3.1), the Blockchain is an unchangeable, everlasting digital data archive. `INCHAIN` is equipped with processes that automatically upload records to Blockchain with data related to audits, risk assessment, forensic investigation, and incidents (see Figures 7.3 and 7.4). A record stored in the chain cannot be altered, deleted, or otherwise tampered with. Moreover, data accumulates when it cannot be removed. In `INCHAIN`, an event will be recorded across nodes (e.g., the record of a cybersecurity incident), also known as on-chain data. This enables continuous cybersecurity data gathering related to IC's PHs. The generation of accurate historical data will be a meaningful indicator for cyber insurance processes (*Under-*

writing and *Pricing Premium*). Furthermore, the `INCHAIN` smart contracts incorporate functions capable of retrieving real-time cybersecurity-related information from PHs, such as the frequency of attacks, and securely storing this data within the Blockchain. The adoption of SSI is pivotal in addressing this challenge, ensuring that the involved ICs collect only accurate and up-to-date PH information. This approach eliminates the reliance on outdated or incomplete data stored in centralized databases. As a result, ICs can provide fair premiums tailored to the specific needs of each PH, leveraging statistics derived from the collected historical data. For instance, they can consider data on the most attacked industry and the most common cybersecurity vulnerabilities.

CH2 – Lack of Automated Tasks. `INCHAIN` integrates Smart Contracts and SSI to introduce automatically performed tasks. First, by automating cyber insurance claims processes, Smart Contracts can eliminate paperwork and time-consuming processes. The `INCHAIN` smart contract includes the *Incident Report* function, enabling PH to automatically report cybersecurity incidents to the IC without the need for email communication. Subsequently, depending on the IC's choice to manage the cyber incident internally, the following functions can be invoked: *Contract Analysis*, *PH Obligation Checks*, and *Violation*. In scenarios where the incident response is outsourced to an external firm, the *HandleIncident* function comes into play. Lastly, the *AssetTransfer* function automates the payment process for submitted claims. In essence, the functions provided by the smart contract play a crucial role by automating significant aspects of Claims Submission (CIP6), Claims Validation and Auditing (CIP7), and Claims Payment (CIP8).

Automating cyber insurance tasks reduces costs significantly; an essential factor for PHs and ICs. Second, SSI enables ICs to perform verification processes automatically (see Section 7.3.3). `INCHAIN` with SSI substitutes the bureaucracy and labor process of verifying paper documents, contracts, attributes, and IDs. In `INCHAIN`, ICs, via SSI and Blockchain, are reassured that the attributes of a submitted identity are accurate, and they can also immediately check its validator (e.g., NCSA) without contacting it.

CH3 – Fraudulent Claims. It is the first time that a work addresses this challenge (see Table 7.8). `INCHAIN` eradicates the frequency of fraudulent claims through the integrated SSI approach since the Insurance Blockchain will be accessed only from verified PHs who meet specific requirements. Furthermore, through the Smart Contract implementation, when a claim is sub-

mitted for a cybersecurity incident, the IC could check if multiple claims are submitted for the same incident, ensuring that only valid claims are reimbursed. In particular, in case of an incident, the IC can search within the Insurance Blockchain to find similar claims by the subject PH investigating the attached logs. Thus, all fraudulent claims are eradicated. Also, within the Insurance Blockchain, each token is unique and the ledger is immutable without replicable assets (e.g., a cybersecurity incident claim can occur only one time).

CH4 – Identity Theft. ICs face attacks from cyber criminals that are tied back to PHs' for credential theft (e.g., a masquerade attack). `INCHAIN` utilizes SSI and aims to defend its infrastructure from attack vectors targeting data verification (e.g., attackers masquerading as PHs to steal reimbursement). The `INCHAIN` verification system is based on SSI and is used to verify the VCs and ensure that the content interactions match the role of the issuer (such as NCSA), preventing collaboration with fake issuers. In addition, the constantly updated SSI Blockchain provides validated issuer information to ICs. Thus, ICs can determine the validity of both the issuer (e.g., NCSA) and the VC when it is submitted to their service. A VC signed by its issuer is stored within a digital identity wallet (see Section 7.2.3.3). Thus, the data contained within it and shared with ICs cannot be changed without being flagged (e.g., as an error) by the original issuer. In essence, only the original issuer can alter a VC's data. In addition, the digital identity wallet remains encrypted at rest as well as in motion. Without the keys (see Section 7.2.3.3) to this encrypted wallet, the data is not accessible outside of it.

CH5 – Loss of Sensitive Data. Centralized verification systems make organizations vulnerable to large-scale hacks and data breaches (e.g., a data breach in Marriott hotels [266]). `INCHAIN` aims to prevent this kind of attack in ICs using SSI. Generally speaking, SSI safeguards privacy by removing the need to store personal information on a central database and gives individuals greater control over what information they share. Through VCs, SSI lets PHs control what they disclose with ICs [265] (i.e., selective disclosure) avoiding centralized data storage. PHs are SSI identity holders and control their own VCs. These VCs are kept locally on a PH's digital identity wallet and digitally signed with its private key and the NCSA keys (see Section 7.2.3.3), ensuring its ownership. ICs receive VCs safely to provide a service. Thus, the PH retains control of its data and only grants the IC access to the information it requires. As a result, there is far less risk of harm to the

IC, as attackers will no longer be able to compromise the IC's database and steal sensitive data. Apart from protecting the ICs, SSI also protects PHs from fraudulent ICs through secure authentication, selective disclosure of information, decentralized verification networks, reputation and trust models, an immutable audit trail, privacy-preserving protocols, and community governance. SSI utilizing cryptographic techniques for secure authentication allows PHs to prove their identity without revealing unnecessary personal information. PHs have control over the information they share, reducing the risk of exposing sensitive data to fraudulent ICs. In addition, SSI's decentralized verification networks and reputation models ensure that trusted entities vouch for authenticity, and users can assess verifiers' trustworthiness through ratings and reviews. The immutable audit trail enables accountability and identification of fraudulent ICs, while privacy-preserving protocols minimize data exposure.

CH6 – Know Your Customer. Another aspect of the proposed architecture is the *Know Your Customer* approach to completion. In `INCHAIN`, the SSI is responsible for the identification of PHs, as the data associated with a PH's identity is stored, shared, and used for verification on distributed ledger technology. The use of VC on SSI enhances the security level of identification as the VC is cryptographically constructed to prove its issuer, owner, and validity. Additionally, the VC claims are not tampered with. On the other hand, the Insurance Blockchain (see Figure 7.1) is responsible for continuously monitoring PHs during a cyber insurance contract. Overall, SSI and the Insurance Blockchain help to reduce costs by decreasing the need for personnel focused on *Know Your Customer* tasks, enhancing the security of identification, shortening processing time, and improving the PHs experience.

CH7 – Information Asymmetry. `INCHAIN` eliminates the information asymmetry between the ICs and PHs regarding the cyber insurance contract misunderstanding. In particular, the `INCHAIN` Smart Contract (see Section 7.3.3.2) is equipped with a specific function (i.e., `ContractAnalysis`). The Smart Contract, which is a digital representation of the cyber insurance contract, includes the definitions of each covered incident. For instance, if the PHs raise the following question: *"What does the insurance cover regarding a cyber-extortion threat?"*, the Smart Contract function `ContractAnalysis` will respond not only with its definition but the circumstances that should be met in order to be covered. Thus, with `INCHAIN`, the PHs will be deterred from decreasing their security investments after obtaining cyber in-

Table 7.7: Cyber insurance challenges and Candidate Technologies

Cyber Insurance Challenges	**Candidate Technologies**		
	Blockchain	**Smart Contracts**	**SSI**
CH1 – Lack of Data	✓	✓	✓
CH2 – Lack of Automated Tasks	✗	✓	✓
CH3 – Fraudulent Claims	✗	✓	✓
CH4 – Identity Theft	✗	✗	✓
CH5 – Loss of Sensitive Data	✓	✗	✓
CH6 – Know Your Customer	✗	✗	✓
CH7 – Information Asymmetry	✗	✓	✗

surance. Moreover, `INCHAIN` contributes significantly to the underwriting process of cyber insurance. In particular, the `INCHAIN` Smart Contract (see Section 7.3.3.2) is equipped with a specific function (i.e., `PH Obligation Checks`) that checks if the installed cybersecurity controls of PH comply with its cyber security contract obligations. This feature of INCHAIN could save the underwriter a significant amount of time that he would have spent with the traditional way of interviewing policyholders and then editing their responses to determine if they are consistent with the policyholder's obligations. What INCHAIN cannot eliminate, however, is the human critical thinking of the underwriter who will make the final underwriting decision. Last but not least, `INCHAIN` via function Incident Response checks if the requested indemnification of PH in Claims Submission (CIP6) can be served by the attribute maximum indemnity limit (or `INCHAIN`'s attribute named Limit of Liability 7.3.3.2). The value of Limit of Liability is defined in `INCHAIN` when it is called the function PH Creation.

Table 7.7 describes the cyber insurance challenges being addressed by the `INCHAIN` candidate technologies. First and foremost, Blockchain contributes to mitigating *CH1 – Lack of Data* and *CH5 – Loss of Sensitive Data* since it provides an immutable and secured data storage at the IC's side and transparency for each related transaction. Next, the integration of Smart Contracts assists in the mitigation of the *CH1 – Lack of Data*, *CH2 – Lack of Automated Tasks*, *CH3 – Fraudulent Claims*, and *CH7 – Information Asymmetry*, since these are equipped with functions (see also Section 7.3.3) to perform the required actions for gathering real-time cybersecurity-related

Table 7.8: Cyber insurance challenges fulfillment of related work

Challenges	Works					
	Franco et al. [225]	Lepoint et al. [226]	Vakilinia et al. [227]	Xu et al. [197]	Farao et al. [8]	INCHAIN
CH1 - Lack of Data	✗	✓	✗	✗	✓	✓
CH2 - Lack of Automated Tasks	✓	✓	✓	✓	✓	✓
CH3 - Fraudulent Claims	✗	✗	✗	✗	✗	✓
CH4 - Identity Theft	✗	✦	✗	✗	✗	✓
CH5 - Loss of Sensitive Data	✗	✦	✗	✗	✗	✓
CH6 - Know Your Customer	✗	✗	✗	✗	✗	✓
CH7 - Information Asymmetry	✗	✗	✗	✗	✓	✓

PHs' data, to automatically execute processes for incident report and handling, as well as, to assist PHs to understand their obligations against their contract. While SSI commits to mitigating *CH1 – Lack of Data*, *CH2 – Lack of Automated Tasks*, *CH3 – Fraudulent Claims*, *CH4 – Identity Theft*, *CH5 – Loss of Sensitive Data*, and *CH6 – Know Your Customer*. This occurs because SSI can allow ICs to gather not only updated but also the minimum required PH's data to perform cyber insurance processes (see also Section 7.3.1) and provide full identity control on the involved PHs. Overall, we can observe that `INCHAIN` aims to face the cyber insurance challenges (see also Section 6.2), combining features from more than one candidate technology and merely exploiting Blockchain features to develop applications for enhancing existing cyber insurance processes.

7.4.2 Comparative Analysis of Related Works and INCHAIN in Addressing Cyber Insurance Challenges

Table 7.8 compares related works (see Section 7.2.2) with `INCHAIN` against the cyber insurance challenges (see Section 6.2); the comparison is based on the following signs: ✓, ✗, ✦. The ✓ sign shows that the respective challenges consist of an advantage of the method over the others, in the sense that the work addresses the challenge. The ✗ sign shows that the challenge is considered a deficiency of the work, in the sense that the challenge is not addressed. When the ✦ sign is displayed, it means that the respective work does not include all the details needed, and assumptions were needed to come to a conclusion. Here, we answer the fourth research question (*RQ4 – How does the literature address the existing challenges of cyber insurance with*

Blockchain and smart contracts?). The selection of works for comparison with INCHAIN was based on the following criteria:

1. The work exclusively lies in the cyber insurance field.
2. The work utilizes at least one of the candidate technologies (see Section 7.2.3).
3. The work aims to address cyber insurance challenges (see Section 6.2).

Franco et al. [225] propose SaCI on top of Ethereum, utilizing Smart Contracts. SaCI uses Smart Contracts to automate the processes of premium payment, contract updates, claim requests, dispute resolutions, and check of contract information and its integrity. Thus, SaCI addresses the challenge CH2. However, because of Ethereum, each Smart Contract function has a gas fee. On the one hand, this can limit the number of claims submitted by a PH, forcing it to submit claims only for real incidents. On the other hand, in case of identity theft, the attacker can overcharge and waste the accumulated money of the limit of liability. Thus, a PH may be unable to submit a claim for a real incident because there will not be enough money in its wallet for spending. Also, this system lacks a verification method to check the PH's legitimacy before submitting a claim request. The authors do not analyze how ICs verify the PHs' attributes. Furthermore, the authors do not consider collecting cybersecurity data for use in future cyber insurance processes. Overall, SaCI does not address CH1, CH3, CH4, CH5, CH6, and CH7.

Lepoint et al. [226] present BlockCIS on top of Hyperledger Fabric, utilizing Smart Contracts. BlockCIS leverages the automated nature of smart contracts (on the IC side) but is entirely decoupled from the payment aspect of the blockchain (contrary to INCHAIN). BlockCIS is a continuous monitoring and processing cyber insurance system focusing on the confidentiality and privacy of the collected and stored data within the system. ICs use Smart Contracts to devise premiums tailored to a PHs's security posture, and the latter can prove that its cyber insurance covers a potential cyber incident. In addition, BlockCIS includes access control rules to limit access to its data. It is assumed that based on the implemented access control rules, BlockCIS may defend against cyberattacks related to identity theft and loss of sensitive data. However, we cannot conclude with 100% confidence because the respective work does not include all the necessary implementation details. Thus, it is assumed that BlockCIS addresses CH1 and CH2 challenges, while

the CH4 and CH5 are addressed under implementation assumptions. However, the authors do not consider a method to verify that PHs submit accurate data nor to monitor any change in its infrastructure. Finally, BlockCIS does not include a method to prevent fraudulent claims and eliminate information asymmetry. Thus, BlockCIS does not address the CH3, CH6, and CH7 challenges.

Vakilinia et al. [227] and Xu et al. [197] propose cyber insurance crowdfunding frameworks on top of the Ethereum network. Smart Contracts can perform crowdfunding initialization, bidding, wrapping, and reimbursement actions. Thus, both works address the CH2 challenge. However, the proposed frameworks lack a method to collect cybersecurity data for future cyber insurance use and to prevent fraudulent claims. Moreover, the frameworks are not equipped with security measures to prevent cybersecurity attacks related to identity theft and loss of sensitive data. Thus, in case of identity theft, the attacker can overcharge and waste the PH's accumulated money of the limit of liability. Hence, a PH may not submit a claim for a real incident because there will not be money in its wallet for spending. Furthermore, the authors do not analyze the method that ICs follow to verify a PH's attributes, do not consider a method to be updated for changes in PHs's infrastructures, and do not include a method to eliminate the information asymmetry. Consequently, both works do not address CH1, CH3, CH4, CH5, CH6 and CH7.

Finally, the SECONDO project [8] has been built on top of Hyperledger Fabric. Its Smart Contracts perform actions related to reporting and responding to an incident as well as to forcing reimbursement. Thus, Farao et al. [8] can address the CH2 challenge. Moreover, SECONDO is equipped with a continuous risk monitoring tool that collects PHs' cybersecurity data and stores it within the Blockchain. The data is used for future cyber insurance processes (i.e., underwriting). Thus, SECONDO addresses the CH1 challenge. Moreover, it includes a cyber insurance policy ontology that eliminates the information asymmetry between the PHs and ICs, addressing the CH7 challenge. However, SECONDO does not have a mechanism in place to prevent eligible PHs from submitting fraudulent claims or to verify the PH's eligibility before the claim submission. Finally, it does not consider a method to gather only accurate PHs data during each cyber insurance process. Overall, SECONDO cannot address the CH3, CH4, CH5 and CH6 challenges.

Overall, the previous analysis raises the following observations. First and foremost, all related works address the challenge CH2 using Smart Contracts. INCHAIN addresses it via the Smart Contracts integration. Next, [226, 8] and

INCHAIN address challenge C1. These works utilize their Blockchain implementation to store cybersecurity data for future cybersecurity use. Furthermore, the literature [225, 226, 227, 197, 8] does not address the challenge CH3 regardless of its importance. However, in INCHAIN, ICs search within the Insurance Blockchain to find similar claims by the subject PHs investigating the attached logs. [226] and INCHAIN address the challenge CH4. The other works do not implement a method to protect their system from this since a PH can use the network certificate to trigger a Smart Contract function. Thus, if attacks steal the credential, they can call any Smart Contract function without limitations. The authors in [226] allow the Smart Contract use based on access control rules to prevent PHs' identity stealing. However, in INCHAIN, a PH has to be authorized via VC verification before submitting a claim. It occurs with VCs stored in secured digital identity wallets. Therefore, INCHAIN depends on the fact that VCs can be accessed only by their eligible holders. It is the one knowing the key pair to access the digital identity wallet and to use its VCs.

In addition, [226] and INCHAIN address the challenge CH5. The works [225, 227, 197] do not include any method to protect data since they do not collect them. However, [8, 226] collect cybersecurity data. The authors in [8] depend on the certificates issued by the Blockchain. Thus, a node with the correct certificate can perform actions to the collected cybersecurity data without limitation. However, the work [226] limits access to the collected data via an access control policy. In contrast, INCHAIN uses VCs to allow access to its collected cybersecurity data stored within the Insurance Blockchain. Further, challenge CH6 has been addressed only by INCHAIN. It includes SSI to collect accurate data regarding PHs's behavior and assets. Finally, [8] and INCHAIN solve the challenge CH7. On the one hand, Farao et al. [8] include a cyber insurance policy ontology that analyzes each contract isolating its coverages and exclusions. On the other hand, INCHAIN uses a Smart Contract function that can be triggered anytime by the PHs and the ICs. It is responsible for defining the cybersecurity threats covered for PHs and outlining the obligations they must fulfill in order to be eligible for reimbursement.

7.5 Discussion

This section presents an analysis of the risks inherited by the integration of Blockchain and SSI, the presentation of well-know and open-source Blockchain

platforms and SSI implementation that could be leveraged by the cyber insurance ecosystem, an analysis of `INCHAIN` limitation, along with suggestions for future research and development avenues that can be pursued to enhance its capabilities and expand its impact.

7.5.1 Inherited Risks of Blockchain and SSI Integration

Now, we analyze the risks inherited to the cyber insurance ecosystem integrating Blockchain and SSI. While Blockchain technology inherits numerous advantages and opportunities, it also poses certain risks in the context of cyber insurance. Below, we highlight the risks associated with the use of blockchain in cyber insurance:

7.5.1.1 Smart Contract Vulnerabilities

Smart contracts, which are self-executing agreements on the blockchain, contain vulnerabilities [267] that attackers can exploit. Bugs or coding errors in smart contracts could lead to unintended consequences or allow unauthorized access to sensitive information. However, a contingency plan includes testing protocols consisting of penetration tests and audits leading to the identification of Smart Contracts' vulnerabilities and their address.

7.5.1.2 Data Privacy and Security

Blockchain is touted for its security; however, it is not immune to cybersecurity attacks [268]. While the decentralized nature of blockchain can make it more difficult to tamper with data, it does not guarantee absolute security. For instance, if the private keys used to access blockchain-based systems are compromised, it could lead to unauthorized access, data leaks, or loss of funds. However, a contingency plan may include actions related to secure storage for keys and certificates, as well as the implementation of robust encryption mechanisms (e.g., AES algorithm).

7.5.1.3 Oracles and External Data Sources

Blockchain-based insurance platforms often rely on oracles to obtain external data, such as information about security breaches or PHs claims [269]. However, the accuracy and reliability of these external data sources can be a concern. If the oracles are compromised or provide inaccurate information, it can undermine the integrity of the insurance claims process. Thus, a contingency plan may include mechanisms for validating and verifying data accuracy obtained from oracles and external data sources.

7.5.1.4 Lack of Standardization and Regulations

The blockchain is still in its infancy; thus, the lack of standardized protocols and interoperability between different blockchain platforms can hinder blockchain's scalability and widespread adoption in the insurance industry. Therefore, ICs may face challenges integrating blockchain-based solutions with their existing systems, leading to inefficiencies or compatibility issues. Yet, a contingency plan may include the development of flexible and modular blockchain solutions that can adapt to future changes and advancements in the blockchain.

Moreover, the integration of SSI inherits risks to the cyber insurance ecosystem, these are elaborated below:

7.5.1.5 Social Engineering and Manipulation

SSI systems rely heavily on user consent and identity control. However, within the cyber insurance ecosystem, this can make PHs more susceptible to social engineering attacks or manipulative practices, where they may unknowingly grant access to their identity information to malicious actors pretending to be their IC. This can lead to unauthorized access to sensitive data and misuse of identity information. Nonetheless, a contingency plan may include actions for educating PHs to detect and avoid phishing attacks, fraudulent requests for identity information, and unauthorized access attempts building and promoting the human firewall approach.

7.5.1.6 Increased Risk of Identity Theft

SSI systems store sensitive data on distributed ledgers, and the security of these systems becomes critical. If vulnerabilities exist in the SSI infrastruc-

ture or malicious actors gain unauthorized access, it could lead to widespread identity theft and fraud. Such incidents could result in a surge in fraudulent claims and financial losses for ICs. A contingency plan may include the utilization of security enclaves, robust access control mechanisms, as well as encryption of data in rest and in transit.

7.5.1.7 System Availability

The risk of a single point of failure is an important consideration when implementing SSI systems. Such a system failure may disrupt and interrupt the availability and functionality of the system, making it inaccessible to legitimate users. However, a contingency plan may include actions related to robust infrastructure design, traffic monitoring, and anomaly detection.

7.5.2 Blockchain Platforms and SSI Implementations Suitable for the Cyber Insurance Ecosystem

Now, we present well-known and open-source block-chain platforms (i.e., Hyperledger Fabric, Ethereum) and SSI implementations (uPort, Hyperledger Aries) that could be used for cyber insurance. E

Hyperledger Fabric is an open-source blockchain platform that enables organizations to construct and administer their own distributed ledger systems. It provides the required tools and frameworks for constructing blockchain-based insurance applications with features such as smart contracts, privacy, and authorized access. The strongest feature of Hyperledger Fabric is the execution of smart contracts. ICs can automate policy issuance, claims processing, and premium calculation processes using smart contracts. Moreover, Hyperledger Fabric enables the construction of private channels in which only a select group of participants can access the shared data. This enables ICs to share sensitive information, such as policy details and claims data, with relevant parties in a secure manner while maintaining data privacy and confidentiality. Finally, Hyperledger Fabric supports pluggable consensus mechanisms, enabling ICs to select the most appropriate consensus algorithm for their particular requirements in cases such as policy revisions, claim settlements, and other crucial network decisions.

Ethereum is a decentralized, open-source blockchain infrastructure that allows the creation of smart contracts and decentralized applications (DApps).

On the Ethereum platform, numerous insurance-related DApps have been developed, offering solutions for areas such as parametric insurance, claims processing, and peer-to-peer insurance. The most crucial feature of Ethereum that can be utilized for cyber insurance purposes is its support for smart contracts. Cyber insurance policies can be implemented on the Ethereum blockchain as smart contracts. Smart contracts automate policy issuance, premium calculation, claims processing, and payout calculations based on predetermined cyber insurance requirements, reducing documentation and administrative costs. Moreover, Ethereum can support asset tokenization, representing a fraction of ownership in the underlying asset. More particularly, a series of token standards have developed to support asset tokenization of Ethereum (i.e., ERC-20, ERC-721, ERC-777, ERC-1155, ERC-4626) [270]. Another unique concept of Ethereum is gas consumption, which refers to the quantity of computational work required to execute a transaction or smart contract. Gas is a fee mechanism to prevent spam and fairly allocate network resources. Spammers would have to pay substantial gas fees to submit a high volume of spam transactions. This economic cost renders spamming economically unviable for most attackers, as they would be required to incur expenses without obtaining a significant advantage. Finally, oracles enable Ethereum to integrate with external data sources collecting data from them and providing it to Ethereum smart contracts. A prime example of oracles utilization is that oracles can provide data feeds pertaining to top vulnerabilities, percentages of cyber-attacks, or other pertinent information, enabling parametric cyber insurance and claim settlement procedures.

uPort is a platform for DID constructed on the Ethereum blockchain and developed by ConsenSys. It can enable users to establish self-governing identities and manage their digital credentials. ICs can use uPort to validate the identities of PHs, reducing the risk of identity fraud and building trust between parties. Moreover, uPort can be used to store and present cyber insurance documentation. Instead of keeping cyber insurance paper documents, PHs can retain their cyber insurance policies in their uPort wallets as digital credentials, simplifying the proof of coverage, reducing paperwork, and enhancing efficiency. Also, having all their claims-related documents (e.g., cyber-attack accident reports) in VCs, PHs can selectively share these documents with ICs, ensuring privacy and control over sensitive data. Lastly, the compatibility of uPort with other decentralized identity systems and platforms can permit the exchange of VCs across networks and ecosystems, enhancing the integration of ICs with existing systems and processes.

Hyperledger Aries is an open-source initiative under the Hyperledger umbrella of the Linux Foundation. It is a framework for developing solutions for DID and interoperable identity systems, and it offers a set of tools, libraries, and reusable components that facilitate the exchange of verifiable credentials and the creation of SSI applications. Hyperledger Aries can enable ICs to establish and authenticate the digital identities of the cyber insurance ecosystem's stakeholders, thereby augmenting the integrity and safety of the cyber insurance process. The VCs can be stored in a PHs' secure storage location named Hyperledger Aries wallet. Beyond the role of VCs in the authentication of digital identities, the content of VCs can be related to PH's cyber incidents, such as cyber incident reports or forensic data. This information can be selectively shared with other parties involved in the claims process through the feature of Hyperledger Aries named Selective Disclosure, thereby securely facilitating the exchange of claim-related information and reducing paperwork. Finally, Hyperledger Aries uses secure messaging protocols and cryptographic mechanisms, since it is based on Hyperledger Ursa [271], to safeguard the confidentiality and integrity of communications.

7.5.3 Limitations

Foremost among the limitations of `INCHAIN` is the absence of a comprehensive module for identifying cyber insurance contracts on the web, making it difficult for PHs to locate the appropriate policy for their needs. Without a simple way to compare contracts from multiple ICs, PHs either struggle to comprehend the terms and conditions of each insurance, or they may overlook critical coverage alternatives that might protect them against cyber attacks. The reason that `INCHAIN` does not deliver such a formula is because of the absence of a crawler to scrap not only the web but also ICs' websites to identify their policies and analyze them at the same time. Thus, in `INCHAIN`, PHs need to work closely with CIBs to find the right policy for their needs.

On top of the aforementioned limitation, `INCHAIN` lacks a well-defined mechanism for calculating cyber insurance premiums. This represents a significant impediment for both ICs seeking to assess risk accurately and potential PHs who require transparent and reliable pricing information. Effective risk assessment is a critical challenge for ICs operating within the `INCHAIN` ecosystem. However, without a precise method for calculating the premium, navigating the complex landscape of potential PHs with varying levels of risk becomes even more challenging. This presents a significant obstacle to

accurately assessing PHs' risk levels and underscores the need for enhanced risk modeling capabilities, leading to coverage overcharging or undercharging. Thus, in INCHAIN, ICs struggle to evaluate premium, while PHs find it challenging to determine which ICs offer the greatest value. The cyber insurance premium is influenced by vast parameters including but not limited to the PH's number of employees, its base rate, and the accepted downtime. The reason for the absence of the INCHAIN cyber insurance premium calculation formula reflects the complexity and constantly changing nature of cybersecurity risks, as well as the need for ICs to tailor their coverage and pricing to the unique needs of each client.

Moreover, INCHAIN, via the use of its candidate technologies, aims to increase the volume of cybersecurity-related data (***CH1***). It is observed that collecting vast amounts of data does not guarantee meaningful insights for cyber insurance. New challenges will emerge related to data quality, relevance, and context. Thus, INCHAIN will not eliminate this lack of historical data; however, it aims to play an essential role in creating a fertile surface for application and collaboration development for gathering accurate cybersecurity data that can be used in the future regardless of the period's technological state-of-the-art.

It is observed that SSI, due to its characteristics (i.e., decentralized data storage, cryptographic security, selective disclosure, user control, immutable audit trail), enhances the protection of ICs against data breaches and the loss of sensitive data (***CH5***). Since it establishes a more secure and privacy-preserving environment for exchanging and managing gathered sensitive information, reducing the potential risks associated with traditional centralized data storage and handling practices. However, the INCHAIN does not protect the involved PHs from being targeted by fraudulent entities that aim to steal their sensitive data pretending to be trustworthy ICs. This is a crucial issue directly related to the human firewall approach. Thus, PHs should create a contingency plan, including cybersecurity awareness training to learn how to avoid cybersecurity attacks (e.g., phishing attempts).

Smart Contracts through predefined rules enhance the elimination of Information Asymmetry (***CH7***). The INCHAIN's effort via the developed functions of Smart Contract has contributed significantly to the misunderstanding of cyber insurance contracts and the improvement of the underwriting process. However, INCHAIN has not managed to disappear human intervention in underwriting. Human criticism and thinking are indispensable mainly to making final decisions in the underwriting process of cyber insurance.

7.5.4 Future Work

The research results presented in this work have the potential to be extended in various ways through future work. First, the proposed cyber insurance architecture can be further analyzed from a functionality and architectural point of view. Use cases and scenarios showcasing the proposed architecture's beneficial aspects can be analyzed in-depth to emphasize the novelty and its relevance to ICs and PHs. Moreover, part of future work is the development of this ecosystem by integrating well-known and robust implementations having the Hyperledger as the main part of the system. In particular, it is a high priority to equip `INCHAIN` with asset transferring Blockchain application to operate the automated reimbursement from an IC to a specific PH, utilizing the IPFS approach [272] to achieve secure data storage and sharing in a distributed file system, and integrate Aries [273] as an SSI implementation. Cyber insurance professionals should assess the implementation against time consumption and resource depletion.

