University of Piraeus

School of Information and Communication Technologies

Department of Digital Systems

Postgraduate Program: Digital Systems Security

Subject: Security and Privacy Protection in IoT and Integration in Smart Cities

Supervisor Professor: Prof. Stefanos Gritzalis

Name-Surname	E-mail	Student ID.
Orestis Kokkolis	mte2110@unipi.gr	MTE2110

Piraeus

May 2023

Summary

The purpose of this work is to investigate how the Internet of Things, a technology that is transforming the way we interact with our surroundings. The rapid growth of this technology also raises significant concerns regarding privacy and security. With a wide range of applications, from smart homes to industrial automation, IoT devices collect and transmit sensitive data that can be exploited if security measures are inadequate. Breaches in IoT devices allow adversaries to gain unauthorized access and misuse personal information for nefarious purposes. Additionally, the interconnected nature of IoT networks makes them susceptible to attacks that compromise the entire system.

This issue becomes even more critical in the context of smart cities, where infrastructure management relies heavily on IoT technology. Protecting privacy and security in smart city networks presents unique challenges due to the sheer number of devices and the complexity of the networks themselves. Furthermore, the diverse range of devices and legacy infrastructure used in these networks complicates the implementation of consistent security measures.

To address these challenges, it is essential to prioritize the implementation of secure authentication mechanisms, regular software updates, and robust encryption to protect data during transit. Additionally, establishing regulatory frameworks to enforce minimum security and privacy standards for IoT devices is crucial. By proactively tackling these issues, we can harness the benefits of IoT technology while ensuring the privacy and security of individuals and organizations in an increasingly connected world.

Περίληψη

Σκοπός αυτής της εργασίας είναι να διερευνήσει πώς το Διαδίκτυο των Πραγμάτων, μια τεχνολογία που μεταμορφώνει τον τρόπο που αλληλεπιδρούμε με το περιβάλλον μας. Η ταχεία ανάπτυξη αυτής της τεχνολογίας εγείρει επίσης σημαντικές ανησυχίες σχετικά με το απόρρητο και την ασφάλεια. Με ένα ευρύ φάσμα εφαρμογών, από έξυπνα σπίτια έως βιομηχανικούς αυτοματισμούς, οι συσκευές IoT συλλέγουν και μεταδίδουν ευαίσθητα δεδομένα που μπορούν να γίνουν αντικείμενο εκμετάλλευσης εάν τα μέτρα ασφαλείας είναι ανεπαρκή. Οι παραβιάσεις σε συσκευές IoT δυνητικά μπορούν να επιτρέψουν σε κακόβουλες οντότητες να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση και να κάνουν κατάχρηση προσωπικών πληροφοριών για κακόβουλους σκοπούς. Επιπλέον, η διασυνδεδεμένη φύση των δικτύων IoT τα καθιστά επιρρεπή σε επιθέσεις που θέτουν σε κίνδυνο ολόκληρο το σύστημα.

Αυτό το ζήτημα γίνεται ακόμη πιο κρίσιμο στο πλαίσιο των έξυπνων πόλεων, όπου η διαχείριση της υποδομής βασίζεται σε μεγάλο βαθμό στην τεχνολογία IoT. Η προστασία του απορρήτου και της ασφάλειας στα έξυπνα δίκτυα πόλεων παρουσιάζει μοναδικές προκλήσεις λόγω του τεράστιου αριθμού συσκευών και της πολυπλοκότητας των ίδιων των δικτύων. Επιπλέον, η ποικιλία των συσκευών και της παλαιού τύπου υποδομής που χρησιμοποιούνται σε αυτά τα δίκτυα περιπλέκει την εφαρμογή συνεπών μέτρων ασφαλείας.

Για την αντιμετώπιση αυτών των προκλήσεων, είναι απαραίτητο να δοθεί προτεραιότητα στην εφαρμογή ασφαλών μηχανισμών ελέγχου ταυτότητας, τακτικές ενημερώσεις λογισμικού και ισχυρή κρυπτογράφηση για την προστασία των δεδομένων κατά τη μεταφορά. Επιπλέον, η θέσπιση ρυθμιστικών πλαισίων για την επιβολή ελάχιστων προτύπων ασφάλειας και απορρήτου για συσκευές IoT είναι ζωτικής σημασίας. Αντιμετωπίζοντας προληπτικά αυτά τα ζητήματα, μπορούμε να εκμεταλλευτούμε τα οφέλη της τεχνολογίας IoT διασφαλίζοντας παράλληλα το απόρρητο και την ασφάλεια των ατόμων και των οργανισμών σε έναν όλο και πιο διασυνδεδεμένο κόσμο.

CONTENTS

1 Introduction

The Internet of Things (IoT) is a type of technology that is undergoing rapid development and is changing the way in which people interact with their surroundings. Devices connected to the IoT are currently being put to use in a wide variety of applications, ranging from smart homes and wearables to industrial automation and infrastructure management. On IoT networks, the requirement for security and privacy protection is growing in tandem with the expansion of the number of connected devices.
Because these devices collect and transmit sensitive data, ensuring that they have adequate privacy and security measures in place is of the utmost importance. An adversary can gain access to this data and use it for nefarious purposes if an IoT device is breached and compromised. In addition, many of the devices that make up the IoT are connected to one another and share data, which makes them susceptible to attacks that can compromise entire networks.
The protection of users' privacy is equally important in IoT networks as the prevention of security breaches. A large number of IoT devices collect personally identifiable information, such as an individual's location and patterns of use, which can be used to identify the device's owner. Because this information lacks adequate privacy protection, it is vulnerable to being accessed and used by unauthorized parties for whatever purpose they choose.
Applications for "smart cities" are increasingly making use of the IoT technology as it continues to expand. The infrastructure of smart cities, such as traffic lights, public transportation, and waste management, is monitored and managed with the help of devices connected to the IoT. However, the scope of IoT networks in smart cities presents significant challenges to both privacy and security.
In a smart city network, one of the challenges is the sheer number of devices and endpoints that need to be protected from unauthorized access. Because of the complexity of these networks, it is difficult to detect and respond to attacks. Since each device represents a potential point of entry for attackers, it is also difficult to detect these attacks.
Another obstacle to overcome is the wide variety of technologies and devices that are used in smart city networks. It's possible that different applications and devices will have varying security requirements; it can be difficult to guarantee that all of your devices will satisfy these requirements. In addition, many IoT networks for smart cities are constructed using legacy infrastructure, which may not have been designed with security in mind. This makes it difficult to retrofit security measures onto these systems.
In spite of these obstacles, there are actions that can be taken to improve the safety as well as the privacy of IoT networks. These actions can be taken in smart cities as well as in other locations. Among these are the implementation of secure authentication mechanisms to prevent unauthorized access, the regular updating of software and firmware to address known vulnerabilities, and the utilization of strong encryption to protect data while it is in transit. In addition, regulatory frameworks can be established to guarantee that IoT devices meet predetermined minimums for both security and privacy. We can ensure

that the IoT technology continues to provide value while protecting the security and privacy of individuals and organizations if we address these challenges and find solutions to them.

2 Acronyms & Abbreviations table

Abbreviation	Meaning
AI	Artificial Intelligence
BAS	Building Automation Systems
C&C/C2	Command and Control
CAV	Connected and Autonomous Vehicles
CMMI	Capability Maturity Model Integration
DDos	Distributed Denial of Service
EBSI	European Blockchain Services Infrastructure
ECU	Electronic Control Unit
EHR	Electronic Health Records
ENISA	European Union Agency for Cybersecurity
EU	European Union
EV	Electronic Vehicle
HIE	Health Information Exchange
HVAC	Heating, Ventilation, and Air Conditioning
IBMS	Integrated Building Management Systems
IEQ	Indoor Environmental Quality
IoT	Internet of Things
IoTCC	IoT Coalition Canada
IRC	Internet Relay Chat
MaaS	Mobility as a Service
ML	Machine Learning
NIS	Network and Information Systems
P2P	Peer to Peer
PCI DSS	Payment Card Industry Data Security Standard
PDoS	Permanent Denial of Service
SCMM	Security Capability Maturity Model
SDLC	Software Development Life Cycle
SME	Small and Medium Enterprises
SMM	Security Maturity Models
TPM	Trusted Platform Module

3 The Emergence of IoT and Smart Cities

The concept of Smart Cities has gained significant attention in recent years, with the aim of improving the quality of life for citizens by utilizing advanced technologies. The Internet of Things has emerged as a key enabler for the development of Smart Cities. IoT technology involves the integration of various sensors, devices, and applications that can connect and communicate with each other, generating vast amounts of data. This data can be analyzed to provide insights and inform decision-making processes, leading to more efficient and sustainable urban environments. However, the implementation of IoT in Smart Cities also presents significant challenges that need to be addressed. This thesis paper will explore the opportunities and challenges associated with the integration of IoT in Smart Cities, drawing on relevant academic literature and research studies.

3.1 Experimental IoT systems by Cities Around the World

IoT (Internet of Things) and Smart Cities are two emerging technologies that have the potential to revolutionize how cities operate and how people live in them. IoT refers to the network of interconnected devices that communicate with each other over the internet. Smart Cities, on the other hand, are cities that use IoT devices and other technology to improve efficiency, sustainability, and the quality of life for their residents.

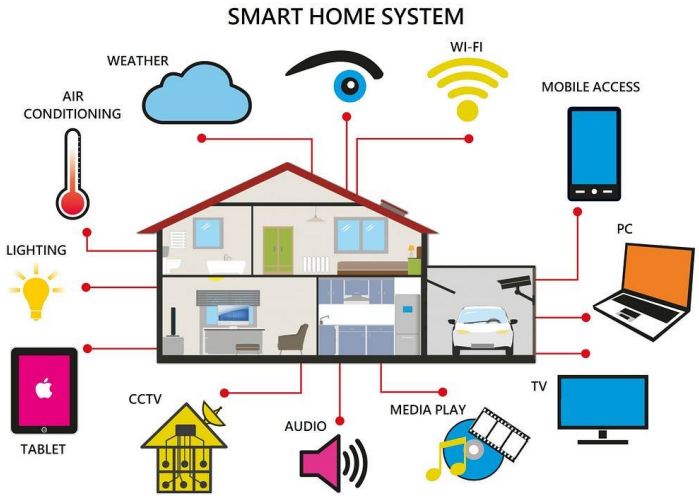

Figure 1: Interconnected home [1]

1 https://miro.medium.com/v2/resize:fit:1100/format:webp/1*hqsFMZmfnVMdO-B_dtOoYg.jpeg

The adoption of IoT and Smart City technology has been rapid in recent years. According to a report by MarketsandMarkets, the global IoT market size is expected to grow from USD 250.72 billion in 2019 to USD 1,463.19 billion by 2027[2]. This growth can be attributed to the increasing number of connected devices, the availability of low-cost sensors, and the development of advanced analytics tools.

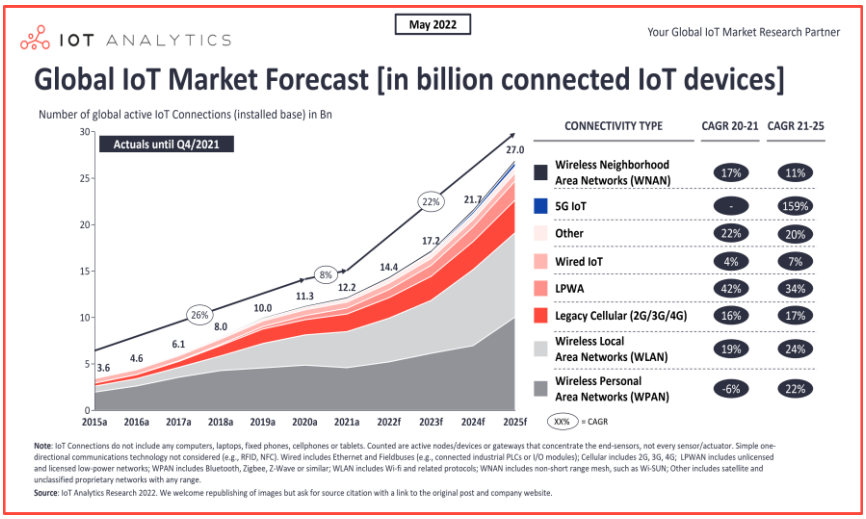

Figure 2: Interconnected IoT devices until May '22 and estimated future progression [3]

One of the primary drivers of IoT adoption has been the increasing number of devices that are becoming connected to the internet. In 2020, it was estimated that there were 31 billion IoT devices in use worldwide, a number that is expected to grow to 75 billion by 2025[4]. This growth is due to the increasing availability of low-cost sensors and the development of new wireless technologies like 5G.

Smart Cities are also gaining traction around the world. According to a report by Navigant Research, the global smart city market is expected to grow from USD 308 billion in 2018 to USD 717 billion by 2023[5]. The report cites the increasing demand for sustainable and efficient urban environments as the primary driver of this growth.

2 MarketsandMarkets (2020). https://marketsandmarkets.com/Market-Reports/iot-market-199913624.html

3 https://h9e3r9w2.rocketcdn.me/wp/wp-content/uploads/2022/05/Global-IoT-Market-Forecast-in-billion-connected-IoT-devices-min.png

4 Statista (2021). https://statista.com/statistics/471264/iot-number-of-connected-devices-worldwide

5 Navigant Research (2018). https://navigantresearch.com/news-and-views/global-smart-city-market-to-reach-717-billion-by-2023

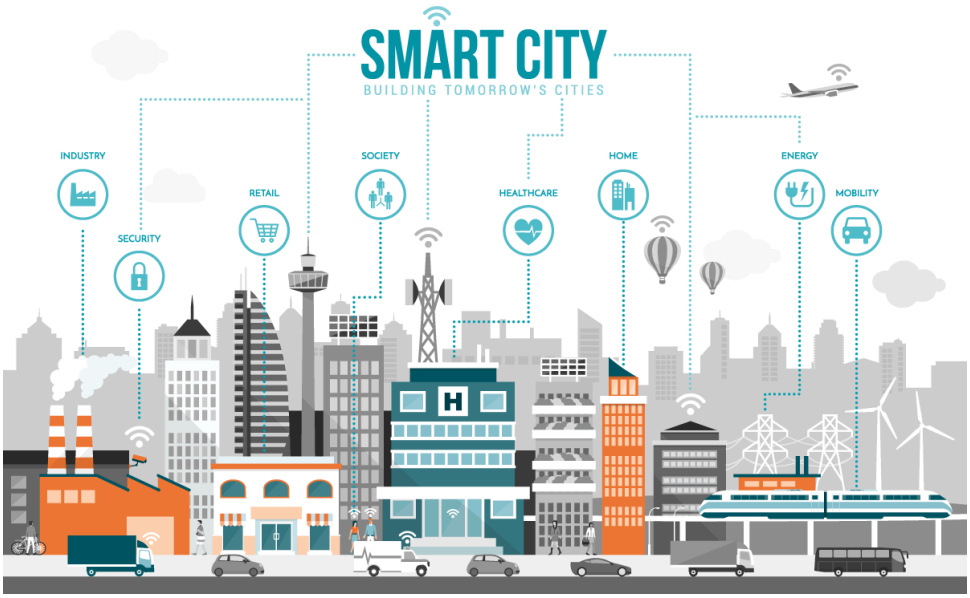

Figure 3: Smart city [6]

Several cities around the world have already implemented IoT and Smart City technology. For example, Barcelona has implemented a Smart Lighting system that uses sensors to detect when a street is empty and automatically dims the lights to save energy. The city has also implemented a Smart Water system that uses sensors to detect leaks and automatically shuts off the water supply to prevent waste[7].

In Amsterdam, the Smart City initiative has focused on improving mobility and reducing traffic congestion. The city has implemented a Smart Parking system that uses sensors to detect available parking spots and directs drivers to them, reducing the time spent looking for parking and therefore reducing traffic[8]

In Singapore, the Smart Nation initiative aims to use IoT and Smart City technology to improve the quality of life for residents. The city-state has implemented a Smart Traffic Management system that uses sensors and cameras to monitor traffic flow and adjust traffic lights accordingly, reducing congestion and improving travel times[9].

The advent of IoT and Smart Cities has the potential to alter how cities operate and how their inhabitants live. Some towns throughout the world have already adopted IoT and Smart City initiatives as the acceptance of these technologies is accelerating. Notwithstanding worries over security and privacy, these technologies provide a promising future for the development of sustainable and efficient urban environments.

---

6 https://hlp.city/wp-content/uploads/2022/01/smart-city-hero-image-5.gif

7 Maksimovic, M. (2018). https://smartcityhub.com/sustainability/smart-city-barcelona-blueprint-sustainable-urban-living

8 Karan, S. (2019). https://cities-today.com/amsterdams-smart-city-a-model-of-innovation-for-urban-transformation

9 Lim, D. (2017). https://mckinsey.com/business-functions/digital-mckinsey/our-insights/singapores-smart-nation-initiative-a-conversation-with-jacqueline-poh

3.2 Opportunities of IoT in Smart Cities

IoT technology provides a multitude of opportunities for the development of Smart Cities. One of the key benefits is the ability to monitor and manage various urban systems, such as transportation, energy, and waste management, in real-time. For instance, IoT-enabled sensors can be used to monitor traffic flow, identify congestion, and optimize traffic signals to reduce congestion and improve the efficiency of the transportation system[10]. IoT can also be used to monitor energy consumption patterns and identify opportunities for energy conservation, such as by turning off lights in unoccupied spaces or optimizing heating and cooling systems based on occupancy[11]. Additionally, IoT can help in the development of sustainable cities by identifying opportunities for waste reduction and recycling[12].

