UNIVERSITY OF PIRAEUS

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
DEPARTMENT OF DIGITAL SYSTEMS

Postgraduate Program of Studies
MSc DIGITAL SYSTEMS SECURITY

MASTER THESIS

Industrial Internet of Things attack vectors, challenges, and mitigations for the realization of Industry 4.0. Case Study: A proposed framework for cybersecurity in IoT using SSI in wind turbines

Submitted by:
Dimitrios A. Maniatis

Master’s Supervisor: Xenakis Christos, Associate Professor at University of Piraeus, Department of Digital Systems

University of Piraeus, Athens, Greece

November 2022

Dimitrios A. Maniatis - A.M.: MTE2019

Abstract

Industry4.0 and the IoT are the 4th Industrial Revolution (IIoT) which brings about changes in the way the economy works, opens new avenues for research and creates new employment opportunities in all scientific fields. IIoT is essential also to the Energy Systems. Various types of sensors and other types of technological equipment are used in energy systems. As a result, large volumes of data are generated which are transferred to a server for processing.

The big challenge in this process is privacy and security when transferring data. In this regard, cybersecurity systems are very important to ensure the encryption of this data. An effective way to integrate verifiable credentials into data workflows is to build and deploy self-sovereign identity (SSI) solutions.

Towards this direction, in the case study of the present work, we present a cybersecure framework which combines SSI for marine wind turbines that can be used in the Greek seas. For our system we suggest many sensors that will collect data and will be connected to an intelligent system that will decide according to the situations. To best of our knowledge this is the first study under this perspective, and we estimate that the proposed framework could potentially be used for the security of data generated by sensors above offshore wind turbines.

Table of Contents

1. Introduction

1.1. Industry 4.0: Strategies and Contents

The idea behind Industrial 4.0 first appeared in an article published by the German government in November 2011. It was intended to be used in the future as a high-tech strategy. The fourth stage of industrialization, ie after mechanization, electrification and information, was named "Industry 4.0". A little later and more specifically in April 2013, the term "Industry 4.0" reappeared at an industrial exhibition in Hannover, Germany and became the country's national strategy. In recent years, "Industry 4.0" has been widely discussed and has become a hotspot for both industries (global and information). Industry 4.0 is a new industrial revolution, which has a great influence on the international industry. Also, as China's manufacturing is in a state of industrial transformation and upgrading, Industry 4.0 offers China even more opportunities and challenges.

Germany is one of the most competitive, global manufacturing industries. For this reason, it is considered a world leader in the field of equipment manufacturing, in many fields. Some examples are BMW, Porsche and Volkswagen in the automotive industry, the sports brand Adidas, the electrical and electronics company Siemens, etc. In response to the European debt crisis, the German government has presented a specialized strategy for Industry 4.0. It did so in order to consolidate and further promote the global influence of German manufacturing. Industry 4.0 is considered to be the fourth industry to emerge from an industrial revolution and lead smart construction. The idea of Industry 4.0 is based on the integration of information and communication technologies, as well as industrial technology. It mainly depends on the creation of a Cyber Physical System (CPS), which aims to implement a digital and intelligent factory. Through this construction, the production can be further upgraded and eventually, become even more digitalized (e.g. led information).

Therefore, the purpose of Industry 4.0 is to create an extremely flexible production model, which in addition to digital services, concerns personalized and digital products. These products have the ability (during the production process) to interact in real time between people, products and devices. For example, a factory that accepts consumer orders and produces and ships the required product directly, distributes separate sales and marketing channels. Thus, according to the authors (Wan et al., 2015), Industry 4.0 not only affects German industry, or even international industrial development, but may be a driving force. Through this, the traditional methods of industrial production will be changed and will lead to future constructions. This practically means that in the future, industrial production systems will become even smarter through the use of digital systems. In the meantime, there will be more so-called ‘knowledge-based factories’ and ‘thinking-type factories’, which will significantly improve efficiency and competitiveness in factories. More specifically, the German electrical industry association has predicted that Industry 4.0 will increase industrial productivity by 30%.

The motivation of our work follows the emerging field 4th Industrial Revolution (IIoT) which offers a framework for improving productivity and efficiency along with lower operating costs in industry. It also improves safety in work environments; however, cybersecurity is a crucial challenge here since we deal with numerous IoT devices. We present a cybersecure framework which uses the function SSI and to the best of our knowledge this is the first study under the perspective of marine wind turbines that can be used in the Greek seas. This framework offers high security of data generated by sensors above offshore wind turbines while it can be adjusted to solve other similar IIoT real-world problems. Finally, through the backend of the application it is possible to manage the data in an efficient and easy-to-use way.