`INCHAIN` can also be armed with a formula to calculate the premium of a cyber insurance contract considering parameters such as the total number of security breaches and PHs' reimbursement history. In addition, `INCHAIN` can be equipped with a cyber insurance policy ontology being responsible to find policies of well-known ICs and analyze them distinguishing their coverage and exclusions. Finally, `INCHAIN` Smart Contracts can be enriched with a new function responsible for performing automated incident investigation and deciding whether to reimburse an incident.

As cybersecurity attacks become increasingly sophisticated and unpredictable, the demand for cyber insurance contracts is expected to increase over time. Cyber insurance offers a means to transfer risks to a third party. However, there are challenges that need to be addressed in order for the cyber insurance market to grow. The research outcomes presented in this paper serve as a precursor to designing cyber insurance schemes and applications that can effectively address the challenges of the growing cyber insurance market.

7.6 Conclusion

This work introduces a novel cyber insurance architecture, INCHAIN, which combines existing technologies such as Blockchain, Smart Contracts, and Self-Sovereign Identity (SSI) to address the challenges of cyber insurance. The proposed architecture is centered around Blockchain, which serves as a fundamental building block, providing security, fairness, trust, and interoperability among the participating entities. Smart Contracts automate the critical tasks of claim handling and payment in the event of a cybersecurity incident. The integration of SSI enables data minimization, robust identification, data interoperability, portability, controllability, decentralization, and transaction transparency, empowering stakeholders to increase their trustworthiness. The proposed ecosystem successfully meets the basic cyber insurance processes and addresses cyber insurance challenges by leveraging the aforementioned technologies, as demonstrated through testing in various scenarios.

In a nutshell, this paper presents INCHAIN as a novel cyber insurance architecture that offers advantages over existing methods. By conducting a comprehensive survey of previous works and comparing them with our proposed architecture, we prove its effectiveness and potential to enhance the cyber insurance industry under a theoretical perspective. The research outcomes presented in this paper not only establish a foundation for the development of cyber insurance schemes and applications but also pave the way for addressing the challenges facing the growing cyber insurance market.

Chapter 8

GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments

Investments on cybersecurity are essential for organizations to protect operational activities, develop trust relationships with clients, and maintain financial stability. A cybersecurity breach can lead to financial losses as well as to damage the reputation of an organization. Protecting an organization from cyber attacks demands considerable investments; however, it is known that organisations unequally divide their budget between cybersecurity and other technological needs. Organizations must consider cybersecurity measures, including but not limited to security controls, in their cybersecurity investment plans. Nevertheless, designing an effective cybersecurity investment plan to optimally distribute the cybersecurity budget is a primary concern. This chapter presents GTM, a methodology depicted as a tool dedicated to providing optimal cybersecurity defense strategies and investment plans. GTM utilizes attack graphs to predict all possible cyber attacks, game theory to simulate the cyber attacks and 0-1 Knapsack to optimally allocate the budget. The output of GTM is an optimal cybersecurity strategy that includes security controls to protect the organisation against potential cyber attacks and enhance its cyber defenses. Furthermore, GTM's effectiveness is evaluated against three use cases and compared against different attacker types under various scenarios

Authors	Title	Venue
Kalderemidis I, **Farao A**, Bountakas P, Panda S, Xenakis C	GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments	ARES 2022, ACM $[Rank : B]$

Table 8.1: List of thesis' publications- Part H

Table 8.1 summarizes the scientific publication related to this chapter.

8.1 Introduction

Modern systems are targeted by sophisticated adversaries that identify vulnerabilities in different components of systems and cleverly allocate their endeavors to compromise the whole organization. In 2021, 21,957 vulnerabilities have been revealed showing a raise of 19.57% compared with 2020 [274], where, in the period July-September 2021, zero-day exploits were accountable for 67.2% of malware[275]. Moreover, email attacks (e.g., phishing) have seen a 64% rise during the last couple of years due to COVID-19 [243]. Phishing attacks constitute the first step towards more complex and large-scale attacks, such as Exploit Kits [192], which are attacks that exploit vulnerabilities in web browsers and silently (i.e., without draw users attention) deliver malware to victims' or Advance Persistent Threats [276], which are attacks that establish an illicit and long-term presence on a network. In [277], the authors have highlighted the fact that the use of vulnerable Node.js functions can lead to Server-Side JavaScript Injection attacks compromising the web servers that execute the JavaScript code resulting in catastrophic consequences for an organization.

On the other hand, one of the most pressing issues that organizations face nowadays is to manage cyber risks, which involves protection [12, 278, 9, 1, 279, 280], mitigation [243, 281, 210, 282] and insurance [8, 283, 191]. The most common reason that hinders this process is the limited budget. The cybersecurity enhancement of an organization's network goes much beyond simply identifying and patching its known flaws towards understanding the behavior of attackers [284]. Although there are numerous solutions that can assist Chief Information Security Officers (CISOs) figure out which parts of

a network are vulnerable (e.g., [285], [286]), these solutions do not take into account other important parameters. For instance, what conditions and requirements might affect the state of the system during a security incident, and how people act inside and outside the network, which toughens the optimal countermeasure identification procedure. Furthermore, organizations face constraints including the limited budget and resources that necessitate making judgments that sometimes require keeping some risks.

Based on the above-mentioned statements, the motivation for this work stems from the need of organizations to strengthen their defenses against cybersecurity threats as well as from the CISOs' concern regarding the allocation of a limited budget to attain optimal protection. While organizations aspire to economically and technologically blossom in the new digital era, cybersecurity professionals have to cope with new threats and efficiently protect the organizations from sophisticated attackers who aim to evade the organizations' defenses. The main challenges that cybersecurity professionals face are summarized below:

1. Limited cybersecurity budget: Contrary to popular belief, corporations seldom attach importance to spending on cybersecurity. While cybersecurity concerns have risen to the top of the priority list, CISOs continue to struggle to get greater budgets, frequently because they cannot demonstrate a clear return on investment. When it comes to appropriately mitigate hazards, budget constraints are often a problem for organizations.

2. Multilevel cybersecurity threats: Organizations struggling to follow the latest technological advances create a fertile surface full of cybersecurity and third-party threats that can be exploited by attackers.

3. Cybersecurity results communication: Employees often are not informed about all components of the security program that affect their working-routine as well as they are not aware of the cybersecurity risks in case they are not familiar with the principles of safe cybersecurity practices rendering them the weakest link in a cybersecurity attack.

Considering the aforementioned motivation and challenges, this work proposes a methodology that is presented as a software tool, named GTM. The latter exploits attack-graph and game theory methods to automatically provide cybersecurity defensive strategies, including security controls that can

mitigate the cybersecurity risk of an organization in a scenario agnostic manner (i.e., One organization with multiple attackers). More specifically, the attack graphs are used in GTM to shape all multi-stage attack paths. Each path portrays a collection of exploits that could be leveraged by an attacker to compromise a network. The interactions between the Attacker and Defender during a cybersecurity incident are treated as a zero-sum game, which is solved using the Nash equilibrium method. In particular, GTM achieves to sculpt the attackers' and defenders' behavior and their strategies. Moreover, the integration of GTM in an organization's working routine can facilitate CISOs to optimally allocate the limited cybersecurity budget to the most appropriate security controls based on the organization's needs.

8.2 Related Work

8.2.1 Optimal Budget Allocation

This section delves into the literature focusing mostly on the domains of optimal budget allocation and attack graphs, which are the two key domains that the proposed work combines.

Panaousis et al. [287] introduced a methodology to facilitate security managers performing an optimal cybersecurity budget allocation. The methodology begins by conducting a risk analysis of the organization's assets and analyzing the efficacy of various security controls against known vulnerabilities. Then, the authors calculate the most optimal way for an organization to implement each control based on control games. The control game is a method to assist a defender to reduce cybersecurity risks by adopting a game-theoretic approach based on Nash Equilibrium that decides how a control will be implemented. The authors treat the problem of the optimal allocation of a cybersecurity budget as a multi-objective Knapsack problem. Finally, to implement the proposed methodology, a case study of an SME has been considered employing 12 of the topmost dangerous vulnerabilities from the 2011 CWE/SANS report[1] as well as 6 critical security controls published by the Council on Cybersecurity[2].

An extension of [287] presented in [210], where Fielder et al. proposed a

[1] http://cwe.mitre.org/top25/

[2] http://www.counciloncybersecurity.org/attachments/article/12/CSC-MASTER-VER50-2-27-2014.pdf

two-stage model to aim security professionals with decisions considering the optimal cybersecurity budget allocation. The authors begin by formulating the environment, where the cybersecurity investments will occur, identifying the targets that an attacker has as well as the defenses of these targets. The environment was later deployed to define control games based on Nash equilibrium. To conclude the optimal budget allocation the problem was formalized as a multi-objective Knapsack problem. The proposed model was compared with two alternative methods, namely with two scenarios that aim to enhance the defense using direct costs and indirect costs. Finally, the authors highlight the impact that indirect costs have on the cybersecurity budget allocation problem.

Towards this direction, Panda et al. [281] focus on the optimal selection of cyber-hygiene controls to minimize the risk of cyberattacks. To achieve their goal, a tool for the optimal selection of safeguards has been proposed, which combines game theory and combinatorial optimization considering the attack probability, the asset value, and the efficacy of each control. In [288], Wang introduced an analytical framework for organizations to improve their cybersecurity and cyber-insurance investments. The framework is based on analytical models to quantify the effect of security investments in tackling cyber threats, vulnerability, and impact on the budget. A limitation of this work is that the organizations need to evaluate their security investment in a long-term multi-period.

Another recent work that focuses on the budget allocation for data privacy protection is proposed in [289]. Particularly, the paper focuses on the improvement of the privacy budget allocation in differential private clustering algorithm DPk-means by introducing a new algorithm named APDk-means, which is based on arithmetic progression privacy budget allocation. The novelty of APDk-means is that it achieves rapid convergence in early iteration by decomposing the total budget into a decreasing arithmetic progression to distribute the privacy budgets from large to small in the repetitive procedure. The evaluation showed that APDK-means accomplished better availability and quality performance and the same privacy protection level in comparison with other deferentially private k-means models.

Previous works that focus on cybersecurity budget allocation mostly focus on a scenario where an attacker has a single target in an organization, neglecting to consider attackers with multiple targets. An attacker that aims to exploit multiple assets represents a more realistic threat scenario for an organization, hence the applicability of these works to real-life situations is

uncertain. GTM addresses this gap by integrating a game-theoretic approach with attack graphs to optimally allocate the cybersecurity budget considering multiple attacks.

8.2.2 Attack Graphs

The generation of attack graphs is a technical approach that demands the collection of assets and vulnerabilities. We can observe that with the increasing number of cyberattacks and the fact that vulnerabilities threaten more than one asset, the complexity of an organization's topology increases exponentially. The automatic generation of attack graphs can be broadly classified into four categories [285], as highlighted below:

1. **Enumeration Based:** The nodes display the condition of the network during an attack, as well as the entities that are participating in the cyber attack.

2. **Topological vulnerability analysis (TVA):** It concentrates on the system's vulnerabilities. The attacker's options for compromising the targeted network assets are then defined after the found vulnerabilities have been analyzed.

3. **Network Security Planning Architecture (NetSPA):** It analyzes the network topology identifying the most critical attack pathways. It is a multi-prerequisite graph with nodes for the state, preconditions, and vulnerabilities allowing the network owner to locate and rectify the network's most vulnerable aspects.

4. **Logic Programming:** It demonstrates the logical relationships between attack objectives and configuration information. Multi-host, Multi-stage, Vulnerability Analysis Language (MulVAL) [290] is a well-known tool that is based on this approach. MulVAL adopts the Datalog modeling language to analyze the elements of a network leveraging existing vulnerability DBs (e.g., NVD) and scanning tools.

Wang et al. [286] developed a framework to link vulnerability analysis with risk assessment. The framework is based on attack graphs to represent network assets and vulnerabilities and Hidden Markov Models to capture the uncertainties of those explicit observations and estimate attack states, which

vary based on the cost that is related to possible attacks and countermeasures.

In [285] the authors proposed a methodology based on probabilistic attack graphs to objectively measure the security risk of organizations. The authors deployed MulVAL for the generation of attack graphs and the CVSS standard to assess the severity of the vulnerabilities.

Kotenko et al. [291] presented and demonstrated a case study risk assessment technique that is based on attack graphs to be implemented in SIEMs. The crux of this work is the developed metrics taxonomy that considers the latest trends in the security metrics domain, the translation of attack steps to attack graphs, and the purposes and results of SIEMs.

The authors in [292] focus on game-theoretic security investments of multiple interdependent assets. The interdependencies between the assets have been modeled using attack graphs, where the edges linking two assets (vertices) contain the probability of a successful pivot. The authors concluded that the human decision-making process (based on the behavioral probability weighting) can have a significant effect on interdependent systems' security.

The article in [293] utilizes attack graphs to elaborate on the attack prediction. To attain their goal the authors first identify all the possible attack paths and then deploy the attack paths combined with common vulnerability data for future attack prediction. The efficacy of the method is evaluated on real data from a maritime supply chain infrastructure showing that is both practical and effective.

An extension of MulVAL [290], which is a popular tool for attack graph generation (see section 8.3.2), proposed in [294] to support network protocol vulnerabilities and support advanced communication types. Particularly, this work considers the physical network topology, implements short-range communication protocols, models vulnerabilities of network protocols, and considers particular industrial communication systems. The authors demonstrate that their extension can model several well-known network attacks, such as spoofing, man-in-the-middle, and DoS as well as attacks on industrial communication systems.

Attack graphs have been proved to be very effective in vulnerability detection and attack prediction domains. However, previous works did not deploy attack graphs on the optimal budget allocation domain. Thus, in this paper, the effectiveness of attack graphs has been exploited to predict all the possible attack scenarios on an organization and conclude the best allocation of the budget to enhance the resilience of the organization against

cyberattacks.

8.3 GTM

8.3.1 GTM Overview

The proposed cybersecurity investment tool, named GTM, aims to greatly facilitate from top to bottom members of cybersecurity Blue and Red Teams, including but not limited to CISOs, C-Suite executives, Security and Information Technology Analysts, Board of Directors of an organization and Security Researchers. To assist the reader to understand the presented notions, CISO is assumed as the end-user of GTM; however, we avoid analyzing CISO's responsibilities and requirements since it is out of the scope of this work. Through GTM, all possible attacking scenarios will be predicted by employing attack graphs, and then utilizing game-theoretic techniques optimal defending strategies will be proposed achieving optimal cybersecurity budget allocation for cybersecurity risk mitigation.

As shown in Figure 8.1, the general structure of GTM is divided into three main modules: i) the Attack Graph Engine; ii) the Data Pool, and iii) the Defense Strategy. The **Attack Graph Engine** as its name implies is responsible to generate attack graphs that model all possible attacking scenarios and paths of an organization. It receives as input a vulnerability assessment report that is the output of a vulnerability assessment tool (e.g., Nessus [295]). The **Data Pool** contains numerous guidelines, laws, and reports related to cybersecurity and privacy, which are used to defend organizations against cyber attacks. In addition, it is utilized as a database and is enriched with new input by CISOs whenever it is necessary (e.g., when a new cybersecurity incident occurs). Finally, the **Defense Strategy** is the most important pillar of GTM as it is responsible not only to calculate the expected loss but also to choose the most appropriate cybersecurity controls optimally allocating the limited cybersecurity budget. In particular, it simulates cyber attacks following the game theory and random attacker's profile to calculate the probability of occurrence of any cyber attack leading to the optimal budget allocation.

The game-theoretic approach that is implemented in the Defense Strategy is scenario agnostic. This characteristic is inherited by the zero-sum game; GTM is capable to support games that include one organization as the De-

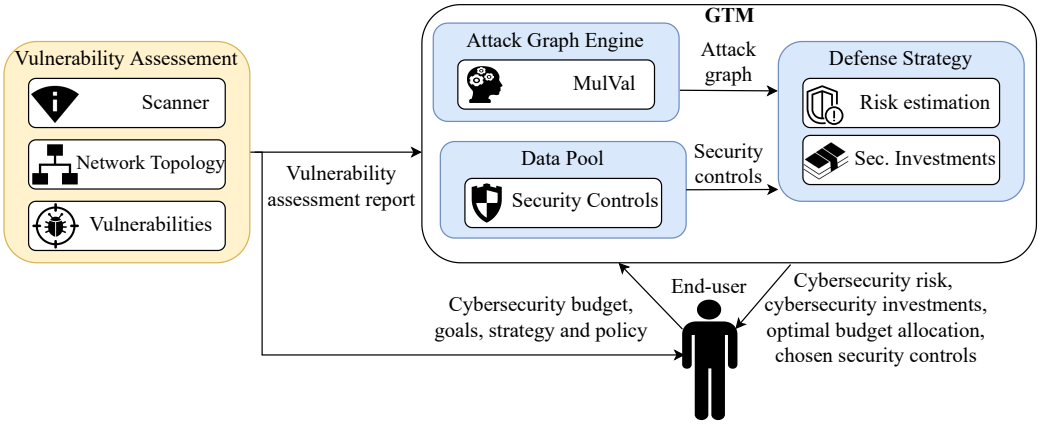


Figure 8.1: GTM blueprint

fender and multiple opponents as Attackers. With such an approach, CISOs can utilize GTM in numerous attacking scenarios, where attackers have at least one target to compromise. Also, GTM stands not only against technical vulnerabilities (e.g., CVEs) that usually could be mitigated following patching approaches provided by vendors, but also against physical and environmental vulnerabilities (e.g., air-conditioning failure) that are also able to lead to catastrophic consequences affecting business continuity.

8.3.2 Attack Graph Engine

GTM has been equipped to construct attack graphs with the commonly used Multi-host, Multi-stage Vulnerability Analysis Language, often known as MulVAL, which is a Logic Programming attack graph tool [290]. The produced graph (see Figure 8.2) is comprised of nodes that represent logical propositions, and it requires that the source of an attacker's potential privileges be expressed as a propositional expression in terms of network configuration parameters. In a MulVAL graph (see Figure 8.2), a rectangle represents the current state of the system, whether it is an antivirus defending a specific host or the presence of a threat. Additionally, the circular one denotes the pre and post-conditions of an attack being connected with diamond shapes. The latter depicts the attacker's potential advantage.

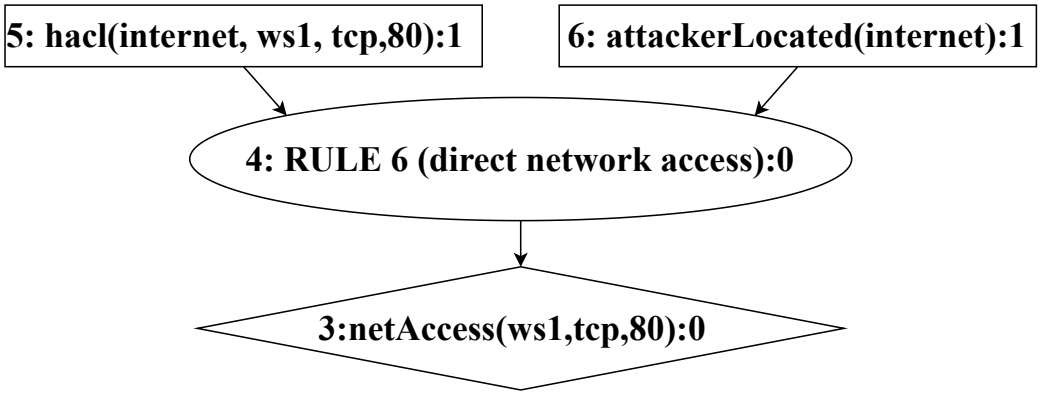


Figure 8.2: Toy-example of a MulVAL attack tree

GTM has the following requirements regarding the utilized attack graph approach: i) being open-source; ii) limited complexity, namely, an attack graph should scale well regardless of the size of the organization network; iii) scalability to Small Office/Home Office (SOHO), a situation that became norm and trend for many professionals due to the working from home situation as a result of COVID-19; iv) the applicability to Small Medium Enterprises (SMEs) since this type of organization is the backbone of Europe's economy [296], and v) the applicability to Large Enterprises (LE) since LE might be susceptible to a large number of vulnerabilities (e.g., CVE) due to the number of devices and application they include to their daily working-routine [8]. Figure 8.3 compares the attack graph generation approaches analyzed in Section 2 against the aforementioned features. For the comparison, we replaced enumeration-based attack graphs approach, since it has been considered as obsolete, with the Attack Graph Toolkit [297] that creates attack graphs and is the closest to the enumeration-based approach architecture. The Attack Graph Toolkit and MulVAL are open-source and available for free. The most efficient complexity can be found by NetSPA. The Attack Graph Toolkit can handle SOHO environments, its scalability in an SME environment depends on the number of assets; however, it is a suitable approach for an LE environment. The performance of TVA depends on the number of the identified assets regardless of the working environment. NetSPA and MulVAL can scale well regardless of the working environment. Overall, the most appropriate methods for GTM are NetSPA and MulVAL;

however, GTM integrates MulVAL due to its open-source characteristic.

Attack Graph Approach	Open-source	Scalability	SOHO	SME	LE
Attack Graph Toolkit	✓	Exponential	✓	# assets	✗
TVA	✗	$O(N^3)$	# vulnerabilities	# vulnerabilities	# vulnerabilities
NetSPA	✗	$O(NlogN)$	✓	✓	✓
MulVAL	✓	$O(N^2) \sim O(N^3)$	✓	✓	✓

Figure 8.3: Comparison of Attack Graph Approaches

8.3.3 Defense Strategy

Risk estimation

As previously stated, attack graphs are constituted of nodes and edges that depending on the graph creation method used, provide a distinct interpretation of the current state of the system. In most cases, attackers exploit these stages as a launching pad to infiltrate their intended target. After figuring out these flaws, a CISO has to decide which defense mechanisms are most important for the network. In this section, a method for evaluating the nodes and possible controls has been provided that will eventually compose an effective network defense.

GTM aims at estimating the expected loss L of an organisation as well as to assist in acquiring an optimal selection of safeguards using game theory. We denote $\mathcal{A}$ the set of assets, which belongs to an organisation $\mathcal{O}$ and express each asset as a, where $a \in \mathcal{A}, \mathcal{A} \in \mathbb{Z}_n^+$. Each asset a is characterized by an impact value I_a, which is displayed in monetary units. The value of I_a is defined by CISO's organization and derives from a Business Impact Analysis (BIA). We express P_a as the probability of occurrence of a threat to a specific asset a, where $P_a = [0, 1]$; $P_a \in \mathbb{R}$ [298], also, denote the probability of a successful exploitation of a cyber attack to an asset a as $R_a = [0, 1]$; $R_a \in \mathbb{R}$ [299]. We measure the expected loss L using the commonly-used risk assessment equation containing the likelihood of a threat event's occurrence (P_A), the likelihood of successful exploitation of the target (P_{SA}), as well as

the potential impact of the successful exploitation (I) [300], as it is displayed in Equation 8.1.

$$L = P_A \times P_{SA} \times I \tag{8.1}$$

In GTM the total expected loss is calculated based on threats that may occur to the assets. We assume that each asset is connected with numerous threats. GTM defines the expected loss that derives from the Equation 8.1 expressing it in monetary units, achieving a quantitative result. Hence, the total expected loss L is given by the sum of the maximal expected losses [301]. The L_a expresses the expected loss associated with a specific asset a. Moreover, we define the $L_{a,i}$ as the expected loss associated with a specific asset a and a specific threat i, $i \in \mathcal{T}$, where $\mathcal{T}$ is the set of treats that can impact the organization $\mathcal{O}$. The total expected loss $L_{\mathcal{O}}$ of an organization is calculated as it is presented in the Equation 8.2.

$$L_{\mathcal{O}} = \sum_{a \in \mathcal{A}} L_a \tag{8.2}$$

However, to integrate the defensive approach in GTM, we take into consideration the parameter $\mathcal{S}$ that represents the level of security provided by a defensive approach. It is calculated by $\mathcal{S} = 1 - e$, where e expresses the efficacy of the implemented control. Finally, the total cybersecurity expected loss is calculated based on the Equation 8.3.

$$L_{\mathcal{O}} = \sum_{a \in \mathcal{A}} L_a = \sum_{a \in \mathcal{A}} I_a \prod_{i \in \mathcal{T}} P_{i,a} \times R_{i,a} \times S_{i,a} \tag{8.3}$$

Security Investments

CISOs can integrate into GTM security controls to defend against an Attacker, who acts based on a game-theoretic approach. This is represented as a game between two players, the Defender and the Attacker [302]. On the one hand, the Defender chooses the security control that will be implemented on a specific asset; however, the integrated security control does not provide full protection against all threats. The game that is created in GTM is a zero-sum game that is solved using the Nash equilibrium approach. Since, if one player loses, the other party wins, and the net change in wealth is zero. For instance, if an attacker achieves to compromise the organization's network then he will win and get benefited from the loots; however, the organization will lose wealth including assets (e.g., confidential data), money

and reputation. On the other hand, the Attacker chooses to attack a specific asset a that she assumes to be more susceptible to specific vulnerabilities. The Attacker is in a dilemma without knowing the next attacking step (e.g., exploiting a vulnerability) which is depicted by the attack graph by splitting into more than one discrete path. In particular, the game-theoretic approach has a close connection with the probability of occurrence of an attack. In this paper, we will determine the occurrence probability of a threat as the attacker's payoff considering that is equal to the vulnerability's CVSS [303] score. CVSS stands for Common Vulnerability Security Score, and has been chosen since it depicts how a vulnerability (CVE) can be exploited (i.e., attack vector, attack complexity, privileges required, user interaction) as well as how its exploitation impacts the organization (i.e., confidentiality impact, integrity impact, availability impact). On the one hand, the Attacker's payoff is considered the CVSS score. On the other hand, the Defender is divided into two discrete instances: i) the first one is the Defender, who does not implement any security control, then his payoff is equal to the negative CVSS score and ii) the second one is the Defender who implements security controls, then his payoff is equal to the aggregated result of CVSS score and the cost that is required to implement the security control.

During the integration of each security control, there will be an economic influence (e.g., cost) on the organization. The cost can be categorized as followed: i) in *Direct Cost* that is a one-time investment that is required for the control to be purchased and ii) in *Indirect Cost* that is not directly accountable to a cost object (e.g., maintenance issues). Security control usually fall into both categories. A control commonly requires a direct cost for its purchase as well as an indirect cost for its maintenance; the total cost of a security control can be calculated by Equation 8.4.

$$Cost_{total} = Cost_{direct} + Cost_{indirect} \tag{8.4}$$

The last feature of GTM is the optimal allocation of a limited budget. To achieve it, GTM utilizes the 0-1 Knapsack problem. The latter is a combinatorial optimization problem in which we must identify the combination of items that will generate the highest value within a specific total weight limit, given a collection of objects each with a weight and a value. However, when it comes to network security, the method differs according to resource interaction and the degree to which resources are divided equally among the targets. The 0-1 Knapsack problem integrated with GTM consists of two parameters: i) the Weight that is equal to the loss that occurred to the system

due to the exploitation of a specific vulnerability (i.e. CVE) and is calculated based on Equation 8.3 and ii) the Cost that depicts the total costs of security control, it is calculated based on Equation 8.4.

8.4 Case Study

In this section, we aim to examine the applicability of GTM to three discrete case studies: i) the first case study represents a SOHO that seeks a defensive strategy against an Attacker who has only one target; ii) the second case study represents an SME that aims to protect itself against an Attacker who has multiple targets (e.g., multiple assets of the SME), and iii) the third case study refers to an SME that aims to find a strategy to protect itself not only from technical vulnerabilities but also from vulnerabilities that impact its physical and environmental security. The experiments were performed in an Ubuntu 18.04 desktop PC equipped with a Quad-Core Processor at 3.2GHz (AMD Ryzen 5 1400) and 8GB RAM. For the implementation of GTM, we have developed our code in Python language. The main goal of our experiments is to determine that GTM can effectively work in numerous different working environments.

8.4.1 Attacker with one target

This case study as it is shown in Figure 8.4 consists of two discrete paths. The attacker aims to remotely install a Trojan horse on the file server. Each node represents a system vulnerability that can be exploited by the Attacker, it also can be partially protected and prevented by implementing certain countermeasures by the Defender. We assume that the CISO has to handle a budget of the 100 monetary units, the efficacy on each node has been set at 0.5. Moreover, the following costs have been set for the security controls of each node to prevent a post-condition step: $C_{(b,c)} = 40$, $C_{(c,d)} = 20$, $C_{(d,f)} = 5$, $C_{(b,e)} = 60$, $C_{(e,f)} = 35$ and $C_{(f,g)} = 120$. Furthermore, the probability of an attack to be successfully executed has been befined as follows, $P_{(b,c)} = 0.64$, $P_{(c,d)} = 0.51$, $P_{(b,e)} = 0.64$, $P_{(e,f)} = 0.51$ and $P_{(f,g)} = 0.53$. At this point, it should be noted that the aforementioned values are arbitrary. The participants of this case study are the following: i) Game Theory attacker: he has a specific attacking strategy targeting every time the most

Table 8.2: Single Target

	Game Theory Attacker	**Disorderly Attacker**
GTM	Total Success: 191 3.19%	Total Success: 156 2.6%
No Sec. Control	Total Success: 756 12.6%	Total Success: 539 8.99%
Randomized	Total Success: 373 6.22%	Total Success: 247 4.65%

vulnerable and susceptible node; ii) Disorderly attacker: he has no attacking strategy and every time hits randomly a node; iii) No security controls: the organization does not implement any security controls; iv) GTM Security Controls: the organization follows all the GTM suggestions and aims to protect its infrastructure by integrating an approach followed by a Game Theory attacker and v) Randomized Security Controls: follows only the 0-1 Knapsack problem and randomly implements security controls. Furthermore, the following experiments have been performed: i) Game Theory attacker VS No security controls; ii) Game Theory attacker VS GTM Security Controls; iii) Game Theory attacker VS Randomized Security Controls; iv) Disorderly attacker VS No security controls; v) Disorderly attacker VS GTM Security Controls and vi) Disorderly attacker VS Randomized Security Controls. Each experiment was executed 6000 times. The results are presented in Table 8.2.