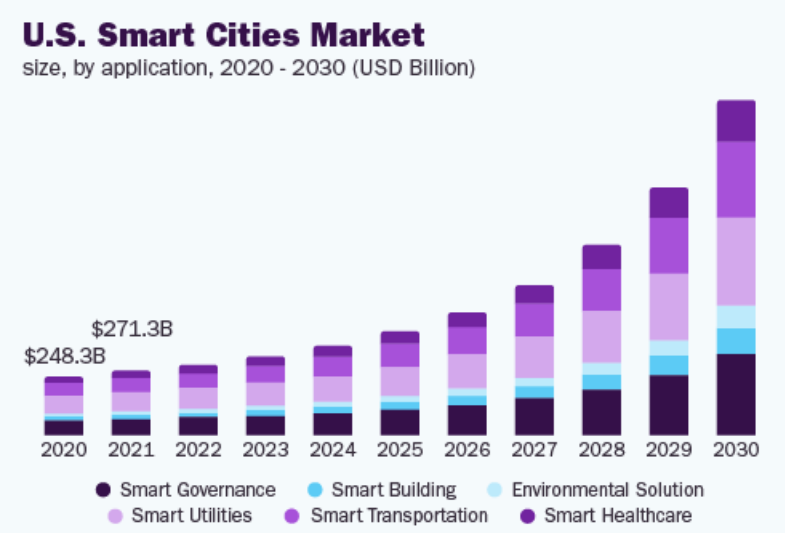

Figure 4:Smart cities size, by application [13]

The integration of IoT and smart technologies has the potential to transform cities into more sustainable, efficient, and livable environments. Here are some examples of the potential benefits:

1. Smart transportation: IoT-enabled systems can optimize traffic flow, reduce congestion, and improve public transportation services. For instance, sensors installed on roads and vehicles

10 Ganti, R. K., Ye, F., & Lei, H. (2016). https://ieeexplore.ieee.org/abstract/document/7507485

11 Yigitcanlar, T., Kamruzzaman, M., Buys, L. (2018). https://emerald.com/insight/content/doi/10.1108/JET-12-2018-0044/full/html

12 Zhang, Z., Zhou, J., & Li, Y. (2018). https://sciencedirect.com/science/article/pii/S2624630118300025

13 https://grandviewresearch.com/static/img/research/us-smart-cities-market.webp

can provide real-time data on traffic conditions and enable intelligent routing and traffic management systems[14].

2. Energy efficiency: Smart grids and IoT-enabled energy management systems can optimize energy consumption and reduce waste. For example, smart sensors can monitor energy usage in buildings and adjust heating, cooling, and lighting systems based on occupancy levels and weather conditions[15].

3. Environmental sustainability: IoT-enabled systems can monitor air and water quality, reduce waste, and promote sustainable practices. For instance, smart waste management systems can optimize waste collection routes and reduce landfill usage[16].

4. Public safety: IoT-enabled systems can enhance public safety and emergency response capabilities. For example, smart surveillance systems can detect and alert authorities to potential security threats, while smart sensors can detect natural disasters and coordinate emergency responses.[17]

Another key benefit of IoT in Smart Cities is the ability to improve citizen engagement and participation. Through IoT-enabled devices and applications, citizens can interact with various urban systems, such as transportation and energy, in real-time. This can lead to increased awareness and understanding of urban issues, and enable citizens to provide feedback and suggestions for improvement[18]. Furthermore, IoT can be used to enhance public safety through real-time monitoring of public spaces, such as parks and streets, and providing alerts in case of any suspicious activities[19].

14 Carpineti, M. (2018). https://ieeexplore.ieee.org/abstract/document/8327449

15 Yang, S., Chen, Y., Huang, X., & Wang, Z. (2017). https://ieeexplore.ieee.org/abstract/document/8062718

16 Sivakumar, A., Kumar, R., & Nagarajan, R. (2020). https://sciencedirect.com/science/article/pii/S2210670720305537

17 Hassani, A., Silva, E. S., & Sadiq, R. (2021). https://sciencedirect.com/science/article/pii/S2210670721002341

18 Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). https://ieeexplore.ieee.org/abstract/document/6875775

19 Yigitcanlar, T.,Kamruzzaman, M., Buys, L. (2018). https://emerald.com/insight/content/doi/10.1108/JET-12-2018-0044/full/html

3.3 Challenges of IoT in Smart Cities

Despite the numerous benefits of IoT in Smart Cities, there are also several challenges that need to be addressed. One of the key challenges is the issue of data privacy and security. The vast amount of data generated by IoT-enabled devices and systems is sensitive and needs to be protected from unauthorized access or misuse[20]. In addition to this, the integration of numerous systems and devices raises the overall complexity of the system, which makes it more susceptible to cyberattacks.

The vulnerability of IoT based applications is directly related to the network paradigm where physical objects such as sensor-based devices collect data on key interactions within the network and communicate via wireless or wired connections. The data which is uploaded, processed and stored can exhibit key vulnerabilities in the form of man-in-the-middle attacks and denial-of-service attacks. As a result, collecting and transferring data via the use of IoT infrastructure could severely impact the security and privacy of smart cities unless precautionary measures are implemented[21].

The problem of interoperability and standardization is still another obstacle to overcome. The Internet of Things requires the integration of a wide variety of systems, apps, and devices, each of which may have unique technical standards and communication protocols. Because of this, it is difficult to ensure that diverse systems are able to communicate with one another in a smooth manner and interoperate, both of which are crucial for the effective operation of smart cities.

Furthermore, there is also the difficulty of managing data and conducting analysis. In order to derive useful insights from the massive amounts of data produced by IoT-enabled devices and systems, sophisticated data analytics and processing capabilities are required. On the other hand, a lot of cities don't have the kind of infrastructure or the experience that's required to successfully handle and analyze this data.

---

20 Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. (2013). https://sciencedirect.com/science/article/pii/S0167739X13000219

21 Awad, A. I., Furnell, S., Hassan, A. M., & Tryfonas, T. (2019). https://doi.org/10.1016/j.adhoc.2019.02.007

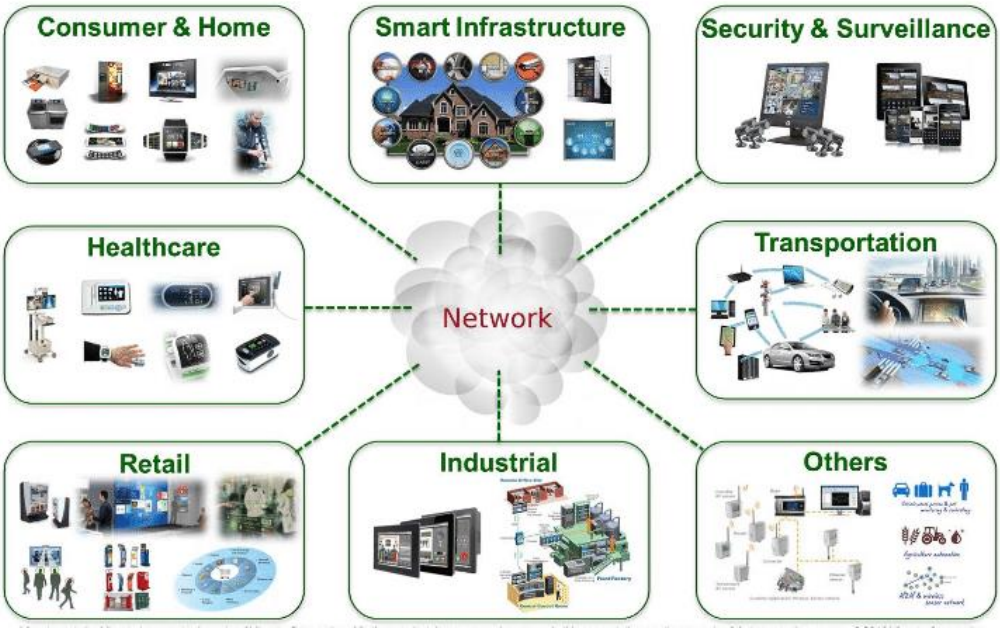

Figure 5:Vast amount of interconnected devices poses a threat for smart cities security [22]

The incorporation of the Internet of Things into Smart Cities has substantial prospects for enhancing the quality of life of city residents and establishing urban landscapes that are more environmentally friendly and resource-friendly. However, it also presents a number of issues, including those pertaining to the administration of data, interoperability, and data privacy and security. Effective laws, legislation, and investments in talent and infrastructure are required to find solutions to these difficulties so that they can be overcome.

Several scholarly investigations have considered these difficulties and made suggestions for possible responses to them. For example, the use of encryption and authentication systems is suggested as a way to preserve the privacy and security of data created by the internet of things. Additionally, the development of standards, protocols and frameworks to ensure that the lowest possible security standards are met between various systems and devices. Last but not least, legislation that is effective, with a focus on the importance of developing the necessary infrastructure and expertise on the management and analysis of sensitive data.

The integration of IoT in Smart Cities presents both opportunities and challenges. While the benefits of IoT are numerous, the challenges cannot be ignored and need to be addressed to ensure the successful implementation and functioning of Smart Cities. Through effective policies and investments in infrastructure and expertise, these challenges can be overcome, leading to more sustainable, efficient, and livable urban environments without sacrificing user privacy, system security and sensitive data protection.

22 https://mdpi.com/sensors/sensors-20-01754/article_deploy/html/images/sensors-20-01754-g001.png

4 Threats and Challenges Regarding Privacy and Security in IoT

4.1 Security Threats in IoT

4.1.1 Privacy and Data Breaches

The data generated by IoT-enabled devices can be sensitive and personal, including financial information, health records, and location data. When this data is collected, it can be used for various purposes such as marketing, research, and advertising, among others. However, the misuse of such data can have severe consequences for citizens.

a) Financial Losses

The sensitive information collected by IoT devices can be used for financial gain by cybercriminals. The data collected can be used to steal identities, access bank accounts, and commit fraud. In 2017, Equifax, a credit reporting agency, suffered a massive data breach that exposed the personal information of over 143 million Americans, including names, social security numbers, and birth dates[23]. This incident highlights the severity of data breaches and the financial losses that citizens can incur.

b) Reputation Damage

The disclosure of personal information can lead to damage to an individual's reputation. This is particularly relevant in cases where the data collected by IoT devices is sensitive, such as health records. In 2020, it was reported[24] that a fertility-tracking app, Premom, exposed the personal information of millions of users, including their ovulation dates and pregnancy statuses. This breach not only exposed the sensitive information of users but also potentially affected their relationships and personal lives.

c) Identity Theft

The data collected by IoT devices can be used for identity theft, which can have severe consequences for citizens. Identity theft occurs when an individual's personal information is used to open bank accounts, obtain loans, and purchase goods and services. In 2019, it was reported[25] that a hacker had accessed the personal information of over 100 million Capital One customers, including names, addresses, and credit scores. This incident highlights the need for strong security measures to protect citizens' personal information.

---

23 Equifax data breach: https://nytimes.com/2017/09/07/business/equifax-cyberattack.html

24 Premom data breach: https://techcrunch.com/2020/07/20/premom-data-leak/

25 Capital One data breach: https://nytimes.com/2019/07/29/business/capital-one-data-breach.html

d) Location Tracking

The use of IoT devices can enable tracking of an individual's location, which can be used for surveillance purposes. This raises concerns about the violation of an individual's privacy and potential misuse of their location data. In 2020, it was reported that the use of a popular weather app, AccuWeather, enabled the company to track users' locations even when they had opted-out of location tracking[26]. This incident highlights the need for transparency and user control over their data.

Figure 6: Strava heatmap of a US military base in Afghanistan [27]

e) Health Risks

IoT devices that collect health data can pose risks to citizens if the data is not secured or is used inappropriately. For example, if an individual's health data is exposed, it could potentially affect their insurance premiums or their ability to obtain insurance. In 2017, it was reported that a vulnerability in a popular insulin pump allowed hackers to remotely control the device, potentially causing harm to the user. This incident highlights the need for strong security measures in healthcare IoT devices.

f) Smart Home Devices

---

26 AccuWeather tracking: https://zdnet.com/article/accuweather-caught-sending-geo-location-data-even-when-users-opt-out/

27 https://i.guim.co.uk/img/media/ae4001f9311f4912db843f79ee2510db6d9419e0/0_180_1472_883/master/1472.png?width=620&quality=45&dpr=2&s=none

Smart home devices such as Amazon Echo, Google Home, and Nest thermostats are some of the most popular IoT devices. These devices are designed to make our lives easier by providing various services such as voice commands, automation, and energy-saving features. However, the data collected by these devices can be sensitive and may include personal information such as voice recordings, device usage, and location data. In 2019, it was reported that Amazon employees were listening to recordings of users' conversations with Alexa, the voice assistant in Amazon Echo[28]. The incident raised questions about the privacy of users' data and whether it was being stored securely.

g) Smart Cars

Smart cars are equipped with various sensors and devices that collect data about the vehicle, such as speed, location, and driver behavior. The data collected can be used to improve the driving experience, such as providing traffic information and reducing accidents. However, the data can also be sensitive, such as the driver's location and driving habits.

In 2015, security researchers Charlie Miller and Chris Valasek demonstrated how they could remotely take control of a Jeep Cherokee's steering, brakes, and other systems through its infotainment system. They were able to do this by exploiting a vulnerability in the car's entertainment system that allowed them to send commands to the car's CAN bus, which controls many of its critical functions[29].

In 2016, a group of Chinese security researchers demonstrated how they could remotely take control of a Tesla Model S through its ECU, which controls many of the car's systems. They were able to do this by exploiting a vulnerability in the car's web browser that allowed them to access the ECU's firmware and install their own code[30].

In 2016, security researcher Troy Hunt discovered a vulnerability in the Nissan Leaf's mobile app that allowed anyone to remotely access the car's systems and control certain functions, such as turning on the air conditioning. Hunt was able to do this by exploiting a weakness in the app's authentication process that allowed him to access other users' accounts[31].

In 2018, security researchers from Tencent's Keen Security Lab demonstrated how they could remotely take control of a BMW's infotainment system and perform a variety of actions, such as opening the car's doors and sunroof, by exploiting a vulnerability in the car's ConnectedDrive system[32].

---

28 Alexa: https://independent.co.uk/tech/amazon-alexa-echo-listening-spy-security-a8865056.html

29 Jeep Cherokee: https://wired.com/2015/07/hackers-remotely-kill-jeep-highway/

30 Tesla Model S: https://wired.com/story/tesla-model-s-hack-china/

31 Nissan Leaf: https://wired.com/2016/02/hackers-can-disable-nissan-leafs-brakes-media-systems-over-the-internet/

32 BMW: https://theverge.com/2018/2/13/17009998/bmw-connecteddrive-hack-remote-unlock-car

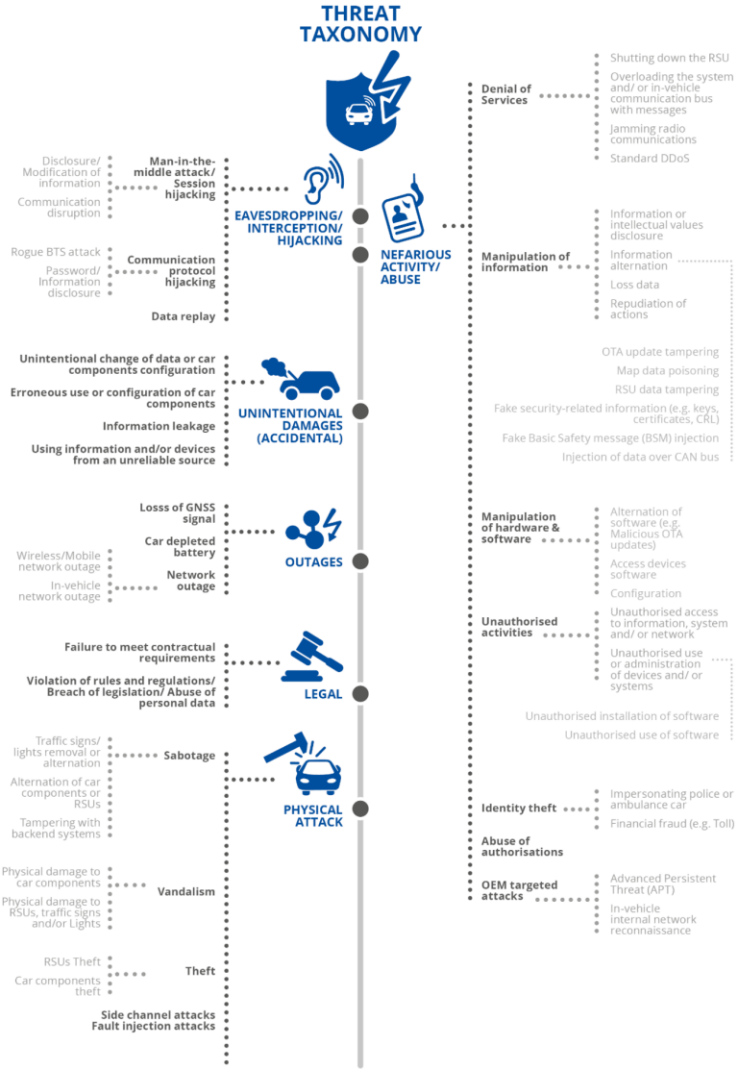

Figure 7: Smart Vehicles attack vectors [33]

h) Healthcare Devices

Healthcare devices such as fitness trackers and medical implants are designed to collect and transmit data about the user's health. The data collected can be sensitive, including personal information such as health records and location data. In 2018, it was reported that a popular fitness tracker, Strava, was revealing the location and routes of military personnel, including those in sensitive areas[34]. The incident raised concerns about the security of the data collected by such devices and whether it was being used responsibly.

4.1.2 Malware and Botnets

33 https://securityguill.com/images/infographics/mirai_works_leplat.jpg

34 Strava tracking: https://theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

A botnet is a set of computers infected by bots. A bot is a piece of malicious software that gets orders from a master. Once bot malware runs on a computer, it has as much access to the computer's resources as its owner. Bots can then read and write files, execute programs, intercept keystrokes, access the camera, send emails, etc. This appellation "bot" comes from the old chat service IRC, where users could develop so-called "bots" that could keep channels alive, deliver funny lines on request, etc. The first botnets were directly built as IRC bots.[35]

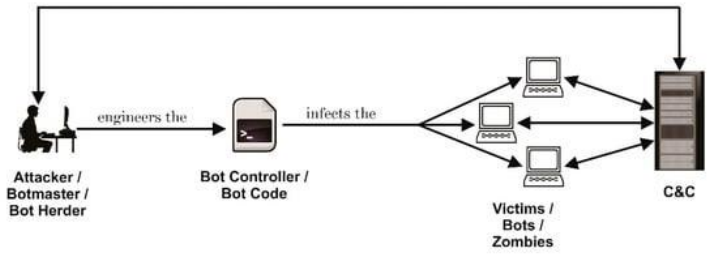

Figure 8: Generic Structure of a Botnet [36]

a) Mirai

The Mirai botnet was first discovered in August 2016 and quickly gained notoriety for its large-scale DDoS attacks. The botnet was responsible for a series of high-profile attacks, including the attack on DynDNS, which disrupted access to popular websites like Twitter, Netflix, and Amazon.