During the first three industrial revolutions, people witnessed and created mechanical, electrical and information technologies. These technologies aimed to improve productivity in industrial processes. More specifically, the first industrial revolution improved efficiency through the use of hydroelectric power, increased use of steam, and the development of machine tools. Subsequently, the second industrial revolution brought electricity and mass production, while the third industrial revolution further accelerated automation, using electronics in conjunction with information technology. Finally, the fourth industrial revolution is driven by CPS technology, aiming to integrate the real world with the information age. Through this union, a future and industrial development can take place.

1.2.Industrial applications of the Internet of Things in Industry 4.0

According to the research of the author (Kurzweil, 2004), the growing need to increase production, efficiency and quality in industrial products, was the defining factor that led people to jointly develop new technologies. Thus, they were able to keep up with the exponential evolution of technology, in production processes. The First Industrial Revolution occurred during the eighteenth and nineteenth centuries and mechanized the production of energy (water and steam). Then, in the twentieth century, the Second Industrial Revolution introduced electricity into factories, combined with mass production. The Third Industrial Revolution was marked by the advent of Computer Numerical Control (CNC) machines, robots, industrial and electronic automation and information technology. The Fourth Industrial Revolution, also known as Industry 4.0, began in the last century and as mentioned in the previous subsection, began in Germany. Its purpose is the effective automation of production systems. In particular, the increasing presence of the Internet (in all key areas), has allowed the emergence of the Internet of things and services. These are capable of networking information, objects, people, and resources. For example, in the areas of energy supply, Smart Grids have emerged. Respectively, in the field of health, some specialized solutions emerged that led to the so-called ‘Smart Health’.

In addition and in terms of its development, Industry 4.0 is utilized through the following, key features: horizontal integration through value networks, converging information technology systems (at different stages of a production) and business planning processes. The latter include data exchange both within a company and between multiple companies. But in addition to the aforementioned features, Industry 4.0 stands out for the digital integration of its engineering (across the value chain) and for the convergent systems used in information technology. These systems are available at different hierarchical levels and are able to provide a complete solution. Therefore, all of the previously stated features, enhance the so-called ‘Smart Factory’ by integrating physical and digital worlds. This is achievable by creating smart products and processes. According to the authors (Carvalho et al., 2018), these products and processes are capable of transforming conventional value chains, ultimately shaping Cyber-Physical Systems.

As a result, merging the Internet of Things and services with Cyber Physical Systems, could clearly affect industrial processes. This condition is usually caused by IT-OT convergence and because of this, it becomes more difficult to process an architectural reference model. This model is used to provide technical descriptions and standards, aiming at the integration and application of these technologies. Finally, a common topic of discussion is how both the CPS proposal and other emerging technologies can be developed in the Industry 4.0 environment. Through this potential development, interoperability between different companies and industry segments can be achieved.

1.2.1. Industry 4.0 and IIoT

Industry 4.0 was approved in 2011 as part of the High-Tech Strategy 2020 Action Plan. This was a strategic initiative of the German government, which was developed with the aim of revolutionizing the production process. Theoretically, this could be achieved by assembling a set of pillars, thus allowing the fusion of the physical, digital, human and biological worlds. In this way, new technologies of the industrial environment could be enhanced (see Fig. 1). Among these pillars, the introduction of the Internet of Things and services, was seen as the main reason for the emergence of the fourth industrial revolution.

Moreover, IIoT contributes to the industrial scenario through its different concepts and technologies. In this way, it can develop a network of industrial devices, which usually consists of sensors and complex industrial robots. Apart from that, several actuators which are connected to communication technologies, are used as well. These technologies make it possible to track, analyze, deliver, collect and change data quickly and easily. Consequently, the combination of IIoT with Industry 4.0, can create many benefits for industrial environments.

One of these benefits, is the convergence of Business Information Technology (IT-OT). More specifically and according to this method, the IT and OT sectors converge, thus, integrating production control systems and data storage, computers and communication. However, although OTs include hardware and software systems for process control, they are often not integrated into a network or a larger electronic system. Nowadays, IT-OT convergence allows OT components to communicate directly with other machines as well as with central servers. This way, they can exchange information through an IT network.

In addition, there may also be a reduction in the amount of work required, better performance and use of assets, minimization of cyclical costs, faster decision making and the ability to buy and sell products as services. Thus, business opportunities and new business models can expand and emerge respectively.