On the one hand, GTM decides to protect the following paths: BE, EF, and DF (see Figure 8.4). On the other hand, the randomized approach protects all nodes apart from path BE. In this case study, GTM and the randomized approach spent the whole budget (100%). GTM combining the game-theoretic approach and the 0-1 Knapsack problem mitigates the cybersecurity risk more than the other approaches. Overall, the GTM protected fewer paths than the randomized approach achieving a higher level of security.

8.4.2 Attacker with multiple targets

In this case study, the results of networking scanning and penetration testing of an e-shop have been utilized for the attack graph generation. The aforementioned data was provided voluntarily by a colleague who serves as CISO in this specific e-shop. The Attacker aims to achieve DoS or SQL injection or

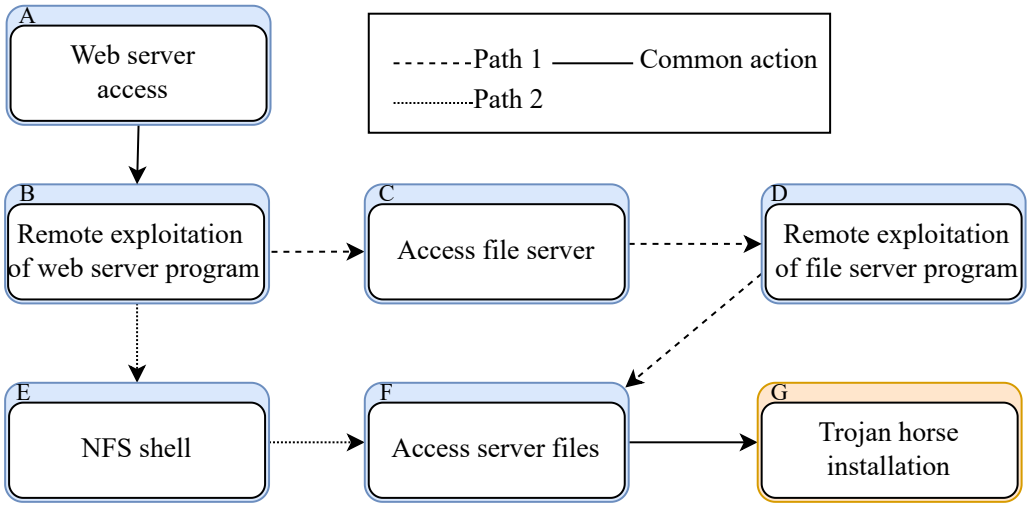


Figure 8.4: Single Target

remote code execution or install and run a malicious program to the Apache server (see Figure 8.5). The budget is set at 100 monetary units. The CISO informed us that the impact of a DoS costs 370 monetary units, the impact of SQL injection costs 490 monetary units, the remote code execution costs 550 monetary units and the execution of a malicious program is 440 monetary units. The probability of an attack to be successfully executed has been defined as follows, $P_{(A,t_1)} = 0.16$, $P_{(A,t_2)} = 0.24$, $P_{(B,t_1)} = 0.8$, $P_{(B,t_2)} = 0.7$, $P_{(B,t_4)} = 0.7$, $P_{(C,t_1)} = 0.6$, $P_{(C,t_2)} = 0.36$, $P_{(D,t_2)} = 0.54$ $P_{(D,t_3)} = 0.2$ and $P_{(D,t_4)} = 0.16$ (see Figure 8.5); the aforementioned are arbitrary values provided by the CISO based on his experience. Also, the following participants have been defined: i) Game Theory attacker: he has a specific attacking strategy targeting every time the most vulnerable and susceptible node; ii) Disorderly attacker: he has no attacking strategy and every time hits randomly a node; iii) No security controls: the organization does not implement any security controls; iv) GTM Security Controls: the organization follows all the GTM suggestions and aims to protect its infrastructure by integrating an approach followed by a Game Theory attacker and v) Randomized Security Controls: follows only the 0-1 Knapsack problem and randomly implements security controls. Furthermore, the following experiments have been performed: i) Game Theory attacker VS No security controls; ii) Game

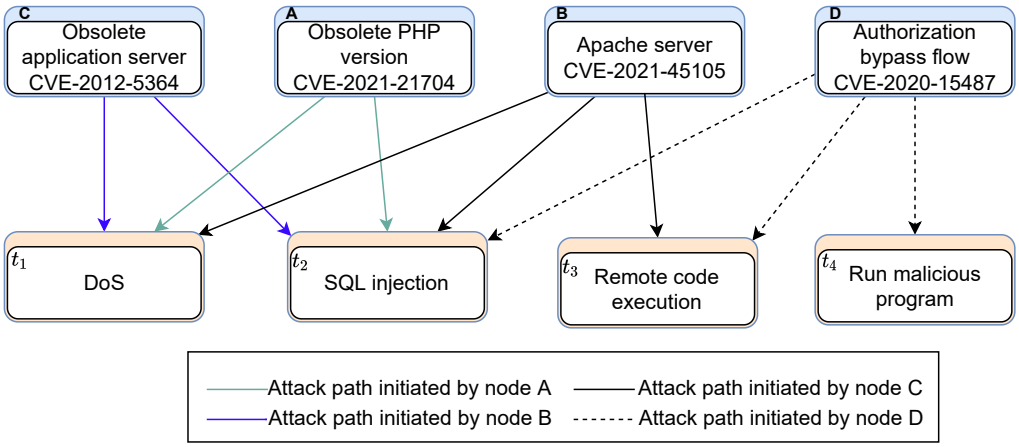


Figure 8.5: Multiple Targets

Theory attacker VS GTM Security Controls; iii) Game Theory attacker VS Randomized Security Controls; iv) Disorderly attacker VS No security controls; v) Disorderly attacker VS GTM Security Controls and vi) Disorderly attacker VS Randomized Security Controls. Each experiment was executed 6000 times. The results are presented in Table 8.3.

On the one hand, GTM decided to protect the paths generated by the attacking source (node) B spending 85% of the budget. On the other hand, the randomized approach protected the paths generated by attacking source A, C, and D spending the whole budget. One can observe that GTM provides the best strategy for the mitigation of the cybersecurity risk, namely, it decreases the cybersecurity risk more than the other approaches. In summary, GTM spent less part of the budget than other approaches to achieving a better security level.

Table 8.3: Multiple Targets

	Game Theory Attacker	**Disorderly Attacker**
GTM (cost 85)	Total Success: 1,500 25%	Total Success: 1,444 24%
No Sec. Control	Total Success: 2,977 49.6%	Total Success: 2,689 44.8%
Randomized (cost 100)	Total Success: 1,782 29.7%	Total Success: 1,384 23%

Threat (i)	Vulnerability	R_i	P_i	Impact	Control	Control Efficacy	Control Cost
Compromised server	No PenTests	M	M	100000	PenTest	0.8	50
Unauthorized network access	No PenTest	M	M	15000	PenTest	0.9	
No replacement for IT admin	SPoF	H	L	250000	Hire replacement	0.9	85
No replacement for IT admin	SPoF	H	L	250000	Outsource the duties	0.7	70
Air condition failure	No generator/UPS	H	M	30000	Provision of generator/UPS	0.9	20
Compromised DB	Obsolete OS	H	M	30000	Server Mitigation	0.8	35
Compromised DB	Obsolete OS	H	M	30000	Move to isolated network zone	0.3	10
Malware infection	No endpoint AV and admin rights to developer PCs	M	M	100000	AV	0.9	25
Fire in the server room	No fire detectors	M	L	100000	fire detectors installation	0.7	10
Data exfiltration	No DLP	H	M	40000	DLP provision	0.9	25
SQLi	CVE-2021-44832	H	H	15000	Security Updates	0.7	
DoS	CVE-2021-44832	H	H	12000	Security Updates	0.7	20
RCE	CVE-2021-44832	M	H	20000	Security Updates	0.7	
Unauthorized entry	No access control	H	M	15000	Access Control	0.8	35

Figure 8.6: Risk assessment report

8.4.3 Technical, physical and environmental vulnerabilities

It is known that the real cost that is spent for cybersecurity is not limited to the technical vulnerabilities (e.g., CVEs) but it includes also physical and environmental vulnerabilities [79]. The CISO of the aforementioned e-shop, informed us that the security budget will not be allocated only in CVE patching processes (because in the majority of cases the CVE-patching is completed through updates and is part of indirect costs), but in activities including but not limited to increasing the awareness of the employees, equipment protection, and operational security (e.g., CRM, ERP). This can be verified by the ISO 27001:2013 [304] that obligates prominent certified organizations to meet specific security requirements, e.g., phishing campaigns against the employees per year, implementation of CCTV, and access control mechanisms in the organization's infrastructure. The CISO provided us with the risk assessment report that is depicted in Table 8.6. The report contains the threats and vulnerabilities that an attacker can exploit, the probabilities of occurrence and exploitation, as well as the impact values describing the organization's damage in monetary units in case of occurrence of each threat. The probabilities have been estimated in qualitative values ($\underline{M}$:Medium - $\underline{L}$:Low - $\underline{H}$:High). Also, the threats that are incorporated in this use-case have been qualitatively predicted ($\underline{L}$: Low occurrence -$\underline{M}$: Medium occurrence - $\underline{H}$: High occurrence) instead of quantitatively. Furthermore, there is a match between threats and controls, together with the efficacy and the cost of the control. However, this case study is not a game between an Attacker

and a Defender, since the SME has to defend against numerous threats instead of a single adversary aiming to compromise an organization, which is independent without interconnections among them.

In this case study, the CISO has to handle a budget that has been set at 100 monetary units. At this point, the GTM via the 0-1 Knapsack algorithm, a pillar of the proposed methodology, chooses to implement the replacement of the IT administrator and install fire detectors spending 95% of the budget. These situations cannot be modeled using game theory due to its incapability to handle complex factors and situations.

8.5 Conclusion

This paper introduces a methodology developed as a software tool has been presented, named GTM. GTM proposes game-theoretic investment strategies against different types of attackers (namely, game-theoretic and disorderly) and is applicable to various scenarios with one or multiple attacking targets. The evaluation of GTM concluded that the beneficiaries are able automatically to create defensive strategies that can effectively operate in various scenarios.

At the core of GTM lies the Game Theory approach based on Nash equilibrium, which when combined with a manual input, regarding the occurrence and exploitation probabilities, from the user (CISO) it can predict an attacker's behavior. As the number of security incidents and challenges is rising, more security vulnerabilities are emerging, creating a fertile surface for adversaries to exploit them for their benefit. GTM can facilitate CISOs' by providing smart defensive strategies which have as main goal to achieve the maximum security level with the minimum budget. The budget is optimally allocated to the nodes that play a key role in a cyber attack.

The outcomes of this paper can be used as the basis for future work in a variety of ways. Particularly, GTM has been developed as a prototype for Linux-based environments for the presented proof-of-concept implementation. Next, we plan to implement the GTM for Windows-based environments removing environment-related barriers, as well as we aim to calculate the return of investment of each node and their interdependencies. Consequently, we intend to integrate the Best-First search algorithm to select the path that is most profitable. We aim to develop an Ant Colony Optimization algorithm populating the most significant system vulnerabilities. Finally, future work

will focus on the GTM's assessment against an attack graph that represents an LE that handles a complex scenario including numerous attackers and numerous targets in one game.

Chapter 9

BRIDGE: BRIDGing the gap bEtween CTI production and consumption

Security for businesses and organizations is essential to protect operational activities, trust relationship with clients and financial viability. Increased interest for research concerning cybersecurity issues has been shown recently, while at the same time professionals of this sector are employed to ensure safety. In turn, the efficacy and performance of both the researchers and professionals rely on the information provided by Cyber Threat Intelligence infrastructures. Automation of procedures regarding the collection, harmonization and processing of information is of utmost importance for Cyber Threat Intelligence, in order to effectively relay to the community data concerning newly emerged threats. Nevertheless, the process regarding the transfer of knowledge between Cyber Threat Intelligence and cybersecurity specialists is based on frameworks and procedures that are not in line with the needs and standards of modern times, being performed through obsolete methods and manual labor. In this chapter, BRIDGE, the first tool that streamlines the flow of intelligence between Cyber Threat Intelligence and cybersecurity professionals, by taking advantage of the Structured Threat Information eXpression standard, utilizing blockchain technology and automatically converting the intelligence needed in the form that researchers and other professionals require. Our experimental results demonstrate the efficiency of BRIDGE in terms of swiftness and performance improvement compared to the mainstream approach.

Authors	Title	Venue
Karatisoglou M, **Farao A**, Bolgouras V, Xenakis C	BRIDGE: BRIDGing the gap bEtween CTI production and consumption	COMM 2022, IEEE $[Rank : B]$

Table 9.1: List of thesis' publications- Part I

Table 9.1 summarizes the scientific publication related to this chapter.

9.1 Introduction

Threat intelligence is rapidly becoming a priority for businesses and organizations across the globe, due to the continuously emerging modern cyberattacks and their sophistication level [8]. Malicious actors performing criminal activities in the cyberspace showcase exceptional skills in their tactics, techniques and procedures, thus it becomes exceedingly difficult and challenging for cybersecurity professionals to investigate and intercept their activity [49]. Cybersecurity researchers and professionals working in environments like the Security Operations Centers (SOCs) [305] are employed in order to find ways to mitigate threats and monitor large amounts of data pertaining to organizations' infrastructures. To that end, cybersecurity tools like firewalls, intrusion detection and prevention systems and Security Information and Event Management systems (SIEMs) are utilized.

To battle the never-ending stream of newly emerged cyberattacks and swiftly update the network among the cybersecurity professionals, Cyber Threat Intelligence (CTI) programs are being widely employed [306]. Through CTI, the community can be up to date regarding existing threats and attacks that have already taken place at least once, giving them the ability to proactively mitigate advanced threats. CTI is a fundamental concept that exists since the early days of cybersecurity's adoption by numerous organizations and institutes, which has evolved according to the advancements that have occurred in this sector. The large scale security event data that is created, the need for swift analysis and processing of intelligence and the never ending growth of the threat landscape, has resulted in the automation of almost all the CTI procedures - intelligence gathering, processing of information and harmonization of reporting.

While CTI infrastructures are vital for researchers and cybersecurity professionals to perform their duties efficiently and minimize risks, there are a few shortcomings[307]:

- CTI consumers (researchers, cybersecurity professionals e.t.c.) have access to intelligence that has been gathered, processed and reported by automated means, but still have to **manually** extract the information needed in order to use it for research or threat mitigation purposes.

- There has been a significant growth in the number of threat data sources, from which a CTI practitioner has to generate useful intelligence that can be used in decision-making processes. 70% of respondents in [308] declared that threat intelligence is too **voluminous and/or complex** to provide actionable intelligence. Unfortunately, companies are collecting massive amounts of data in a wide variety of different formats such as Structured Threat Information eXpression standard (STIX), JSON, XML,PDF, CSV, email without keeping a standard format hardening CTI consumers to manually processes and review the gathered data.

- Lastly, CTI consumers [305] in their effort to mitigate threats[309, 310] must control all the data created by the growing number of data locations and sources. This undertaking becomes increasingly complex because of the variety of security measures and tools utilized for this purpose. As a result, it is vital to establish standards and procedures that ensure **interoperability** among these components, facilitating security operations and response procedures throughout the whole security ecosystem.

We solve the aforementioned challenges with BRIDGE, a novel implementation and to the best of our knowledge the first effort to bridge the gap between CTI and its consumers, by automating the process of converting information stemming from CTI reports to the format needed by the researchers and cyber security professionals. Employing the STIX standard to store information at CTI reports, BRIDGE gives the ability to the CTI consumers to automatically apply the information provided on a variety of tools. No further manual input or modification is required. Moreover, the blockchain technology is also utilized to safely store in a single but decentralized repository all the CTI data, which gives the ability to the professionals

to easily monitor the information that is provided and ensure certain level of quality, as they are not required to oversee numerous repositories.

9.2 Background

This Section presents the CTI [311] concept and describes how cybersecurity researchers and professionals utilize the CTI infrastructure, improving the defense against threats.

9.2.1 The CTI concept

The implementation of CTI follows a defined lifecycle that consists of seven discrete phases: (i) requirements; (ii) collection, processing; (iii) analysis; (iv) dissemination, (v) consumption and (vi) feedback. This flow ensures that CTI actions are in line with the organization's goals and produce actionable data with the appropriate meanings. Following this lifecycle, an organization can achieve constant improvement, which is one of the most important aspects in order to keep the CTI productive and effective.

Requirements: Threat intelligence's initial phase is responsible to establish the goal and scope of all intelligence actions. Also, it identifies the information assets and business processes that need to be protected, alongside with the potential impacts of losing those assets or interrupting those processes. These have been prioritized according to what is more important to protect. Finally, this phase defines the possible attackers, their actions and their motivation.

Collection: Once the requirements are defined, the CTI team will seek to collect the required data to achieve those objectives. On the one hand, internal sources will be exploited such as metadata and traffic logs from internal networks and devices. On the other hand, external sources will be utilized such as scrapping and crawling dark web forums and open source intelligence databases, as well as human intelligence will be investigated [277].

Processing: Processing entails converting raw data, that came from the *Collection* phase, into a format suitable for further investigation and analysis, e.g., harmonization. Processors might be either humans or robots executing specific algorithms depending on how the data was collected.

Analysis: After the raw data is processed in the aforementioned step, the CTI team will undertake a comprehensive analysis to meet the goals set in the initial phase, also its outcome is a report summarizing the security data. In particular, artificial intelligence, data analytics and machine learning are utilized by the CTI team to make predictions and extract insights and patterns, to analyze raw data to make conclusions, as well as to predict and find representative values for the missing data

Dissemination: Dissemination entails delivering the completed intelligence product to the appropriate audience. First and foremost, this phase identifies the detected threats. Once the identification is completed the organization's cybersecurity status is evaluated and the most optimal strategies and security controls are proposed to strengthen the organization to defend future cybersecurity threats. The proposed security solutions include but are not limited to risk transfer, installation of security tools as well as compliance with standards [283].

Consumption: CTI consumers receive the data from the corresponding repositories, which then has to be processed in order to meet the requirements of the tools and technologies that will utilize it. This step can be time consuming and because of the lack of automated means, the manual process that is carried out may result in the corruption of information.

Feedback: This is the last phase, that is responsible to assess on a continuous basis the cybersecurity level of the organization as well as the performance of the implemented cybersecurity controls.

We can observe that CTI is not a process with start and end point, but it is a loop consisting of phases that feed off each other.

9.2.2 Related work

Numerous works related to the CTI concept are focused on the enhancement and improvement of the performance concerning the corresponding procedures followed by CTI producers. Like BRIDGE, automation of processes is the key for the majority of solutions which focus on many of the aforementioned phases. Below we mention indicatively some works that aim to automate CTI procedures.

For the collection of data, the authors of [312] propose an automatic approach to generate the CTI records, which is based on the Natural Language Processing (NLP) and machine learning concepts. Other efforts focusing

on the automatic collection and processing of can be found in the works of [313] and [314], where Indicators Of Compromise (IOCs) are extracted from the corresponding data. To both process and analyse the collected data, the authors of [315] propose a solution that processes Malware Information Sharing Platform (MISP) data automatically, prioritizes cybersecurity threats for Small and medium-sized enterprises (SMEs), and provides SMEs with actionable recommendations tailored to their context. On top of solutions like the ones mentioned above, in order to facilitate the automation of processes regarding the CTI, standardization efforts have been made. STIX [316], which is also utilized by BRIDGE, is considered the main standard that should be adopted in order to describe threat intelligence data and be used by threat intelligence sharing platforms [317].

All solutions regarding the automation of the procedures found in CTI's lifecycle focus on the phases of collection, processing and analysis of corresponding data. Regarding the Consumption phase of the produced intelligence there had been no efforts so far. This gap will be filled with BRIDGE, a solution that aims in automating the process of converting data that stems from CTI infrastructures to the form that each consumer needs it.

9.3 BRIDGE

9.3.1 Software architecture

BRIDGE aims to greatly facilitate from top to bottom members of CTI consumption ecosystem, including but not limited to SOC teams, Security and Information Technology Analysts (Sec/IT Analysts), Computer Security Incident Response Teams (CSIRT), Intelligence Analysts, Board of Directors and Security Researchers. Through BRIDGE, sharing CTI results among the aforementioned parties will result in establishing interoperability, maintaining the integrity of the produced CTI information and create the ideal conditions to effectively extract crucial intelligence.

As shown in Fig. 9.1 the general structure of the BRIDGE is divided into three main modules: i) the Parser; ii) the Translator, and iii) the Data Pool. We have to note that for demonstrative purpose and ease of understanding, BRIDGE is presented assuming that SOC teams will be the end consumers - however, we avoid analyzing SOC processes since it is out of scope of this work. The **Parser** module as its name implies, is responsible to receive the

CTI reports in STIX 2.1 [318] format standard generated by the corresponding team. The STIX 2.1 report is stored to the **Data Pool**. The latter is built based on blockchain technology and plays the role of the database providing the information system with immutability, integrity, transparency, and traceability of data shared across the organization network. We have to note, that each time the CTI team aims to store a report, a new block is added to the blockchain containing the information of the corresponding report. Then the **Translator** is getting requests from the organization SOC teams that manage different SIEM tools. Each SOC team requests from the **Translator** to get a CTI report, then a Sigma file is supplied describing the indicators found in the corresponding report. By utilizing Sigma files, which include Sigma rules, SOC teams are able to describe relevant log events in a flexible and standardized format. More specifically, the aforementioned report contains a description of the detection method that a SOC member should follow to detect the IOCs that are included in the CTI report.

The Sigma detection rule is vendor agnostic. With such a rule in arsenal, the SOC team can automatically generate a query to search for those indicators specifically crafted for the SIEM that they are using. Apart from the CTI report, the SIEM that the team uses for investigation can also be specified in the request. By supplying this, any actionable intelligence found in the form of indicators inside the report, will be returned inside a query for the desired SIEM.

9.3.2 Technical approach and methodology

In this section we analyze how BRIDGE operates providing a workflow that should be followed. In particular, BRIDGE consists of two discrete phases: i) CTI production and ii) CTI consumption.

The first phase entitled **CTI production** is responsible to receive the generated CTI report. First and foremost, the CTI team gathers intelligence about threat actors, cyberattacks and malware, which will be shared with SOC teams, and store them under STIX 2.1 format via the BRIDGE parser (see Fig. 9.1). A new block is added to the blockchain for every new report that is being published, maintaining its integrity while being available for all the legitimate members in the blockchain.

After the successful completion of the first phase (CTI production), **CTI consumption** is being performed by the SOC teams. The latter utilize various SIEM tools for event investigation. After the CTI report of interest

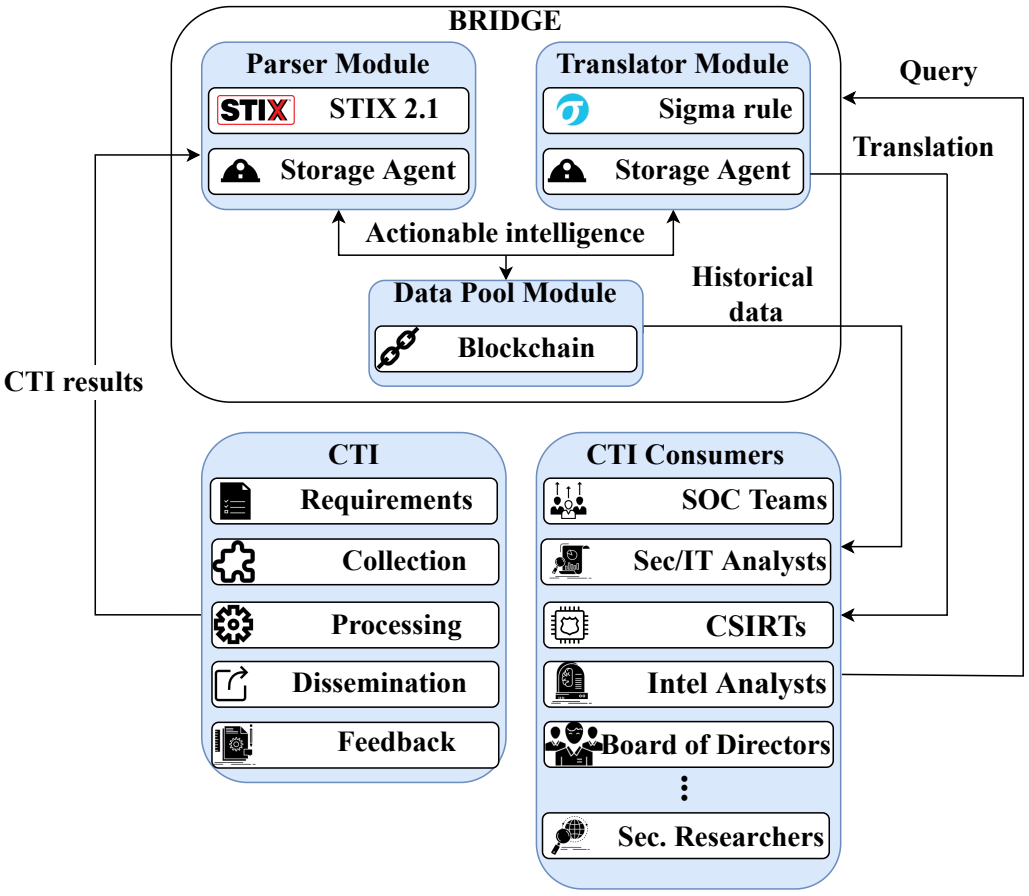


Figure 9.1: BRIDGE architectural components

has been found within the blockchain and the request to retrieve this report is being made, the CTI consumer is given the ability to select in which SIEM the threat intelligence will be searched upon. The key element of a CTI report is the IOCs that constitute it. Moreover, once the SIEM option is supplied, two more items will accompany the STIX report. The first one will be a Sigma rule that matches the IOCs inside the report, and the second one will be a text file containing the query that searches for those indicators for the particular SIEM.

Overall, after the CTI report has been delivered at the SOC teams, the latter not only have saved time creating SIEM queries automatically via

BRIDGE, but also human errors that can lead to malformed queries have been eliminated due to the acceleration that BRIDGE provides incorporating that Sigma. In addition, the involved analysts utilizing the BRIDGE tool are certain that the query matches all the IOCs in the CTI report since it has been created based on the Sigma rule containing the threat intelligence. Finally, multiple teams investigating the same incident that may work on different SIEM have overcome the interoperability issue.

9.4 Performance Evaluation

In this Section, we analyze the performance of the tool as a whole, investigating its feasibility and efficiency against incidents that come from real working environment. BRIDGE has been developed in Python (version 3.8.10) language, utilizes the CTI reports strictly following the STIX 2.1 language standard, version 2.1, finally the dedicated SIEM rule is generated by the sigma rule. The experiments have been conducted in a Ubuntu Desktop 20.04.4 being equipped with an Intel i5-10600K processor with 6 cores that support hyperthreading at 4.1 GHz, 16GB RAM and 500GB disk storage. By now, BRIDGE runs in Unix-based operation systems (i.e. Linux). We have conducted two experiments to evaluate BRIDGE efficiency and to compare its effectiveness against the method that is currently being used by the SOC teams, which has been chosen to represent the consumer of BRIDGE in our evaluation. SOC is among the top professional groups that will utilize the produced CTI reports (see Fig. 9.1), while at the same time they lack proper and automated bridge hub solution in order to fetch IOCs for their SIEMs. We have to note that the conducted experiments aim to evaluate the performance of BRIDGE's main modules; however, the blockchain component is utilized as a database and does not have any impact on the performance of the BRIDGE tool, which is evaluated after the data has already been fetched. Thus, no measurements regarding the blockchain infrastructure's performance were taken.

The first experiment aims to measure the time consumed solely for parsing the IOCs from a CTI report. In particular, we generate one query for the Splunk SIEM [319] that is executed many times against one CTI report. Each query fetched 414, 828, 1656, 3312, 6624, 13248 and 19872 IOCs. The experiment was conducted 5 times. The produced results revealed that our tool required less than a minute to fetch thousands of IOCs from one CTI

report (see Table 9.2). The same experiment has been conducted by the assistance of 10 professional cybersecurity analysts, who are members of SOC teams (they voluntarily participated). They executed one query to the CTI report (used before) fetching 5, 10, 15 and 20 IOCs (see Table 9.2). The comparison proved that the traditional way that SOC teams process their daily routine has became rigid, while the cybersecutiy needs are in rise; however, our implementation is able to fight this rigid way providing effectiveness and speed maintaining the quality that is required in these critical tasks.

Table 9.2: Fetching numerous IOCs of one CTI report

Evaluated method	**# of IOCs fetched per query**	**Time (sec.)**
BRIDGE	414	0.01
	828	0.04
	1656	0.08
	3312	0.16
	6624	0.33
	13248	0.68
	19872	0.91
Traditional SOC method	5	70.2
	10	182.4
	15	247.2
	20	274.2

For the second experiment completion, we used one CTI report with many IOCs and executed numerous queries at the same time for 4, 8, 12, 16, 20, 24 and 28 different SIEM tools. Each query fetches the same 44 IOCs (see Fig. 9.2). Also, the experiment was conducted 5 times. We can observe that time needed to create queries for different SIEM fetching standard number of IOCs increases linearly. Overall, we can validate that the time consumed for parsing the numerous IOCs for a specific SIEM is negligible compared to the time needed to generate the SIEM queries manually. Also, we can observe that BRIDGE performs better when requesting multiple indicators on a single SIEM query rather than requesting queries for multiple SIEMs.