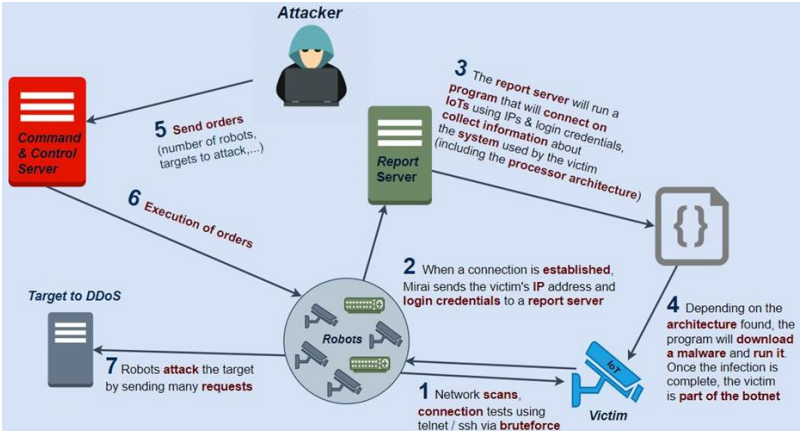

Figure 9: How Mirai botnet was operating [37]

35 ENISA: https://www.enisa.europa.eu/topics/incident-response/glossary/botnets

36 Emmanuel C. Ogu, Olusegun Ojesanmi, Oludele Awodele, Shade Kuyoro (2019). https://mdpi.com/2078-2489/10/11/337/htm

37 https://securityguill.com/images/infographics/mirai_works_leplat.jpg

The Mirai botnet worked by scanning the Internet for IoT devices that were running with default usernames and passwords. Once a device was identified, Mirai would attempt to login using a list of commonly used credentials. If successful, the botnet would take control of the device and add it to its network.

One of the reasons Mirai was so successful was its ability to infect a wide range of IoT devices, including cameras, routers, and digital video recorders. These devices typically have weak security and are often overlooked by their owners. Mirai was also able to propagate itself rapidly due to the large number of vulnerable devices on the Internet.

Mirai used a centralized C2 server to communicate with infected devices. This allowed the botnet operator to issue commands to all infected devices simultaneously. Mirai was capable of launching DDoS attacks with a bandwidth of up to 1 terabit per second, making it one of the largest botnets in history.

Country	% of Mirai IPs
Vietnam	12.8%
Brazil	11.8%
United States	10.9%
China	8.8%
Mexico	8.4%
South Korea	6.2%
Taiwan	4.9%
Russia	4.0%
Romania	2.3%
Colombia	1.5%

Figure 10: Mirai attacks countries of origin [38]

To mitigate the threat of Mirai, security researchers developed tools that could detect and remove the botnet from infected devices. They also worked with device manufacturers to release firmware updates that addressed vulnerabilities exploited by the botnet.

The Mirai botnet case highlighted the security risks associated with the growing number of IoT devices. It also underscored the importance of proper security measures, such as changing default passwords and keeping firmware up to date, to prevent devices from being compromised by botnets like Mirai.

38 https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/

In addition to the technical details, the Mirai botnet case also had significant legal and social implications. The botnet was operated by a group of young hackers, who were eventually identified and arrested by law enforcement agencies.

The case sparked a debate about the ethics of using botnets for malicious purposes and the responsibility of manufacturers and users in securing IoT devices. It also highlighted the need for improved collaboration between industry, government, and academia to address cybersecurity challenges.

The Mirai botnet case also led to increased awareness and investment in cybersecurity for IoT devices. Device manufacturers and service providers began to prioritize security in their products and services, and governments around the world introduced new regulations and guidelines for IoT security.

b) Reaper

The Reaper botnet, also known as IoTroop, was first discovered in 2017 and is considered to be a successor to the Mirai botnet. Like Mirai, Reaper is an IoT botnet that targets vulnerable devices and uses them to launch DDoS attacks and other malicious activities.

Reaper is considered to be more sophisticated than Mirai, as it uses a range of exploits to infect devices, rather than relying on default usernames and passwords. The botnet is capable of infecting a wide range of IoT devices, including routers, IP cameras, and digital video recorders.

One of the unique features of Reaper is its ability to evolve and adapt to new security measures. The botnet uses a modular design that allows it to download and execute new code, making it more difficult to detect and remove.

Reaper also uses a decentralized P2P network to communicate with infected devices, rather than a centralized C&C server. This makes it more difficult for law enforcement agencies to take down the botnet, as there is no single point of control.

The potential impact of Reaper is significant. Security researchers estimate that the botnet has the potential to infect millions of devices and launch DDoS attacks with a bandwidth of up to 1 terabit per second.

To mitigate the threat of Reaper, security researchers and device manufacturers have worked to identify and patch vulnerabilities exploited by the botnet. Some researchers have also developed tools that can detect and remove the botnet from infected devices.

c) Hajime

Hajime is another IoT botnet that emerged in 2016, shortly after the Mirai botnet. Unlike Mirai and Reaper, however, Hajime has been described as a "white hat" or benevolent botnet, with the goal of securing IoT devices rather than using them for malicious activities.

Hajime uses a similar strategy to Mirai in identifying and infecting vulnerable IoT devices, but once a device is infected, the botnet does not immediately launch any attacks. Instead, it takes control of the device and uses it to scan the Internet for other vulnerable devices, effectively creating a network of "zombie" devices that are under its control.

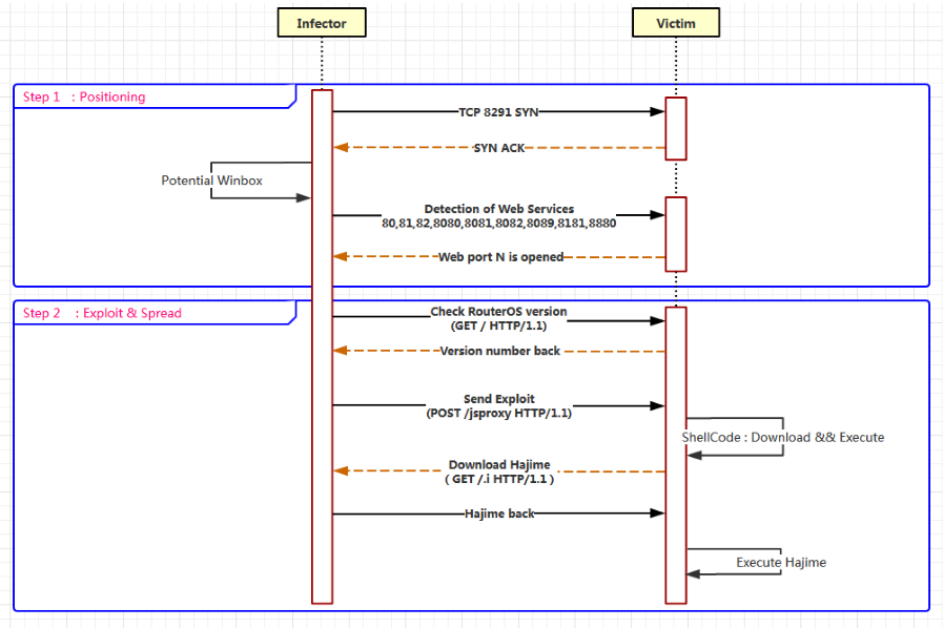

Figure 11: Hajime low level operational process [39]

Once a device is added to the Hajime botnet, it is protected from other malware and security threats. The botnet has been observed patching vulnerabilities on infected devices and even removing other malware that may be present.

Hajime is also unique in that it uses a P2P network to communicate with infected devices, rather than a centralized C&C server. This makes it more difficult for law enforcement agencies to take down the botnet, as there is no single point of control.

Despite its apparent benevolent intentions, the Hajime botnet is still considered a security risk. While it may protect infected devices from other malware, it also has the potential to be used for malicious purposes in the future. In addition, the fact that it uses the same infection methods as other IoT botnets means that it can still contribute to the overall insecurity of IoT devices.

d) BrickerBot

39 https://www.bleepingcomputer.com/news/security/hajime-botnet-makes-a-comeback-with-massive-scan-for-mikrotik-routers/

BrickerBot, also known as BrickerBot.1 and BrickerBot.2, is an IoT botnet that emerged in 2017. Unlike other IoT botnets, however, BrickerBot does not aim to create a network of infected devices for malicious purposes. Instead, it seeks to destroy vulnerable IoT devices, effectively rendering them inoperable (PDoS).

BrickerBot targets devices that have known security vulnerabilities and uses a variety of techniques to exploit these vulnerabilities and disable the device such as insecure default passwords or open Telnet ports, to gain access to the device. Once it gains access, the botnet launches a series of commands that overwrite the firmware of the device, effectively bricking it and rendering it useless. This can include deleting all files from the device, corrupting its firmware, or overwriting its storage with random data.

The creator of BrickerBot, who goes by the pseudonym "Janit0r," claimed that the botnet was designed to be a "vigilante" solution to the problem of insecure IoT devices, which can be easily exploited by other botnets for malicious purposes. While the intentions may have been good, security experts have criticized the botnet's methods, which can cause irreparable damage to IoT devices and potentially cause harm to individuals and organizations that rely on these devices.

BrickerBot has been identified as a significant threat to IoT security, with the potential to cause widespread disruption and damage. The botnet has been responsible for thousands of attacks on IoT devices around the world, and its impact is likely to continue as long as vulnerable devices remain online and the creator has faced criticism for not disclosing the vulnerabilities exploited by the botnet to device manufacturers.

4.1.3 Physical Security

Within the realm of cybersecurity, the problem of physical security for IoT devices is becoming an increasingly essential one. Because Internet of Things devices are becoming increasingly common in private residences, commercial establishments, and public places, it is more important than ever before to safeguard these devices against the risk of theft and tampering by unauthorized individuals. In this thesis, we will investigate the significance of physical security for Internet of Things devices, as well as the dangers that are associated with inadequate physical security and the solutions that can be used to reduce those risks.

Devices that are part of the Internet of Things are often very small, portable, and highly networked. They are built to connect to the internet and communicate with other devices, most of the time without the need for any assistance from a human. This indicates that they are susceptible to a wide variety of different types of destructive physical attacks, including robbery, tampering, and destruction. Locks, alarms, and surveillance cameras are all examples of physical security measures that can be used to

protect against various forms of assault. Physical security is the process of protecting these equipment against such assaults.

Theft is one of the most significant threats that is related with inadequate physical protection for IoT equipment. The fact that Internet of Things devices are frequently pricey and carry sensitive information makes them desirable acquisitions for burglars. A hacker might, for instance, steal a smart thermostat from a house or office, then use it to get access to a network and steal sensitive data from that network. In addition, a hacker might take a connected automobile or drone and then use it for malevolent purposes, such as conducting surveillance or launching an assault.

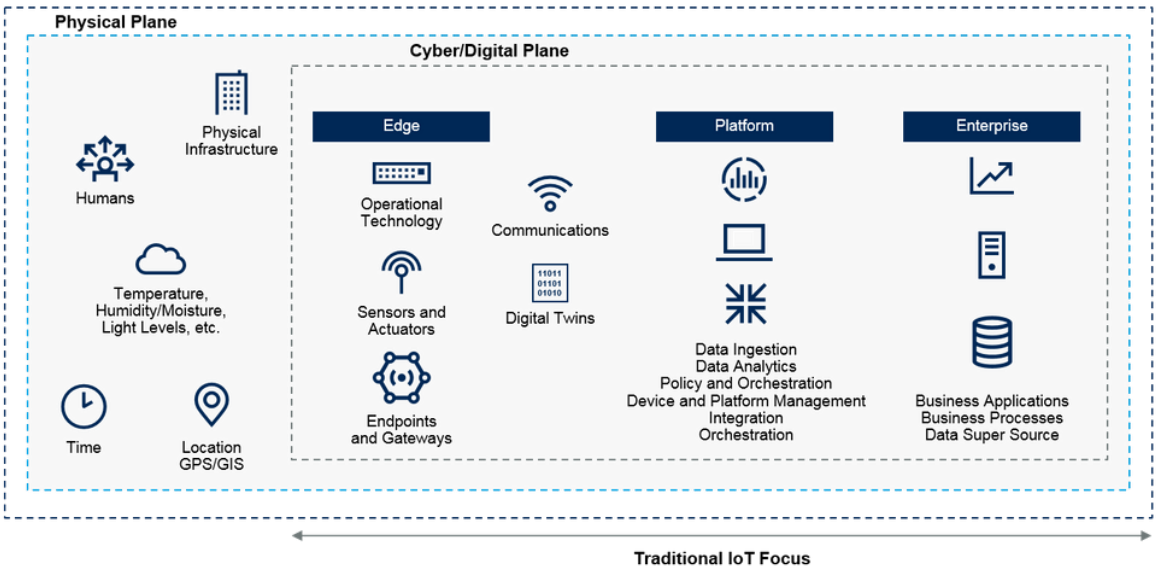

Figure 12: IoT attack vectors in perspective [40]

Tampering is an additional danger that is related with inadequate physical security. IoT devices are typically quite compact and simple to open, which makes it quite simple for an adversary to alter or change the hardware or software on the device. A hacker, for instance, might install a malicious program on a smart refrigerator, which could then be used to conduct a cyber attack on the network belonging to the user. A hacker might also change the firmware of a connected car or drone, which could subsequently be utilized to cause damage or harm to a person's body.

There are a number of different approaches that may be taken in order to strengthen the IoT devices' physical security and reduce the likelihood of these dangers occurring. When it comes to protecting the data that is being transmitted from one device to another, one of the most efficient methods is to employ robust encryption. This can make it more difficult for potential thieves to take the device as well as

40 https://techcommunity.microsoft.com/t5/image/serverpage/image-id/331521i15616D9F6DA17EE6/

prevent them from intercepting or changing the data. It can also assist prevent potential thieves from stealing the data.

Figure 13: How Cyber-Physical Systems Challenge Traditional Cybersecurity Concepts [41]

Using physical security measures such as locks, alarms, and video cameras is yet another efficient tactic that can be used. This can be helpful in discouraging potential attackers and making it more challenging for them to obtain access to the device. For instance, a smart thermostat might have a lock that can only be opened with a unique key, and a connected car might have a motion sensor that sounds an alert if the vehicle is moved without the owner's permission.

In addition to these techniques, it is essential to inform end users on the need of maintaining a high level of physical security for IoT devices. This can help users understand the actions they can take to safeguard their devices and promote awareness about the risks associated with poor physical security.

41 https://techcommunity.microsoft.com/t5/image/serverpage/image-id/

4.2 Security Challenges in IoT

4.2.1 Complexity

The Internet of Things has completely changed the way in which people interact with their surroundings and has opened up countless opportunities for innovation and business expansion. Devices connected to the Internet of Things are utilized in a variety of industries, such as healthcare, transportation, and energy management, to mention a few. On the other hand, as the number of Internet of Things devices continues to increase, the complexity of the software and hardware components of those devices also continues to increase. Because of this complexity, there are substantial security concerns that need to be solved to guarantee the safety and security of these devices as well as the data that they collect.

The increasing likelihood of cyberattacks is one of the key challenges posed by the complexity of the Internet of Things. The attack surface area of a network grows larger as more devices are added to it, making it simpler for malicious actors to locate weaknesses in the network that can be exploited. Because of the interconnected nature of IoT devices, even a breach in the security of a single item might potentially affect the integrity of the entire network. Because of the complexity of IoT devices, it can be difficult to identify vulnerabilities and apply patches in a timely manner, which makes them more vulnerable to assaults.

Another issue of IoT devices is the fact that it can make it more challenging to locate and patch vulnerabilities in a timely manner. It is difficult to create a universal solution to the issue of security because there is a lack of uniformity in the design of devices and there is a variation in the devices themselves. As a consequence of this, manufacturers are required to build individualized safety solutions for each device, which can be an expensive and time-consuming process. In addition, the sheer volume of Internet of Things devices that might be connected to a network can make it challenging to efficiently monitor those devices, particularly in the absence of centralized management tools.

The complexity of the system also makes it more difficult to put security measures into action, which is another security risk. IoT devices are typically equipped with constrained amounts of computing power and memory due to their compact size, low cost, and focus on maximizing energy efficiency. Because of this, putting in place solid security mechanisms like encryption, authentication, and access control can be difficult. In addition, it is challenging to deploy similar security measures across all IoT devices because of the variety of IoT devices and the lack of standardization in their designs.

The management and upkeep of the gadget are both made more difficult by the device's level of complexity. When there are more devices connected to a network, it becomes significantly more challenging to efficiently manage and monitor all of those devices. This can lead to devices being used without supervision, which increases the risk of security flaws going unpatched. In addition, the complexity of IoT devices makes it difficult to perform updates and maintenance on those devices, which might result in devices running software that is out of date and potentially susceptible.

Another problem that arises as a result of the complexity of Internet of Things devices is the lack of transparency regarding the manner in which they function. Because many Internet of Things devices make use of proprietary software and hardware components, it can be difficult to comprehend how these devices function and the information that they gather. Because there is a lack of transparency, it is difficult to evaluate the devices' level of security and to locate any potential flaws.

Using a strategy known as "security by design" is one possible approach to resolving the problems with data protection that are caused by complexity. Instead of attempting to add security to Internet of Things devices as an afterthought, this strategy entails integrating security into the design process of IoT devices from the very beginning. This strategy can be helpful in ensuring that security is incorporated into the design of the device from the very beginning, rather than being a secondary concern in the design process. In addition, the standardization of the design of IoT devices and security protocols can assist in simplifying the installation of security measures across a variety of devices.