Finally, despite the many advantages offered through the IIoT-Industry 4.0 combination, there are some disadvantages as well. Two of these, are the complexity of the system and the large volume of digitization and networking of the companies involved. The second, tends to increase the number of architectures and as a result, problems arise related to communications networking and systems interoperability.

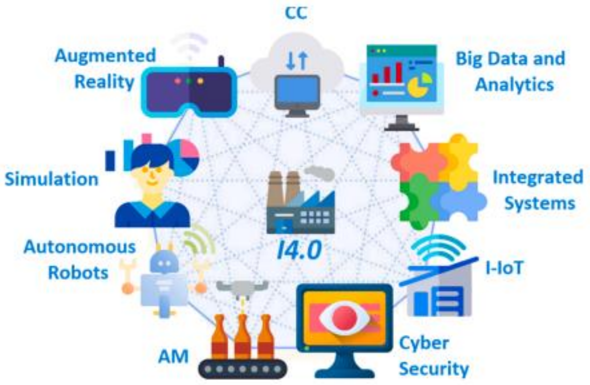


Figure 1: The pillars of industry 4.0. (Pivoto et al., 2021).

1.3.Cyber-Physical Systems

Cyber-Physical Systems (CPS) were proposed by American scientist Hellen Gil in 2006, as one of the leading technologies in Industry 4.0 (Lee, 2006). In addition to dealing with various concepts in the IIoT, CPSs are responsible for the connection between virtual spaces and physical reality. This connection is achieved through the integration of networking, computers and data storage. In this way, an interactive industrial environment is created, which in turn creates Smart Factories.

In addition, CPSs are automated and distributed systems that integrate physical reality with communication networks and computing infrastructures. According to the author's study (Lee, 2008) and in contrast to traditional embedded systems, the main focus of these systems is on the networking of various devices (for Industry 4.0). In particular, a

CPS system consists of a control unit, which is capable of handling sensors and actuators. These devices have the ability to interact with the physical world, process the received data and exchange them with other systems or Cloud services (via a communication interface). In other words, CPSs can be thought of as systems that are capable of sending and receiving data from devices over a network.

An important feature of a CPS, is its ability to obtain information and services in real time. These can be obtained from the construction machines via the Internet, regardless of their location. But in addition to real-time communication, it is essential to ensure the stability, reliability, efficiency and security of the system. For this reason, one of the main goals of Industry 4.0 is to provide (high level) security support at all levels of a CPS architecture. Thus, it can protect confidential information while providing data anonymity.

More specifically, CPSs are applied in many different areas. Some of them are: Manufacturing, Health, Renewable Energy, Smart Building, Transport, Agriculture areas and Computers' Network. Initially, in the field of Manufacturing, a CPS system is used for automatic monitoring, production control and real-time information exchange. In the field of Health, this system can also be used in real time, for the remote monitoring of patients (controlling their physical condition). Also, in the field of Renewable Energy Sources, the sensors allow the monitoring and control of the network. In this way, they ensure reliability and efficiency in energy consumption.

On the other hand, in the field of Smart Building, the interaction between a CPS and smart devices, can reduce energy consumption and at the same time, provide an increase in protection, security and comfort for the residents (of each corresponding area). In the field of transport, this technology allows communication between vehicles and infrastructure, sharing information such as traffic volume, congestion location and accidents. Thus, it can help prevent further accidents or traffic jams. In the field of Agriculture, the user can collect information about both the weather and several resources (e.g. irrigation and humidity data). Therefore, accuracy in systems related to agricultural management, can keep increasing at ease. In conclusion, in Computer Networks, this concept is applied for the better understanding of the systems but also, for the behaviors of the users in virtual environments.

1.4.Parts of a cyberphysical system

Data exchange is the most important feature of a cyberphysical system, due to the need to transmit and evaluate data from its various subsystems. In other words, a cyberphysical system is an embedded system that can send and receive data over a network. More specifically, the parts of a cyberphysical system will either function as data collection or signal control, resulting in their categorization into two main categories, the Sensing Components and the Controlling Components respectively.

Sensing Components consist of sensors, which collect data and transmit it to the aggregators, which in turn forward the information to the actuators to perform the appropriate physical processes. These parts of the system occur primarily on the physical level. Below are the main parts regarding Sensing Components.