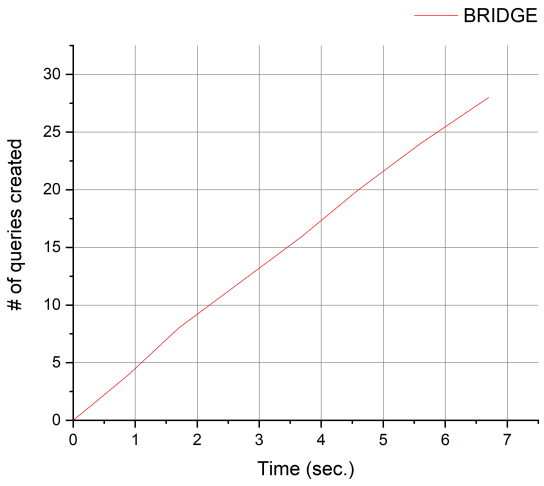


Figure 9.2: Fetching numerous queries for numerous SIEM tools

9.5 Conclusions

In this paper we presented the first CTI sharing tool, which is focused on the automation of the information consumption phase, specifically designed for cybersecurity professionals and practitioners. Evaluating BRIDGE, we have proven that the beneficiaries and especially *SOC* teams can take advantage of BRIDGE to automatically create queries for their SIEM and at the same time eliminate human errors, enable interoperability via the STIX format and Sigma rules, and establish a transparent method for managing security incidents. The aforementioned benefits are only the technical advantages that follow BRIDGE; however, the integration of BRIDGE to the arsenal of CTI consumers can also increase the quality of security decisions taken from them.

At the core of the BRIDGE tool we find the integration of STIX standard, which offers indisputable interoperability and creating a common expression within the CTI ecosystem. Having designed and developed the BRIDGE tool, we quantitatively evaluated its performance and proven that it is able to successfully cope with the current issues that SOC members meet in their working routine. As the number of security incidents and challenges are in the rise, more security information will be produced by the CTI mechanism and new SIEM tools will emerge. Our belief is that the BRIDGE

research outcomes will pave the way for a CTI ecosystem armed with a unified expression to fight back and defend against various critical cybersecurity threats. We also expect that BRIDGE will be the precursor for an automated CTI ecosystem being able to address the numerous cybersecurity threats that daily emerge. Additionally, more Threat Intelligence Sharing Platforms start producing CTI reports in STIX format and together with the integration of BRIDGE tool can achieve automation and high-success-levels in security incidents handling.

The research outcomes of this paper can be extended as future work in many ways. For this proof-of-concept implementation of BRIDGE, we designed and developed a prototype for Unix-based environments. Next, we plan to implement BRIDGE for Windows based environments removing environment-related barriers. In addition, we aim to develop and integrate a Self-Sovereign-Identity approach within blockchain technology to create an ecosystem with trustworthy CTI consumers, who may belong to different organizations but should share their intelligence and security information increasing. Also, we aim to enhance the list of SIEM that Sigma suports by increasing interoperability.

Chapter 10

Analyzing Coverages of Cyber Insurance Policies Using Ontology

In an era where all the transactions, businesses and services are becoming digital and online, the data assets and the services protection are of utmost importance. Cyber-insurance companies are offering a wide range of coverages, but they also have exclusions. Customers of these companies need to be able to understand the terms and conditions of the related contracts and furthermore they need to be able to compare various offerings in order to determine the most appropriate solutions for their needs. The research in the area is very limited while at the same time the related market is growing, giving every potential solution a high value. In this paper, we propose a methodology and a prototype system that will help customers to compare contracts based on a pre-defined ontology that is describing cyber-insurance terms. After a first preliminary analysis and validation, our approach accuracy is averaging at almost 50%, giving a promising initial evaluation. Fine tuning, larger data set assessment and ontology refinement will be our next steps to improve the accuracy of our tool. Real user evaluation will follow, in order to evaluate the tool in real world cases.

Table 10.1 summarizes the scientific publication related to this chapter.

Authors	Title	Venue
Charalambous M, **Farao A**, Kalantzantonakis G, Kanakakis P, Salamanos N, Kotsifakos E, Froudakis E	Analyzing Coverages of Cyber Insurance Policies Using Ontology	ARES 2022, ACM $[Rank : B]$

Table 10.1: List of thesis' publications- Part J

10.1 Introduction

As more and more businesses are going online – offering their products and services using online platforms, shared cloud and infrastructure [1] – the exposure to cyber-threats and the risk for breaches and business interruption is getting higher [320]. The cost [321] of such threats can be enormous, especially for small businesses that do not have the budget to build highly secure infrastructures or to recover from attacks– especially if this involves fines that they have to pay for not being able to protect their data [79]. At the same time, the cyber-insurance market [283] is growing and evolving at a fast pace trying to offer solutions that will safeguard the online businesses. Selecting the proper cyberinsurance policy is a difficult task; especially, trying to understand what they cover and what they do not and comparing the offers as well as their prices. The evaluation of different policies and contracts is a manual and time consuming process, often requiring technical or legal knowledge. However, one of the biggest drawbacks is the Information Asymmetry that has a negative effect on the cyber insurance ecosystem and includes two components: (i) the inability of the insurer to distinguish between insureds of different (high and low risk) types, and (ii) insurers undertaking actions (i.e., reckless behavior) that affect loss probability after the insurance contract is signed, knowing that they would be insured. The reasons that lead to information asymmetry are the following: (i) insurers lacking vital information regarding applications, software products installed by insureds, and security maintenance habits, which correlate to the risk types of insureds, and (ii) insureds hiding information about their reckless behavioral intentions from their insurers, after they get insured, knowing that they would be compensated – irrespectively of their malicious behavior (e.g., being careless with security settings, etc.,) [322].

In this work, we propose a prototype system for parsing cyber-insurance policies/contracts and extracting inclusions and exclusions, offering to the user a list of what is covered and what is not. In this way, the user will be able to easily compare several policies/contracts and to choose the one that fits he/she needs in a better way.

10.2 Background

As the cyber-attacks become more sophisticated targeting a broad range of companies and state or private institutions, the cyber-security is evolving too, together with the cyber-insurance. Cyber insurance is a rapidly developing area and an alternative way to deal with residual risks [8], [188]. Cyber-insurance is a powerful tool to incentivize the market towards protecting online businesses from information technology-related risks. The cyber insurance market is still immature facing several challenges on the way of becoming a common reality for online businesses and individuals [283], [322], [323]. Information asymmetry is one of the most prominent challenges and refers to the lack of information between the insurer and insured. First, as the cyber-insurance market is growing, it becomes more and more challenging for the insured to search and compare the various cyber-insurance policies (i.e., coverages and exclusions) that are offered by the market. In addition, the cyber insurance policies often list details about coverages and exclusions, using legal terms that can be difficult to be comprehended by the insured organization. Thus, moral hazard can occur where the insured organization could increase its exposure to risk, as well as the probability of loss during the contract period. Secondly, it is difficult for the insurer to distinguish between high and low risk businesses and individuals.

Although the cyber-insurance market is rapidly growing, few studies have been conducted in this area. The problem of identifying the coverages that an insurance company offers regarding cyber-security is relatively new and therefore not a lot of solutions are available. Analyzing the cyber-insurance contracts is mainly a problem about text analysis and keyword extraction, while being able to semantically distinguish what the insurance is covering and what is not.

Romanosky et al. [204] have presented qualitative research, of the current state of the cyber-insurance market. First, the authors collected insurance policies from state insurance commissioners in the United States. They col-

lected over 235 policies from New York, Pennsylvania, and California, as well as policies posted publicly on various insurance companies' websites. Then they examined the composition and variation across three components: (i) the coverage and exclusions (ii) the security application questionnaires – by which an applicant's security risk level is estimated– and (iii) the rate schedules which define the method used to compute premiums. The finding depicts that there is a strong similarity regarding the covered losses, with more variation in exclusions. Bohme et al. [187] proposed a unifying framework to illustrate the parameters that should be included in the model of cyber insurance. The framework features a common terminology and deals with the specific properties of cyber-risk in a unified way. It unites phenomena such as interdependent security, correlated risk, and information asymmetries, in a common risk arrival process. Their framework offers a unified terminology to deal with specific properties of cyber risk and helps to alleviate discovered shortcomings.

The automatic ontology population from raw texts is a powerful procedure, since it extracts data from various documents which even if they contain irregular and ambiguous information, it is still able to enrich and assign the data with a precise structure and semantics. In this context, Ganino et al. [324] presented a methodology for the automatic population of predefined ontologies with data extracted from text and they proposed the design of a pipeline based on the General Architecture for Text Engineering system. Elnagdy et al. [325] presented the Semantic Cyber Incident Classification (SCIC) model, an ontology-based knowledge representation methodology for cyber-insurance. The method uses semantic techniques to provide a consistent knowledge representation for mapping the entities in the Cyber insurance system. Finally, other studies on populating ontology schema for legal text documents are: [326] for service level agreements and [327] for web service provider privacy policies.

Addressing the information asymmetry problem, one prominent approach is by parsing the various cyber-insurance policies and contracts that are offered by the insurance companies, to extract, and categorize the coverages and exclusions in a completely automatic way. One of the first studies that followed the aforementioned approach is the work of Joshi et al. [328]. The authors have presented a framework that automatically extracts keywords from cyber insurance policy documents and populates an ontology schema (or knowledge graph) to represent the extracted keywords as coverages and exclusions. The proposed cyber insurance ontology has been constructed by an-

alyzing publicly available insurance policies from seven insurance providers. Moreover, the key ontology classes along with their relations are based on industry standards proposed by the United States Federal Trade Commission (FTC). Finally, they applied a grammar-based natural language parser using deontic expressions, to extract coverages and exclusions from the policy documents. Deontic logic describes statements containing permissions, and obligations, whereas temporal logic describes time-based requirements. The use of domain-specific ontologies, is a popular approach to represent domain knowledge.

Our approach presented in this paper is different in several points from the one in [328]. First, the dataset used in [328]is not publicly available, hence, we were not able to use it in our model. Moreover, apart from the very limited research in cyber-insurance contract evaluation, there is neither commonly agreed list of coverages and exclusions that serves as an official terminology, nor official cyber-insurance ontology available. As Romanosky et al. [329] pointed out, there is lack of clarity in what is covered and excluded by a given policy, in the event of a security incident. Thus, the lack of comprehensibility of a policy rule often leads to courtroom discussion to determine the validity of coverage clauses. Many "ontology standards" exist, but none is explicitly defined as "information security ontology". For this reason, we have manually analyzed several available contracts and cyber - insurance policies from various companies to define our own list of terms and consequently to construct related information-security ontology. Furthermore, our approach is able to deal with large collection of documents due to the simpler text parsing and keywords extracting method. Therefore, our approach is scalable, time and memory efficiently.

10.3 SECONDO APPROACH

Our approach is based on the following main methodology. First, we parse the contract/ policy document and we extract the text that refers to the coverages and the text related to the exclusions. Then, using these two different texts as input, along with a generalized cyber-insurance terms ontology, we define which of the terms of the ontology are found in the coverages or in the exclusions. The use of the ontology allows us to be able to categorize coverages and to have a tree-like structure, where a category can include various coverages. This gives us the flexibility: (i) to include a set of cov-

erages that are categorized, and they might not be mentioned by the exact wording in the policy; (ii) to allow the user to provide their own ontology (either defined manually or provided by an organization). One of our goals is to have an extensible tool so that the user will be able to use their one ontology-vocabulary. The final output of our approach is a table with the terms of the ontology and an indication whether this is covered or not by the specific policy. With this approach, we can also deal with the language problem, since the tool gets as input a manually created ontology file, that can be in any language and it matches the terms with the policy text in the same language. In other words, although we have evaluated our tool with policies in English, the tool is language-independent.

The first step of our process is to automatically extract the coverages from an original contract in .pdf format and depict them in such a way that it would be easier to analyze them in the next steps of the process. For designing this, we examined two approaches. The first approach we examined and the approach that we finally decided to implement was to make an automated process with python3 code that would take each original contract in .pdf format as input, it would map each line of text as a type of header or paragraph by the .html format to the file and output it in a .txt file. After that, another function would take as input the .txt file and remove unnecessary headers and footers, find keywords that show if some damage is or is not covered by the contract and list the covered and not covered damages in two final .txt files that are the final output from the program. This approach was easily executable and, the program could be easily evaluated, and micro adjustment could be made to work properly in all the possible formats of contracts (making the final outcome reliable).

Another approach we examined was that of automation by trained neural networks. The way that this approach would work is that we would make a fully or partially connected neural network that would take as input the contract in .pdf form and output a boolean value for all the possible coverages. In the training stages the output would be compared with the expected output and the distance (in the geometrical space that is defined by the vectors-coverages) between them would be the value of this performance. After each performance, a backward propagation function would make micro adjustments to the connections of the network in order to minimize that value for all the given contracts. This approach would not only be more universal, because all of the possible contract types would have been analyzed and trained on, but the further development and the adaptability of the process

would be easier as we would not need to reprogram the whole program but to add some more specialized functions or continue the training in new sets of data. Nevertheless, the neural network approach was abandoned as there was not a fitting trained network in the bibliography. Another risk that this approach would pose is the credibility of the result as in those methods even the slightest unpredicted change could have an effect in the result.

10.4 System Architecture

Concern over cybersecurity is growing across all sectors of the global economy, as cyber risks have grown, and cyber criminals have become increasingly sophisticated. For insurers, cybersecurity incidents can harm the ability to conduct business, compromise the protection of commercial and personal data, and undermine confidence in the sector. The participants who take part in the cyber insurance market are the following: i) Insurer; ii) Insured; iii) Agent and iv) Broker.

Insurer: Insurers offer premiums that can cover a variety of cyber risks and incidents, such as phishing, data breaches, or malware that can affect companies and individuals. It can provide first-party coverages, such as damage on digital assets, business interruption, and incident response costs, as well as third-party coverage, such as privacy and confidentiality-related liabilities. Moreover, insurers provide policy holders with premiums and with the element of risk assessment, in case they fall victim to a cyber threat, providing technical, legal support in case of an incident. There is quite a lot of variation between the contracts, and this always depends on the needs of individuals or organizations. It also depends on the need for insurance coverage as well as the type and level of risks that will be exposed. Insurers offer cyber insurance policies as part of a contract or as a standalone product.

Insured is a person whose assets (tangible and intangible assets) are protected by an insurance policy; moreover, he is a person who contracts for an insurance policy that indemnifies him against loss. In terms of cyber insurance individuals and organizations can benefit, as cyber incidents can evoke cyber risks. Aftermaths of a cyber threat may have a negative impact on individuals and businesses, including the loss of customers and revenue. Cyber insurance policies may change as an impact of the continuously changing market. Insurers nowadays are facing many challenges in the insurance industry such as, the need to find a trusted advisor, to find the proper in-

surance program, to find a broker or agent who addresses their specific and special insurance needs, a competitive insurance program in comparatively the current market environment and to find a tailor-made contract in their needs.

Agent: An insurance agent is a licensed person who has an important role to achieve an agreement and to conduct business on behalf of insurance companies. He is the professional who has the necessary knowledge needed to transmit the multifarious to the prospective clients. He is the intermediary who has undertaken the difficult role of approaching the client, informing him about the offered products of the insurance company, convincing him to buy them, and most important and the most difficult part is to acquire trust and become the person who will be interested in satisfying him, regarding the agreed claim that the insured has. However, the insurance agent is the one who must study the financial conjunctions, analyze them, predict the changes that affect the interested parties by all factors such as consumers, investors, those who are interested in savings plans, and all those who are interested to be insured.

Brokers organize and execute financial transactions on behalf of their respective clients for categories such as assets, stocks, forex, real estate, and insurance. For the orders he executes, the customers are charged with a commission according to the agreement of the contract. A broker can have an advising role on buying or selling products as some can provide their customers with market data analytics to help them make the right decision. The broker may be full-time or only for executions. To do the above he must be certified to provide the appropriate advice as well as the client's permission to perform any action.

As shown in Figure 10.1, the general structure of our tool is divided into two discrete main sub-modules: i) the Parser and ii) the Cyber Insurance Ontology. On the one hand, the Parser sub-module (as its name implies) is responsible to receive the contract that will be under process and in the end discretely present the coverages and exclusion that the aforementioned contract bears with. On the other hand, the Cyber Insurance Ontology contains lists regarding the common coverages and exclusion that the majority of cyber insurance contracts bear with, as well as it contains the cyber insurance ontology. The proposed ontology will be used between the Insured, the Broker and the Agent. We have to note the cyber insurance ontology is not standalone, but it is part of the SECONDO [8] architecture, which is responsible for providing a holistic security solution as a platform for organi-

zations to fight cyber risks providing them with innovative security controls including risk transfer.

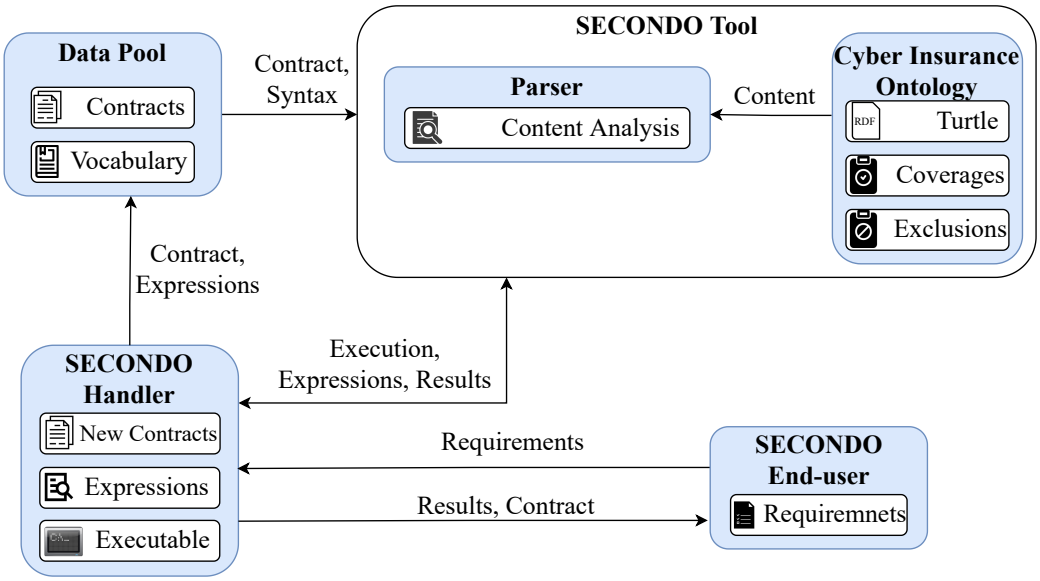


Figure 10.1: System architecture

Our tool interacts with the following entities: i) the SECONDO handler and ii) the SECONDO end-user. At this point we have to note the term SECONDO handler contains the following entities [330]: i) Insurance company; ii) Insurance agent and iii) Insurance broker. This stakeholder is responsible to feed the tool with new cyber insurance contracts, expressions that are used in the contracts to express the existence of a coverage and exclusion, as well as to execute the tool. While the end-user could be a prominent insurer having specific requirements. Finally, there is a Data Pool that is responsible to securely store the vocabularies and the contracts that have been analyzed.

10.5 Implementation

Our tool implementation is a combination of bash scripting, python development and ardf ontology in turtle format. The bash environment helps us orchestrate the execution flow as it controls the input/output of the core

environment, the python scripts. Our implementation is a pipeline of steps which contains contract reprocess, the core of our tool and result combination. Each step is given an input and extracts an output which is given to the next stage.

The first steps of our process are to clean our file from the different fonts and all the graphical parts that are useless to us. This happens with the two first functions *fonts()* and *font_tags().* Specifically, the first function extracts and returns all the fonts and their usage. The second function takes as input and returns a dictionary with font sizes and tags as keys and values respectively. After that the function *headers_para()* takes all the headers and paragraphs from the .pdf file and with the help of the output of the *font_tag()* function and returns them as text with element tags.

The next step is to select the covered and not covered parts. First, we make all the characters lowercase for easier and better handling. Then we remove headers that came from headers and footers of the .pdf file and not from actual titles and subtitles with the function *remove_headers_footers().* Those headers and footers do not contain any new information but are very confusing to the algorithm. The algorithm recognizes them because they are repeated on every page. After that we use the function *coverd_and_not_coverd()* to separate files that contain the covered and not covered damages by the contract. The algorithm finds the covered and not covered damages by searching for keywords as "cover", "covered", "coverage", "not covered" and "not cover" in the lines that came from subtitles and titles to recognize which paragraphs are talking about the coverages. The main core of our implementation is described by a python script file which is executed given the output of the previous step, the covered and not covered text, as long as the ontology file.

Our aim is the use of the well-defined ontology to find keywords in text files that will help us understand whether something is covered or not. To efficiently find the similar words, the input text files were tokenized to ngrams and stored in memory as python sets. As continuous sequences of words or tokens in a document, the n-grams in our case are defined in sets of two words. The choice of two words is based on the fact that our ontology contains mainly single terms and occasionally terms of two words. Thus, it is more efficient to compare the contracts text with the ontology terms. Subsequently, the ontology is turned to an in-memory RDF graph and using a sparql query the necessary information is obtained as a python set too. The final step of our algorithm is the creation of two new sets which will describe the covers

and not covers. To obtain the covers, we need to intersect the covered set of ngrams with our ontology whereas to find the non covers we need to use the non-covered set of ngrams. Our results are written in an xlsx format file where every sheet is named by the main ontology class and contains all the subclasses along with a yes or no-depending on the insurance coverage.

Overall, the proposed implementation is able to receive a set of contracts at the same time that will be processed sequentially, and the output will be a set of files, one for each policy, with the coverages and exclusions of each policy.

10.6 Performance-evaluation

In this section, we aim to evaluate the applicability and effectiveness of the proposed approach that has been introduced as a tool as well as its performance in terms of speed, resource consumption and scalability. For the proof of concept implementation, we have developed our own code (see Section 5), also, we have isolated cyber insurance policies from leading insurance companies to evaluate the proposed tool against their policies. The experiments were performed in an Ubuntu 18.04 desktop PC being equipped with an Intel Xeon(R) Silver 4114 CPU @ 2.20 GHz and 12GB RAM.

To evaluate our system, we performed an initial assessment. First, we defined an ontology with terms that we extracted from a set of insurance contracts from well-known companies, like AXA, Vero, RSA, Allianz, Tokio Marine, Travelers, Philadelphia, Delta, Hartford, Zurich and Hiscox. To achieve that we manually read and analyzed the contracts extracting a list of insurance terms. We consolidated the terms from the various contracts in order to obtain a generic list of terms that would suit all the contracts. Using this list, we created a table with the coverages and the exclusions of these contracts. This table is our "ground-truth", considering that we manually performed the semantic analysis of the contracts. The table contains terms that are under the categories of business interruption and cyber-crime. The terms that we included under the first category are the following: adware, brute force attack, cookies, Denial of service (DoS), Distributed denial of service (DDoS) attack, hacker attacks, key stroke loggers, logic bombs, Malicious code, Malware, past of present employee, phishing, spider ware, spyware, Trojan horses, Un-authorized access to a Computer System, Un-authorized access to data assets, Un-authorized used of a Computer System,

Un-authorized used of data assets, virus, worms, zero-day. The terms under the second category are: fraudulent funds, theft loss, communications loss, fraudulent signature, vandalism loss, credit account, debit account, Telecom fraud, Social Engineering Fraud.

In the next step, we created an ontology using these terms and along with the analyzed contracts, we provided them as input to our tool. The ontology is manually created as an ascii file, with specific format. This is done ones and in the future amendments can be easily done. The output of the tool is a list of coverages and exclusions for each of the contracts. In the next steps we compared this list with the ground-truth table to see how many of the coverages and exclusions were correctly identified by our tool. Our tool utilizes the categorized terms as follows. If the name of a category is found in the coverages of a contract, it assumes that all the terms under this category are covered by the contract.

This initial evaluation showed that the accuracy of our tool varies, from 27% to 87% without any tuning. The average accuracy is 45%. In our approach, the accuracy of the results depends mainly on the definition of the ontology and how close the terms are defined in comparison with the actual policy wording. For this reason, it is expected that a more well-defined ontology, or a richer one, will give better results.

A second test has been performed using the same terms for the ontology but without classifying them under categories, having no hierarchies. This means that the algorithm will consider coverages only for the terms that are explicitly mentioned in the contracts, making it "stricter".

It is observed that in the case of the use of an ontology without hierarchy, the results are quite different in some of the contracts. The overall accuracy is also a bit better.The accuracy in this case variesalso from 27% to 87% but it differs for some of the contracts. The average accuracy here is 50%. What we can conclude by these two initial experiments is that the accuracy of the system depends on the ontology definition by the expert. In the case we have a very detailed ontology, the results should be better. On the other hand, having hierarchies in the ontology, although it is more appropriate semantically, it might not have the desired accuracy in our system.Therefore, more experiments should be performed using different ontology structures and definitions in order to conclude the most suitable one for most of the test contracts.

Regarding performance, we evaluated it in terms of speed, resource consumption and scaling, we performed several tests using a different number of

contracts - pdf files, of various size. The experiments have been conducted 5 in the tested reported above. In particular, the experiments contained input with 10, 20, 100 and 200 discrete policies. The first experiment contained 10 contracts, and the time that the proposed ontology needed to complete the analysis was 62 seconds. During the second experiment, we fed the ontology with 20 unique policies, which the SECONDO achieved to successfully process them in 165 seconds. Later, the ontology assessed against 100 contracts and 200 individual contacts, the ontology spent 950 and 1451 second respectively to process them. We can observe that the time needed by the ontology to process the input is relatively linear in relation to the number of contracts it analyzed (see Figure 10.3). In addition, we have evaluated the resource depletion due to the ontology process. In terms of processing power, the program needed 15% CPU and 3% of the RAM regardless of the number of fields that feed the ontology (see Figure 10.2). This occurs because our tool does not multi-process the policies, instead it processes one file per execution circle.

Moreover, we have assessed the ontology against a large pdf file (26.5 MB) and it terminated successfully after 594 seconds. We have to note that the size of a cyber insurance policy is not more than 1MB.Overall, we can observe that our proposed tool performs reasonably well, and the time needed to analyze the contracts is acceptable.

Based on the above initial experiments we can identify the following advantages of our approach. Scalable (resource-depletion): The proposed solution is a tool that scales well without significant performance drawbacks in issues related to CPU and RAM consumption; it is a characteristic that leads to the fact that end-users can easily use it without specific hardware.
Scalable (words): The proposed solution is scalable regarding the wording. It is word-independent; by this, we mean that the proposed tool can be refined, re-edited and altered based on end-user requirements and desires. This allows the tolls to be updated any-time, a back-end feature.
Scalable (language): The proposed solution is scalable regarding the language. Currently, the tool works only for cyber insurance policies written in English. It is language-dependent; by this, we mean that the proposed tool can be refined, re-edited and altered based on end-users requirements and desires. For instance, correct words in different languages (Greek, Spanish, etc.) can be added to utilized vocabularies. This allows the tolls to be updated any-time, a back-end feature.
Time efficient: The proposed solution scales well regarding time management

issues; we have already proven that the tool regardless of the size of the processed files performs well and is not a time-consuming tool.
Environment independent/ deployment: Currently the existing implementation is environment independent; by this, we mean that the proposed tool can work not only in a UNIX based environment (like the tested one, see Section 4 and 5), but also in a windows-based environment. The only requirement is the installation of Python in the working environment.

On the other hand, our approach also has some technical limitations that are listed below.
Contract parsing and formatting: We have tried to use a pdf parsing library that can analyze all the pdf contract files but since the contracts do not have a generic, globally accepted and defined structure or formatting, there is the possibility that a pdf cannot be analyzed correctly, giving wrong results. This issue cannot be addressed beforehand, but a mechanism to report any parsing errors can be developed.
Terms matching: The algorithm that does the matching between the ontology terms and the extracted terms from the contracts use exact word matching, meaning that if we have words that are not the same, the algorithm will not consider them a match. This limitation, though, can be overcome if we define an ontology using all the terms in all their possible forms. Since the ontology is to be defined once, this can be done initially and, in the future, it can be updated.
Different languages: Our system is flexible, and it can be used for different languages. Although, for each language we need to define the appropriate ontology, defining the terms that are used in each language. This of course, on the other hand has the advantage of not having to change the code or the algorithm in order to use it for any language.
Semantic contract analysis: Our system does not use an AI based approach to analyze the contracts or/and automatically define the ontology. It is probable that such a solution could have better results. Of course, in order to verify this, we have to compare our tool with another one that uses the AI-based approach.
Ontology creation: Our solution requires manual ontology creation, by an expert. This is a step that has to be done initially and this also gives the possibility to easily extend and refine the ontology, having more control over it. Since the ontology creation is done only once, this does not add a lot of complexity. An already defined ontology can be also used, as long as it can

be extracted and then transformed in the format that our tool receives it as input.

10.7 Conclusion

An initial evaluation of our tool shows that our approach is valid and that the results are promising. Although it has been only assessed against a very limited number of documents and it has not been tuned to increase the accuracy and optimize the results. For this reason, the next step is to first optimize the ontology and the way our tool is using its terms to identify the coverages and exclusions of a contract. Another area of improvement is the parsing of the contracts and the extraction of the paragraphs that are mentioning the inclusions and exclusions. The text analysis is based on specific keywords and not in a semantic analysis of the document. While this seems to be accurate enough, more research is needed in order to validate it. Providing a broader list of terms or using a semantic analysis approach, may lead to better accuracy on extracting the parts of the document that are related to coverages and exclusions. Finally, a larger number of contracts has to be assessed and the list of terms and the ontology needs to be refined in order to be able to be more accurate in the coverages and exclusions extraction. Real user evaluation will follow, in order to evaluate the tool in real world cases.

In our future plans there is also the goal to define a generic ontology for the cyber-insurance domain which could be adopted by the major insurance companies. Finally, there is a provision to transform our tool to an online service providing an API that can be used to directly evaluate the various contracts, expand the contracts dataset and gain statistics insights to the cyber-insurance market.