4.2.2 Lack of Standards

IoT devices are produced by a wide variety of companies, each of which utilizes its own unique combination of hardware, software, and communication protocols. This lack of standards produces a fragmented ecosystem, which makes it difficult to build uniform security protocols. Moreover, this lack of standardization is a barrier to innovation. Frequently, manufacturers place a higher emphasis on functionality and affordability than they do on security, which results in products that have insufficient encryption, weak passwords, and unpatched vulnerabilities.

IoT devices are therefore great targets for hackers who aim to exploit their vulnerabilities in order to obtain unauthorized access to networks, steal sensitive data, and launch attacks. These goals can be accomplished by exploiting the IoT devices' weaknesses. For example, in 2016, cybercriminals deployed a botnet known as Mirai to perform a DDoS attack on Dyn, a domain name service provider. This attack caused extensive disruptions across the internet. The botnet targeted Internet of Things devices with insecure default passwords, illustrating the dangers posed by insufficiently protected Internet of Things equipment.

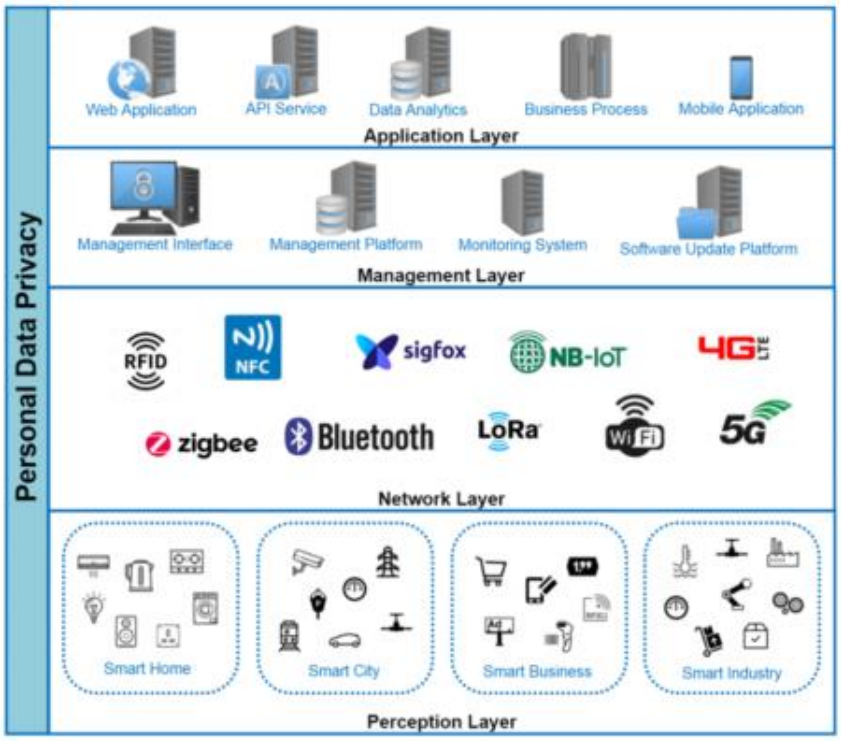

Figure 14: IoT Layered Architecture Model [42]

It is difficult for regulatory agencies to design effective regulations that can keep up with the rapid pace of IoT growth since there are no standards in place for the devices that make up the IoT. As a direct consequence of this, a great deal of Internet of Things devices slip through regulatory cracks, making them susceptible to various forms of attack.

Another key challenge for IoT service providers is that there are multiple, and often-inconsistent, laws dealing with privacy and data protection. Different laws may apply in different countries, depending on the types of data involved, as well as the industry sector and services that the service provider is offering. This has implications for a number of consumer oriented IoT service providers.[43]

Additionally, the lack of standards affects efforts to build industry-wide security frameworks that can guide manufacturers in the design of safe equipment. These frameworks can be helpful if they are developed properly. For example, the lack of defined communication protocols makes it impossible to develop encryption and authentication systems that are consistent. Because of this lack of consistency, it is difficult for enterprises to successfully manage and secure their Internet of Things deployments.

A multi-pronged strategy is required in order to address the dearth of standards that apply to Internet of Things devices. First, regulatory organizations need to formulate all-encompassing criteria that address

---

42 https://wsperanzainc.com/wp-content/uploads/2021/12/%E5%9C%96%E7%89%87-2-4-466x400.png

43 IoT SECURITY GUIDELINES (2020). https://gsma.com/iot/wp-content/uploads/2020/05/CLP.11-v2.2-GSMA-IoT-Security-Guidelines-Overview-Document.pdf

all areas of Internet of Things device security, beginning with the manufacturing phase and continuing through the deployment phase. The rules should contain requirements for secure password procedures, regular software upgrades, and data encryption, among other safety precautions, in addition to the other safety precautions. Also, manufacturers should make security a top priority in the design procedures they use for their products. This will ensure that products are secure by design and can be easily upgraded to counteract new threats.

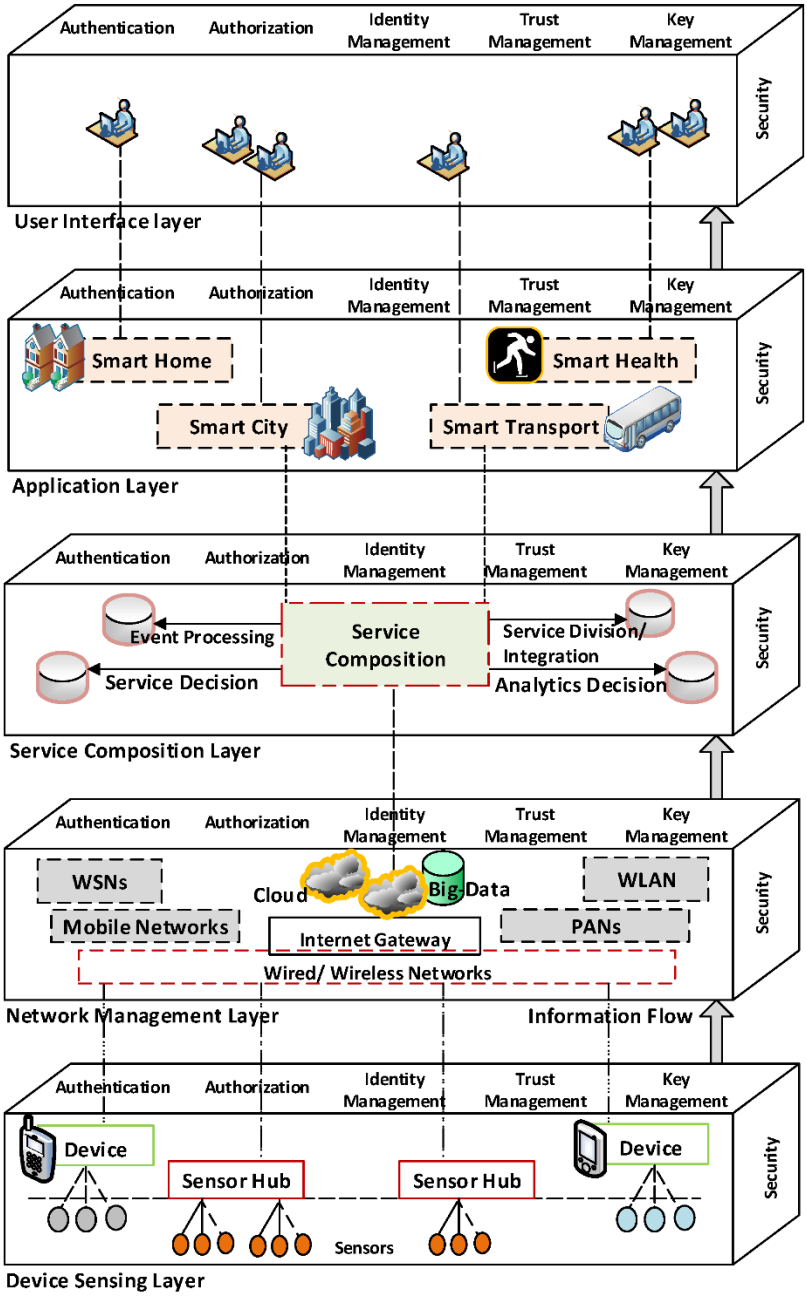

Figure 15: The functional layers of an IoT security architecture, showcasing why there is such a difficulty in developing universal standards [44]

Second, organizations representing the industry should work together to build standardized communication protocols and security frameworks. These will serve as a roadmap for manufacturers as they create safe equipment. These frameworks ought to have the degree of adaptability necessary to support a wide variety of Internet of Things devices while retaining a constant level of security.

44 https://www.mdpi.com/sensors/sensors-20-05897/article_deploy/html/images/sensors-20-05897-g001-550.jpg

Finally, businesses that use Internet of Things devices should take preventative measures to ensure the safety of their deployments. This includes conducting frequent vulnerability assessments, implementing network segmentation, and building incident response strategies in order to reduce the impact of any security breaches that may occur.

In conclusion, the lack of standards on IoT devices is a huge security concern that poses a risk to individuals, businesses, and entire sectors. This risk can be spread across multiple levels. In order to effectively address this issue, it will be necessary for regulatory organizations, manufacturers, and industry bodies to work together to develop comprehensive rules and security frameworks. In addition, businesses should take preventative steps to secure their Internet of Things deployments in order to reduce the likelihood of experiencing a security breach. If this issue is not addressed, it could lead to catastrophic outcomes that could have far-reaching effects for the ecosystem of the internet of things.

4.2.3 Scale

The Internet of Things has made it possible to connect a wide range of devices, appliances, and sensors not only to the internet but also to one another, allowing them to interact with one another and collaborate efficiently. The proliferation of IoT devices has greatly expanded the reach of the Internet of Things, which has led to the creation of new concerns, particularly in the sphere of cybersecurity.

Because IoT devices collect and handle vast volumes of data, there is great cause for concern over their security. This information can be utilized by hackers to commit a range of crimes, including identity theft, financial fraud, and blackmail. Moreover, Internet of Things devices are commonly networked with other devices and systems, which could grant thieves access to new network domains. A hacker, for instance, may exploit an infiltrated IoT consumer gadget to conduct a larger scale cyberattack against an entire network.

The lack of security updates is one of the most significant challenges in terms of the magnitude of security dangers posed by Internet of Things devices. Due to the lengthy lifespans of many Internet of Things devices and the fact that their manufacturers may not provide regular security updates, a large number of devices are vulnerable to hacking. In addition, the use of outdated software that is not maintained by the vendor can result in additional security vulnerabilities.

The lack of encryption is another element that raises concerns about the security of large-scale Internet of Things devices. A substantial majority of IoT devices lack the encryption mechanisms required to protect sensitive data from unauthorized access. This can lead to data breaches, which can result in significant financial losses and reputational harm for a business. These losses may result from illegal access to sensitive data.

Moreover, there are so many internet-connected devices that it is impossible to monitor and govern their security. Large quantities of IoT devices are routinely deployed, making it difficult to track their location

and guarantee that they are correctly linked. Due of this, it may be challenging to detect security breaches in a timely manner and devise an appropriate reaction.

The introduction of blockchain technology is one option for addressing these security concerns. If blockchain technology is implemented, it will be more difficult for hackers to manipulate data since it provides a decentralized, immutable ledger of all transactions. Moreover, blockchain could provide a framework for secure identity management, which can help prevent unauthorized access to Internet of Things devices.

Concerns regarding the security of IoT devices can also be addressed by employing artificial intelligence and machine learning techniques. These algorithms can analyze vast quantities of data collected from IoT devices in order to identify anomalies and establish the nature of any potential security issues. With these tools, businesses can detect and respond to security breaches more quickly, which is a significant competitive advantage.

In conclusion, the sheer number of IoT devices poses significant security vulnerabilities that must be addressed to ensure the safe and secure use of this technology. Manufacturers and organizations of IoT devices must take precautions to ensure that their products are secure, that they receive frequent upgrades, and that they apply the necessary encryption techniques. Using emerging technologies such as blockchain, artificial intelligence, and machine learning can also assist in addressing the security issues associated with the large size of IoT devices. These are instances of what are referred to as emergent technologies.

4.3 Privacy Concerns on IoT

IoT devices frequently capture vast quantities of personal information without the user's consent. This is one of the most significant problems with IoT devices. These devices continuously track and monitor the activities, movements, and interactions of their users with their environment, collecting sensitive data such as health data, location data, and financial data. This data can be accessed and analyzed by multiple parties, including device manufacturers, service providers, and third-party organizations, resulting in the construction of a massive digital footprint that can be used for various purposes.

One of the most major concerns with IoT devices is the lack of control that users have over their own personal information. Several Internet of Things devices collect data without explicitly notifying users, and in certain situations, this data may be shared with other parties without the knowledge or consent of customers. Given the sensitive nature of the data obtained by IoT devices, such as health data, financial information, and location data, this provides a very challenging obstacle.

A second significant issue with IoT devices is that not enough security measures are in place to protect user data. These devices are susceptible to hacking and data breaches because they lack key security measures such as password protection, encryption, and regular software updates. Cybercriminals can gain access to sensitive data such as login credentials, credit card information, and personal identifiers such as Social Security numbers by exploiting these vulnerabilities.

Another significant issue with Internet of Things devices is that they frequently lack proper security safeguards, leaving them vulnerable to being hacked and having their data stolen. Cybercriminals can exploit the security flaws of IoT devices to gain access to the personal information of users, steal identities, and engage in a range of other illicit activities. In addition, the networked nature of IoT devices allows attackers to acquire access to other linked devices, so triggering a cascade of data breaches and cyberattacks.

According to the study, three quarters of UK consumers are concerned about how smart devices are using their data without permission, with 67% worried about these devices eavesdropping. These worries come despite a high level of technical competency, with almost two thirds (64%) well aware of using encryption to protect themselves, and 76% understanding how to apply security updates on a regular basis. However, the poor user interface on many IoT devices can make it difficult to apply this knowledge, increasing the risk of outdated software patches and consequently, security flaws.

This lack of trust is reinforced by the survey's findings that almost half (43%) of UK consumers admitted that they do not trust IoT devices to handle data responsibly, and the same percentage (43%) not believing that IoT devices would stop unauthorized data access. There have been many well-publicized occasions when IoT devices have been recruited into botnets, which can mine cryptocurrency, carry out DDoS attacks or even distribute malware in turn.[45]

---

45 https://www.itsecurityguru.org/2019/07/31/91-of-the-uk-would-like-better-privacy-laws-for-iot-devices-to-prevent-data-misuse/

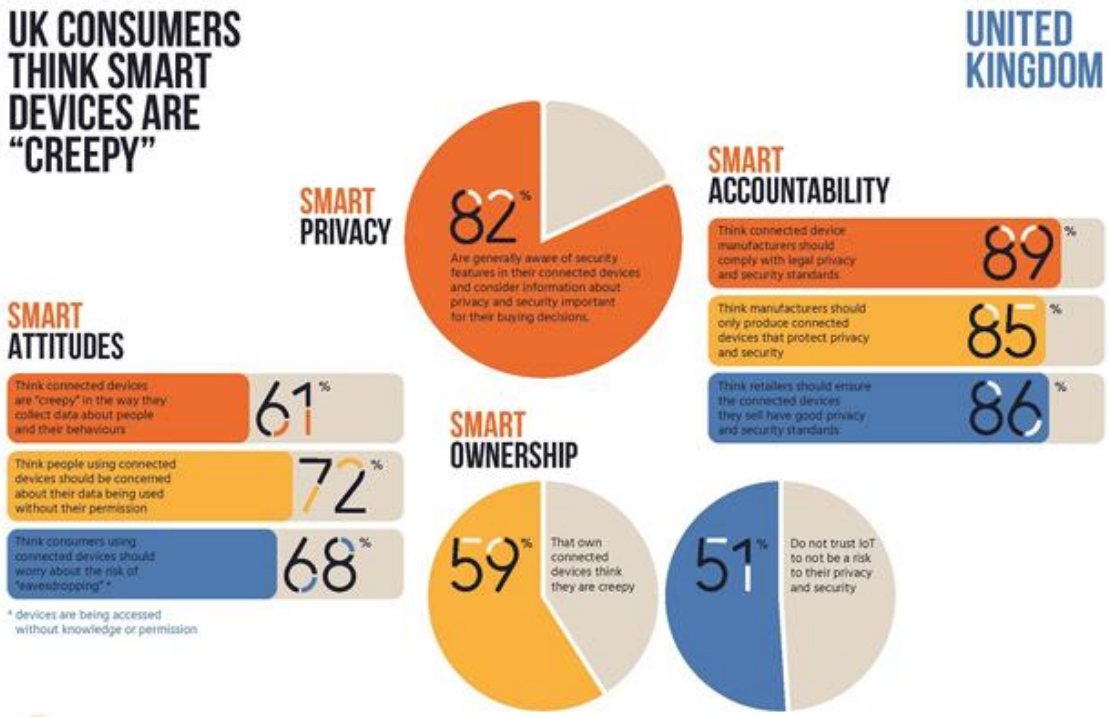

Figure 16: Study infographic [46]

In a 2018 global survey, researchers found that close to half (43%) of IT and security decision makers agree that security is an afterthought when implementing IoT projects, while only half (53%) think connected devices are a threat to their own organizations, even though nearly two-thirds (63%) acknowledged that IoT-related cybersecurity threats have increased over the past 12 months. This seeming inability to connect the dots between increased risk and the need to address organizational vulnerability appears difficult to reconcile; at the same time, it does reflect broad market attitudes that new research from the IoTCC is designed to address. While many organizations remain unclear on tactics and strategy to protect IoT deployments, others assume that traditional approaches to IT security and privacy used by the organization will also manage risks associated with IoT adoption.[47]

46 https://www.itsecurityguru.org/wp-content/uploads/2019/08/Iot.jpg

47 https://insightaas.com/new-research-privacy-and-security-in-the-internet-of-things-era-iotcc-best-practices-guidance/

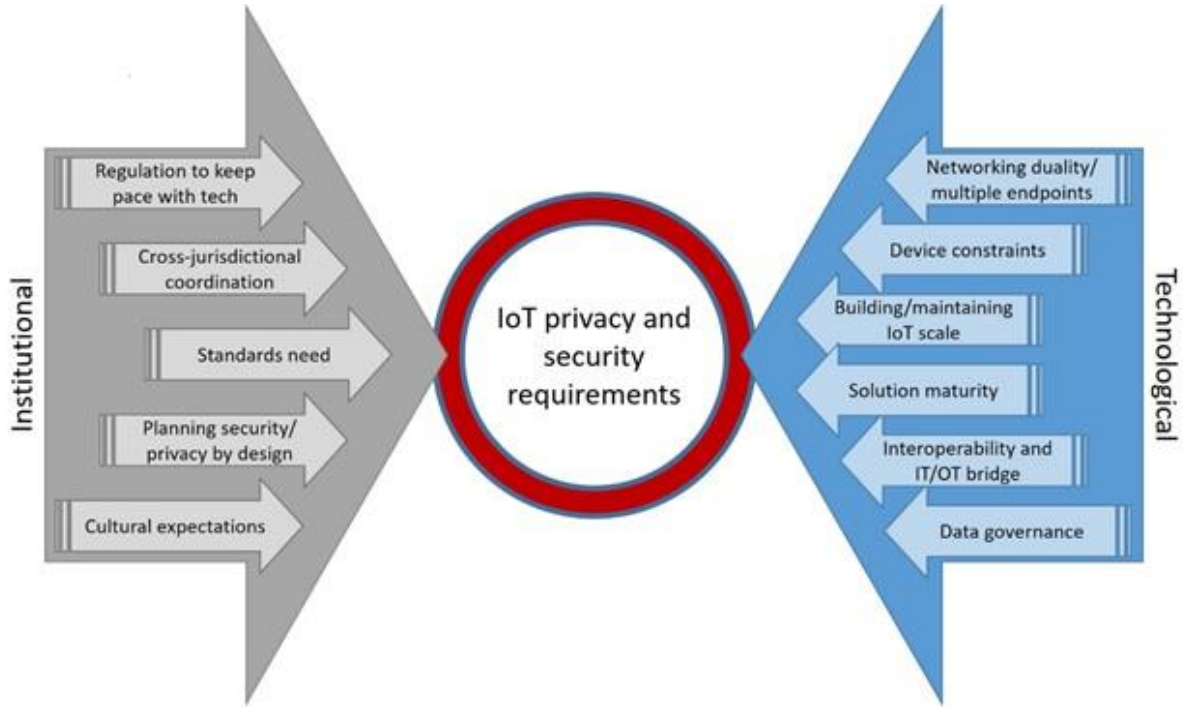

Figure 17: IoT privacy and security requirements [48]

It is difficult for users to comprehend what data is being collected, how it is being used, and who has access to it due to the complexity of IoT devices and the absence of industry-wide standardization. Consumers commonly agree to the terms and conditions of several Internet of Things devices without fully understanding the extent of data collection and sharing because these terms and conditions are frequently lengthy and difficult to comprehend.