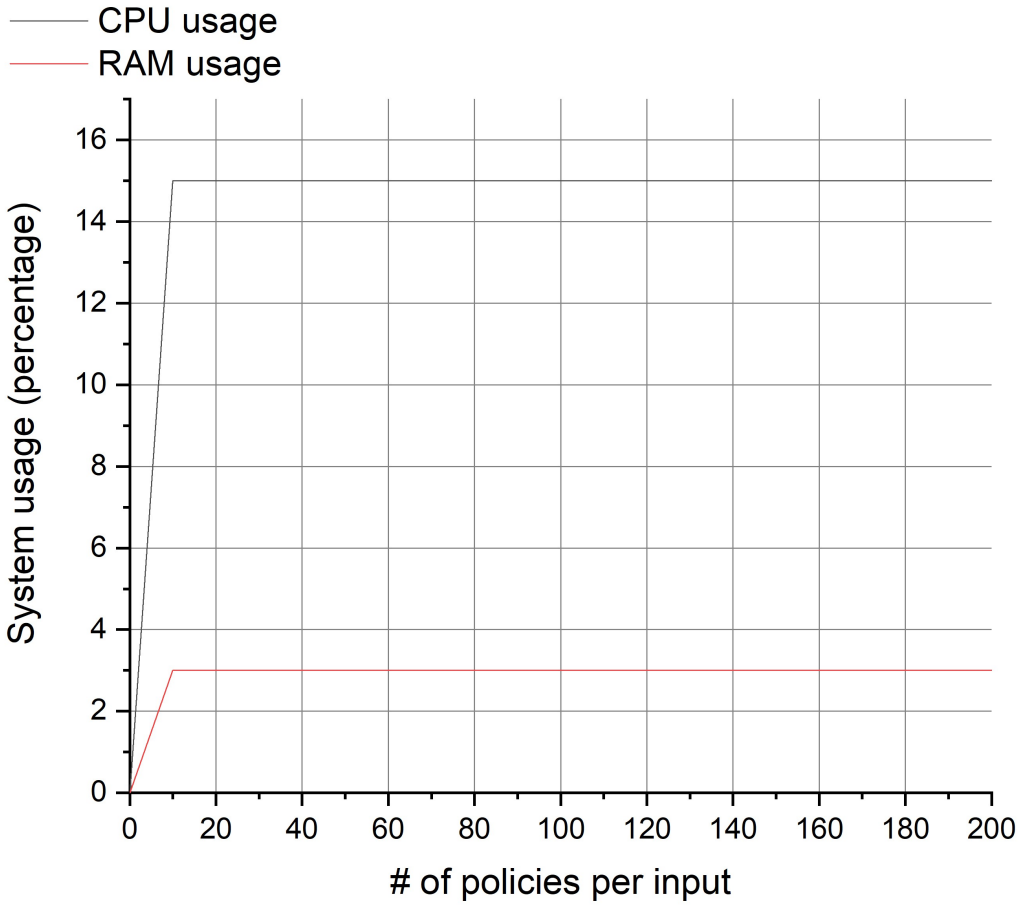


Figure 10.2: Resource usage

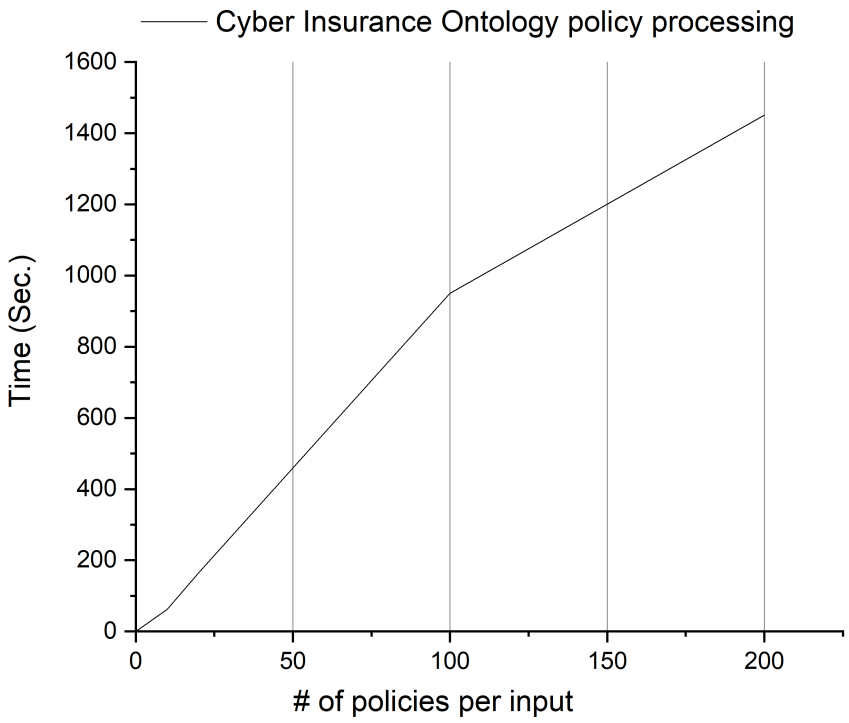


Figure 10.3: Cyber insurance ontology policy processing evaluation

Chapter 11

A Bring Your Own Device security awareness survey among professionals

The increasing prevalence of Bring Your Own Device (BYOD) practices in the workplace has posed significant challenges to organizations in terms of security and management. This chapter presents a survey-based study aimed at exploring the adoption, implications, and security considerations associated with BYOD policies. The study utilized a questionnaire developed based on guidelines provided by the National Institute of Standards and Technology (NIST). The primary objectives of this research are to investigate the cautiousness and awareness of BYOD users, as well as the effectiveness of security measures implemented by organizations, in order to gain insights into the key aspects of BYOD practices in the workplace. The findings of this paper highlight the need for increased caution among BYOD users regarding device security, a lack of knowledge among users about organizational security measures, and the potential for enhancing security policies and implementing additional measures despite organizations having achieved a satisfactory level of security for BYOD.

Table 11.1 summarizes the scientific publication related to this chapter.

Authors	Title	Venue
Petihakis G, Kiritsis D, **Farao A**, Bountakas P, Panou A, Xenakis C	A Bring Your Own Device security awareness survey among professionals	ARES 2022, ACM $[Rank : B]$

Table 11.1: List of thesis' publications- Part K

11.1 Introduction

In recent years, organizations and companies worldwide have embraced the Bring Your Own Device (BYOD) trend (the BYOD market has increased 1000% from 2014 to 2022 [331]), allowing employees to use their personally owned devices like smartphones, tablets, and laptops for work-related tasks. This shift offers numerous advantages. Firstly, it boosts employee satisfaction as they can use devices they are familiar with and have chosen for themselves, creating a sense of comfort and convenience [332]. Secondly, productivity tends to increase when employees work on their own devices, enabling them to work efficiently and complete tasks more quickly. This improved efficiency can lead to greater output, benefiting employers [333]. Moreover, BYOD provides flexibility, empowering employees to work from anywhere without relying on company tools or constantly transferring documents back and forth. This freedom eliminates the need for cumbersome processes and streamlines workflow [333]. Lastly, BYOD often results in cost savings for companies, as employees bear the expenses associated with their own devices, hardware, voice or data services, and related costs. This alleviates financial burdens on organizations [332].

However, alongside these benefits, the use of BYOD introduces significant challenges that organizations must address. Stolen or compromised personal devices pose a considerable threat, potentially exposing sensitive corporate data to malicious actors seeking to harm the organization. Unauthorized access to unsecured data on these devices can have severe consequences [334] . Furthermore, personal devices may not adhere to the organization's security policies or lack the necessary security software, making them vulnerable to various cybersecurity threats [333]. The end node problem further complicates matters, as BYOD intersects with managing devices accessing both sensitive and vulnerable networks and services. Some risk-averse orga-

nizations adopt an Inverse-BYOD approach, issuing devices exclusively for internet use. Effectively controlling and managing employees' personal devices presents its own challenges, requiring efficient inventory management systems to track device usage, location, and software configurations [335]. Additionally, monitoring employees' personal devices is a complex task for IT security departments, as they must strike a balance between monitoring work-related activities and respecting personal privacy while accessing company data or information [335]. These risks underscore the critical need for cybersecurity awareness among both employees and organizations when implementing BYOD policies.

In this study, our objective is to investigate the cybersecurity awareness and behavior of users who bring their own devices into organizational settings by addressing the following three research questions:

R1: Are BYOD users cautious when utilizing their personal laptop devices within their organizations?

R2 : Are BYOD users knowledgeable about the security measures imposed on them by their organizations?

R3 : Do organizations implement adequate levels of security when allowing BYOD?

To achieve this, we conducted a survey among a sample of 80 employees who had permission to use BYOD in their organizations. The survey questions were based on BYOD guidelines referenced from "Guide rise Telework, Remote Access, and BYOD Security" [336]. The findings of our survey provided valuable insights into the cybersecurity awareness of both employees and their organizations. Specifically, the contributions of this paper lie in the following aspects:

- We conduct a security awareness survey, among security professionals, regarding the BYOD paradigm.
- We have identified several pitfalls regarding the adoption of BYOD.
- Based on the conducted research, we have identified and proposed directions for future research.

The rest of the paper is organized as follows. Section 11.2 presents the existing related works that explore various challenges of the BYOD approach

and security measures to mitigate them. Section 11.3 presents the methodology used in this research, while Section 11.4 presents descriptive and inferential statistics of the results, and Section 11.5 describes the limitations of the research. Finally, Section 11.6 discusses the results of this work, and Section 11.7 concludes the paper.

11.2 Related Work

This research primarily focuses on the topic of BYOD and explores the different security measures that can be implemented to ensure a secure environment for organizations and their employees. The related work covers a range of research studies related to this domain.

A significant amount of research has been conducted on the subject of BYOD since the term gained popularity in 2009. The majority of existing works explore the diverse range of threats and risks associated with BYOD. In particular, Miller et al. [337] concentrate on the threats posed by BYOD. In their paper, they identify two main risks and threats to corporate information security, malware intrusion (worms, viruses, trojans) and the increased possibility of data loss. Respectively, in their study, [338] assesses the characteristics of BYOD and evaluates the related risks, threats, and vulnerabilities. On the other hand, [339] explores the trend of BYOD in corporate IT, providing an overview of security challenges, risks, and liabilities involved.

In addition to the aforementioned research, numerous other studies have been conducted with a focus on BYOD security. These studies offer guidelines or frameworks that can be employed to enhance the security of BYOD implementations. More specifically, the work of Souppaya et al. [336] which is the base of this research, provides guidelines that assist organizations in safeguarding their IT systems and information against the security risks associated with the utilization of telework and remote access technologies. Moreover, [340] compares currently available BYOD solutions and introduces a comprehensive BYOD security framework that offers valuable guidance for enterprises during the adoption of BYOD. Shumate et al. [333] examines the security challenges associated with BYOD programs, examining the advantages, risks, existing controls, and potential solutions to address the inherent security concerns associated with mobile devices in general, and specifically focus on BYOD programs. Lastly, but equally important Hajdaveric et al. [341] introduces a methodology for developing metrics that align security

policies with BYOD policies. They propose the utilization of metrics based on the ISO 27000 standard family to facilitate this alignment.

Furthermore, to the prior research that primarily examines the overall aspects of BYOD, including threats and security measures, there exist other studies that concentrate on more specific domains. As an example, Koohang et al. [342] endeavor to construct a research model to assess how security policy awareness and data protection awareness on mobile devices impact employees' trust beliefs. Similarly, Li et al. [343] propose a periodic smartphone sampling mechanism that significantly enhances the effectiveness of BYOD security mechanisms without incurring additional costs. Additionally, in the context of BYOD in education, AlHarthy et al. [344] aims to safeguard network data from unauthorized access and manage uncontrolled devices, including smartphones and mobile devices. Moreover, concerning BYOD in healthcare, Wani et al. [345] identify critical security challenges associated with the use of BYOD in hospitals and present pertinent solutions derived from a comprehensive review of gray literature.

Another area of research focuses on BYOD and access control methods. Within this domain, notable work includes the research conducted by M. Muhammad et al. [346]. Their study aims to address the access control challenges in the BYOD environment by developing an Intelligent Filtering Technique (IFT) that leverages Artificial Intelligence (AI) techniques. Similarly, Concepcion et al. [347] aim to establish and enforce security policies in BYOD through the integration of Network Access Control (NAC) and Mobile Device Management (MDM) using the in-band approach.

Last, but certainly not least, there are surveys conducted to explore the realm of BYOD and yield valuable insights. For instance, in reference [348], the authors conducted a survey that involved over 1000 employees who utilize BYOD. The survey aimed to gather information regarding their device preferences, the impact of their devices on productivity and work-life balance, and their awareness of security measures. Similarly, Singh et al. [349], conducted a survey to investigate the current level of security and privacy awareness in BYOD within the higher education sector in Malaysia. The survey findings demonstrated the significance of fundamental security and privacy awareness and knowledge pertaining to mobile devices and applications for safeguarding personal devices and data.

Our research addresses the topic of BYOD risks and countermeasures in organizations, aligning with the subject matter explored in the above research works. However, our work distinguishes itself in two significant ways. Firstly,

it does not confine itself to a specific field. More specifically, our research includes results from the various job sectors encompassing a broader perspective. The primary differentiation, however, lies in the fact that our research does not seek to present general conclusions on the broad topic of BYOD. Instead, it takes pre-established and validated guidelines from NIST [336] as input and aims to provide valuable insights into their practical implementation by both companies and employees. These distinctions make our work distinctive, contributing additional knowledge to the existing literature.

11.3 Methodology

Between March 2022 and March 2023, an online survey was undertaken to evaluate the security preferences, awareness behavior, and education of BYOD users. The survey's ethical considerations, its process, and information on the statistical significance of the results are briefly explained below.

The fact that this survey focuses on people may raise issues regarding ethics. Below are enumerated the 10 most significant ethical issues in surveys, according to [350].

1. Research participants should not be subjected to harm in any way whatsoever.

2. Respect for the dignity of research participants should be prioritized.

3. Full consent should be obtained from the participants prior to the study.

4. The protection of the privacy of research participants has to be ensured.

5. Adequate level of confidentiality of the research data should be ensured.

6. Anonymity of individuals and organizations participating in the research has to be ensured.

7. Any deception or exaggeration about the aims and objectives of the research must be avoided.

8. Affiliations in any forms, sources of funding, as well as any possible conflicts of interests have to be declared.

9. Any type of communication in relation to the research should be done with honesty and transparency.

10. Any type of misleading information, as well as representation of primary data findings in a biased way must be avoided.

Private connections and a number of professional networking sites, including LinkedIn, Research Gate, and Reddit, were used to distribute the questionnaire. This was considered crucial in order to make sure that the questionnaire was disseminated to a variety of nations. Anyone above the age of 18 who is employed and uses a personal computer for business is considered to be a member of the targeted audience. Other restrictions, such as those based on age, gender, nationality, years of experience, position seniority, or the kind of workplace, were not used because the goal was to collect a diverse sample of responses. Additionally, a disclaimer page was provided at the start of the questionnaire as soon as the participant visited the form, outlining the research and soliciting their agreement. The survey itself consisted of 38 questions (35 multiple choice, and 3 free response). Overall, the questionnaire respects the previous points, and the result is safe in terms of ethics. Regarding the questionnaire's structure, it is broken up into four distinct sections that can be referred to individually by their respective names. The completed questionnaire may be found in [351]. Below there are their names and brief descriptions:

Introduction and Ethics: The questionnaire's description and information on ethics are included in this section. Additionally, there is a mandatory user consent area that determines whether the questionnaire will pass to the next section or be terminated based on the users' choice.

User Demographics In this section, survey participants' demographic information is questioned. These questions include the: age, gender, country of employment, level of education, industry, subject's job department, subject's job position, and if the subject uses her personal device for employment purposes.

Questions about BYOD This is the questionnaire's main section and icludes the *BYOD-related* questions. The majority of the information gathered that forms the basis of the survey is presented in this part.

Cybersecurity awareness In the final part, the questionnaire asks cybersecurity awareness-related questions about the subject's training and familiarity with cybersecurity.

Regarding the analysis of the survey outcomes, both descriptive and inferential statistics have been used. In order to display and characterize the outcomes of each inquiry, we first do descriptive statistics. Then, we do a comparative statistical analysis to see if there is a link between two or more groups. If necessary, we use x^2 tests (statistical hypothesis tests) to look for significant differences between the expected and observed rates. A x^2 statistic test compares the observed and anticipated frequencies of a set of events or variables. It helps analyze category variables, especially nominal ones. It tests whether two variables are connected or independent based on the difference between actual and observed values, degrees of freedom, and sample size. Finally, x^2 may examine the goodness-of-fit between an actual distribution and a theoretical frequency distribution [352].

11.4 Results

11.4.1 Descriptive statistics

11.4.1.1 Demographics

The questionnaire's demographics section (questions 2-9) gathers general information about the participants, including their gender, age, job sector, and country of work, among others. This section provides valuable insights into the participants' background and demographic characteristics. The analysis of this data reveals interesting findings. Among the 80 participants, it is observed that a majority of them are males, accounting for 53 participants. Additionally, the majority of participants work in Greece. In terms of age distribution, the most common age range is 25-34 years old, with 45 participants falling within this range, followed by the 35-44 years old category, consisting of 24 participants. Notably, more than half of the participants hold a master's degree, with 42 individuals having this qualification. The participants primarily belong to the Information Technology field, with 36 individuals employed in this sector. Telecommunications and the Business-Finance-Insurance sector follow, with 12 and 11 participants, respectively. Regarding the department within their organization, the majority of participants work in R&D and software development (27 participants), followed by IT (5 participants), Information Security (5 participants), and Legal departments (5 participants). Furthermore, the majority of participants (75

out of 80) hold employee positions, while 5 participants occupy high official positions. The demographic results are visually presented in Table 11.2.

11.4.1.2 Cyber Security section results

The pivotal section of the survey lies in the results of the Cyber Security section, encompassing questions 11-35 (Table 11.3). Through their responses, participants demonstrate their level of awareness and adherence to the security guidelines proposed in [336].

Initial, it is notable that a significant portion of participants (70%) have permission to store sensitive corporate data on their personal laptops (Q11 - "Are you allowed to store sensitive data of your organization in your laptop?"). While this is often necessary, it necessitates the implementation of various measures by both the company and its employees to protect such data. One such measure is the encryption of sensitive data by the organization itself. Our survey reveals that in most cases (58.75% participants), organizations indeed encrypt their sensitive data (Q12 - "Does your organization encrypt its sensitive data?"). However, a considerable number of participants stated that their companies do not employ encryption (16.25% participants), while others were uncertain about the existence of encryption measures (25% participants). Another protective measure against data theft is the encryption of employees' laptop storage. According to our survey (Q13 - "Does your organization encrypt your laptop's storage?"), the majority of organizations do not encrypt laptop storage, as indicated by the negative responses from the majority of participants (56.25).

The following set of four questions focuses on connectivity, authentication methods, and system threat models. Notably, a majority of participants (77.5%) employ a second security factor alongside their password to connect to their company's network or VPN (Q14 - "Do you use multi-factor authentication or other types of authentication when connecting from your laptop to your company's network?"). Additionally, participants indicated that their organizations utilize Network Access Control (NAC) solutions to safeguard access to network nodes, as confirmed by 82.5% of the respondents (Q15 - "Does your organization use Network Access Control (NAC) solutions to secure access to its network nodes?"). However, when asked about whether their organizations have developed system threat models for remote access servers and accessed resources, a majority of participants (52.5%) expressed uncertainty (Q16 - "Has your organization developed system threat models

for the remote access servers and the resources that are accessed through remote access?"). Although it is common for this information to be sparingly shared with regular employees, this also suggests a potential lack of emphasis placed by organizations on communicating such important details or a lack of attention from employees towards relevant announcements. This underscores a diminishing emphasis on security for both organizational management and regular employees. Lastly, most participants indicated the use of tunneling (VPN) as their chosen method to connect to their organization's network (Q17 - "Which remote access method do you use to connect to your organization's network?"). The alternative choices included "Application Portals," "Remote Desktop," "Direct Application Access," and "None.".

The next set of three questions pertains to whether organizations have established separate external networks for BYOD (Bring Your Own Device) devices and the corresponding measures implemented for these networks. Based on the responses (51.25% of the participants), it is evident that most organizations utilize distinct networks for their BYOD employees (Q18 - "Has your organization established separate, external networks for remote and BYOD devices within enterprise facilities?"). However, the nearly equal number of negative responses suggests the need for increased attention by organizations in these cases. Participants who answered "Yes" in the previous question were further asked about the security and monitoring of these separate networks (Q19 - "If yes, are these networks secured and monitored in a manner consistent with how remote access segments are secured and monitored?"). Of those, more than half (30% of the participants) confirmed that these networks were secured and monitored in line with remote access segments, while 20% of the participants responded with "I do not know". Lastly, responses to the question "Does this networks' traffic pass through a firewall?" (Q20) were divided between "Yes" (35% of the participants) and "I do not know" (16.252% participants). The prevalence of "I do not know" answers in both questions indicates that many employees lack awareness of the security measures implemented by their companies and organizations. This highlights potential weaknesses in communication between higher management and regular employees, or a lack of employee attention to management announcements.

Following that, three questions are presented concerning tools that can enhance the security of users' devices. In the first question (Q21 - "Do you use antimalware software in your laptop?"), 77.5% of the participants responded with "Yes." This is an encouraging finding as it demonstrates the partic-

ipants' recognition of the various risks associated with viruses. However, 22.5% of the participants responded with "No," indicating that a significant number of participants are exposed to potential virus threats, even if some of them may use more secure operating systems such as Unix-like systems. Similarly, the subsequent question (Q22 - "Do you use a firewall?") yielded comparable results. Once again, 81.25% of the participants confirmed using a firewall, while 18.75% of the participants responded negatively. Those who answered "No," along with their respective organizations, are exposed to risks. These risks encompass unsolicited and unwelcome inbound network traffic originating from malicious sources such as malware or hackers. Generally, a firewall serves as the first line of defense for a computer, safeguarding personal information against the prevalent and ever-evolving cyber threats . In Q23 - "Is your firewall properly configured for the enterprise environment?," the results are evenly divided. This suggests that either the organization has not enforced a security policy for its BYOD employees, or these employees are not adhering to the existing security policy [353]. In either case, the outcome presents potential risks for both the BYOD devices and the organizations permitting their usage. For instance, if a BYOD user fails to comply with the company's security policy that prohibits AnyDesk, there is a possibility that an attacker with knowledge of the user's AnyDesk ID and password could gain full access to the device based on the available permissions. Subsequently, the attacker can pilfer sensitive corporate data and passwords or traverse within the corporate network to gain access to additional resources and potentially sensitive information [354].

The subsequent two questions center around the security of BYOD users against malicious individuals aiming to steal their physical devices, along with the corporate data stored on them, particularly in shared workspaces like cafes or remote working locations. In Q24 - "Do you use any physical security means to protect your device from theft?" only 25% of the participants responded with "Yes." Consequently, the remaining 75% of the participants are vulnerable to potential device theft by opportunistic thieves. It is important to note that the theft of a personal laptop used for BYOD can have further detrimental effects on the victim's organization. In contrast, in Q25 - "Do you lock your device when you leave your desk?" the majority of participants (72.5% of the participants) answered affirmatively. This crucial practice serves as a deterrent for any potential malicious users who might contemplate taking advantage of an individual's absence from their device and pilfering sensitive corporate data.

In the subsequent question (Q26 - "Has your organization provided you with flash drives that are specifically configured for telework use in order to prevent you from using your own?"), the overwhelming majority of participants (87.5%) responded with "No." Consequently, most participants utilize their personal flash drives, which could potentially be infected with viruses or other forms of malware [355]. The risk of infection becomes even greater when participants do not employ antivirus or firewall tools. Similarly, in the following question (Q27 - "Has your organization provided you with a bootable OS and read-only removable media with pre-configured remote access client software?"), 90% of the participants answered with "No." This indicates that participants rely on their own system, including the operating system and software. While it can be sufficient if the user possesses strong knowledge of computer security, in many cases, it is safer to utilize a preconfigured environment developed by security professionals.

In Q28 - "Are the capabilities of your mobile devices limited in your organization's network?" more than half of the participants (51.25%) responded with "Yes." This indicates that the majority of users are restricted from accessing various websites [356, 357] such as Facebook, Instagram, Spotify, and are also prohibited from using Bluetooth while connected to their organization's network. Furthermore, in Q29 - "Does your organization enforce full disk encryption to protect data at rest?", 65% of the participants answered with "No" or "I don't know." This implies a potential risk as data at rest is typically vulnerable to threats from hackers and malicious users who aim to gain access either digitally or through physical theft of the data storage media. Conversely, the remaining 35% of the participants reported having their disks encrypted using specific tools like BitLocker, IBM Guardium, and so on. Lastly, in Q30 - "Does your organization prompt you to use virtual machines (VMs) in order to carry out your job?", 63.75% of the participants answered negatively.

Continuing with the findings from the Cyber Security section, we come across questions related to data backups. In Q31 - "Are you backing up data on your telework device?", the responses are evenly split. Unfortunately, a 50% non-compliance rate in data backups is significant and highlights that many users do not take security risks seriously. Among those who responded "Yes", 11 participants perform backups on a monthly basis, 7.5% of the participants do so weekly, 10% participants do so daily, and 17.5% of the participants selected the option "Other" (Q32 - "If yes, how regularly do you take backups?").

The final three questions in the Cyber Security section pertain to potential security policies within organizations. In Q33 - "Has your organization developed a security policy that defines telework, remote access, and BYOD requirements?", 30% of the participants responded with "No". This substantial number signifies that some organizations may not prioritize cybersecurity adequately. However, it is also plausible that these participants are unaware of their organization's security policy. Among those who answered "Yes" in the previous question, there was nearly an even split when asked whether they had read the security policy of their organization (Q34 - "If yes, did you read the security policy?"). Specifically, 46.5% of the participants replied "No", while 53.5% of the participants replied "Yes". Finally, in regards to Q35 - "Do you put the security policy into practice?", 66.1% of the participants responded "Yes", while 32.1% of the participants responded "No" (with one blank response).

11.4.1.3 Cyber Awareness section results

The concluding section of the questionnaire encompasses three inquiries relating to participants' familiarity with cybersecurity and any cybersecurity awareness training they may have received. In Q36 - "How familiar are you with Cybersecurity?", participants responded as follows:

- Novice – 30%
- Advanced Beginner – 31.25%
- Competent – 21.25%
- Proficient – 11.25%
- Expert – 6.25%

These results indicate that a significant number of participants lack experience in cybersecurity, which may explain the weaker outcomes observed in previous questions. Subsequently, participants were asked about their attendance of security awareness trainings in Q37 - "Have you attended any security awareness trainings?". Of the respondents, 62.5% of the participants answered "Yes", while the remaining 37.5% answered "No". This implies that almost 40% of the participants have not attended any security awareness trainings. This further amplifies the risks associated with using

BYOD, thereby jeopardizing the security of participants' organizations and companies.

In the final question of the questionnaire (Q38 - "If yes, were these security trainings organized by your company?"), participants who responded "Yes" to the previous question were queried about whether their companies had organized cybersecurity awareness trainings. The outcome revealed that 78% of the participants answered "Yes", while 22% of the participants answered "No". This suggests that the majority of companies are aware of the various hazards associated with using BYOD and are taking steps to educate their employees. However, it should be noted that organizing such trainings does not guarantee complete safety from the various risks posed by BYOD. Nevertheless, these companies are in a relatively safer position compared to those that do not provide such trainings at all. The results of the preceding questions are depicted in Table 11.4.

11.4.2 Inferential statistics

In this section, we aim to examine the most captivating outcomes from our survey by utilizing inferential statistics. Specifically, due to the majority of responses being in the form of nominal data (categorical data lacking a value order), we will employ chi-square-tests for independence to assess the independence of response categories. The null hypothesis for each chi-square-test conducted in subsequent pages asserts the absence of any relationship or correlation between the counts of categories and variable values. Conversely, the research hypothesis posits the existence of an underlying association between them [358]

11.4.2.1 Correlation between Participants' Cybersecurity Familiarity and Implied Security Measures

We proceed to conduct chi-square tests of independence to explore the potential correlation between security familiarity and other security measures Table 11.5 taken by the participants of the questionnaire

The insignificance of all the aforementioned associations becomes evident as their x^2 values fall below the critical chi-square value (9.488) for df = 4 and a = 0.05. Consequently, it can be concluded that the variables tested are independent of each other, lacking any significant relationship. In a broader context, the results of the x^2 tests indicate that the participants surveyed

do not support the hypothesis that a higher level of familiarity with cybersecurity leads to a more secure BYOD device. This realization highlights the potential risks faced by their organizations, which necessitate proactive measures to prevent potential security vulnerabilities, possibly through the implementation of a stringent BYOD security policy.

11.4.2.2 Correlation between Job Sector and Organizational Measures

In the upcoming test, we will examine the hypothesis that the job sector of participants significantly influences whether companies have implemented a security policy. We posit that due to the reliance on technology in the majority of participants' fields, their respective companies are compelled to establish a security policy to safeguard their digital and physical assets. The null hypothesis contradicts this assertion. Table 11.5 presents the associations under discussion, with only four job fields included as the remaining fields lacked the necessary number of participants to validate the test.

Table 11.6 displays the connections between the participants' job sectors and the diverse security measures implemented by their organizations

The analysis of the results presented in Table 11.6 reveals that the job field of the participants is independent of several factors pertaining to their organizations, including:

- The permission to save sensitive data on their BYOD devices
- The utilization of multi-factor authentication
- The implementation of NAC solutions
- The imposition of limitations on BYOD device capabilities within the organization's network
- The employment of virtual machines

However, Regarding the hypothesis concerning the significance of the participants' job sectors in determining whether companies have implemented a security policy (Table 11.6), the chi-square value of 11.28654602 surpasses the critical statistic, specifically 11.28654602 ¿ 7.815. This outcome indicates a significant relationship between the job sector of the participants and the

security policy of their organizations. Furthermore, the test examining the independence between the job sectors of the participants and the presence of distinct external networks for BYOD users within their organizations yields significant results. Specifically, the chi-square value ($x^2 = 12.55838143$) exceeds the critical threshold of 7.815. Notably, this outcome primarily stems from the responses of participants in the Telecommunications field, as 11 out of 12 individuals reported that their organizations have implemented separate, external networks for BYOD usage. Thus, based on our sample, it can be inferred that the job sector can influence the establishment of external networks for BYOD users, indicating a dependent relationship between these two variables.