If a firm undergoes a merger, acquisition, or declares bankruptcy, it is possible for personal information to be disclosed and transferred to other organizations. Massive technical corporations are acquiring smaller competitors in the same field with increasing frequency. As a result of their industry's increasing market dominance and concentration of power, large technology businesses are now able to collect massive quantities of data about individuals across a number of platforms and devices. This increases the opportunity for technology titans to gain deeper insights into the routines and preferences of individuals. The convergence of data across different devices and platforms has the potential to exacerbate data security vulnerabilities.

The potential for governments and law enforcement agencies to misuse acquired data is an additional important cause for IoT concern. The massive amounts of data collected by IoT devices can be accessed and utilized by authorities to track the movements, acts, and activities of individuals, which may violate their right to privacy. With the data gathered by IoT devices, which may also be utilized by governments

48 https://insightaas.com/wp-content/uploads/2018/07/IoT-privacy-and-security-requirements.jpg

for mass surveillance, it is possible to establish a dystopian society in which every person's action is tracked and monitored.

An immediate consequence of the diversity of the current standardization ecosystem, and because of the extremely rapid pace of change, is that it is increasingly difficult to authoritatively determine if gaps in standardization or in capability exist. Any failure to recognize the reality of the ecosystem and the constituent members will gravely harm the aims of the NIS Directive and the harmonization of NII/NIS.[49]

Just to put under perspective how vast the initiative is and what are the objective difficulties, the following pictures showcase the relationship diagrams among the entities involved in standardization prototyping.

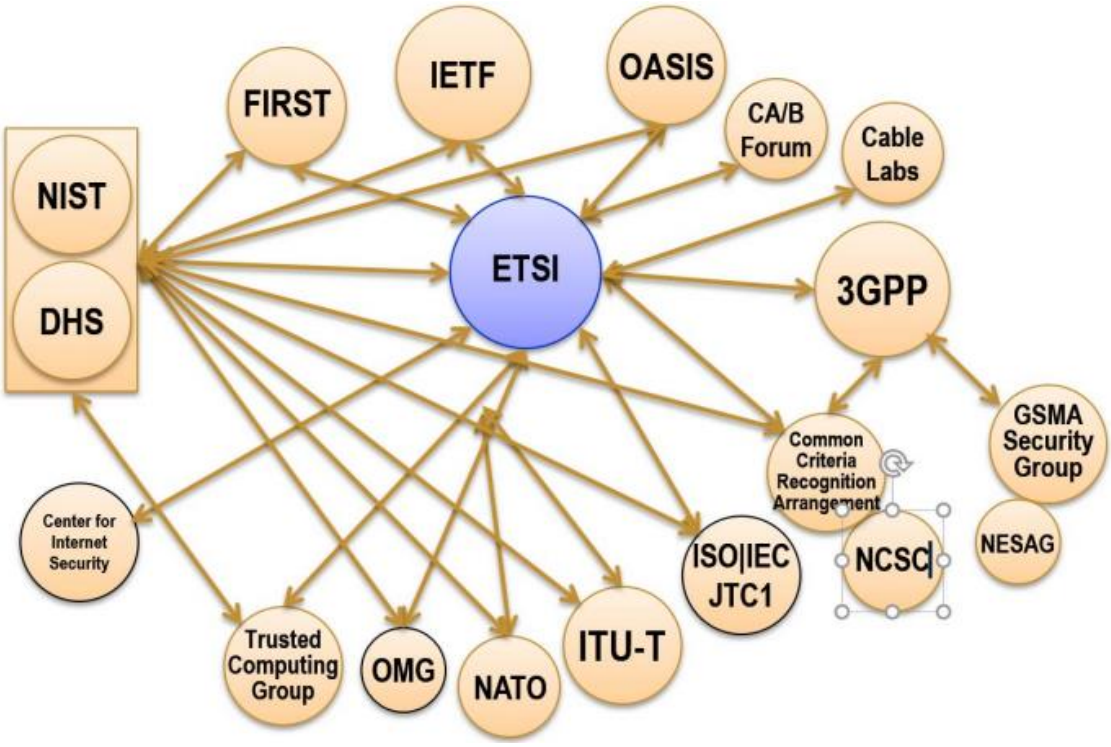

Figure 18: Relationship diagram 1 [50]

49 Gaps in NIS Standardization: https://enisa.europa.eu/publications/gaps-eu-standardisation/@@download/fullReport

50 Gaps in NIS Standardization: https://enisa.europa.eu/publications/gaps-eu-standardisation/@@download/fullReport

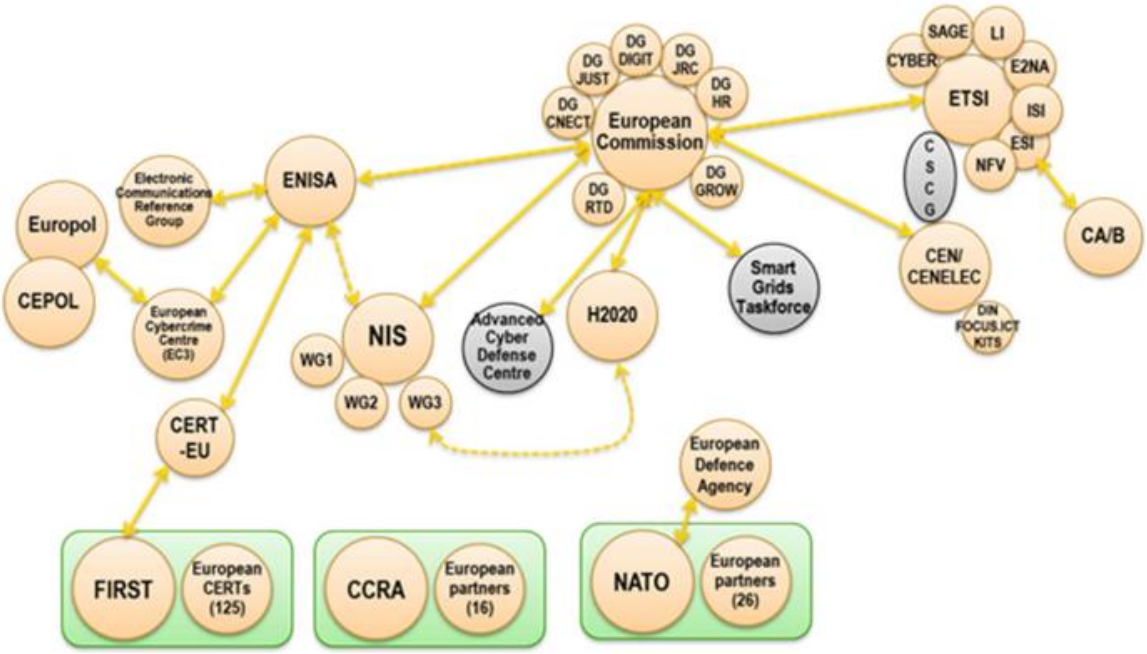

Figure 19: Relationship diagram 2 [51]

51 Gaps in NIS Standardization: https://enisa.europa.eu/publications/gaps-eu-standardisation/@@download/fullReport

5 Novel Approaches to Securing IoT

In a 2019 publication ENISA has made clear that security in IoT should be incorporated as a fundamental element into the product lifecycle.

Hackers can exploit vulnerabilities in IoT devices to gain unauthorized access to networks and sensitive data. Therefore, incorporating security for IoT devices into the SDLC is essential.

The SDLC is a process that guides the development of software applications from conception to deployment. It is a framework that helps developers produce high-quality software that meets customer needs and is secure. By integrating security into the SDLC, developers can identify and mitigate security risks early in the development process, minimizing the likelihood of security breaches.

Figure 20:Typical pillars of secure SDLC [52]

When it comes to IoT devices, security must be an integral part of the SDLC. The first step is to conduct a security assessment to identify potential vulnerabilities in the device. This assessment should include an analysis of the device's hardware, firmware, and software components. Once

52 https://eu-images.contentstack.com/v3/assets/blt66983808af36a8ef/blt85100d6c13369fe0/60d950c6e1461d39eb854b57/secure-sldc-diagram-green-center.png

potential security risks have been identified, developers can then create a security plan that includes measures to mitigate those risks.

One crucial aspect of incorporating security into the SDLC is the use of secure coding practices. Developers should follow established guidelines, such as the OWASP Top 10, to ensure that their code is secure. This includes implementing secure authentication and encryption protocols, as well as regular code reviews to identify and address any security vulnerabilities.

Another essential element of SDLC security is testing. Developers should perform regular security testing throughout the development process to identify any security issues that may have been missed during the design or coding phases. This testing should include both manual and automated testing to ensure that all potential security risks are identified and addressed.

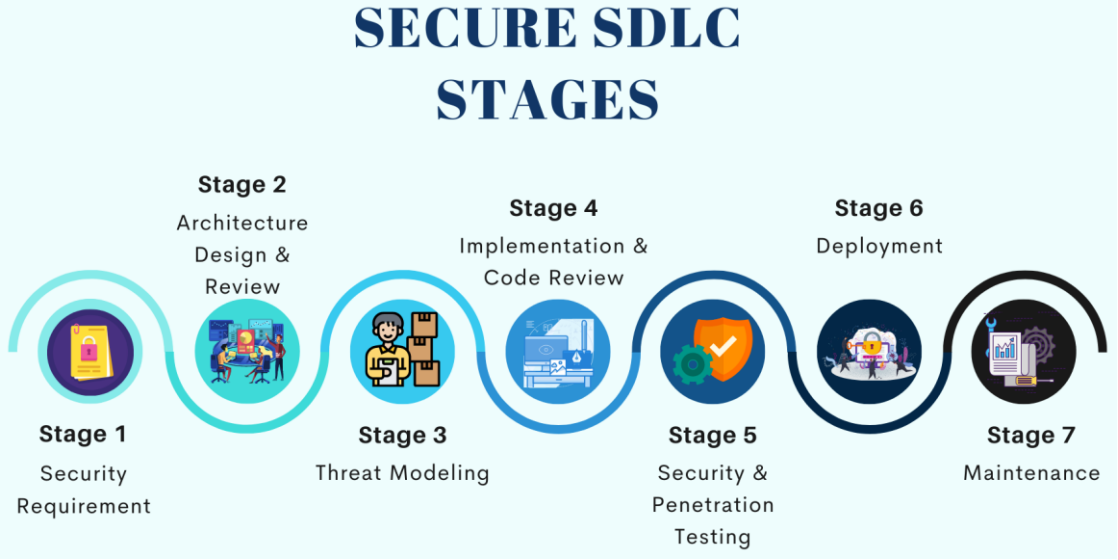

Figure 21: Secure SDLC stages [53]

Incorporating security for IoT devices into the SDLC is essential to ensure the security and reliability of these devices. Developers must take a proactive approach to security by conducting security assessments, following secure coding practices, and performing regular security testing. By doing so, IoT devices can be developed and deployed with the confidence that they are secure and able to withstand any potential security threats.

53 https://iosentrix.com/blog/assets/images/secure-sdlc-stages.png

5.1 Legislative Security and Privacy Protection Measures in IoT

ENISA, is tasked with enhancing cybersecurity throughout the EU by providing guidance and assistance to EU member states. ENISA has designated the development of security standards and best practices for NIS as one of its key areas of focus. Even though ENISA has made significant efforts in this area, there are still gaps to be closed in the standardization of NIS.

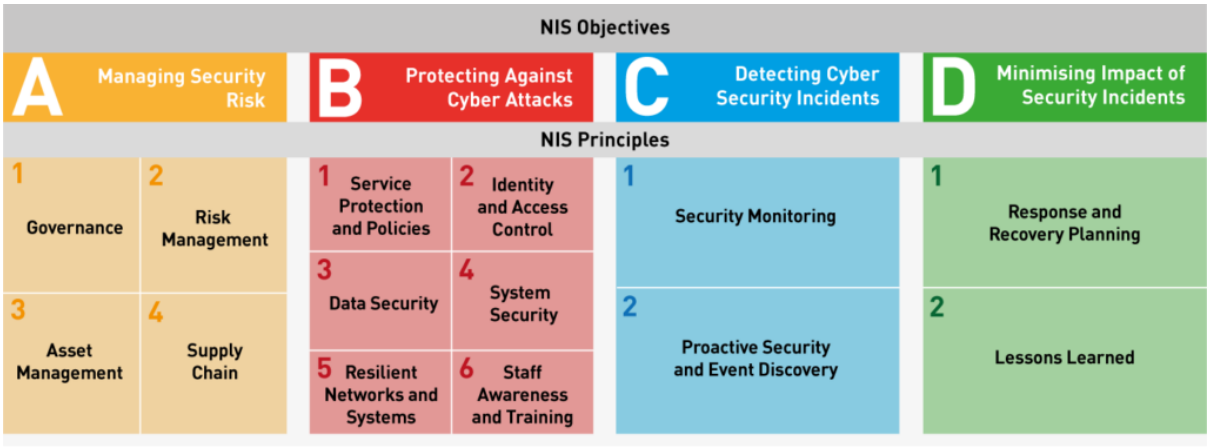

Figure 22: NIS objectives [54]

One of the most fundamental flaws of this standardization endeavor is the failure to reconcile the numerous standards and guidelines utilized by NIS. Although there are numerous standards and guidelines for NIS security, they are typically developed independently. This might lead to inconsistencies and misunderstanding among businesses striving to adhere to the rules and norms. ENISA is aware of this issue and has been attempting to promote the use of harmonized standards and recommendations; nonetheless, there is still a substantial amount of work to be done before this can be accomplished entirely.

54 https://www.nexor.com/wp/wp-content/uploads/2019/06/Nis-Objectives-and-Directive.png

Figure 23: NIS Regulations and Principles [55]

The lack of guidance for specific industries and sectors is another deficiency of the NIS standards. Despite the fact that several industries have their own standards and regulations, such as PCI DSS for the payment card industry, a large number of businesses lack readily available particular guidelines. This can make it difficult for firms in many industries to choose which standards and principles to follow, leading to a lack of uniformity in the security of NIS across a range of industries.

Along with this issue is the absence of direction for SMEs. Many SMEs are vulnerable to cyberattacks while lacking the resources and expertise required to implement complex NIS protection measures. ENISA recognizes the importance of providing support to SMEs and has produced specific guidelines for this group; nonetheless, more effort is required to ensure that SMEs are adequately protected.

One of the flaws of the NIS standardization process is that it does not pay sufficient attention to emerging technologies. As new types of cybercrime emerge in reaction to the development of newly

55 https://e.itgovernance.co.uk/l/500371/2018-05-11/b7hxw/500371/91266/NIS_Regulations_compliance_framework.pdf

developed and widely adopted technologies, they must be resisted. Yet, a substantial proportion of established norms and regulations do not account for these growing technologies, leaving organizations vulnerable to the introduction of new threats. ENISA is aware of this issue and has been attempting to develop standards for developing technologies such as the Internet of Things and artificial intelligence (AI), but there is still a great deal of work to be done in this area.

Finally, there is a gap in NIS standardization in terms of enforcement. While there are many standards and guidelines available for NIS security, there is a lack of consistency in their implementation and enforcement across different organizations and industries. This can lead to significant vulnerabilities in cybersecurity, as companies may interpret and apply the standards differently or fail to comply with them altogether. Without a uniform and rigorous approach to enforcing NIS standards, it becomes difficult to ensure the security of critical infrastructure, such as power grids, financial systems, and transportation networks. Additionally, the lack of standardization in enforcement can create confusion for consumers and users who may not understand the level of security provided by a particular product or service. To address these issues, there is a need for greater collaboration and coordination among policymakers, regulators, and industry leaders to establish clear and effective NIS standards and ensure their consistent implementation and enforcement.