11.5 Limitations

Like any research based on questionnaires, this study has its limitations. The first limitation pertains to the method of collecting survey responses, as discussed in Section 3 - Methodology. The survey was promoted through internet channels and various contact networks, including Facebook groups, LinkedIn, working groups, and forums. Consequently, the collected sample is not entirely independent, and the randomness of the survey is constrained due to the self-selection bias commonly observed in internet surveys.

Another limitation is the composition of the questionnaire recipients, with the majority falling within the 25-34 age range, predominantly well-educated, and mainly originating from Greece. To enhance the quality and validity of the results, a more diverse range of participants from different countries, age groups, and educational backgrounds would be beneficial. Similarly, the distribution of job sectors among the questionnaire recipients is skewed, with a predominant presence of participants from the Information Technology field. This bias implies that the participants in this study likely possess greater knowledge in computer security compared to individuals from other fields, which may influence the outcomes and potentially lead to inflated results regarding computer security awareness.

Lastly, a larger sample size would improve certain aspects of the statistical analysis, particularly the chi-square tests for independence. With a larger sample, the tests would yield more robust outcomes by enhancing the statistical power. This increase in sample size would provide more reliable results as the correlations between different tables would become more representative

and ensure greater confidence in the chi-square tests.

11.6 Discussion

The results of our survey reveal intriguing patterns and behaviors, which will be thoroughly discussed in this section, addressing the three research questions that guided our investigation. In order to draw meaningful conclusions, we compare the survey findings with the guidelines for BYOD provided by NIST [336], which served as the foundation for designing the survey questions.

Regarding R1 – "Are BYOD users careful when using their personal laptop devices in their organizations?", The following interesting facts emerge from our findings. Firstly, 77.5% of the participants use antimalware software on their devices, while 81.25% of the participants utilize a firewall. These percentages indicate a high adherence to NIST guidelines, which recommend the use of antimalware software and firewalls in BYOD devices. However, the remaining participants are at significant risk. According to the SonicWall Cyber Threat Report [359], there were billions of malware attacks, ransomware attacks, and intrusion attempts in 2022, emphasizing the importance of these security measures for both personal and corporate devices [192, 277, 360]. Regarding firewalls, only 50% of the participants stated that their firewall is properly configured for the enterprise environment, which raises concerns as it deviates from NIST guidelines.

Another concerning finding pertains to the use of physical security measures to protect devices from theft. Only 25% of the participants employ cable locks or other deterrents, leaving their devices vulnerable to theft in various locations. Research by Gartner reveals that a laptop is stolen every 53 seconds, while the University of Pittsburgh highlights a mere 2% chance of recovery for stolen laptops [361]. Therefore, BYOD users should prioritize the physical security of their devices by implementing preventive measures against theft. Fortunately, when it comes to screen locking, 72.5% of the participants lock their devices when leaving their desks. However, nearly 30% of the participants do not follow the NIST guideline, jeopardizing important corporate and personal information. Additionally, 50% of the survey participants do not back up their data, which is a high percentage considering the potential risks such as data deletion, security incidents, and hardware failures. Lastly, 53.6% of the participants read their organization's security

policy, while approximately 66% of the participants actually implement it. These percentages are relatively low, indicating that the surveyed BYOD users do not prioritize their organization's security policy. However, it is also the responsibility of each organization to enforce rules for their employees [7].

In conclusion, it is crucial for BYOD users to exercise greater caution regarding the security of their devices [79, 9]. Several of the aforementioned percentages raise significant concerns. One potential solution could involve scheduling security awareness trainings conducted by management to enhance employee awareness. It is noteworthy that the inferential statistics results (Security measures implied by the participants are correlated with their Cybersecurity familiarity) indicate that familiarity with cybersecurity does not necessarily lead to a more secure BYOD device, as even advanced users may follow weak practices.

Regarding R2 "Are BYOD users aware of the security measures implied on them by their organizations?", We analyzed the more complex survey questions that included the option "I do not know" and obtained the following data. Initially, 25% of the BYOD users were uncertain about whether their organization encrypts sensitive data, while 16.25% of the participants were unaware of whether their organization encrypts their device storage. These percentages are concerning, particularly the latter (16.25%), which indicates a lack of awareness among employees regarding the software running on their devices. Furthermore, 52.5% of the participants were unsure if their organizations had developed system threat models for remote access servers and accessed resources. As previously discussed, while this may not be a widely known countermeasure, the high percentage of unaware employees is problematic, highlighting a communication gap between management and employees.

Subsequently, 39% of the BYOD users did not know if their organizations' external networks for remote and BYOD devices were secured and monitored in a manner consistent with remote access segments, and similarly, 31.7% of the participants were uncertain if the network traffic passed through a firewall. Finally, 33.75% of the BYOD users were unsure if their organization enforced full disk encryption to protect data at rest. These percentages are significantly high, indicating a lack of knowledge among BYOD users regarding the security measures implemented by their organizations.

Regarding R3 – "Do organizations implement the appropriate levels of security when they allow BYOD?", Firstly, 78.3% of the participants reported their organizations using encryption methods for sensitive data. Additionally,

32.8% of the participants stated that their organization encrypts employees' device storage. In terms of authentication, 77.5% of the participants use a second type of authentication when connecting to their company network. However, organizations should be cautious not to overly complicate the authentication process for employees. Regarding security measures, 82.5% of BYOD users mentioned their organizations using Network Access Control (NAC) solutions. However, only 51.25% of the participants reported separate networks for remote and BYOD devices, and 55.3% of the participants stated the existence of system threat models for remote access servers and resources. Most organizations seem confident in their existing security measures and are not inclined to invest further. Nevertheless, organizations with separate networks for BYOD users expressed high levels of security and monitoring. Regarding remote access, 82.5% of the participants utilize Virtual Private Networks (VPNs) to connect to their organization's network. Only 7.5% of the participants do not use any remote access method. However, 48.75% of the participants mentioned their organizations not imposing limitations on personal devices' capabilities, which poses risks such as malware spread and reduced bandwidth availability. Most organizations allow employees to use their own devices without pre-configured environments. Specifically, 90% of the participants do not use bootable OS or read-only removable media with pre-configured remote access client software, and 63.75% of the participants are not prompted to use Virtual Machines (VMs). Establishing a security policy is crucial for maintaining device security [1, 6]. Approximately 70% of participants reported their organizations having a security policy defining telework, remote access, and BYOD requirements. However, there is room for improvement in this area.

While many companies are aware of the potential risks associated with BYOD and are taking steps to educate their employees, there are various ways organizations can further enhance security awareness and education among their workforce. Exploring practical strategies and interventions can be instrumental in achieving this goal. For instance, incorporating gamification elements into security training programs can transform the learning process into an engaging and interactive experience. By utilizing interactive learning techniques, offering rewards and incentives, and implementing leaderboards, organizations can effectively motivate employees and encourage active participation.Another valuable approach is the use of scenario-based simulations, which provide a safe environment for employees to gain first-hand experience with real-world security scenarios. By immersing employees

in simulated situations, organizations can help them develop crucial skills and decision-making abilities. Recognizing and showcasing employees' security knowledge and expertise through badging and certification systems can further encourage their commitment to maintaining a secure work environment.Moreover, fostering collaboration and promoting shared responsibility among teams is vital for maintaining security. Team-based activities can facilitate knowledge sharing, problem-solving, and collective vigilance, enabling employees to collectively contribute to the overall security posture of the organization. [362, 363, 364]. However, it is important to acknowledge that implementing these measures and exploring additional strategies does not guarantee absolute protection against all risks. Nevertheless, companies that invest in security training and awareness programs are generally in a more secure position compared to those that neglect such initiatives altogether.

In conclusion, while most organizations have implemented a satisfactory level of security for BYOD, enhancements can be made in security policies and additional security measures. The influence of job sectors, such as Information Technology and Telecommunications, on security policies and separate networks should be taken into account.

11.7 Conclusion

In general, there is a pressing need for BYOD users to prioritize the security of their devices. Although they predominantly rely on conventional security measures such as antimalware software and firewalls, they often neglect other equally critical practices like backing up data or securing their devices against theft, despite being aware of the potential risks posed to their organizations. As previously mentioned, addressing this issue would involve the inclusion of cybersecurity and safety education within school and university curricula [365]. Simultaneously, companies should consistently schedule security awareness training sessions to enhance employees' awareness of security practices.

However, our findings highlight that even advanced users with higher levels of security familiarity exhibit weak security practices. This implies that education alone will not fully resolve the issue, as employees tend to underestimate security risks. Consequently, the responsibility for addressing employees' behavior lies with the respective organization. Specifically, while organizations, in general, have implemented a commendable level of security

when allowing BYOD, the most crucial step is to enforce security policies that clearly define rules for BYOD usage. Additionally, organizations should effectively communicate these policies to their employees, emphasizing the importance of adherence and the potential benefits that can be achieved.

The survey results indicate several areas that warrant further exploration in future research. For instance, a significant aspect that has already been discussed in previous sections of this document and merits further investigation is the tendency of BYOD users to neglect security measures, regardless of their level of security familiarity. Specifically, it would be intriguing to comprehend why advanced BYOD users (those with higher cybersecurity familiarity) tend to overlook certain security measures despite being aware of the various risks involved.

Furthermore, another intriguing question pertains to the actions taken by organizations that permit BYOD after experiencing a cyberattack [8]. For instance, do they enforce stricter rules for their BYOD employees? Do they enhance their systems in alignment with existing BYOD guidelines? How do they handle their BYOD employees in response to such incidents? Do they organize cybersecurity awareness trainings? Exploring their responses and evaluating the potential positive effects on these organizations would be particularly captivating.

Gender	
Female	31.25%
Male	66.25%
Non-binary	2.5%
Age	
18-24	10%
25-34	56.25%
35-44	30%
45-54	2.5%
>54	1.25%
Country	
Albania	1.25%
Greece	87.5%
Germany	5%
Netherlands	2.5%
Switzerland	1.25%
USA	2.5%
Education	
Bachelor's Degree	40%
Master's Degree	52.5%
High School Graduate	3.75%
Doctoral Degree	3.75%
Job Sector	
Accommodation	1.25%
Finance	13.75%
Culture & Arts	2.5%
Education	1.25%
Energy	1.25%
Engineering	7.5%
Health Care	1.25%
Information Technology	45%
Law	6.25%
Marketing	2.5%
Physics	1.25%
Public Sector	1.25%
Telecommunications	15%

Table 11.2: Demographics.

Question	Yes (%)	No(%)	I don't Know(%)
Q11	30%	70%	N/A
Q12	58.75%	16.25%	25%
Q13	27.5%	56.25%	16.25
Q14	77.5%	22.5%	N/A
Q15	82.5%	17.5 %	N/A
Q16	26.25%	21.25%	52.5%
Question:		Q17	
Tunneling (VPN)		82.5%	
Remote Desktop		6.25%	
None		7.5%	
Direct Application Access		1.25%	
Applications Portals		2.5%	
Question	Yes (%)	No(%)	I don't Know(%)
Q18	51.25%	48.75%	N/A
Q19	58.5%	2.5%	39%
Q20	68.3%	0%	31.7%
Q21	77.5%	22.5%	N/A
Q22	81.25%	18.75%	N/A
Q23	50%	50%	N/A
Q24	25%	75%	N/A
Q25	72.5%	27.5%	N/A
Q26	12.5%	87.5%	N/A
Q27	10%	90%	N/A
Q28	51.25%	48.75%	N/A
Q29	35%	31.25%	33.75%
Q30	36.25%	63.75%	N/A
Q31	50%	50%	N/A
Question:		Q32	
Daily		20%	
Weekly		15%	
Monthly		27.5%	
Other		35%	
Blank		2.5%	
Question	Yes (%)	No(%)	I don't Know(%)
Q33	70%	30%	N/A
Q34	53.5%	46.5%	N/A
Question	Yes (%)	No(%)	blank(%)
Q35	66.1%	32.1%	1.8%

Table 11.3: Questions results 11-35

Question	Yes (%)	No(%)	I don't Know(%)
Q37	62.5%	37.5%	N/A
Q38	78%	22%	N/A

Table 11.4: Questions results 37-38

Variables	chi-square value	df
Security familiarity and using malware	1.246093658.	4
Security familiarity and taking backups	6.209019608	4
Security familiarity and properly configured firewall for enterprise environment	6.582352941	4
Security familiarity and locking device when leaving desk	2.702727068	4
Security familiarity and physical security to protect BYOD device from theft	1.979084967	4

Table 11.5: Job Sector and Organizational Measures implementations

Variables	chi-square value	df
Job sector and security policy	11.28654602	3
Job sector and sensitive data storage in BYOD devices	0.838231683	3
Job sector and multi-factor authentication	3.752799219	3
Job sector and NAC solutions	0.805232459	3
Job sector and separate, external networks for BYOD users	12.55838143	3
Job sector and limited capabilities for BYOD devices in organization's network	0.520092019	3
Job sector and use of virtual machines	1.567182547	3

Table 11.6: chi-square test values associated with 'Job Sector and Organizational Measures'

Chapter 12

Research Contributions

The research that has been conducted and presented in this thesis mainly formed the following that can be classified into the following distinct areas: i) identify privacy issues in existing Smart Grid (SG) and cyber insurance ecosystems; ii) develop and implement an holistic security architecture dedicated to SG; iii) define a new ecosystem entitled G2Go as part of the existing SG ecosystem and implement a privacy-preserving architecture protecting the security poster of the G2Go ecosystem itself and its consumers; and iv) develop and implement security applications for the cyber insurance ecosystem to upgrade its effectiveness without affecting the classic cyber insurance processes.

Overall the research contributions of this thesis are listed below:

RC1 Define the G2Go concept and present its functional, security and privacy requirements. This is the first time a scenario for roaming energy consumers is being proposed by the literature.

RC2 Propose P4G2Go, a privacy-preserving scheme designed for the G2Go concept based on well-established security and privacy-preserving technologies.

RC3 Assess P4G2Go's performance and qualitatively reason about its security and privacy properties. For this purpose, the main components of P4G2Go including the Idemix anonymous credential system were implemented.

RC4 Provide security and privacy requirements for a module dedicated to

delivering security authorization and monitoring the security status of the participating nodes of the Smart Grid (SG) network.

RC5 Propose SAMGRID, a novel authorization and security monitoring module tailored to SG needs based on well-established security technologies.

RC6 Implement and assess the SAMGRID's performance in a simulation environment.

RC7 Define security and functional requirements of a tool that is meant to provide developers with CI/CD features following a security by design approach.

RC8 Propose P2ISE, a solution for integrity preservation for software projects within CI/CD environments based on the use of secure elements, in particular the TPM chipset. This is the first work that proposes a tool to bridge the identified security gap.

RC9 Assess the proposed P2ISE's performance and qualitatively reason about its security properties against various projects.

RC10 Provide a comprehensive overview of the challenges plaguing the cyber insurance ecosystem.

RC11 Conduct an in-depth analysis of existing research that leverages Blockchain and Smart Contracts to address the cyber insurance challenges.

RC12 Propose a novel and comprehensive architecture, titled INCHAIN, that integrates Blockchain, Smart Contracts, and SSI technologies to tackle the challenges the cyber insurance industry faces.

RC13 Evaluate the efficacy of INCHAIN architecture, analyzing its suitability for integration within the cyber insurance ecosystem and assessing its ability to address the identified cyber insurance challenges compared to existing research incorporating Blockchain and Smart Contracts.

RC14 Propose a prototype system for parsing cyberinsurance policies/contracts and extracting inclusions and exclusions, offering to the end-user a list of what is covered and what is not. In this way, the user will be able to easily compare several policies/contracts and to choose the one that fits she needs in a better way.

RC15 Implement a decentralized CTI sharing platform based on blockchain so that CTI consumers can automatically generate data in the desired format for their tools, based on indicators provided by CTI reports and fill the gap between CTI and its consumers.

RC16 Introduce a methodology and its implementation as a software tool to facilitate security managers identifying the most appropriate defensive strategies regardless of the organization's environment.

RC17 Automatically calculate the optimal allocation of the limited cybersecurity budget of an organization.

RC18 Effectively combine attack graphs and game theory for the generation of an optimal budget allocation plan.

RC19 Evaluate the proposed tool against three realistic case studies proving its effectiveness in real-life working environments.

Chapter 13

Conclusions

The work of this dissertation lies in two discrete fields, the first one is the smart grid and the second one is the cyber insurance.

Safeguarding the cybersecurity posture of the smart grid is imperative due to its role as the linchpin of modern societies. Operating as critical infrastructure, the smart grid ensures the seamless delivery of essential services and the functioning of vital facilities. The grid's heavy reliance on interconnected digital systems makes it susceptible to various cybersecurity threats that, if exploited, could result in disruptive power supply interruptions affecting emergency services, communication networks, and critical infrastructure. Additionally, the smart grid's reliance on extensive data necessitates stringent measures to preserve data integrity and privacy, as unauthorized access could lead to financial losses and compromise sensitive information. Beyond the immediate societal impacts, the national security implications are substantial, as cyberattacks on the smart grid could be orchestrated to destabilize economies and compromise a nation's overall security. Ensuring a robust cybersecurity posture for the smart grid is not just a technological necessity; it is a safeguard against economic repercussions, a protector of public trust, and an investment in the resilience of critical infrastructure for the prosperity and well-being of nations. This dissertation focused on not increasing the cybersecurity posture of the smart grid by various application focusing in protecting not only the system's availability, integrity and confidentiality, but also its user's privacy. In particular, within this dissertation three security application applied to the smart grid filed have been presented. The first one entitled SAMGRID is able to equip the smart grid network with robust authorization system based on well-defined roles, as well as, a dynamic cyber-

security posture monitoring system. Its performance was presented against various cybersecurity real-life scenarios. Secondly, the work entitled P2ISE was presented that proposed a method for secure code development based on CI/CD process equipped with secure elements, and particularly a TPM. Its performance was evaluated against real-life projects. Last but not least, this dissertation presented for first time a smart grid concept G2Go that allows consumer to travel abroad managing their electricity consumption on the go. However, this concept is consider by numerous security challenges. These were identified by the work and faced by a architecture entitled P4G2Go. This was based on well-known security application such as FIDO 2, TEE and MASKER. The collaboration of these robust technologies assembled a robust cybersecurity application. Its effectiveness and performance was also proved.

The imperative to develop and implement robust cyber insurance programs is underscored by the escalating threat landscape in the digital age. As organizations increasingly rely on technology to conduct business, the potential financial and reputational fallout from a cyber incident has become more pronounced. Cyber insurance serves as a crucial risk management tool, providing a safety net against the potentially catastrophic consequences of data breaches, ransomware attacks, and other cyber threats. By offering financial protection, these policies can assist organizations in covering the costs of incident response, legal fees, and even reputational damage control, thereby promoting resilience in the face of unforeseen cyber challenges. Moreover, cyber insurance can incentivize companies to invest in cybersecurity measures as insurers often require policyholders to adhere to specific security protocols, fostering a proactive approach to risk mitigation.

However, despite its evident advantages, the realm of cyber insurance is not without challenges. The evolving nature of cyber threats poses difficulties in accurately assessing and quantifying risks, leading to complexities in underwriting policies. Insufficient historical data and a lack of standardized risk metrics further compound these challenges. Additionally, the interconnected and global nature of cyberspace means that a single cyber incident can have far-reaching consequences, making it challenging to determine the appropriate scope and coverage for insurance policies. Furthermore, the dynamic nature of cyber risks requires constant adaptation in policy terms and conditions, creating a potential mismatch between evolving threats and the effectiveness of insurance coverage. Striking the right balance between offering comprehensive coverage and maintaining affordability remains an

ongoing challenge for the cyber insurance industry. Despite these hurdles, the pressing need for cyber insurance as a strategic risk management tool is evident, as organizations navigate an increasingly complex and perilous digital landscape. Thus this dissertation includes various works dedicated to the cyber insurance field. First and foremost, a work that describes the existing situation of the cyber insurance was presented. Moreover, a work entitled INCHAIN was presented. It identified the challenges and the basic processes that characterize this field. Also, an architecture was presented with the same name, consisting of Blockchain applications such as Smart Contracts and SSI. The use of SSI was introduced for first time in the cyber insurance field. moreover, a work entitled GTM was presented. This proposed a cyber insurance application dedicated to assist SMEs how to invest their limited budget to specific cybersecurity countermeasures. In addition, the work BRIDGE is presented; it is tools that aims to close the gap between the CTI production and consumption. Its effectiveness was evaluation against real-life scenarios. Furthermore, a cyber insurance ontology was presented dedicated to minimize the information asymmetry among the stakeholders. While, the survey related the Bring Your Own Device proved how important is for the Large Enterprises and SMEs to build the human firewall.

Bibliography

[1] A. Farao, E. Veroni, C. Ntantogian, C. Xenakis, P4g2go: A privacy-preserving scheme for roaming energy consumers of the smart grid-to-go, Sensors 21 (8) (2021) 2686.

[2] G. Suciu, A. Farao, G. Bernardinetti, I. Palamà, M.-A. Sachian, A. Vulpe, M.-C. Vochin, P. Muresan, M. Bampatsikos, A. Muñoz, et al., Samgrid: Security authorization and monitoring module based on sealedgrid platform, Sensors 22 (17) (2022) 6527.

[3] M. Charalambous, A. Farao, G. Kalantzantonakis, P. Kanakakis, N. Salamanos, E. Kotsifakos, E. Froudakis, Analyzing coverages of cyber insurance policies using ontology, in: Proceedings of the 17th International Conference on Availability, Reliability and Security, 2022, pp. 1–7.

[4] G. Petihakis, D. Kiritsis, A. Farao, P. Bountakas, A. Panou, C. Xenakis, A bring your own device security awareness survey among professionals, in: Proceedings of the 18th International Conference on Availability, Reliability and Security, 2023, pp. 1–10.

[5] V. Pantelakis, P. Bountakas, A. Farao, C. Xenakis, Adversarial machine learning attacks on multiclass classification of iot network traffic, in: Proceedings of the 18th International Conference on Availability, Reliability and Security, 2023, pp. 1–8.

[6] M. Karatisoglou, A. Farao, V. Bolgouras, C. Xenakis, Bridge: Bridging the gap between cti production and consumption, in: 2022 14th International Conference on Communications (COMM), IEEE, 2022, pp. 1–6.

[7] I. Kalderemidis, A. Farao, P. Bountakas, S. Panda, C. Xenakis, Gtm: Game theoretic methodology for optimal cybersecurity defending strategies and investments, in: Proceedings of the 17th International Conference on Availability, Reliability and Security, 2022, pp. 1–9.

[8] A. Farao, S. Panda, S. A. Menesidou, E. Veliou, N. Episkopos, G. Kalatzantonakis, F. Mohammadi, N. Georgopoulos, M. Sirivianos, N. Salamanos, et al., Secondo: A platform for cybersecurity investments and cyber insurance decisions, in: Trust, Privacy and Security in Digital Business: 17th International Conference, TrustBus 2020, Bratislava, Slovakia, September 14–17, 2020, Proceedings 17, Springer, 2020, pp. 65–74.

[9] A. Muñoz, A. Farao, J. R. C. Correia, C. Xenakis, Icitpm: Integrity validation of software in iterative continuous integration through the use of trusted platform module (tpm), in: European Symposium on Research in Computer Security, Springer, 2020, pp. 147–165.

[10] A. Farao, J. E. Rubio, C. Alcaraz, C. Ntantogian, C. Xenakis, J. Lopez, Sealedgrid: A secure interconnection of technologies for smart grid applications, in: Critical Information Infrastructures Security: 14th International Conference, CRITIS 2019, Linköping, Sweden, September 23–25, 2019, Revised Selected Papers 14, Springer, 2020, pp. 169–175.

[11] A. Farao, C. Ntantogian, C. Istrate, G. Suciu, C. Xenakis, Sealedgrid: Scalable, trusted, and interoperable platform for secured smart grid, in: 6th International Symposium for ICS & SCADA Cyber Security Research 2019 6, 2019, pp. 74–81.

[12] G. Suciu, C.-I. Istrate, A. Vulpe, M.-A. Sachian, M. Vochin, A. Farao, C. Xenakis, Attribute-based access control for secure and resilient smart grids, in: 6th International Symposium for ICS & SCADA Cyber Security Research 2019 6, 2019, pp. 67–73.

[13] G. Suciu, C. Istrate, M.-A. Sachian, A. Vulpe, M. Vochin, A. Farao, C. Xenakis, Fi-ware authorization in a smart grid scenario, in: 2020 Global Internet of Things Summit (GIoTS), IEEE, 2020, pp. 1–5.

[14] L. et.al, Survey of publicly available reports on advanced persistent threat actors, Computers & Security 72 (2018) 26 – 59.

doi:https://doi.org/10.1016/j.cose.2017.08.005.
URL http://www.sciencedirect.com/science/article/pii/S0167404817301608

[15] R. Langner, Stuxnet: Dissecting a cyberwarfare weapon, IEEE Security Privacy 9 (3) (2011) 49–51. doi:10.1109/MSP.2011.67.

[16] TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case, March 18, 2016, E-ISAC.

[17] A. Cherepanov, GreyEnergy White Paper: A successor to BlackEnergy, 2018.

[18] Cherepanov, A., TeleBots are back – Supply-chain attacks against Ukraine, 2017.

[19] Cyber security in the smart grid: Survey and challenges, Computer Networks 57 (5) (2013) 1344 – 1371. doi:https://doi.org/10.1016/j.comnet.2012.12.017.
URL http://www.sciencedirect.com/science/article/pii/S1389128613000042

[20] http://www.politico.eu/article/smart-grids-and-meters-raise-hacking-risks/.

[21] J. Kim, H. Choi, An efficient and versatile key management protocol for secure smart grid communications, in: 2012 IEEE Wireless Communications and Networking Conference (WCNC), 2012, pp. 1823–1828. doi:10.1109/WCNC.2012.6214081.

[22] M. et. al, A novel identity-based key establishment method for advanced metering infrastructure in smart grid, IEEE Transactions on Smart Grid 9 (4) (2018) 2834–2842. doi:10.1109/TSG.2016.2620939.

[23] P. et. al, Securing metering infrastructure of smart grid: A machine learning and localization based key management approach, Energies 9 (9) (2016). doi:10.3390/en9090691.
URL http://www.mdpi.com/1996-1073/9/9/691

[24] Trusted Computing Group, TPM Mobile with Trusted Execution Environment for Comprehensive Mobile Device Security, Whitepaper, June 2012.

[25] GlobalPlatform: Trusted Execution Environment System Architecture, 2011.

[26] P. et.al, A specification-based intrusion detection engine for infrastructure-less networks, Computer Communications 54 (2014) 67 – 83. doi:https://doi.org/10.1016/j.comcom.2014.08.002.
URL http://www.sciencedirect.com/science/article/pii/S0140366414002813

[27] W. Chin, Y. Lin, H. Chen, A framework of machine-to-machine authentication in smart grid: A two-layer approach, IEEE Communications Magazine 54 (12) (2016) 102–107. doi:10.1109/MCOM.2016.1600304CM.

[28] R. Lu, X. Lin, , X. Shen, Eath: An efficient aggregate authentication protocol for smart grid communications, in: 2013 IEEE Wireless Communications and Networking Conference (WCNC), 2013, pp. 1819–1824. doi:10.1109/WCNC.2013.6554840.

[29] DNP3 Users Group Technical Committee. DNP3 Secure Authentication Specification Version 2.0, DNP Users Group Documentation as a supplement to Volume 2 of DNP3. Technical report, DNP Users Group, 2008.

[30] IEC TS 62351 series, Power systems management and associated information exchange – Data and communications security, Tech specification, 2007.

[31] Secure interoperability in cyber-physical systems (Sep 2017).
URL https://doi.org/10.4018/978-1-5225-1829-7.ch008

[32] N. Saxena, B. J. Choi, R. Lu, Authentication and authorization scheme for various user roles and devices in smart grid, IEEE Transactions on Information Forensics and Security 11 (5) (2016) 907–921. doi:10.1109/TIFS.2015.2512525.

[33] K. et.al, Interoperable device identification in smart-grid environments, in: 2011 IEEE Power and Energy Society General Meeting, 2011, pp. 1–7. doi:10.1109/PES.2011.6039416.

[34] Veichtlbauer et. al Advanced metering and data access infrastructures in smart grid environments. In: The seventh international conference

on sensor technologies and applications (SENSORCOMM), p. 63–8, 2013.

[35] C. Alcaraz, J. Lopez, S. Wolthusen, Policy enforcement system for secure interoperable control in distributed smart grid systems, Journal of Network and Computer Applications 59 (2016) 301 – 314. doi:https://doi.org/10.1016/j.jnca.2015.05.023.
URL http://www.sciencedirect.com/science/article/pii/S1084804515001629

[36] L. Chen, R. Lu, Z. Cao, Pdaft: A privacy-preserving data aggregation scheme with fault tolerance for smart grid communications, Peer-to-Peer Networking and Applications 8 (6) (2015) 1122–1132. doi:10.1007/s12083-014-0255-5.
URL https://doi.org/10.1007/s12083-014-0255-5

[37] F. et. al, A robust and privacy-preserving aggregation scheme for secure smart grid communications in digital communities, Security and Communication Networks 9 (15) (2016) 2779–2788. arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/sec.1188, doi:10.1002/sec.1188.
URL https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1188

[38] K. Kursawe, G. Danezis, M. Kohlweiss, Privacy-friendly aggregation for the smart-grid, in: S. Fischer-Hübner, N. Hopper (Eds.), Privacy Enhancing Technologies, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011, pp. 175–191.

[39] CEN/CENELEC/ETSI, Smart Grid Information Security, December 2014.

[40] F. Knirsch, G. Eibl, D. Engel, Error-resilient masking approaches for privacy preserving data aggregation, IEEE Transactions on Smart Grid 9 (4) (2018) 3351–3361. doi:10.1109/TSG.2016.2630803.

[41] K. Papadamou, S. Zannettou, B. Chifor, S. Teican, G. Gugulea, A. Caponi, A. Recupero, C. Pisa, G. Bianchi, S. Gevers, et al., Killing the password and preserving privacy with device-centric and attribute-based authentication, IEEE Transactions on Information Forensics and Security 15 (2019) 2183–2193.

[42] F. F. Demertzis, G. Karopoulos, C. Xenakis, A. Colarieti, Self-organised key management for the smart grid, in: Ad-hoc, Mobile, and Wireless Networks: 14th International Conference, ADHOC-NOW 2015, Athens, Greece, June 29–July 1, 2015, Proceedings 14, Springer, 2015, pp. 303–316.

[43] G. Karopoulos, C. Ntantogian, C. Xenakis, Masker: Masking for privacy-preserving aggregation in the smart grid ecosystem, Computers & Security 73 (2018) 307–325.

[44] G. Karopoulos, C. Xenakis, S. Tennina, S. Evangelopoulos, Towards trusted metering in the smart grid, in: 2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE, 2017, pp. 1–5.

[45] J. E. Rubio, R. Roman, C. Alcaraz, Y. Zhang, Tracking advanced persistent threats in critical infrastructures through opinion dynamics, in: Computer Security: 23rd European Symposium on Research in Computer Security, ESORICS 2018, Barcelona, Spain, September 3-7, 2018, Proceedings, Part I 23, Springer, 2018, pp. 555–574.

[46] M. W. Khan, J. Wang, M. Ma, L. Xiong, P. Li, F. Wu, Optimal energy management and control aspects of distributed microgrid using multi-agent systems, Sustainable Cities and Society 44 (2019) 855–870.

[47] A. Ghosal, M. Conti, Key management systems for smart grid advanced metering infrastructure: A survey, IEEE Communications Surveys & Tutorials 21 (3) (2019) 2831–2848.

[48] I. Rendroyoko, A. D. Setiawan, et al., Development of meter data management system based-on event-driven streaming architecture for iot-based ami implementation, in: 2021 3rd International Conference on High Voltage Engineering and Power Systems (ICHVEPS), IEEE, 2021, pp. 403–407.

[49] V. Bolgouras, C. Ntantogian, E. Panaousis, C. Xenakis, Distributed key management in microgrids, IEEE Transactions on Industrial Informatics 16 (3) (2019) 2125–2133.

[50] G. Suciu, M.-A. Sachian, A. Vulpe, M. Vochin, A. Farao, N. Koutroumpouchos, C. Xenakis, Sealedgrid: Secure and interoperable platform for smart grid applications, Sensors 21 (16) (2021) 5448.

[51] BlackEnergy APT Attack in Ukraine.

[52] Colonial Announces Pipeline Restart, Says Normal Service Will Take 'Several Days'.

[53] Hackers Breached Colonial Pipeline Using Compromised Password.

[54] The Cyber Kill Chain.

[55] T. Yadav, A. M. Rao, Technical aspects of cyber kill chain, in: Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3, Springer, 2015, pp. 438–452.

[56] J. E. Rubio, C. Alcaraz, J. Lopez, Preventing advanced persistent threats in complex control networks, in: Computer Security–ESORICS 2017: 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II 22, Springer, 2017, pp. 402–418.

[57]

[58] A. Nisioti, G. Loukas, A. Laszka, E. Panaousis, Data-driven decision support for optimizing cyber forensic investigations, IEEE Transactions on Information Forensics and Security 16 (2021) 2397–2412.

[59] J. E. Rubio, R. Roman, C. Alcaraz, Y. Zhang, Tracking apts in industrial ecosystems: A proof of concept, Journal of Computer Security 27 (5) (2019) 521–546.

[60] J. E. Rubio, R. Roman, J. Lopez, Integration of a threat traceability solution in the industrial internet of things, IEEE Transactions on Industrial Informatics 16 (10) (2020) 6575–6583.

[61] A. Gopstein, C. Nguyen, C. O'Fallon, N. Hastings, D. Wollman, et al., NIST framework and roadmap for smart grid interoperability standards, release 4.0, Department of Commerce. National Institute of Standards and Technology . . . , 2021.

[62] C. Alcaraz, J. Lopez, Secure interoperability in cyber-physical systems, in: Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications, IGI Global, 2020, pp. 521–542.

[63] A. Hasankhani, S. M. Hakimi, M. Bisheh-Niasar, M. Shafie-khah, H. Asadolahi, Blockchain technology in the future smart grids: A comprehensive review and frameworks, International Journal of Electrical Power & Energy Systems 129 (2021) 106811.

[64] N. Javaid, H. Gul, S. Baig, F. Shehzad, C. Xia, L. Guan, T. Sultana, Using gancnn and ernet for detection of non technical losses to secure smart grids, IEEE Access 9 (2021) 98679–98700.

[65] H. Yang, S. Liu, C. Fang, Model-based secure load frequency control of smart grids against data integrity attack, IEEE Access 8 (2020) 159672–159682.

[66] S. Boudko, P. Aursand, H. Abie, Evolutionary game for confidentiality in iot-enabled smart grids, Information 11 (12) (2020) 582.

[67] A. Veichtlbauer, D. Engel, F. Knirsch, O. Langthaler, F. Moser, Advanced metering and data access infrastructures in smart grid environments, in: The seventh international conference on sensor technologies and applications (SENSORCOMM), 2013, pp. 63–68.

[68] C. Alcaraz, J. Lopez, S. Wolthusen, Policy enforcement system for secure interoperable control in distributed smart grid systems, Journal of Network and Computer Applications 59 (2016) 301–314.

[69] L. Duan, D. Liu, Y. Zhang, S. Chen, R. P. Liu, B. Cheng, J. Chen, Secure data-centric access control for smart grid services based on publish/subscribe systems, ACM Transactions on Internet Technology (TOIT) 16 (4) (2016) 1–17.

[70] R. Alcarria, B. Bordel, T. Robles, D. Martín, M.-Á. Manso-Callejo, A blockchain-based authorization system for trustworthy resource monitoring and trading in smart communities, Sensors 18 (10) (2018) 3561.

[71] OpenWay Riva, OpenWay Riva, `https://blogs.itron.com/tag/openway-riva/`.

[72] J. R. French Jr, A formal theory of social power., Psychological review 63 (3) (1956) 181.

[73] M. H. DeGroot, Reaching a consensus, Journal of the American Statistical association 69 (345) (1974) 118–121.

[74] Y. Dong, M. Zhan, G. Kou, Z. Ding, H. Liang, A survey on the fusion process in opinion dynamics, Information Fusion 43 (2018) 57–65.

[75] H. Noorazar, Recent advances in opinion propagation dynamics: A 2020 survey, The European Physical Journal Plus 135 (2020) 1–20.

[76] M. Grabisch, A. Rusinowska, A survey on nonstrategic models of opinion dynamics, Games 11 (4) (2020) 65.

[77] J. Lopez, J. E. Rubio, C. Alcaraz, A resilient architecture for the smart grid, IEEE Transactions on Industrial Informatics 14 (8) (2018) 3745–3753.

[78] M. Z. Gunduz, R. Das, Cyber-security on smart grid: Threats and potential solutions, Computer networks 169 (2020) 107094.

[79] A. Muñoz, A. Farao, J. R. C. Correia, C. Xenakis, P2ise: Preserving project integrity in ci/cd based on secure elements, Information 12 (9) (2021) 357.

[80] L. Bass, I. Weber, L. Zhu, DevOps: A Software Architect's Perspective, SEI Series in Software Engineering, Addison-Wesley, New York, 2015.
URL `http://my.safaribooksonline.com/9780134049847`

[81] J. Humble, D. G. Farley, Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation, Addison-Wesley, Upper Saddle River, NJ, 2010.
URL `http://my.safaribooksonline.com/9780321601919`

[82] M. Tichy, M. Goedicke, J. Bosch, B. Fitzgerald, Rapid continuous software engineering, Journal of Systems and Software 133 (2017) 159.

[83] DigitalOcean, Currents: A quarterly report on developer trends in the cloud.

[84] P. André, O. Cardin, Trusted services for cyber manufacturing systems, in: Service Orientation in Holonic and Multi-Agent Manufacturing, Springer, 2018, pp. 359–370.

[85] Justin Ellingwood, An Introduction to CI/CD Best Practices, https://www.digitalocean.com/community/tutorials/an-introduction-to-ci-cd-best-practices, online; accessed on 3 September 2021 (2018).

[86] National Cyber Security Centre, Multi-factor authentication for online services, https://www.digitalocean.com/community/tutorials/an-introduction-to-ci-cd-best-practices, online; accessed on 3 September 2021 (2013).

[87] G. Milka, Anatomy of account takeover, in: Enigma 2018 (Enigma 2018), 2018.

[88] C. Paule, T. F. Düllmann, A. Van Hoorn, Vulnerabilities in continuous delivery pipelines? a case study, in: 2019 IEEE International Conference on Software Architecture Companion (ICSA-C), IEEE, 2019, pp. 102–108.

[89] N. Sathyanarayanan, M. N. Nanda, Two layer cloud security set architecture on hypervisor, in: 2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAECC), IEEE, 2018, pp. 1–5.

[90] J. Mahboob, J. Coffman, A kubernetes ci/cd pipeline with asylo as a trusted execution environment abstraction framework, in: 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, 2021, pp. 0529–0535.

[91] T. Rangnau, R. v. Buijtenen, F. Fransen, F. Turkmen, Continuous security testing: A case study on integrating dynamic security testing tools in ci/cd pipelines, in: 2020 IEEE 24th International Enterprise Distributed Object Computing Conference (EDOC), 2020, pp. 145–154. doi:10.1109/EDOC49727.2020.00026.

[92] L. Bass, R. Holz, P. Rimba, A. B. Tran, L. Zhu, Securing a deployment pipeline, in: 2015 IEEE/ACM 3rd International Workshop on Release Engineering, IEEE, 2015, pp. 4–7.

[93] F. Ullah, A. J. Raft, M. Shahin, M. Zahedi, M. A. Babar, Security support in continuous deployment pipeline, arXiv preprint arXiv:1703.04277 (2017).

[94] P. Rimba, L. Zhu, L. Bass, I. Kuz, S. Reeves, Composing patterns to construct secure systems, in: 2015 11th European Dependable Computing Conference (EDCC), IEEE, 2015, pp. 213–224.

[95] S. Buchanan, J. Rangama, N. Bellavance, Ci/cd with azure kubernetes service, in: Introducing Azure Kubernetes Service, Springer, 2020, pp. 191–219.

[96] V. Mohan, L. B. Othmane, Secdevops: Is it a marketing buzzword?-mapping research on security in devops, in: 2016 11th International Conference on Availability, Reliability and Security (ARES), IEEE, 2016, pp. 542–547.

[97] P. Jauernig, A.-R. Sadeghi, E. Stapf, Trusted execution environments: properties, applications, and challenges, IEEE Security & Privacy 18 (2) (2020) 56–60.

[98] S.-J. Moon, V. Sekar, M. K. Reiter, Nomad: Mitigating arbitrary cloud side channels via provider-assisted migration, in: Proceedings of the 22nd acm sigsac conference on computer and communications security, 2015, pp. 1595–1606.

[99] G. Deepa, P. S. Thilagam, Securing web applications from injection and logic vulnerabilities: Approaches and challenges, Information and Software Technology 74 (2016) 160–180.

[100] T. Lee, G. Won, S. Cho, N. Park, D. Won, Detection and mitigation of web application vulnerabilities based on security testing, in: IFIP International Conference on Network and Parallel Computing, Springer, 2012, pp. 138–144.

[101] S. Lipke, Building a secure software supply chain (2017).

[102] C. Schneider, Security devops-staying secure in agile projects, OWASP AppSec Europe (2015).

[103] N. Koutroumpouchos, C. Ntantogian, C. Xenakis, Building trust for smart connected devices: The challenges and pitfalls of trustzone, Sensors 21 (2) (2021). doi:10.3390/s21020520.
URL https://www.mdpi.com/1424-8220/21/2/520

[104] D. Cerdeira, N. Santos, P. Fonseca, S. Pinto, Sok: Understanding the prevailing security vulnerabilities in trustzone-assisted tee systems, in: 2020 IEEE Symposium on Security and Privacy (SP), IEEE, 2020, pp. 1416–1432.

[105] A. Farao, J. E. Rubio, C. Alcaraz, C. Ntantogian, C. Xenakis, J. Lopez, Sealedgrid: A secure interconnection of technologies for smart grid applications, in: S. Nadjm-Tehrani (Ed.), Critical Information Infrastructures Security, Springer International Publishing, Cham, 2020, pp. 169–175.

[106] S. Matetic, M. Schneider, A. Miller, A. Juels, S. Capkun, Delegatee: Brokered delegation using trusted execution environments, in: 27th {USENIX} Security Symposium ({USENIX} Security 18), 2018, pp. 1387–1403.

[107] A. Vasudevan, E. Owusu, Z. Zhou, J. Newsome, J. M. McCune, Trustworthy execution on mobile devices: What security properties can my mobile platform give me?, in: International Conference on Trust and Trustworthy Computing, Springer, 2012, pp. 159–178.

[108] G. Beniamini, War of the worlds-hijacking the linux kernel from qsee (2016).

[109] A. Machiry, E. Gustafson, C. Spensky, C. Salls, N. Stephens, R. Wang, A. Bianchi, Y. R. Choe, C. Kruegel, G. Vigna, Boomerang: Exploiting the semantic gap in trusted execution environments., in: NDSS, 2017.

[110] D. Rosenberg, Reflections on trusting trustzone, BlackHat USA (2014).

[111] Y. Chen, Y. Zhang, Z. Wang, T. Wei, Downgrade attack on trustzone, arXiv preprint arXiv:1707.05082 (2017).

[112] D. A. Osvik, A. Shamir, E. Tromer, Cache attacks and countermeasures: the case of aes, in: Cryptographers' track at the RSA conference, Springer, 2006, pp. 1–20.

[113] Y. Yarom, K. Falkner, Flush+ reload: A high resolution, low noise, l3 cache side-channel attack, in: 23rd {USENIX} Security Symposium ({USENIX} Security 14), 2014, pp. 719–732.

[114] D. Gruss, C. Maurice, K. Wagner, S. Mangard, Flush+ flush: a fast and stealthy cache attack, in: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, 2016, pp. 279–299.

[115] F. Brasser, U. Müller, A. Dmitrienko, K. Kostiainen, S. Capkun, A.-R. Sadeghi, Software grand exposure:{SGX} cache attacks are practical, in: 11th {USENIX} Workshop on Offensive Technologies ({WOOT} 17), 2017.

[116] A. Moghimi, G. Irazoqui, T. Eisenbarth, Cachezoom: How sgx amplifies the power of cache attacks, in: International Conference on Cryptographic Hardware and Embedded Systems, Springer, 2017, pp. 69–90.

[117] M. Schwarz, S. Weiser, D. Gruss, C. Maurice, S. Mangard, Malware guard extension: Using sgx to conceal cache attacks, in: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, 2017, pp. 3–24.

[118] M. Lipp, D. Gruss, R. Spreitzer, C. Maurice, S. Mangard, Armageddon: Cache attacks on mobile devices, in: 25th {USENIX} Security Symposium ({USENIX} Security 16), 2016, pp. 549–564.

[119] N. Zhang, K. Sun, D. Shands, W. Lou, Y. T. Hou, Truspy: Cache side-channel information leakage from the secure world on arm devices., IACR Cryptol. ePrint Arch. 2016 (2016) 980.

[120] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, M. Hamburg, Meltdown, arXiv preprint arXiv:1801.01207 (2018).

[121] P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, et al., Spectre attacks: Exploiting speculative execution, in: 2019 IEEE Symposium on Security and Privacy (SP), IEEE, 2019, pp. 1–19.

[122] M. Dheerendra, M. Sourav, K. Saru, K. M. Khurram, C. Ankita, Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce, Journal of medical systems 38 (5) (2014) 41.

[123] K. Saru, D. A. Kumar, L. Xiong, W. Fan, K. M. Khurram, J. Qi, I. S. Hafizul, A provably secure biometrics-based authenticated key agreement scheme for multi-server environments, Multimedia Tools and Applications 77 (2) (2018) 2359–2389.

[124] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, Y. Markov, The first collision for full sha-1, in: Annual International Cryptology Conference, Springer, 2017, pp. 570–596.

[125] IBM's TPM 2.0 TSS, `https://sourceforge.net/projects/ibmtpm20tss/`, online; accessed on 3 September 2021.

[126] Microsoft, Tpm software stack (tss) implementations from microsoft, `https://github.com/microsoft/TSS.MSR`, online; accessed on 3 September 2021 (2013).

[127] Server Operating System Market Share, `https://www.t4.ai/industry/server-operating-system-market-share`, online; accessed on 3 September 2021.

[128] Caddy server v2 official one, `https://github.com/caddyserver/caddy`, online; accessed on 3 September 2021.

[129] Nuxt.js+vuetify project, `https://gitlab.com/tip-benchmarking/nuxt-vuetify`, online; accessed on 3 September 2021.

[130] Svelte project, `https://gitlab.com/tip-benchmarking/svelte`, online; accessed on 3 September 2021.

[131] X. Fang, S. Misra, G. Xue, D. Yang, Smart grid—the new and improved power grid: A survey, IEEE communications surveys & tutorials 14 (4) (2011) 944–980.

[132] Vacation Rentals. Homes, Experiences & Places—Airbnb, `https://www.airbnb.com/`, online (2021).

[133] Are Hosts Allowed to 'Spring' Utility Bills on Guests?, https://airhostsforum.com/t/are-hosts-allowed-to-spring-utility-bills-on-guests/122, online (2021).

[134] Electricity Payment on Consumption, https://community.withairbnb.com/t5/Hosting/electricity-payment-on-consumption/td-p/8931, online (2021).

[135] As a Host, How Does One Go about Charging Extra for Water and Electricity When It Is Applicable?, :https://community.withairbnb.com/t5/Help/Extra-charges-for-water-and-electricity/td-p/72432, online (2021).

[136] MBO Partners. COVID-19 and the Rise of the Digital Nomad. White Report. MBO Partners: Herndon, VA, USA, 2020.

[137] Laurent, L., WFH in Greece or Barbados? The Fight for Covid's Digital Nomads., https://www.bloomberg.com/view/articles/2020-11-16/greece-or-barbados-the-tax-fight-for-covid-s-wfh-nomads-begins, online (2020).

[138] Hermann, I.; Paris, C.M. Digital Nomadism: The nexus of remote working and travel mobility. Inf. Technol. Tour. 2020, 22, 329–334.

[139] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, F. Pérez-González, Privacy-preserving data aggregation in smart metering systems: An overview, IEEE Signal Processing Magazine 30 (2) (2013) 75–86.

[140] D. Gabay, K. Akkaya, M. Cebe, Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs, IEEE Transactions on Vehicular Technology 69 (6) (2020) 5760–5772.

[141] J. Camenisch, A. Lysyanskaya, An efficient system for non-transferable anonymous credentials with optional anonymity revocation, in: Advances in Cryptology—EUROCRYPT 2001: International Conference on the Theory and Application of Cryptographic Techniques Innsbruck, Austria, May 6–10, 2001 Proceedings 20, Springer, 2001, pp. 93–118.

[142] F. Veseli, J. Serna, Evaluation of privacy-abc technologies-a study on the computational efficiency, in: Trust Management X: 10th IFIP WG

11.11 International Conference, IFIPTM 2016, Darmstadt, Germany, July 18-22, 2016, Proceedings 10, Springer, 2016, pp. 63–78.

[143] FIDO2: WebAuthn & CTAP, Moving the World Beyond Passwords, `https://fidoalliance.org/fido2`, online.

[144] W. Han, Y. Xiao, Privacy preservation for v2g networks in smart grid: A survey, Computer Communications 91 (2016) 17–28.

[145] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, L. Shu, A systematic review of data protection and privacy preservation schemes for smart grid communications, Sustainable cities and society 38 (2018) 806–835.

[146] M. Kim, K. Park, S. Yu, J. Lee, Y. Park, S.-W. Lee, B. Chung, A secure charging system for electric vehicles based on blockchain, Sensors 19 (13) (2019) 3028.

[147] Y. Zhang, J. Zou, R. Guo, Efficient privacy-preserving authentication for v2g networks, Peer-to-Peer Networking and Applications 14 (3) (2021) 1366–1378.

[148] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, M. Guizani, Lightweight mutual authentication protocol for v2g using physical unclonable function, IEEE Transactions on Vehicular Technology 69 (7) (2020) 7234–7246.

[149] Y. Su, G. Shen, M. Zhang, A novel privacy-preserving authentication scheme for v2g networks, IEEE Systems Journal 14 (2) (2019) 1963–1971.

[150] M. Kaveh, D. Martín, M. R. Mosavi, A lightweight authentication scheme for v2g communications: A puf-based approach ensuring cyber/physical security and identity/location privacy, Electronics 9 (9) (2020) 1479.

[151] M. H. Au, J. K. Liu, J. Fang, Z. L. Jiang, W. Susilo, J. Zhou, A new payment system for enhancing location privacy of electric vehicles, IEEE transactions on vehicular technology 63 (1) (2013) 3–18.

[152] R. Schwerdt, M. Nagel, V. Fetzer, T. Gräf, A. Rupp, P6v2g: a privacy-preserving v2g scheme for two-way payments and reputation, Energy Informatics 2 (1) (2019) 1–21.

[153] C. Höfer, J. Petit, R. Schmidt, F. Kargl, Popcorn: privacy-preserving charging for emobility, in: Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles, 2013, pp. 37–48.

[154] M. A. Mustafa, N. Zhang, G. Kalogridis, Z. Fan, Roaming electric vehicle charging and billing: An anonymous multi-user protocol, in: 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, 2014, pp. 939–945.

[155] K. Shuaib, E. Barka, J. A. Abdella, F. Sallabi, Secure charging and payment protocol (scpp) for roaming plug-in electric vehicles, in: 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT), IEEE, 2017, pp. 0173–0178.

[156] D. Zelle, M. Springer, M. Zhdanova, C. Krauß, Anonymous charging and billing of electric vehicles, in: Proceedings of the 13th International Conference on Availability, Reliability and Security, 2018, pp. 1–10.

[157] N. Saxena, S. Grijalva, V. Chukwuka, A. V. Vasilakos, Network security and privacy challenges in smart vehicle-to-grid, IEEE Wireless Communications 24 (4) (2017) 88–98.

[158] M. Fazouane, H. Kopp, R. W. van der Heijden, D. Le Métayer, F. Kargl, Formal verification of privacy properties in electric vehicle charging, in: Engineering Secure Software and Systems: 7th International Symposium, ESSoS 2015, Milan, Italy, March 4-6, 2015. Proceedings 7, Springer, 2015, pp. 17–33.

[159] N. Saxena, B. J. Choi, Authentication scheme for flexible charging and discharging of mobile vehicles in the v2g networks, IEEE Transactions on Information Forensics and Security 11 (7) (2016) 1438–1452.

[160] M. Tao, K. Ota, M. Dong, Z. Qian, Accessauth: Capacity-aware security access authentication in federated-iot-enabled v2g networks, Journal of Parallel and Distributed Computing 118 (2018) 107–117.

[161] D. Liu, D. Li, X. Liu, L. Ma, H. Yu, H. Zhang, Research on a cross-domain authentication scheme based on consortium blockchain in v2g networks of smart grid, in: 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), IEEE, 2018, pp. 1–5.

[162] P. Gope, B. Sikdar, An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication, IEEE Transactions on Smart Grid 10 (6) (2019) 6607–6618.

[163] F. G. Mármol, C. Sorge, O. Ugus, G. M. Pérez, Do not snoop my habits: preserving privacy in the smart grid, IEEE Communications Magazine 50 (5) (2012) 166–172.

[164] A. Abdallah, X. Shen, Security and privacy in smart grid, Springer, 2018.

[165] Y. Zhang, S. Gjessing, H. Liu, H. Ning, L. T. Yang, M. Guizani, Securing vehicle-to-grid communications in the smart grid, IEEE Wireless Communications 20 (6) (2013) 66–73.

[166] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, R. Cepeda, Privacy for smart meters: Towards undetectable appliance load signatures, in: 2010 first IEEE international conference on smart grid communications, IEEE, 2010, pp. 232–237.

[167] C. Efthymiou, G. Kalogridis, Smart grid privacy via anonymization of smart metering data, in: 2010 first IEEE international conference on smart grid communications, IEEE, 2010, pp. 238–243.

[168] L. Chen, J. Zhou, Y. Chen, Z. Cao, X. Dong, K.-K. R. Choo, Padp: Efficient privacy-preserving data aggregation and dynamic pricing for vehicle-to-grid networks, IEEE Internet of Things Journal 8 (10) (2020) 7863–7873.

[169] J. Camenisch, E. Van Herreweghen, Design and implementation of the idemix anonymous credential system, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002, pp. 21–30.

[170] FIDO Security Reference. FIDO Alliance, : https://fidoalliance.org/specs/fido-v2.0-rd-20180702/fido-security-ref-v2.0-rd-20180702.html, online (2018).

[171] C. Panos, S. Malliaros, C. Ntantogian, A. Panou, C. Xenakis, A security evaluation of fido's uaf protocol in mobile and embedded devices,

in: Digital Communication. Towards a Smart and Secure Future Internet: 28th International Tyrrhenian Workshop, TIWDC 2017, Palermo, Italy, September 18-20, 2017, Proceedings 28, Springer, 2017, pp. 127–142.

[172] F. Benzi, N. Anglani, E. Bassi, L. Frosini, Electricity smart meters interfacing the households, IEEE Transactions on Industrial Electronics 58 (10) (2011) 4487–4494.

[173] FIDO2 Server. Community Edition Provided by StrongKey., `https://github.com/StrongKey/fido`, online.

[174] MASKER Implementation, `https://github.com/gkarop/masker`, online.

[175] Dataset of Hourly Electricity Consumptions from the European Network of Transmission System Operators for Electricity, `https://www.entsoe.eu/data/data-portal/consumption/Pages/default.aspx`, online.

[176] LOCUST, An Open Source Load Testing Tool, `https://locust.io/`, online.

[177] C. Paquin, G. Zaverucha, U-prove cryptographic specification v1. 1, Technical Report, Microsoft Corporation (2011).

[178] P. Vullers, G. Alpár, Efficient selective disclosure on smart cards using idemix, in: IFIP Working Conference on Policies and Research in Identity Management, Springer, 2013, pp. 53–67.

[179] J.-E. Ekberg, K. Kostiainen, N. Asokan, The untapped potential of trusted execution environments on mobile devices, IEEE Security & Privacy 12 (4) (2014) 29–37.

[180] European Commission. Best Available Techniques Reference Document, for the Cyber-Security and Privacy of the 10 Minimum Functional Requirements of the SMART Metering Systems, Smart-Grid Task Force Stakeholder Forum; European Commission: Brussels, Belgium, 2016., .

[181] ENISA. Smart Grid Security. In Annex II. Security Aspects of the Smart Grid; ENISA: Iraklion, Greece, online (2012).

[182] World Wide Web Consortium (W3C), Decentralized identifiers (dids) v1.0, https://www.w3.org/TR/did-core/.

[183] Lodder, M., Khovratovich, D., Anonymous credentials 2.0., https://bit.ly/3dSvUKG.

[184] R. J. Anderson, Liability and computer security: Nine principles, in: European Symposium on Research in Computer Security, Springer, 1994, pp. 231–245.

[185] D. Woods, I. Agrafiotis, J. R. Nurse, S. Creese, Mapping the coverage of security controls in cyber insurance proposal forms, Journal of Internet Services and Applications 8 (1) (2017) 1–13.

[186] B. Schneier, Insurance and the computer industry, Communications of the ACM 44 (3) (2001) 114–114.

[187] R. Böhme, G. Schwartz, et al., Modeling cyber-insurance: towards a unifying framework., in: WEIS, 2010.

[188] A. Marotta, F. Martinelli, S. Nanni, A. Orlando, A. Yautsiukhin, Cyber-insurance survey, Computer Science Review 24 (2017) 35–61.

[189] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, S. K. Sadhukhan, Cyber-risk decision models: To insure it or not?, Decision Support Systems 56 (2013) 11–26.

[190] C. Biener, M. Eling, J. H. Wirfs, Insurability of cyber risk: An empirical analysis, The Geneva Papers on Risk and Insurance-Issues and Practice 40 (1) (2015) 131–158.

[191] S. Panda, D. W. Woods, A. Laszka, A. Fielder, E. Panaousis, Post-incident audits on cyber insurance discounts, Computers & Security 87 (2019) 101593.

[192] P. Bountakas, C. Ntantogian, C. Xenakis, Eknad: Exploit kits' network activity detection, Future Generation Computer Systems 134 (2022) 219–235.

[193] S. Dambra, L. Bilge, D. Balzarotti, Sok: Cyber insurance–technical challenges and a system security roadmap, in: 2020 IEEE Symposium on Security and Privacy (SP), IEEE, 2020, pp. 1367–1383.

[194] A. Tsohou, V. Diamantopoulou, S. Gritzalis, C. Lambrinoudakis, Cyber insurance: state of the art, trends and future directions, International Journal of Information Security (2023) 1–12.

[195] Insurance Fraud Bureau New Zealand Sophos News, Claiming with multiple insurers., `https://bit.ly/42bkhHc`, online.

[196] ENISA, Identity theft: ENISA Threat Landscape.

[197] J. Xu, Y. Wu, X. Luo, D. Yang, Improving the efficiency of blockchain applications with smart contract based cyber-insurance, in: ICC 2020-2020 IEEE International Conference on Communications (ICC), IEEE, 2020, pp. 1–7.

[198] InsurTech, 5 cybersecurity threats hitting insurance companies in 2022., `https://bit.ly/3TeDhAA`, online.

[199] SCMedia, Insurance companies increasingly fall prey to cyberattacks., `https://bit.ly/3Tl8TEO`, online.