5.2 SDLC phases

1. **Planning**: This phase involves understanding the project's objectives, scope, timelines, resources, and potential risks.
2. **Requirements**: In this phase, the development team identifies, documents, and analyzes the software requirements based on the project objectives and the needs of the stakeholders.
3. **Design**: The design phase involves creating a blueprint for the software solution based on the requirements gathered in the previous phase.
4. **Development**: During this phase, the software is actually built, tested, and integrated.
5. **Testing**: Once the software is developed, it undergoes several testing stages to detect any defects or errors before deployment.
6. **Deployment**: After testing is complete, the software is deployed in the production environment for use.
7. **Maintenance**: The software is continuously monitored and maintained to ensure that it continues to function correctly, is updated, and remains relevant to the evolving needs of the stakeholders.
8. **Retirement**: Finally, when the software is no longer required or is obsolete, it is retired from use, and its data is securely archived or destroyed.

5.2.1 Conceptual Level

An important aspect that is commonly overlooked when integrating security in a process (such as in the SDLC) is that of assessment and evaluation. Understanding the current cybersecurity posture is the first step towards establishing a plan to maintain this posture and improve it. In this respect, SMM are a very useful tool since they guide organizations to define their level of security in accordance with the requirements they wish to fulfil.[56]

Security maturity models are frameworks used to assess an organization's security posture and identify areas where improvements can be made. These models provide a set of benchmarks or standards that help organizations understand the level of security maturity they have achieved and what steps are needed to move to the next level.

The most commonly used security maturity models are CMMI and the SCMM. CMMI provides a comprehensive approach to improving organizational processes and includes a security component that helps organizations establish and maintain secure processes. The SCMM, on the other hand, focuses

56 https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_FINAL_Updated_V1.1.pdf

exclusively on security and is designed to assess an organization's security practices across seven different domains, including risk management, incident management, and access control.[57]
Using security maturity models can help organizations identify weaknesses in their security posture, develop a roadmap for improving security, and measure progress over time. By understanding where they stand in terms of security maturity, organizations can prioritize security investments, allocate resources effectively, and ensure that security practices are aligned with business goals.
However, it's important to note that security maturity models are not one-size-fits-all and should be tailored to the specific needs of an organization. Additionally, organizations should view security as an ongoing process rather than a one-time project and use security maturity models as a tool to continually improve their security posture over time.

5.2.2 Planning

The first step in SDLC is Planning. This phase is defining the project's objectives, scope, timelines, resources, and potential risks. Without proper planning, a project may face challenges such as delays, budget overruns, and unexpected roadblocks.
During the planning phase, the project team establishes a project plan, which outlines the project's scope and objectives, identifies the key stakeholders, and establishes the project's timelines and milestones. The project plan also includes a risk management plan that identifies potential risks and outlines strategies to mitigate them.

5.2.3 Requirements

The second phase of the SDLC is Requirements Gathering. This phase involves gathering, analyzing, and documenting the software requirements to meet the stakeholders' needs and expectations.
The requirements gathering phase enables the development team to work with stakeholders to identify the software's functional and non-functional requirements. Functional requirements specify what the software should do, while non-functional requirements specify how well the software should do it, such as performance, security, and usability.

5.2.4 Design

The third phase of the SDLC is Design. This phase involves transforming the software requirements gathered in the previous phase into a blueprint for the software solution.

---

57 https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/ssca/2017-winter/TueAM2_2_CMMI.pdf

During the design phase, the development team creates a detailed design for the software that includes the software architecture, user interface design, data design, and the algorithmic design. The design phase is critical because it sets the foundation for the software's implementation in the development phase.

5.2.5 Development

The fourth phase of SDLC is Development. This phase involves the actual development of the software solution based on the requirements and design specifications gathered in the previous phases.
During the development phase, the development team writes the code for the software solution, tests it, and implements it.

5.2.6 Maintenance

The fifth and final phase of SDLC is Maintenance. This phase involves maintaining the software solution to ensure that it continues to meet the stakeholders' needs and expectations over time.

During the maintenance phase, the development team provides ongoing support to the software solution, such as fixing bugs, making enhancements, and performing upgrades.

5.3 Security Applied into SDLC

Overall, security is an integral part of SDLC. It ensures that the software application is safe and secure from potential threats and vulnerabilities that can affect its functioning, data privacy, and confidentiality. The importance of security in SDLC has increased in recent years due to the rise in cyber threats and attacks, which can lead to data breaches and financial losses for organizations.

The first stages of SDLC, are where security requirements and objectives are defined. This involves identifying potential threats and risks that the software application may face and creating security measures to mitigate them. During the design phase, security controls are incorporated into the software architecture to prevent attacks and ensure secure data handling. Secure coding practices are followed during the implementation phase to minimize security vulnerabilities.

The testing phase involves various types of security testing, including penetration testing, vulnerability testing, and security audits. These tests are designed to identify any potential security weaknesses in the application, such as SQL injection or cross-site scripting, and ensure that the software is secure and ready for deployment. In addition, during the testing phase, security-related documentation is developed, which includes security policies, procedures, and guidelines for secure software development.

The final phases is where software updates, patches, and upgrades are made to ensure the software remains secure over time. Regular security assessments and audits are conducted to identify any new vulnerabilities or threats and take appropriate action to mitigate them.

5.4 Hardware Level Protections

Additional security measures should include integrating Secure boot mechanisms into IoT devices, that involves incorporating TPM hardware into the device's design, as well as developing software to interact with the TPM.

Secure boot mechanisms are critical security features for IoT devices. They ensure that the device's firmware and software are authentic and have not been tampered with before the device starts up. The following are some of the common secure boot mechanisms in IoT:

a) **TPM:** TPM is a hardware-based security module that provides secure storage and cryptographic functions. It can be used to store a device's private keys, certificates, and other sensitive information. TPM can be used to verify the integrity of the firmware and boot loader during the boot process.

b) **Secure Boot:** Secure Boot is a firmware feature that ensures that only trusted code is loaded during the boot process. It checks the digital signature of the firmware and boot loader to ensure that they are signed by a trusted entity.

c) **Code Signing:** Code signing involves digitally signing the firmware and software with a private key. The public key is stored in the device's firmware, and the boot loader verifies the signature during the boot process.

d) **Hardware Root of Trust:** The hardware root of trust is a secure element embedded in the device's hardware. It can be used to store cryptographic keys and other sensitive information. The boot loader verifies the integrity of the firmware and boot loader using the keys stored in the hardware root of trust.

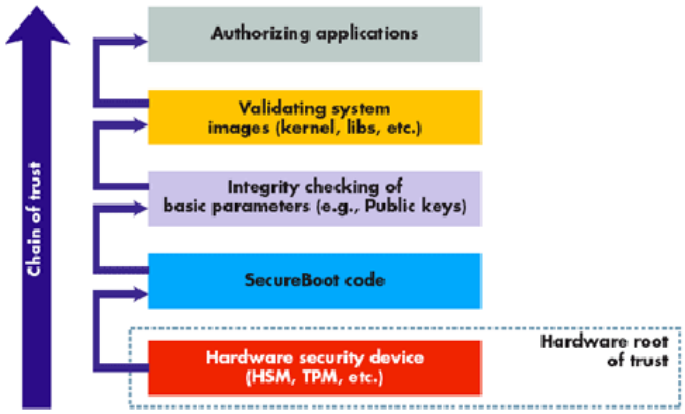

Figure 24: How secure boot mechanisms work on top of one another [58]

When TPM is added to an IoT device, it can provide a range of security benefits, such as secure storage of cryptographic keys, secure boot processes, and secure communication with other devices.

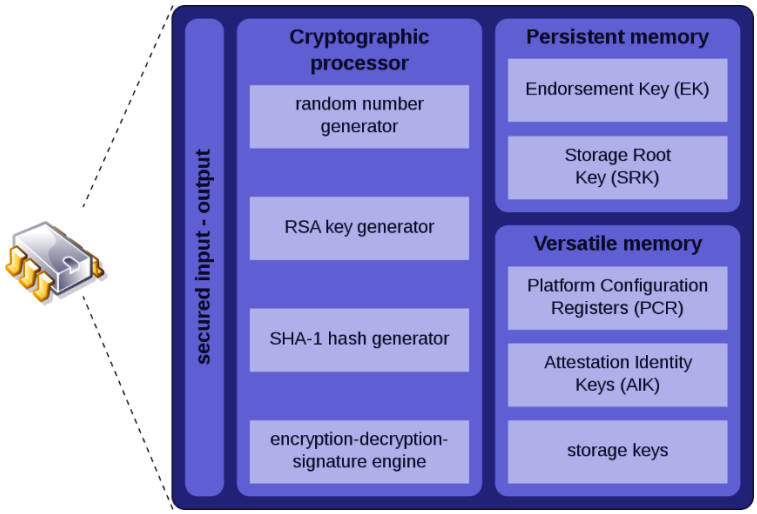

Figure 25: High level representation of TPM [59]

The process of adding TPM to IoT devices should be part of the SDLC, just like adding security features. The first step is to conduct a security assessment to identify the device's security requirements. Once the security requirements have been identified, the device's hardware must be

---

58 https://researchgate.net/publication/224230457/figure/fig5/AS:302815932108805@1449208353001/Generic-secure-boot-architecture.png

59 https://upload.wikimedia.org/wikipedia/commons/thumb/b/be/TPM.svg/1200px-TPM.svg.png

designed to accommodate the TPM. This will involve selecting the right TPM module and designing the device's architecture to support it.

Once the device's hardware is designed to support TPM, the next step is to develop software that interacts with the TPM. This software will allow the device to take advantage of the TPM's security features, such as secure boot processes and secure storage of cryptographic keys. The software must be developed with security in mind and should follow secure coding practices to ensure that it does not introduce vulnerabilities into the device.

Testing is also an essential part of adding TPM to IoT devices. Developers should perform regular security testing to ensure that the device's security features are working correctly and that there are no security vulnerabilities that could be exploited. This testing should include both manual and automated testing to ensure that all potential security risks are identified and addressed.

6 Scaling Security and Privacy in Smart Cities

6.1 From IoT to Smart Cities: Pioneering a Connected Urban Future

The revolutionary concept of interconnected IoT devices being capable of sharing data and communicating with one another, has not only transformed industries and homes but has also paved the way for the development of smart cities.

Smart cities harness the power of IoT technology to improve the quality of life for their residents and optimize urban operations. By integrating various IoT devices and systems, cities can gather and analyze vast amounts of data in real-time, enabling them to make informed decisions and enhance efficiency across different sectors.

One of the primary areas where IoT has made a significant impact is in urban infrastructure. By embedding sensors and connected devices into transportation systems, streetlights, waste management, and utilities, cities can monitor and manage these resources more effectively. For example, traffic sensors can collect data on congestion patterns, allowing authorities to optimize traffic flow and reduce congestion. Smart grids can adjust energy consumption based on demand, leading to improved energy efficiency and cost savings.

IoT technology also enhances public safety and security in smart cities. Video surveillance cameras equipped with facial recognition and behavioral analysis can detect and respond to potential threats swiftly. Emergency response systems can be interconnected to provide real-time alerts and optimize resource allocation during critical situations. This interconnectedness enhances the overall safety and security of residents.

Furthermore, IoT-driven smart cities promote sustainability and environmental conservation. By monitoring air quality, water usage, and waste management systems, cities can implement proactive measures to minimize pollution levels and conserve natural resources. Smart sensors can detect leakages and optimize water distribution, while intelligent waste management systems can optimize collection routes, reducing fuel consumption and emissions.

Another vital aspect of smart cities is citizen engagement. IoT devices and applications enable residents to actively participate in the decision-making process and provide feedback to city authorities. Through mobile apps and smart devices, citizens can access real-time information about transportation, energy usage, and community events. This involvement fosters a sense of belonging and empowerment among residents, ultimately leading to a stronger community bond.

While IoT-driven smart cities offer tremendous benefits, they also present challenges that need to be addressed. Ensuring data security and privacy is paramount, as interconnected systems are vulnerable to cyber threats. Robust cybersecurity measures and policies are essential to safeguard sensitive data and maintain public trust.

In conclusion, the evolution from IoT to smart cities represents a significant leap in urban development. By harnessing the potential of IoT technology, cities can optimize resource management, enhance public safety, promote sustainability, and foster citizen engagement. As this transformative journey continues, it is crucial for governments, organizations, and individuals to collaborate and navigate the challenges to create truly connected and intelligent urban environments for the benefit of all.

The fundamental architectural changes that will be revolutionized by Smart Cities must unequivocally encompass the following core pillars:

1. Governance
2. Healthcare
3. Buildings
4. Transportation
5. Energy

6.2 Governance

In a smart city context, a smart government refers to the application of advanced technologies and data-driven approaches by the government to enhance the quality of governance and public services. It aims to leverage digital innovations to improve efficiency, sustainability, and citizen engagement while addressing the challenges faced by urban areas.

Here are some key aspects of a smart government:

1. Digital Infrastructure: A smart government relies on robust digital infrastructure, including high-speed internet connectivity, data centers, and communication networks. These technological foundations enable seamless data exchange, real-time monitoring, and efficient service delivery.
2. Open Data and Data Analytics: A smart government makes use of open data initiatives, ensuring that relevant government data is easily accessible to the public and businesses. This data can be analyzed using advanced analytics techniques to gain insights, identify patterns, and make informed decisions. It facilitates evidence-based policymaking, improved resource allocation, and better urban planning.
3. E-Government Services: A smart government provides digital services and platforms for citizens to interact with government agencies. These services can include online portals for accessing information, submitting applications, paying bills, and registering for various government programs. E-government services streamline administrative processes, reduce paperwork, and enhance convenience for citizens.
4. Smart Mobility: A smart government focuses on intelligent transportation systems to enhance mobility within the city. This includes smart traffic management systems, real-time public transportation information, digital parking solutions, and integration of different modes of transport. By promoting sustainable and efficient mobility options, a smart government reduces congestion, improves air quality, and enhances the overall quality of life for residents.
5. Citizen Engagement and Participation: A smart government fosters active citizen engagement through digital platforms and tools. It encourages citizen participation in decision-making processes, solicits feedback, and enables collaboration between the government and the public. This can be achieved through social media, mobile applications, online surveys, and virtual town halls, promoting transparency, trust, and inclusiveness in governance.
6. Sustainability and Resource Management: A smart government embraces sustainability as a core principle. It adopts innovative approaches to resource management, including smart grid systems for efficient energy distribution, water management systems for conservation, waste management solutions for recycling and waste reduction, and green building initiatives. By

incorporating sustainable practices, a smart government contributes to environmental preservation and the overall resilience of the city.

7. Safety and Security: A smart government leverages technology for enhancing safety and security measures. This includes the deployment of surveillance systems, intelligent emergency response systems, and data-driven crime prevention strategies. By leveraging real-time data and analytics, a smart government can identify potential risks, respond effectively to emergencies, and ensure the safety of its citizens.

6.3 Healthcare

Smart healthcare aims to leverage digital innovations to improve patient care, enable preventive measures, and optimize healthcare delivery within a city.

Here are key aspects of smart healthcare:

1. Electronic Health Records: Smart healthcare systems utilize electronic health records to store and manage patient information securely. EHRs allow healthcare providers to access patient data in real-time, leading to better coordination and continuity of care. It enables healthcare professionals to make informed decisions, reduce medical errors, and provide personalized treatment plans.
2. Telehealth and Remote Monitoring: Smart healthcare incorporates telehealth and remote monitoring technologies to enable virtual consultations and remote patient monitoring. Through video calls, chat platforms, and mobile applications, patients can receive medical advice, prescriptions, and follow-up care without physically visiting healthcare facilities. Remote monitoring devices, such as wearables or connected sensors, allow healthcare providers to track vital signs and health parameters remotely, providing proactive care and early interventions.
3. Health Information Exchange: Smart healthcare systems facilitate secure sharing of health information across different healthcare providers and organizations. This interoperability enables seamless transfer of patient data, reducing duplication of tests, and ensuring comprehensive care. HIE promotes collaboration among healthcare professionals, streamlines care coordination, and improves patient outcomes.
4. Data Analytics and Predictive Modeling: Smart healthcare leverages data analytics and predictive modeling to derive insights and make data-driven decisions. By analyzing large volumes of healthcare data, such as patient records, clinical trials, and population health data, healthcare providers can identify disease trends, predict outbreaks, and implement targeted interventions. Data analytics also helps in resource allocation, optimizing healthcare services, and identifying high-risk patients for proactive care management.
5. IoT in Healthcare: IoT devices and sensors play a significant role in smart healthcare. These devices can monitor patients' health conditions, track medication adherence, and enable real-time data collection. For example, smart wearable devices can measure heart rate, sleep patterns, and activity levels, providing valuable information for personalized care. IoT in healthcare enhances remote patient monitoring, chronic disease management, and preventive healthcare interventions.

6. Precision Medicine and Personalized Care: Smart healthcare embraces the concept of precision medicine by tailoring treatments based on an individual's genetic, lifestyle, and environmental factors. Advances in genomic sequencing and personalized medicine enable targeted therapies, improved medication management, and reduced adverse drug reactions. Smart healthcare systems integrate these approaches to provide patient-centric care and improve treatment outcomes.
7. Health Promotion and Preventive Measures: Smart healthcare places a strong emphasis on health promotion and preventive measures. It leverages technology to deliver personalized health education, promote healthy behaviors, and encourage proactive healthcare management. Mobile applications, wearables, and online platforms can provide real-time health tips, reminders for vaccinations or screenings, and personalized wellness programs.

8. Artificial Intelligence in Healthcare: Smart healthcare incorporates AI applications to support diagnosis, treatment planning, and decision-making processes. AI algorithms can analyze medical images, interpret lab results, and assist healthcare professionals in making accurate diagnoses. AI-driven chatbots and virtual assistants also enhance patient engagement by providing immediate responses to inquiries and offering basic medical advice.

By integrating advanced technologies and data-driven approaches, smart healthcare in a smart city context aims to improve healthcare accessibility, enhance patient outcomes, and enable proactive health management. It promotes a more efficient and patient-centric healthcare system, leading to healthier communities within the city.