[200] PWC, Blockchain, a catalyst for new approaches in insurance.

[201] ZYEN, Interexchainz research project, `https://bit.ly/3mVDr3T`, online.

[202] K. Ruan, Digital asset valuation and cyber risk measurement: Principles of cybernomics, Academic Press, 2019.

[203] R. P. Majuca, W. Yurcik, J. P. Kesan, The evolution of cyberinsurance, arXiv preprint cs/0601020 (2006).

[204] S. Romanosky, L. Ablon, A. Kuehn, T. Jones, Content analysis of cyber insurance policies: How do carriers price cyber risk?, Journal of Cybersecurity 5 (1) (2019) tyz002.

[205] R. Böhme, G. Kataria, Models and measures for correlation in cyber-insurance., in: WEIS, Vol. 2, 2006, p. 3.

[206] R. Böhme, Cyber-insurance revisited., in: Weis, 2005.

[207] B. Aziz, et al., A systematic literature review of cyber insurance challenges, in: 2020 International Conference on Information Technology Systems and Innovation (ICITSI), IEEE, 2020, pp. 357–363.

[208] R. Oppliger, Quantitative risk analysis in information security management: a modern fairy tale, IEEE Security & Privacy 13 (6) (2015) 18–21.

[209] P. Nespoli, D. Papamartzivanos, F. G. Mármol, G. Kambourakis, Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks, IEEE Communications Surveys & Tutorials 20 (2) (2017) 1361–1396.

[210] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, F. Smeraldi, Decision support approaches for cyber security investment, Decision Support Systems 86 (2016) 13–23.

[211] I. M. Organization, Guidelines on maritime cyber risk manageme, http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Default.aspx.

[212] D. Cimpean, J. Meire, V. Bouckaert, S. Vande Casteele, A. Pelle, L. Hellebooge, Analysis of cyber security aspects in the maritime sector (2011).

[213] EIOPA, Cyber risk for insurers– challenges and opportunities, https://eiopa.europa.eu/Publications/Reports/EIOPA_Cyber%20risk%20for%20insurers_Sept2019.pdf.

[214] T. balance small business, What does a cyber liability policy cover?, https://www.becyberawareatsea.com/awareness.

[215] SANS, Bridging the insurance/infosec gap: The sans 2016 cyber insurance survey, https://www.advisenltd.com/2016/06/21/bridging-the-insuranceinfosec-gap-the-sans-2016-cyber-insurance-survey/.

[216] I. Mrakovic, R. Vojinović, Maritime cyber security analysis – how to reduce threats?, Transactions on Maritime Science 8 (2019) 132–139. doi:10.7225/toms.v08.n01.013.

[217] W. E. Forum, The global risks report 2022, 17th edition.

[218] S. Panda, A. Farao, E. Panaousis, C. Xenakis, Cyber-insurance: Past, present and future, in: Encyclopedia of Cryptography, Security and Privacy, Springer, 2021, pp. 1–4.

[219] PANASEER, 2022 cyber insurance market trends report.

[220] Sophos News, Cyber insurance: there's bad news and there's good news., `https://bit.ly/3YQBqmP`, online.

[221] NEW AMERICAS, Are state-sponsored cyber attacks covered by your insurance?, `https://bit.ly/42g0pTa`, online.

[222] K. S. Wan, NotPetya, Not Warfare: Rethinking the Insurance War Exclusion in the Context of International Cyberattacks, Wash. L. Rev. 95 (2020) 1595.

[223] LLOYD'S, Shen attack: Cyber risk in asia pacific ports.

[224] LOCKTON, The cyber insurance dilemma - investment in cyber insurance vs further investment in cyber security.

[225] M. Franco, N. Berni, E. Scheid, C. Killer, B. Rodrigues, B. Stiller, Saci: A blockchain-based cyber insurance approach for the deployment and management of a contract coverage, in: Economics of Grids, Clouds, Systems, and Services: 18th International Conference, GECON 2021, Virtual Event, September 21–23, 2021, Proceedings 18, Springer, 2021, pp. 79–92.

[226] T. Lepoint, G. Ciocarlie, K. Eldefrawy, Blockcis—a blockchain-based cyber insurance system, in: 2018 IEEE International Conference on Cloud Engineering (IC2E), IEEE, 2018, pp. 378–384.

[227] I. Vakilinia, S. Badsha, S. Sengupta, Crowdfunding the insurance of a cyber-product using blockchain, in: 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), IEEE, 2018, pp. 964–970.

[228] F. Loukil, K. Boukadi, R. Hussain, M. Abed, Ciosy: A collaborative blockchain-based insurance system, Electronics 10 (11) (2021) 1343.

[229] S. Kumar, U. Dohare, O. Kaiwartya, et al., Flame: Trusted fire brigade service and insurance claim system using blockchain for enterprises, IEEE Transactions on Industrial Informatics (2022).

[230] A. S. Yadav, V. Charles, D. K. Pandey, S. Gupta, T. Gherman, D. S. Kushwaha, Blockchain-based secure privacy-preserving vehicle accident and insurance registration, Expert Systems with Applications (2023) 120651.

[231] A. Karmakar, P. Ghosh, P. S. Banerjee, D. De, Chainsure: Agent free insurance system using blockchain for healthcare 4.0, Intelligent Systems with Applications 17 (2023) 200177.

[232] I. Bashir, Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more, Packt Publishing Ltd, 2020.

[233] D. Mahmudnia, M. Arashpour, R. Yang, Blockchain in construction management: Applications, advantages and limitations, Automation in Construction 140 (2022) 104379.

[234] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, M. Imran, An overview on smart contracts: Challenges, advances and platforms, Future Generation Computer Systems 105 (2020) 475–491.

[235] A. Sarma, Smart contracts: A way to modern digital world, in: Blockchain and Deep Learning: Future Trends and Enabling Technologies, Springer, 2022, pp. 67–106.

[236] V. Bolgouras, A. Angelogianni, I. Politis, C. Xenakis, Trusted and secure self-sovereign identity framework, in: Proceedings of the 17th International Conference on Availability, Reliability and Security, 2022, pp. 1–6.

[237] A. Mühle, A. Grüner, T. Gayvoronskaya, C. Meinel, A survey on essential components of a self-sovereign identity, Computer Science Review 30 (2018) 80–86.

[238] World Wide Web Consortium (W3C), Verifiable credentials data model v1.1, `https://bit.ly/3Lqde7M`, online.

[239] N. Naik, P. Jenkins, Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology, in: 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), IEEE, 2020, pp. 90–95.

[240] SELFKEY, The self-sovereign digital identity wallet, `https://bit.ly/3yD8qEr`, online.

[241] ENISA, Cyber insurance: Recent advances, good practices and challenges.

[242] D. Woods, A. Simpson, Policy measures and cyber insurance: a framework, Journal of Cyber Policy 2 (2) (2017) 209–226.

[243] P. Bountakas, K. Koutroumpouchos, C. Xenakis, A comparison of natural language processing and machine learning methods for phishing email detection, in: Proceedings of the 16th International Conference on Availability, Reliability and Security, 2021, pp. 1–12.

[244] W. Baer, Rewarding it security in the marketplace, Contemporary security policy 24 (1) (2003) 190–208.

[245] ADVISEN Transforming Insurance, Cyber liability insurance market trends: Survey.

[246] L. Joshila Grace, S. Vigneshwari, R. Sathya Bama Krishna, B. Ankayarkanni, A. Mary Posonia, A joint optimization approach for security and insurance management on the cloud, in: Advances in Intelligent Computing and Communication: Proceedings of ICAC 2021, Springer, 2022, pp. 405–413.

[247] M. M. Khalili, P. Naghizadeh, M. Liu, Designing cyber insurance policies: The role of pre-screening and security interdependence, IEEE Transactions on Information Forensics and Security 13 (9) (2018) 2226–2239.

[248] J. R. Nurse, L. Axon, A. Erola, I. Agrafiotis, M. Goldsmith, S. Creese, The data that drives cyber insurance: A study into the underwriting and claims processes, in: 2020 International conference on cyber situational awareness, data analytics and assessment (CyberSA), IEEE, 2020, pp. 1–8.

[249] Z. Amin, A practical road map for assessing cyber risk, Journal of Risk Research 22 (1) (2019) 32–43.

[250] S. Varga, J. Brynielsson, U. Franke, Cyber-threat perception and risk management in the swedish financial sector, Computers & security 105 (2021) 102239.

[251] S. Chaudhary, V. Gkioulos, S. Katsikas, Developing metrics to assess the effectiveness of cybersecurity awareness program, Journal of Cybersecurity 8 (1) (2022) tyac006.

[252] U. Franke, The cyber insurance market in sweden, Computers & Security 68 (2017) 130–144.

[253] I. goverernance, Iso 27000 series of standards, `https://bit.ly/2zyd9eR`, online.

[254] K. Kirkpatrick, Cyber policies on the rise, Communications of the ACM 58 (10) (2015) 21–23.

[255] S. Mansfield-Devine, Security guarantees: building credibility for security vendors, Network Security 2016 (2) (2016) 14–18.

[256] R. Anderson, R. Böhme, R. Clayton, T. Moore, Security economics and the internal market, Study commissioned by ENISA (2008).

[257] MARSH, Covid-19: Implications for cyber, media, and tech e&o coverage, `https://bit.ly/404bMwl`, online.

[258] AXIS INSURANCE COMPANY, Claim supplemental application.

[259] D. Woods, R. Bohme, J. Wolff, D. Schwarcz, Lessons lost: Incident response in the age of cyber insurance and breach attorneys, in: Proceedings of the 32nd USENIX Security Symposium, 2023.

[260] G. Mott, S. Turner, J. R. Nurse, J. MacColl, J. Sullivan, A. Cartwright, E. Cartwright, Between a rock and a hard (ening) place: Cyber insurance in the ransomware era, Computers & Security (2023).

[261] D. W. Woods, R. Böhme, How cyber insurance shapes incident response: A mixed methods study, in: Workshop on the Economics of Information Security, 2021.

[262] D. W. Woods, J. Weinkle, Insurance definitions of cyber war, The Geneva Papers on Risk and Insurance-Issues and Practice 45 (2020) 639–656.

[263] Z. Lin, T. Sapp, R. Parsa, J. Rees Ulmer, C. Cao, Pricing cyber security insurance, Lin, Zhaoxin, Travis Sapp, Rahul Parsa, Jackie Rees-Ulmer, and Chengxin Cao (2022)," Pricing Cybersecurity Insurance," Journal of Mathematical Finance 12 (1) (2018).

[264] World Wide Web Consortium (W3C), Verifiable credentials json schema specification, draft community group report.

[265] R. Mukta, J. Martens, H.-y. Paik, Q. Lu, S. S. Kanhere, Blockchain-based verifiable credential sharing with selective disclosure, in: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE, 2020, pp. 959–966.

[266] C. Dive, Marriott is still covering — and recovering — expenses from its 2018 data breach, `https://bit.ly/3JFM0sd`, online.

[267] H. Chu, P. Zhang, H. Dong, Y. Xiao, S. Ji, W. Li, A survey on smart contract vulnerabilities: Data sources, detection and repair, Information and Software Technology (2023) 107221.

[268] S. Aggarwal, N. Kumar, Attacks on blockchain, in: Advances in computers, Vol. 121, Elsevier, 2021, pp. 399–410.

[269] B. Putz, G. Pernul, Detecting blockchain security threats, in: 2020 IEEE International Conference on Blockchain (Blockchain), IEEE, 2020, pp. 313–320.

[270] Ethereum Organization, Token standards of ethereum, `https://ethereum.org/en/developers/docs/standards/tokens/`, online.

[271] Hyperledger Foundation, Hyperledger ursa, `https://bit.ly/3OgMYOb`, online.

[272] Protocol Labs, Ipfs powers the distributed web, `https://bit.ly/3ZPEtgg`, online.

[273] Hyperledger Foundation, Hyperledger aries, https://bit.ly/42pFM7o, online.

[274] R. Europe., 25+ cyber security vulnerability statistics and facts of 2021, https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/, [Online; accessed 19-April-2022] (2022).

[275] R. Europe., Internet security report - q3 2021, https://www.watchguard.com/wgrd-resource-center/security-report-q3-2021, [Online; accessed 19-April-2022] (2021).

[276] B. Stojanović, K. Hofer-Schmitz, U. Kleb, Apt datasets and attack modeling for automated detection methods: A review, Computers & Security 92 (2020) 101734.

[277] C. Ntantogian, P. Bountakas, D. Antonaropoulos, C. Patsakis, C. Xenakis, Nodexp: Node. js server-side javascript injection vulnerability detection and exploitation, Journal of Information Security and Applications 58 (2021) 102752.

[278] N. Boumkheld, S. Panda, S. Rass, E. Panaousis, Honeypot type selection games for smart grid networks, in: International Conference on Decision and Game Theory for Security, Springer, 2019, pp. 85–96.

[279] M. G. Ahmed, S. Panda, C. Xenakis, E. Panaousis, Mitre att&ck-driven cyber risk assessment, in: The 17th International Conference on Availability, Reliability and Security, 2022.

[280] S. Panda, S. Rass, S. Moschoyiannis, K. Liang, G. Loukas, E. Panaousis, Honeycar: A framework to configure honeypot vulnerabilities on the internet of vehicles, arXiv preprint arXiv:2111.02364 (2021).

[281] S. Panda, E. Panaousis, G. Loukas, C. Laoudias, Optimizing investments in cyber hygiene for protecting healthcare users, in: From Lambda Calculus to Cybersecurity Through Program Analysis, Springer, 2020, pp. 268–291.

[282] E. Scott, S. Panda, G. Loukas, E. Panaousis, Optimising user security recommendations for ai-powered smart-homes, in: 2022 IEEE Conference on Dependable and Secure Computing (DSC), IEEE, 2022.

[283] S. Panda, A. Farao, E. Panaousis, C. Xenakis, Cyber-Insurance: Past, Present and Future, Springer Berlin Heidelberg, Berlin, Heidelberg, 2019, pp. 1–4.
URL https://doi.org/10.1007/978-3-642-27739-9_1624-1

[284] S. Panda, I. Oliver, S. Holtmanns, Behavioural modelling of attackers' choices, in: Safety and Reliability–Safe Societies in a Changing World, CRC Press, 2018, pp. 119–126.

[285] A. Singhal, X. Ou, Security risk analysis of enterprise networks using probabilistic attack graphs, in: Network Security Metrics, Springer, 2017, pp. 53–73.

[286] S. Wang, Z. Zhang, Y. Kadobayashi, Exploring attack graph for cost-benefit security hardening: A probabilistic approach, Computers & security 32 (2013) 158–169.

[287] E. Panaousis, A. Fielder, P. Malacaria, C. Hankin, F. Smeraldi, Cybersecurity games and investments: A decision support approach, in: International Conference on Decision and Game Theory for Security, Springer, 2014, pp. 266–286.

[288] S. S. Wang, Integrated framework for information security investment and cyber insurance, Pacific-Basin Finance Journal 57 (2019) 101173.

[289] Z. Fan, X. Xu, Apdpk-means: A new differential privacy clustering algorithm based on arithmetic progression privacy budget allocation, in: 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), IEEE, 2019, pp. 1737–1742.

[290] X. Ou, S. Govindavajhala, A. W. Appel, et al., Mulval: A logic-based network security analyzer., in: USENIX security symposium, Vol. 8, Baltimore, MD, 2005, pp. 113–128.

[291] I. Kotenko, E. Doynikova, Security assessment of computer networks based on attack graphs and security events, in: Information and Communication Technology-EurAsia Conference, Springer, 2014, pp. 462–471.

[292] M. Abdallah, P. Naghizadeh, A. R. Hota, T. Cason, S. Bagchi, S. Sundaram, Behavioral and game-theoretic security investments in interdependent systems modeled by attack graphs, IEEE Transactions on Control of Network Systems 7 (4) (2020) 1585–1596.

[293] N. Polatidis, E. Pimenidis, M. Pavlidis, S. Papastergiou, H. Mouratidis, From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks, Evolving Systems 11 (3) (2020) 479–490.

[294] O. Stan, R. Bitton, M. Ezrets, M. Dadon, M. Inokuchi, O. Yoshinobu, Y. Tomohiko, Y. Elovici, A. Shabtai, Extending attack graphs to represent cyber-attacks in communication protocols and modern it networks, IEEE Transactions on Dependable and Secure Computing (2020) 1–1.

[295] Tenable, Nessus: Network vulnerability scanning tool, `https://www.tenable.com/products/nessus`, [Online; accessed 14-April-2022].

[296] R. Europe., Smes in the european data-economy, `https://www.reneweuropegroup.eu/campaigns/2021-07-01/europes-small-and-medium-sized-enterprises-start-ups-and-entrepreneurs-are-a-renew-europe-priority`, [Online; accessed 19-April-2022] (2021).

[297] S. Yi, Y. Peng, Q. Xiong, T. Wang, Z. Dai, H. Gao, J. Xu, J. Wang, L. Xu, Overview on attack graph generation and visualization technology, in: 2013 International Conference on Anti-Counterfeiting, Security and Identification (ASID), IEEE, 2013, pp. 1–6.

[298] NIST, Information security handbook: A guide for managers, nist special publication 800-100. (2007).

[299] M. E. Whitman, H. J. Mattord, Management of information security, Cengage Learning, 2013.

[300] NIST, Nist. guide for conducting risk assessment, nist special publication 800-30 revision 1. (2012).

[301] C. Taylor, A. Krings, J. Alves-Foss, Risk analysis and probabilistic survivability assessment (rapsa): An assessment approach for power substation hardening, in: Proc. ACM Workshop on Scientific Aspects of Cyber Terrorism,(SACT), Washington DC, Vol. 64, 2002.

[302] P. Mishra, G. Tyagi, Game theory based attack graph analysis for cyber war strategy, INDIACom (2018).

[303] Common vulnerability scoring system sig, `https://www.first.org/cvss/`, [Online; accessed 19-April-2022].

[304] ISO, Iso/iec 27001:2013, `https://www.iso.org/standard/54534.html`, [Online; accessed 19-April-2022] (2013).

[305] D. Shahjee, N. Ware, Integrated network and security operation center: A systematic analysis, IEEE Access 10 (2022) 27881–27898. `doi:10.1109/ACCESS.2022.3157738`.

[306] X. Bouwman, V. Le Pochat, P. Foremski, T. Van Goethem, C. H. Gañán, G. Moura, S. Tajalizadehkhoob, W. Joosen, M. van Eeten, Helping hands: Measuring the impact of a large threat intelligence sharing community, in: Proceedings of the 31st USENIX Security Symposium, USENIX Association, 2022.

[307] M. S. Abu, S. R. Selamat, A. Ariffin, R. Yusof, Cyber threat intelligence–issue and challenges, Indonesian Journal of Electrical Engineering and Computer Science 10 (1) (2018) 371–379.

[308] P. I. LLC., The value of threat intelligence : A study of north american & united kingdom companies sponsored by anomali. (2016).

[309] E. Agyepong, Y. Cherdantseva, P. Reinecke, P. Burnap, Challenges and performance metrics for security operations center analysts: a systematic review, Journal of Cyber Security Technology 4 (3) (2020) 125–152.

[310] M. Vielberth, F. Böhm, I. Fichtinger, G. Pernul, Security operations center: A systematic study and open challenges, IEEE Access 8 (2020) 227756–227779. `doi:10.1109/ACCESS.2020.3045514`.

[311] D. Schlette, M. Caselli, G. Pernul, A comparative study on cyber threat intelligence: The security incident response perspective, IEEE Communications Surveys Tutorials 23 (4) (2021) 2525–2556. doi:10.1109/COMST.2021.3117338.

[312] T. Sun, P. Yang, M. Li, S. Liao, An automatic generation approach of the cyber threat intelligence records based on multi-source information fusion, Future Internet 13 (2) (2021) 40.

[313] S. Zhou, Z. Long, L. Tan, H. Guo, Automatic identification of indicators of compromise using neural-based sequence labelling, arXiv preprint arXiv:1810.10156 (2018).

[314] Z. Long, L. Tan, S. Zhou, C. He, X. Liu, Collecting indicators of compromise from unstructured text of cybersecurity articles using neural-based sequence labelling, in: 2019 International Joint Conference on Neural Networks (IJCNN), IEEE, 2019, pp. 1–8.

[315] M. van Haastrecht, G. Golpur, G. Tzismadia, R. Kab, C. Priboi, D. David, A. Răcătăian, L. Baumgartner, S. Fricker, J. F. Ruiz, et al., A shared cyber threat intelligence solution for smes, Electronics 10 (23) (2021) 2913.

[316] S. Barnum, Standardizing cyber threat intelligence information with the structured threat information expression (stix), Mitre Corporation 11 (2012) 1–22.

[317] C. Sillaber, C. Sauerwein, A. Mussmann, R. Breu, Data quality challenges and future research directions in threat intelligence sharing practice, in: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, 2016, pp. 65–70.

[318] O. C. T. I. C. TC, Stix™ version 2.1, https://docs.oasis-open.org/cti/stix/v2.1/csprd01/stix-v2.1-csprd01.html (Online).

[319] S. SIEM, https://www.splunk.com/ (Online).

[320] S. Magazine, 92% of data breaches in q1 2022 due to cyberattacks, securitymagazine.com/articles/97431-92-of-data-breaches-in-q1-2022-due-to-cyberattacks, [Online; accessed 19-June-2022] (2022).

[321] IBM, Cost of a data breach report 2021 (2022).

[322] R. Pal, Cyber-insurance in internet security: A dig into the information asymmetry problem, arXiv preprint arXiv:1202.0884 (2012).

[323] T. Bandyopadhyay, V. S. Mookerjee, R. C. Rao, Why it managers don't go for cyber-insurance products, Communications of the ACM 52 (11) (2009) 68–73.

[324] G. Ganino, D. Lembo, M. Mecella, F. Scafoglieri, Ontology population for open-source intelligence: A gate-based solution, Software: Practice and Experience 48 (12) (2018) 2302–2330.

[325] S. A. Elnagdy, M. Qiu, K. Gai, Cyber incident classifications using ontology-based knowledge representation for cybersecurity insurance in financial industry, in: 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), IEEE, 2016, pp. 301–306.

[326] A. Gupta, S. Mittal, K. P. Joshi, C. Pearce, A. Joshi, Streamlining management of multiple cloud services, in: 2016 IEEE 9th International Conference on Cloud Computing (CLOUD), IEEE, 2016, pp. 481–488.

[327] K. P. Joshi, A. Gupta, S. Mittal, C. Pearce, A. Joshi, T. Finin, Semantic approach to automating management of big data privacy policies, in: 2016 IEEE International Conference on Big Data (Big Data), IEEE, 2016, pp. 482–491.

[328] K. Joshi, K. P. Joshi, S. Mittal, A semantic approach for automating knowledge in policies of cyber insurance services, in: 2019 IEEE International Conference on Web Services (ICWS), IEEE, 2019, pp. 33–40.

[329] S. Romanosky, L. Ablon, A. Kuehn, T. Jones, Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk?, Available at SSRN 2929137 (2017).

[330] S. Magazine, Secondo, `https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=`

080166e5dab106e5&appId=PPGMS7, [Online; accessed 19-June-2022] (2021).

[331] ZIPPIA THE CAREER EXPERT, 26 surprising byod statistics [2023]: Byod trends in the workplace, https://www.zippia.com/advice/byod-statistics/, online (2022).

[332] C. Caldwell, S. Zeltmann, K. Griffin, Byod (bring your own device), in: Competition forum, Vol. 10, American Society for Competitiveness, 2012, pp. 117–121.

[333] T. Shumate, M. Ketel, Bring your own device: Benefits, risks and control techniques, in: Ieee Southeastcon 2014, IEEE, 2014, pp. 1–6.

[334] D. Wiech, The benefits and risks of byod, Manufacturing Business Technology 28 (2013).

[335] K. C. Laudon, J. P. Laudon, Management information system, Pearson Education India, 2015.

[336] M. Souppaya, K. Scarfone, Guide to enterprise telework, remote access, and bring your own device (byod) security (2016-07-29 2016). doi:https://doi.org/10.6028/NIST.SP.800-46r2.

[337] K. Miller, J. Voas, G. Hurlburt, Byod: Security and privacy considerations, IT Professional 14 (2012) 53–55. doi:10.1109/MITP.2012.93.

[338] E. Osei Yeboah-Boateng, F. E. Boaten, Bring-Your-Own-Device (BYOD): An Evaluation of Associated Risks to Corporate Information Security, arXiv e-prints (2016) arXiv:1609.01821arXiv:1609.01821, doi:10.48550/arXiv.1609.01821.

[339] B. Hayes, K. Kotwica, Bring your own device (BYOD) to work: Trend report, Newnes, 2013.

[340] Y. Wang, J. Wei, K. Vangury, Bring your own device security issues and challenges, in: 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), 2014, pp. 80–85. doi:10.1109/CCNC.2014.6866552.

[341] K. Hajdarevic, P. Allen, M. Spremic, Proactive security metrics for bring your own device (byod) in iso 27001 supported environments, in: 2016 24th Telecommunications Forum (TELFOR), IEEE, 2016, pp. 1–4.

[342] A. Koohang, K. Floyd, N. Rigole, J. Paliszkiewicz, Security policy and data protection awareness of mobile devices in relation to employees' trusting beliefs, Online Journal of Applied Knowledge Management 6 (2018) 7–22. doi:10.36965/OJAKM.2018.6(2)7-22.

[343] F. Li, C.-T. Huang, J. Huang, W. Peng, Feedback-based smartphone strategic sampling for byod security, in: 2014 23rd International Conference on Computer Communication and Networks (ICCCN), 2014, pp. 1–8. doi:10.1109/ICCCN.2014.6911814.

[344] K. AlHarthy, W. Shawkat, Implement network security control solutions in byod environment, in: 2013 IEEE International Conference on Control System, Computing and Engineering, 2013, pp. 7–11. doi:10.1109/ICCSCE.2013.6719923.

[345] T. A. Wani, A. Mendoza, K. Gray, Hospital bring-your-own-device security challenges and solutions: Systematic review of gray literature, JMIR Mhealth Uhealth 8 (6) (2020) e18175. doi:10.2196/18175.
URL https://doi.org/10.2196/18175

[346] M. A. Muhammad, A. Ayesh, P. B. Zadeh, Developing an intelligent filtering technique for bring your own device network access control, in: proceedings of the international conference on future networks and distributed systems, 2017, pp. 1–8.

[347] J. Concepcion, J. Chua, G. Siy, A. Ballon, Securing android byod (bring your own device) with network access control (nac) and mdm (mobile device management), in: Teoksessa Proceedings of the DLSU Research Congress, Vol. 3, 2015, pp. 2–4.

[348] B. I. Blog, Byod: Exploring the evolution of work device practices in a new remote-forward era [survey] (May 2021).
URL https://www.beyondidentity.com/blog/byod-exploring-evolution-work-device-practices-survey

[349] M. M. Singh, C. W. Chan, Z. Zulkefli, Security and privacy risks awareness for bring your own device (byod) paradigm, International Journal of Advanced Computer Science and Applications 8 (2) (2017).

[350] E. Bell, A. Bryman, B. Harley, Business research methods, Oxford university press, 2022.

[351] George Petihakis, Dimitrios Kiritsis, Panagiotis Bountakas, Aristeidis Farao, Aggeliki Panou, and Christos Xenakis, The complete questionnaire of the survey., `https://drive.google.com/open?id=1csWu_GXKfAn4_4U61GMg-KHKi3XqrYvX&usp=drive_fs`, online (2023).

[352] H. O. Lancaster, E. Seneta, Chi-square distribution, Encyclopedia of biostatistics 2 (2005).

[353] F. Valenza, M. Cheminod, An optimized firewall anomaly resolution., J. Internet Serv. Inf. Secur. 10 (1) (2020) 22–37.

[354] Q. Liu, J. W. Stokes, R. Mead, T. Burrell, I. Hellen, J. Lambert, A. Marochko, W. Cui, Latte: Large-scale lateral movement detection, in: MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM), IEEE, 2018, pp. 1–6.

[355] P. Mueller, B. Yadegari, The stuxnet worm, Département des sciences de linformatique, Université de lArizona. Recuperado de: https://www2. cs. arizona. edu/˜ collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report. pdf (2012).

[356] V. W.-S. Tseng, M. L. Lee, L. Denoue, D. Avrahami, Overcoming distractions during transitions from break to work using a conversational website-blocking system, in: Proceedings of the 2019 CHI conference on human factors in computing systems, 2019, pp. 1–13.

[357] G. Mark, M. Czerwinski, S. T. Iqbal, Effects of individual differences in blocking workplace distractions, in: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 2018, pp. 1–12.

[358] A. Ugoni, B. F. Walker, The chi square test: an introduction, COMSIG review 4 (3) (1995) 61.

[359] I. DEN, S. MONATEN, P. VON, D. PANDEMIE, P. ALS, J. ZUVOR, I. I. S. D. EINEN, C. GEFÄHRDET, Sonicwall cyber threat report (2021).

[360] P. Bountakas, C. Xenakis, Helphed: Hybrid ensemble learning phishing email detection, Journal of Network and Computer Applications 210 (2023) 103545.

[361] Grand Canyon University, A lost laptop is a cybersecurity threat, `https://www.gcu.edu/blog/engineering-technology/lost-laptop-cybersecurity-threat`, online (2019).

[362] K. Khando, S. Gao, S. M. Islam, A. Salman, Enhancing employees information security awareness in private and public organisations: A systematic literature review, Computers & security 106 (2021) 102267.

[363] E. G. B. Gjertsen, E. A. Gjære, M. Bartnes, W. R. Flores, Gamification of information security awareness and training., in: ICISSP, 2017, pp. 59–70.

[364] K. H. Sharif, S. Y. Ameen, A review of security awareness approaches with special emphasis on gamification, in: 2020 International Conference on Advanced Science and Engineering (ICOASE), IEEE, 2020, pp. 151–156.

[365] I. Androulidakis, G. Kandus, Mobile phone security awareness and practices of students in budapest, in: Proceedings of the 6th International Conference on Digital Telecommunications, 2011, pp. 17–22.