6.4 Buildings

Smart buildings as an umbrella term, refers to structures that incorporate advanced technologies and intelligent systems to optimize energy efficiency, enhance occupant comfort, improve operational efficiency, and promote sustainable practices. These buildings leverage connectivity, automation, and data analytics to create more efficient, responsive, and environmentally friendly spaces.

Here are key aspects of smart buildings:

1. Building Automation Systems: Smart buildings employ building automation systems to centrally control and monitor various building functions, such as lighting, HVAC, security, and occupancy. BAS uses sensors, actuators, and controllers to automate processes, optimize energy consumption, and improve operational efficiency. For example, smart lighting systems adjust based on natural light availability or occupancy, reducing energy waste.
2. Energy Management and Efficiency: Smart buildings prioritize energy management and efficiency through advanced technologies. They integrate energy monitoring systems to track real-time energy consumption, identify areas of waste, and optimize energy usage. Automated controls and smart meters enable efficient management of heating, cooling, and lighting, leading to reduced energy costs and carbon footprint.
3. Indoor Environmental Quality: Smart buildings focus on enhancing occupant comfort and well-being. They employ sensors to monitor indoor air quality, temperature, humidity, and occupancy levels. This data is used to automatically adjust HVAC systems and ventilation rates to maintain optimal indoor conditions. Improved IEQ leads to increased productivity, reduced health risks, and enhanced overall occupant satisfaction.
4. Integrated Building Management Systems: Smart buildings utilize integrated building management systems that consolidate data from various building systems into a unified platform. IBMS provides a holistic view of the building's operations, enabling centralized control, real-time monitoring, and data analytics. Facility managers can proactively identify issues, streamline maintenance, and make informed decisions to optimize building performance.
5. Predictive Maintenance: Smart buildings employ predictive maintenance techniques to anticipate and address potential equipment failures or maintenance needs. By analyzing data from sensors and equipment performance, predictive algorithms can detect patterns and identify maintenance requirements before major breakdowns occur. This approach reduces downtime, extends equipment lifespan, and optimizes maintenance schedules.
6. Occupancy Management and Space Utilization: Smart buildings use occupancy sensors and analytics to optimize space utilization. Real-time data on occupancy patterns and utilization

rates help facility managers make informed decisions about space allocation, desk sharing, and meeting room bookings. Optimizing space utilization leads to cost savings, reduced real estate footprint, and improved efficiency.

7. Integration of Renewable Energy: Smart buildings embrace the integration of renewable energy sources to reduce reliance on traditional energy grids. They may include solar panels, wind turbines, or geothermal systems to generate clean energy on-site. Energy storage systems, such as batteries, allow for efficient energy distribution and usage during peak demand periods. Integration of renewables promotes sustainability and contributes to the overall resilience of the smart city's energy infrastructure.
8. Connectivity and IoT Integration: Smart buildings leverage connectivity and the IoT to enable seamless communication between various building systems. IoT devices, sensors, and actuators collect and exchange data, allowing for real-time monitoring, analysis, and control. This integration enhances operational efficiency, improves safety and security, and enables smart decision-making.

6.5 Transportation

Smart transportation encompasses the integration of advanced technologies and data-driven solutions to enhance the efficiency, safety, and sustainability of transportation systems within urban environments, promoting seamless and intelligent mobility. It focuses on leveraging connectivity, automation, and real-time data to optimize mobility, reduce congestion, and improve the overall transportation experience for residents and visitors.

Here are key aspects of smart transportation in a smart city context:

1. Intelligent Traffic Management Systems: Smart transportation incorporates intelligent traffic management systems that use real-time data and advanced analytics to monitor and manage traffic flow. These systems utilize sensors, cameras, and data from various sources to detect congestion, optimize traffic signal timing, and provide dynamic routing suggestions. Intelligent traffic management reduces travel times, minimizes congestion, and enhances overall traffic efficiency.
2. Connected and Autonomous Vehicles: Smart transportation integrates connected and autonomous vehicles into the transportation ecosystem. Connected vehicles communicate with each other and with infrastructure, sharing real-time data on traffic conditions, road hazards, and optimal routes. Autonomous vehicles use sensors and AI algorithms to navigate roads, reducing human error and improving safety. CAVs enhance traffic flow, increase safety, and offer potential for reduced emissions.
3. Multi-Modal Transportation Solutions: Smart transportation promotes multi-modal solutions by integrating different modes of transportation, such as public transit, cycling, walking, and ride-sharing services. It provides real-time information on public transit schedules, availability, and routes through mobile apps or digital signage. Integrated payment systems and seamless transfers between modes encourage the use of sustainable transportation options and reduce reliance on private vehicles.
4. Mobility as a Service: Smart transportation incorporates Mobility as a Service platforms that provide on-demand and integrated transportation services. MaaS platforms offer a single interface for users to plan, book, and pay for different modes of transportation. It facilitates seamless interconnectivity between public transit, ride-sharing, bike-sharing, and other transportation options, making it convenient for users to choose the most efficient and sustainable travel options.
6. Intelligent Parking Systems: Smart transportation incorporates intelligent parking systems to improve parking management and reduce congestion. These systems provide real-time information on parking availability, guiding drivers to vacant spots and reducing the time spent

searching for parking. Smart parking solutions may include mobile apps, sensors, and digital signage that provide information on parking locations, pricing, and availability.

8. Data-Driven Transportation Planning: Smart transportation relies on data analytics and predictive modeling to inform transportation planning and decision-making. Data from various sources, including sensors, GPS devices, and ticketing systems, are analyzed to identify travel patterns, demand hotspots, and potential areas for infrastructure improvements. Data-driven planning enables the optimization of transportation networks, the identification of bottlenecks, and the development of more efficient routes and schedules.
9. Real-Time Travel Information: Smart transportation provides real-time travel information to commuters through various channels, such as mobile apps, websites, and electronic displays. This includes real-time updates on public transit schedules, delays, and alternative routes. Real-time travel information allows users to make informed decisions, adjust their travel plans, and choose the most efficient and reliable transportation options.
10. Sustainability and Environmental Considerations: Smart transportation focuses on promoting sustainable transportation options to reduce emissions and environmental impact. This includes incentivizing the use of electric vehicles, promoting bike-sharing and walking infrastructure, and integrating renewable energy sources into transportation systems. By prioritizing sustainability, smart transportation contributes to a cleaner and greener urban environment.

6.6 Energy

Smart energy in a smart city context refers to the integration of advanced technologies and data-driven solutions to optimize energy generation, distribution, consumption, and management within urban areas. It involves leveraging innovative approaches to increase energy efficiency, promote renewable energy sources, and reduce environmental impact.

Here are key aspects of smart energy in a smart city context:

1. Smart Grid Infrastructure: Smart energy systems rely on smart grid infrastructure to enable the efficient and reliable distribution of electricity. Smart grids incorporate digital communication technologies, sensors, and automation to monitor and manage electricity flow, detect outages, and optimize energy distribution. These systems facilitate two-way communication between utilities and consumers, enabling real-time data exchange and load balancing.
2. Demand Response and Energy Management: Smart energy encourages demand response programs that incentivize consumers to adjust their energy usage based on supply and demand dynamics. By leveraging real-time data and smart meters, consumers can actively participate in load management, reducing peak demand and optimizing energy consumption. Energy management systems provide insights and control over energy usage, enabling consumers to make informed decisions and reduce waste.
3. Renewable Energy Integration: Smart energy promotes the integration of renewable energy sources, such as solar and wind, into the urban energy infrastructure. Smart cities leverage solar panels, wind turbines, and other renewable energy systems to generate clean electricity locally. Advanced technologies and analytics optimize the integration of renewables into the grid, ensuring efficient energy generation, storage, and distribution.
4. Energy Storage Solutions: Smart energy systems incorporate energy storage technologies, such as batteries or flywheels, to store excess energy generated from renewable sources. Energy storage systems enable the balancing of supply and demand, support grid stability, and provide backup power during peak demand or outages. By optimizing energy storage, smart cities can maximize the utilization of renewable energy resources and enhance grid reliability.
5. Energy Efficiency and Building Management: Smart energy promotes energy efficiency practices within buildings by leveraging technologies like smart meters, sensors, and automation. Energy-efficient building designs, smart lighting systems, HVAC optimization, and intelligent energy management systems help reduce energy consumption. Real-time data analytics enable facility managers to identify energy-saving opportunities, optimize operations, and track performance to achieve sustainable and cost-effective energy usage.

6. Electric Vehicle Infrastructure: Smart energy systems support the integration of EVs into urban transportation. This includes the deployment of EV charging infrastructure and smart charging solutions that consider energy demand, pricing, and grid stability. Smart cities incentivize the adoption of EVs, promote electric public transportation, and facilitate seamless charging experiences to reduce dependence on fossil fuels and decrease greenhouse gas emissions.
7. Energy Monitoring and Analytics: Smart energy systems utilize data analytics and monitoring tools to track and analyze energy usage patterns. Real-time energy monitoring provides insights into consumption patterns, identifies inefficiencies, and helps stakeholders make informed decisions regarding energy management and optimization. Advanced analytics enable predictive maintenance, demand forecasting, and energy planning to enhance efficiency and reliability.
8. Citizen Engagement and Energy Awareness: Smart energy initiatives actively engage citizens in energy conservation and sustainability efforts. Smart cities provide platforms for energy education, awareness campaigns, and citizen participation in energy-saving programs. This engagement fosters a culture of energy consciousness, empowering individuals and communities to contribute to the overall energy efficiency and sustainability goals.

By integrating advanced technologies and data-driven approaches, smart energy aims to optimize energy generation, distribution, and consumption while promoting renewable energy sources and reducing environmental impact. It enables cities to become more resilient, sustainable, and efficient in their energy usage, contributing to a greener and more livable urban environment.

6.7 Challenges

Establishing a security framework is crucial for scaling security and privacy from the IoT to smart cities. As smart cities become more prevalent, the interconnectedness of various IoT devices and infrastructure creates vulnerabilities that can be exploited by malicious actors. A robust security framework ensures that communication and data exchange between IoT devices and smart city systems remain secure and private.

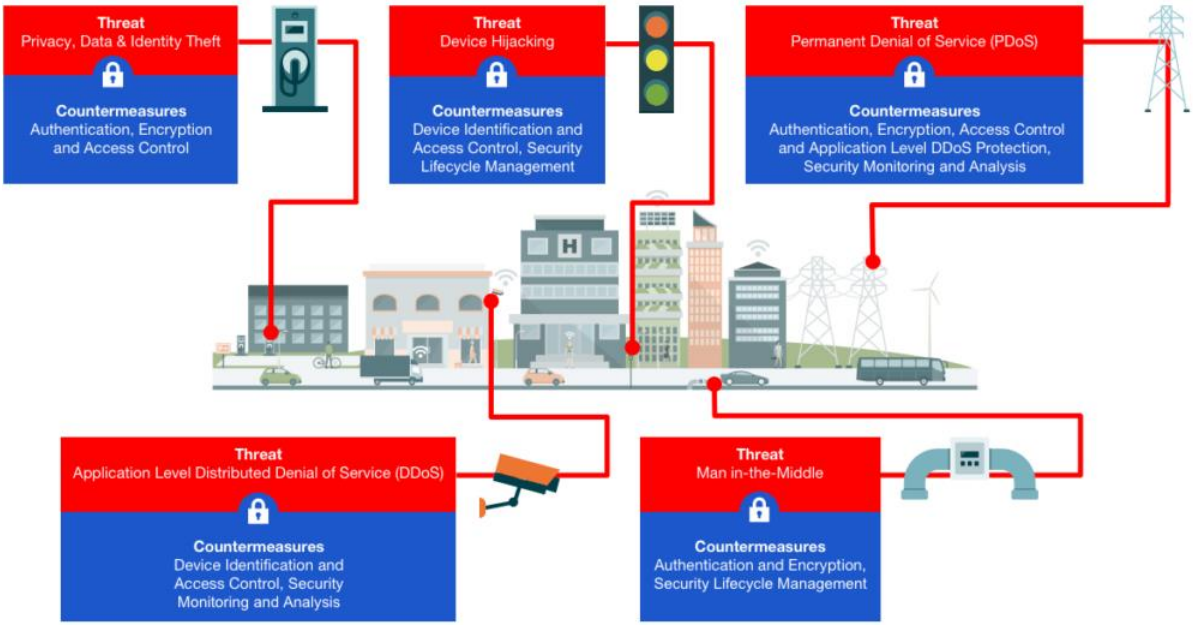

Figure 26: Threats and Countermeasures in Smart Cities [60]

Authentication and access control play a vital role in mitigating security risks. Implementing strong authentication protocols ensures that only authorized individuals or devices can access sensitive systems and data. This prevents unauthorized access and reduces the likelihood of cyber-attacks. Access controls further enhance security by enforcing granular permissions, allowing only necessary privileges for different users and devices.

60 https://www.rambus.com/wp-content/uploads/2017/12/Smart-City-Threats-and-Countermeasures-1024x576.png

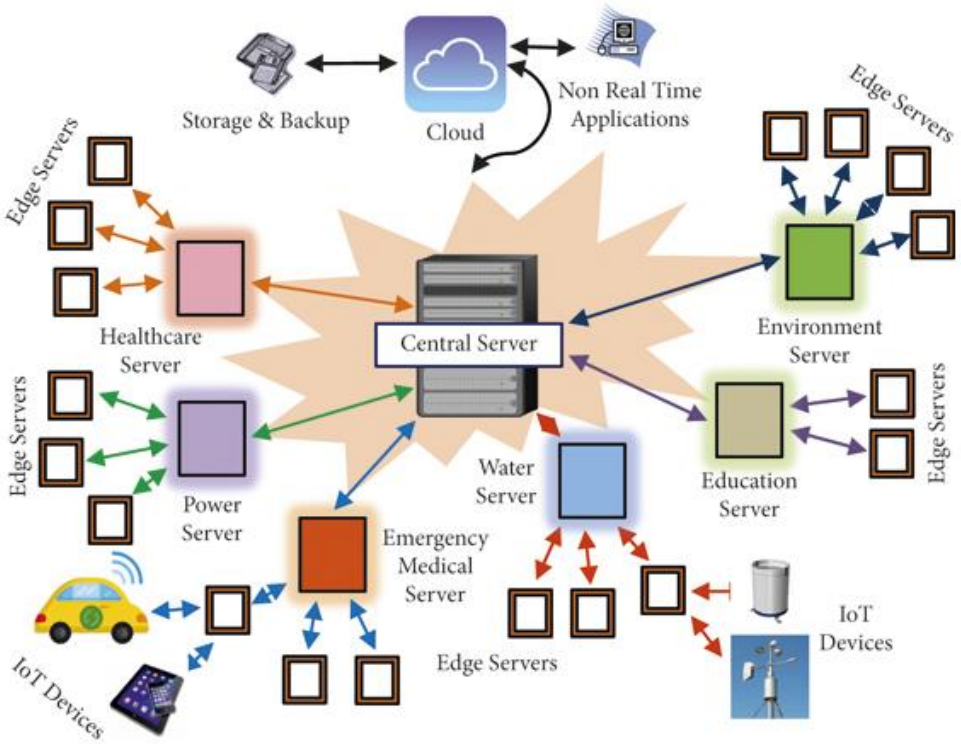

Figure 27: Smart city authentication system based on a centralized authority [61]

Data encryption is another crucial aspect of scaling security and privacy. As data flows between IoT devices and smart city infrastructure, it needs to be encrypted to protect it from interception or tampering. Advanced encryption techniques, such as strong cryptographic algorithms, can safeguard sensitive information from unauthorized access, ensuring that data remains confidential and integral during transmission and storage.

Developing an effective incident response plan is essential to swiftly and efficiently address security breaches or cyber-attacks. A well-defined plan outlines the steps to be taken in the event of a security incident, including containment, investigation, and recovery. This proactive approach minimizes the impact of security breaches, allows for faster remediation, and helps prevent future incidents.

Compliance with privacy and security regulations is paramount for smart cities. Adhering to applicable laws and regulations protects the privacy rights of individuals and ensures that security measures meet established standards. Compliance efforts involve regular audits, assessments, and updates to keep up with evolving regulatory requirements.

Conducting risk assessments on a regular basis helps identify potential vulnerabilities and risks within smart city infrastructure. By identifying weak points, security professionals can implement appropriate safeguards and countermeasures to mitigate potential threats. Risk assessment should encompass all layers of the smart city ecosystem, including devices, networks, and data management systems.

Continuous monitoring is crucial to maintain a proactive security posture. Real-time monitoring allows for the detection and response to security threats as they occur, minimizing the window of

61 https://www.hindawi.com/journals/scn/2022/5186376/fig1/

opportunity for attackers. Monitoring systems can employ advanced techniques like anomaly detection, behavior analysis, and threat intelligence to identify and mitigate potential security incidents.

Public awareness and education are essential in scaling security and privacy efforts. Citizens should be educated about the risks associated with IoT and the importance of protecting their personal data. Promoting good security practices, such as strong passwords, regular software updates, and cautious sharing of personal information, can empower individuals to contribute to the overall security and privacy of smart cities.

Collaboration between government agencies, private sector companies, and academia is vital to tackle the challenges of scaling security and privacy. Sharing knowledge, resources, and best practices allows for the development and implementation of effective solutions. This collaborative approach fosters innovation, enabling smart cities to address emerging threats and evolving technologies.

Lastly, future-proofing security and privacy measures is essential. As technology advances, new vulnerabilities and attack vectors may emerge. Building scalable and adaptable security solutions ensures that smart cities can keep pace with the evolving threat landscape. Regular assessments, updates, and investments in emerging security technologies are necessary to maintain a high level of protection.

In conclusion, scaling security and privacy from IoT to smart cities requires a multi-faceted approach. By establishing a comprehensive security framework, implementing strong authentication and encryption measures, developing incident response plans, ensuring regulatory compliance, conducting risk assessments, maintaining continuous monitoring, fostering public awareness, promoting collaboration, and future-proofing security measures, smart cities can create a secure and privacy-centric environment for their residents and stakeholders.

6.8 AI and ML

With the increased reliance on interconnected devices and systems, security concerns have become paramount. To address these challenges, AI and ML technologies have emerged as vital tools for securing smart cities.

How AI and ML can be used to enhance security and privacy in Smart Cities:

1. Real-time Threat Detection: AI and ML algorithms can analyze vast amounts of data from various sources, including surveillance cameras, sensors, social media feeds, and network logs, to identify and flag potential security threats in real-time. These algorithms can learn from historical patterns and anomalies, enabling them to detect and respond to abnormal activities swiftly and accurately.[62]
2. Predictive Analytics for Crime Prevention: By leveraging historical crime data, AI and ML can predict crime hotspots and patterns, allowing law enforcement agencies to allocate resources efficiently. Police departments can deploy patrol units, CCTV cameras, and other surveillance systems strategically based on the predictive models generated by AI algorithms, thereby deterring criminal activities and enhancing public safety.[63]
3. Anomaly Detection in Critical Infrastructure: Smart cities rely on interconnected systems, including power grids, transportation networks, and water supply systems. AI and ML can play a crucial role in detecting anomalies or cyber-attacks in these critical infrastructures. By continuously monitoring network traffic and system behavior, AI algorithms can identify suspicious activities and potential vulnerabilities, enabling proactive measures to secure the infrastructure.[64]
4. Intelligent Video Surveillance: AI-powered video surveillance systems can automatically analyze video feeds, recognizing and tracking objects, people, and vehicles. These systems can identify unusual behaviors, such as unauthorized access to restricted areas or abandoned objects, and promptly alert security personnel. ML algorithms improve over time by learning from new data, allowing for more accurate threat detection and reduced false alarms.[65]

---

62 Chouhan, A., Gogate, M., & Thampi, S. M. (2020). Intelligent Framework for Smart City Security: Issues, Challenges, and Mitigation. In Cybersecurity for Smart Cities (pp. 45-65). Springer

63 Berman, M., & Lawton, G. (2018). Smart policing: Machine learning and predictive analytics for law enforcement. John Wiley & Sons.

64 Yang, S., Ma, M., Zhang, Y., & Shen, X. (2020). Critical Infrastructure Protection in Smart Cities: A Machine Learning Approach. IEEE Internet of Things Journal, 7(6), 4853-4862

65 Smeureanu, I., & Fratu, O. (2019). Machine learning algorithms for video surveillance systems. In 2019 13th International Symposium on Advanced Topics in Electrical Engineering (ATEE) (pp. 1-6). IEEE

Securing smart cities is a complex and ongoing challenge. However, AI and ML technologies offer significant potential in enhancing the security posture of these urban environments. By utilizing real-time threat detection, predictive analytics, anomaly detection, and intelligent video surveillance, smart cities can become more resilient and better equipped to mitigate security risks.

6.9 EBSI

The European Blockchain Services Infrastructure program is an initiative by the European Commission that aims to build a blockchain-based infrastructure for the public sector across Europe. The program seeks to provide a trusted and secure digital infrastructure that can be used by governments, businesses, and citizens to exchange data and services across borders.

The EBSI program is based on blockchain technology, which is a distributed ledger that allows for secure and transparent transactions without the need for intermediaries. The use of blockchain technology in the EBSI program is expected to increase the efficiency, security, and trustworthiness of public services while reducing costs and promoting innovation.

The EBSI program is designed to support the implementation of a range of use cases, including electronic identity, document management, supply chain management, and the verification of academic credentials. The program is also intended to support cross-border collaboration and the sharing of data and services between EU member states.

Overall, the EBSI program represents a significant investment by the European Union in the development of blockchain-based infrastructure for the public sector, with the potential to transform the way that governments, businesses, and citizens interact and exchange information.

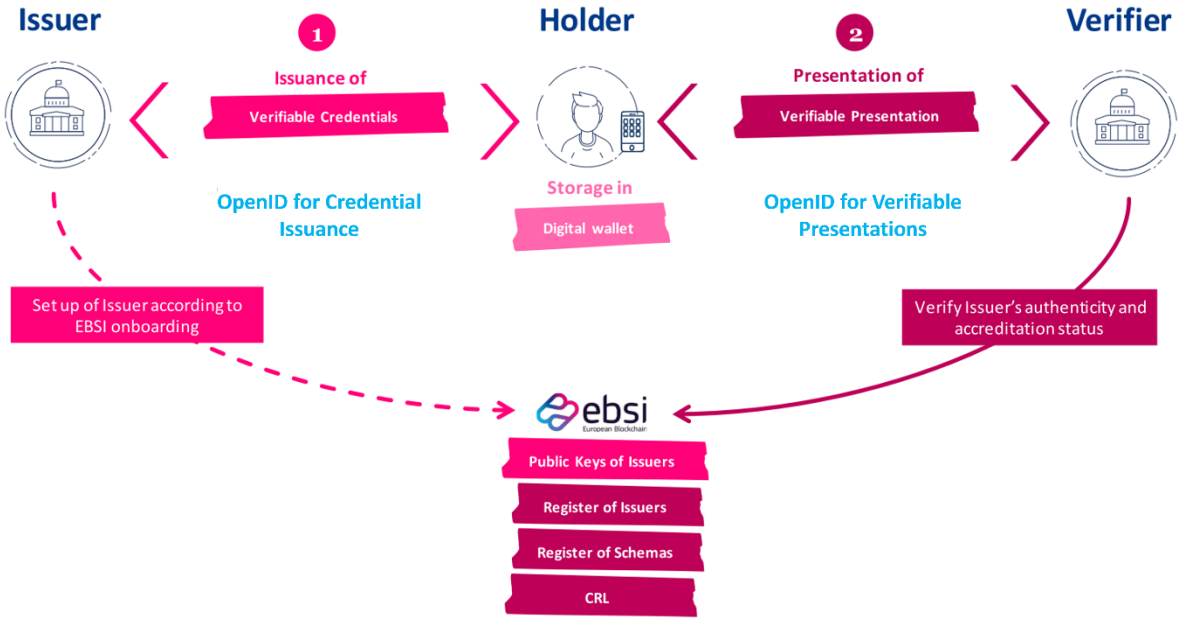

Figure 28: Example of interaction EU aims with EBSI program.[66]

The EBSI program has several real-life goals that it aims to achieve. These include:

66 *https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Playbook*

1. Enhancing Efficiency: The program aims to increase the efficiency of public services by leveraging blockchain technology. By utilizing decentralized and transparent systems, processes can be streamlined, reducing administrative burdens and improving service delivery.
2. Strengthening Trust and Security: Blockchain technology provides enhanced security and trust in data exchanges. The EBSI program seeks to leverage these features to ensure the integrity of public services and foster trust between governments, businesses, and citizens.
3. Promoting Interoperability: The EBSI program intends to establish a standardized framework for blockchain-based applications and services, enabling seamless interoperability between different systems and stakeholders. This interoperability will facilitate cross-border collaboration and the exchange of information.
4. Facilitating Cross-Border Services: By utilizing blockchain technology, the EBSI program aims to enable the efficient provision of cross-border services within the European Union. This includes areas such as electronic identification, procurement, and document management, making it easier for businesses and citizens to interact and engage in cross-border activities.
5. Fostering Innovation: The EBSI program encourages the development of innovative blockchain-based solutions by providing a platform and infrastructure for experimentation and collaboration. It aims to stimulate the creation of new services and applications that can benefit public administrations, businesses, and citizens.
6. Cost Reduction: By streamlining processes, reducing administrative burdens, and improving efficiency, the EBSI program seeks to contribute to cost savings for public administrations. This can free up resources that can be allocated to other important areas and investments.

7 Conclusion

The advent of smart cities has brought forth numerous advancements and opportunities for urban development. With the integration of technology and data-driven solutions, smart cities aim to enhance the quality of life for residents and optimize resource management. However, the widespread implementation of these intelligent systems raises significant concerns regarding security and privacy. As we conclude our exploration of this subject, let us reflect on the key findings and outline the future directions for ensuring robust security and privacy in smart cities.

Throughout our analysis, we have identified several critical challenges that smart cities face in terms of security and privacy. These challenges include vulnerabilities in interconnected systems, data breaches, surveillance concerns, and the potential misuse of personal information. The implications of these issues can be far-reaching, eroding public trust and hindering the adoption of smart city technologies. Therefore, it is crucial to address these concerns proactively and develop comprehensive strategies to safeguard security and privacy.

To tackle these challenges, collaboration between various stakeholders is paramount. Governments, city planners, technology developers, and citizens must work together to establish robust frameworks and regulations that prioritize security and privacy in smart city initiatives. This collaborative effort should involve conducting thorough risk assessments, implementing strong data protection measures, and promoting transparency and accountability.

One promising avenue for enhancing security and privacy in smart cities lies in the adoption of cutting-edge technologies such as AI and blockchain. AI can be leveraged to detect and respond to security threats in real-time, while blockchain technology offers decentralized and tamper-proof data storage, ensuring the integrity and confidentiality of sensitive information. These technologies, when integrated thoughtfully, can significantly bolster the security and privacy of smart city infrastructure.

Furthermore, the education and awareness of citizens are vital components of a secure and privacy-conscious smart city. By providing comprehensive information on the benefits, risks, and measures taken to protect privacy, residents can make informed decisions about their engagement with smart city technologies. Engaging the public through educational campaigns and involving them in the decision-making processes will foster trust and encourage active participation in building secure and privacy-respecting smart cities.

Looking ahead, future research and development should focus on addressing emerging security and privacy challenges associated with the evolution of smart cities. As new technologies and applications emerge, there is a need for continuous assessment and improvement of security protocols. This includes exploring innovative encryption techniques, enhancing authentication mechanisms, and ensuring secure interoperability among various systems and devices.

Additionally, as smart cities become more interconnected, cross-city collaborations can play a pivotal role in sharing best practices, exchanging knowledge, and collectively addressing security and privacy concerns. Establishing global standards and frameworks will foster consistency and cooperation, enabling cities to learn from each other's experiences and collectively build resilient and secure smart city ecosystems.

In conclusion, the realization of smart cities presents immense potential for urban development. However, ensuring robust security and privacy in this context is of paramount importance. By embracing collaboration, leveraging cutting-edge technologies, fostering citizen engagement, and embracing continuous research and development, we can forge a path toward secure and privacy-respecting smart cities. Through these efforts, we can create a future where innovation and protection go hand in hand, enabling smart cities to thrive while safeguarding the fundamental rights and well-being of their inhabitants.

References

1. https://miro.medium.com/v2/resize:fit:1100/format:webp/1*hqsFMZmfnVMdO-B_dtOoYg.jpeg
2. MarketsandMarkets (2020). https://marketsandmarkets.com/Market-Reports/iot-market-199913624.html
3. https://h9e3r9w2.rocketcdn.me/wp/wp-content/uploads/2022/05/Global-IoT-Market-Forecast-in-billion-connected-IoT-devices-min.png
4. Statista (2021). https://statista.com/statistics/471264/iot-number-of-connected-devices-worldwide
5. Navigant Research (2018). https://navigantresearch.com/news-and-views/global-smart-city-market-to-reach-717-billion-by-2023
6. https://hlp.city/wp-content/uploads/2022/01/smart-city-hero-image-5.gif
7. Maksimovic, M. (2018). https://smartcityhub.com/sustainability/smart-city-barcelona-blueprint-sustainable-urban-living
8. Karan, S. (2019). https://cities-today.com/amsterdams-smart-city-a-model-of-innovation-for-urban-transformation
9. Lim, D. (2017). https://mckinsey.com/business-functions/digital-mckinsey/our-insights/singapores-smart-nation-initiative-a-conversation-with-jacqueline-poh
10. Ganti, R. K., Ye, F., & Lei, H. (2016). https://ieeexplore.ieee.org/abstract/document/7507485
11. Yigitcanlar, T., Kamruzzaman, M., Buys, L. (2018). https://emerald.com/insight/content/doi/10.1108/JET-12-2018-0044/full/html
12. Zhang, Z., Zhou, J., & Li, Y. (2018). https://sciencedirect.com/science/article/pii/S2624630118300025
13. https://grandviewresearch.com/static/img/research/us-smart-cities-market.webp
14. Carpineti, M. (2018). https://ieeexplore.ieee.org/abstract/document/8327449
15. Yang, S., Chen, Y., Huang, X., & Wang, Z. (2017). https://ieeexplore.ieee.org/abstract/document/8062718
16. Sivakumar, A., Kumar, R., & Nagarajan, R. (2020). https://sciencedirect.com/science/article/pii/S2210670720305537
17. Hassani, A., Silva, E. S., & Sadiq, R. (2021). https://sciencedirect.com/science/article/pii/S2210670721002341
18. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). https://ieeexplore.ieee.org/abstract/document/6875775
19. Yigitcanlar, T.,Kamruzzaman, M., Buys, L. (2018). https://emerald.com/insight/content/doi/10.1108/JET-12-2018-0044/full/html

20. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. (2013). https://sciencedirect.com/science/article/pii/S0167739X13000219
21. Awad, A. I., Furnell, S., Hassan, A. M., & Tryfonas, T. (2019). https://doi.org/10.1016/j.adhoc.2019.02.007
22. https://mdpi.com/sensors/sensors-20-01754/article_deploy/html/images/sensors-20-01754-g001.png
23. Equifax data breach: https://nytimes.com/2017/09/07/business/equifax-cyberattack.html
24. Premom data breach: https://techcrunch.com/2020/07/20/premom-data-leak/
25. Capital One data breach: https://nytimes.com/2019/07/29/business/capital-one-data-breach.html
26. AccuWeather tracking: https://zdnet.com/article/accuweather-caught-sending-geo-location-data-even-when-users-opt-out/
27. https://i.guim.co.uk/img/media/ae4001f9311f4912db843f79ee2510db6d9419e0/0_180_1472_883/master/1472.png?width=620&quality=45&dpr=2&s=none
28. Alexa: https://independent.co.uk/tech/amazon-alexa-echo-listening-spy-security-a8865056.html
29. Jeep Cherokee: https://wired.com/2015/07/hackers-remotely-kill-jeep-highway/
30. Tesla Model S: https://wired.com/story/tesla-model-s-hack-china/
31. Nissan Leaf: https://wired.com/2016/02/hackers-can-disable-nissan-leafs-brakes-media-systems-over-the-internet/
32. BMW: https://theverge.com/2018/2/13/17009998/bmw-connecteddrive-hack-remote-unlock-car
33. https://securityguill.com/images/infographics/mirai_works_leplat.jpg
34. Strava tracking: https://theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases
35. ENISA: https://www.enisa.europa.eu/topics/incident-response/glossary/botnets
36. Emmanuel C. Ogu, Olusegun Ojesanmi, Oludele Awodele, Shade Kuyoro (2019). https://mdpi.com/2078-2489/10/11/337/htm
37. https://securityguill.com/images/infographics/mirai_works_leplat.jpg
38. https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/
39. https://www.bleepingcomputer.com/news/security/hajime-botnet-makes-a-comeback-with-massive-scan-for-mikrotik-routers/
40. https://techcommunity.microsoft.com/t5/image/serverpage/image-id/331521i15616D9F6DA17EE6/
41. https://wsperanzainc.com/wp-content/uploads/2021/12/%E5%9C%96%E7%89%87-2-4-466x400.png

42. IoT SECURITY GUIDELINES (2020). https://gsma.com/iot/wp-content/uploads/2020/05/CLP.11-v2.2-GSMA-IoT-Security-Guidelines-Overview-Document.pdf
43. https://www.mdpi.com/sensors/sensors-20-05897/article_deploy/html/images/sensors-20-05897-g001-550.jpg
44. https://www.itsecurityguru.org/2019/07/31/91-of-the-uk-would-like-better-privacy-laws-for-iot-devices-to-prevent-data-misuse/
45. https://www.itsecurityguru.org/wp-content/uploads/2019/08/Iot.jpg
46. https://insightaas.com/new-research-privacy-and-security-in-the-internet-of-things-era-iotcc-best-practices-guidance/
47. https://insightaas.com/wp-content/uploads/2018/07/IoT-privacy-and-security-requirements.jpg
48. Gaps in NIS Standardization: https://enisa.europa.eu/publications/gaps-eu-standardisation/@@download/fullReport
49. Gaps in NIS Standardization: https://enisa.europa.eu/publications/gaps-eu-standardisation/@@download/fullReport
50. Gaps in NIS Standardization: https://enisa.europa.eu/publications/gaps-eu-standardisation/@@download/fullReport
51. https://eu-images.contentstack.com/v3/assets/blt66983808af36a8ef/blt85100d6c13369fe0/60d950c6e1461d39eb854b57/secure-sldc-diagram-green-center.png
52. https://iosentrix.com/blog/assets/images/secure-sdlc-stages.png
53. https://www.nexor.com/wp/wp-content/uploads/2019/06/Nis-Objectives-and-Directive.png
54. https://e.itgovernance.co.uk/l/500371/2018-05-11/b7hxw/500371/91266/NIS_Regulations_compliance_framework.pdf
55. https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_FINAL_Updated_V1.1.pdf
56. https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/ssca/2017-winter/TueAM2_2_CMMI.pdf
57. https://researchgate.net/publication/224230457/figure/fig5/AS:302815932108805@1449208353001/Generic-secure-boot-architecture.png
58. https://upload.wikimedia.org/wikipedia/commons/thumb/b/be/TPM.svg/1200px-TPM.svg.png
59. https://www.rambus.com/wp-content/uploads/2017/12/Smart-City-Threats-and-Countermeasures-1024x576.png
60. https://www.hindawi.com/journals/scn/2022/5186376/fig1/

61. Chouhan, A., Gogate, M., & Thampi, S. M. (2020). Intelligent Framework for Smart City Security: Issues, Challenges, and Mitigation. In Cybersecurity for Smart Cities (pp. 45-65). Springer
62. Berman, M., & Lawton, G. (2018). Smart policing: Machine learning and predictive analytics for law enforcement. John Wiley & Sons.
63. Yang, S., Ma, M., Zhang, Y., & Shen, X. (2020). Critical Infrastructure Protection in Smart Cities: A Machine Learning Approach. IEEE Internet of Things Journal, 7(6), 4853-4862
64. Smeureanu, I., & Fratu, O. (2019). Machine learning algorithms for video surveillance systems. In 2019 13th International Symposium on Advanced Topics in Electrical Engineering (ATEE) (pp. 1-6). IEEE
65. https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Playbook