- **Sensors**: Collect real-time system-environment data and record it. In addition, some kind of data calibration can be performed to assess their accuracy (Loukas, 2015). Data collection is important for the system because based on this data decisions will be made about what to do next.
- **Aggregators**: Their function is to collect and process the information received from the sensors before the decision-making stage. They are usually found at the communication layer (transmission layer) and examples are routers, switches and gateways.
- **Actuators**: Their function is to receive electrical signals as input and to produce mechanical movements as output. They are components useful for the interaction between cyberspace and the physical world by exchanging information. They are found at the application layer and the example is the hydraulic cylinder, the electric motor, etc.

On the other hand, Controlling Components are used to control the signals and through the monitoring and management of the signals, a higher degree of accuracy is sought, but also protection against possible errors and malicious attacks. As a result, the resilience of PLCs, DLCs and their subsystems, which are analyzed below, has proven to be particularly important for the smooth operation of the cyberphysical system. Below are the main parts regarding Computing Components.

- **Programmable Logic Controller (PLC)**: They are considered as industrial digital computers that control industrial processes. An example of their operation is the processing of system error diagnostic results in order to achieve better durability and adaptation to change.
- **Distributed Control Systems (DCS)**: These are control systems that allow the distribution of autonomous system controllers using a central supervisory controller. Remote monitoring and system monitoring process achieve on the one hand increased reliability and on the other lower installation costs.
- **Remote Terminal Units (RTU)**: These are electronic devices that are controlled by microprocessors. They are more suitable for wireless communication in extensive geographical areas where telemetry is used. They link physical objects to a SCADA system using a supervisory messaging system that controls these objects via telemetry data transmission (Jazdi, 2014; Yaacoub et al., 2020).

1.5.Areas of application of cyberphysical systems

The term cyberphysical system is a superlative for systems of various fields and functions such as machine automation, industrial cyberphysics systems (ICS), control and data acquisition systems (SCADA), but also the Internet of Things (IoT). The areas in which cyberphysical systems are used can be not only of industrial but also personal use. The first ones are in abundance in the industrial sector with special emphasis on their physical part and the cyberspace to operate for control of the machines and ease of access. On the other hand the cyberphysical systems that are used for personal purposes aim at the automation of functions with emphasis on cyberspace while the physical part is used to improve the usefulness of the respective information systems used (Lozano et al., 2020).

Below are the areas in which cyberphysical systems are used or can be used.

- In energy management systems aiming at their most efficient operation through the adapted and optimal production, distribution and consumption of energy, also known as smart grid. In addition, as the electricity network is a key sector of each country, with huge economic and social consequences in case of inability to operate, the use of cyberphysical systems protect it from possible attacks and errors.

- In the automotive industry with the aim of operating autonomous car driving systems, but also optimizing their construction. In addition, a similar area of use of cyberphysical systems is the aviation industry and in particular the operation of unmanned vessels.
- Cyberphysical systems play an important role in the health sector by developing real-time patient monitoring and control sensors, telemedicine systems for the remote use of machines, medical devices and highly trusted systems. An example is Therac-25 which aims to provide an appropriate dose of radiation to patients (Wolf & Serpanos, 2020).
- In the field of agriculture in order to find suitable places for cultivation and monitoring of the crop. In addition, they can play an important role in increasing production through the use of technologies aimed at smart water management, and the selection of more efficient cultivation methods. The maximum possible result can be achieved by continuous monitoring of the crop environment and crop yield. A specific example is the cyberphysical system which provided the infrastructure for monitoring and managing rodents in crops by reducing the damaged quantities of crops and the cost of managing rodents.
- Cyberphysical systems can be used to monitor the environment (forests, rivers, mountains). The use of multiple sensors provides useful environmental information to the cyberphysical system which, based on the measurements, can identify natural disasters and activate appropriate mechanisms to limit and avoid the effects. These systems are preferred due to their operation without human intervention and low consumption, which allows them to operate for long periods of time.
- In transportation systems, real-time information sharing clearly improves motorway safety and reduces traffic congestion. With the use of advanced technologies with sensors, control mechanisms and their interconnection through a communication network, autonomous movement is optimized by reducing accidents in the transmission network.
- In the control of industrial systems processes, aiming at the autonomous management of production processes. Cyberphysical systems have the ability to provide extensive controls on large and complex industrial operations through the

cooperation of sensors, the communication network and actuators. This results in the smooth and orderly operation of the processes, but also the implementation of efficient production lines that allow the mass personalization of products in real time.

- In the implementation of smart homes which are integrated with a number of sensors to measure physical properties in order to create a more comfortable environment and reduce the required actions by users.

1.6.Industrial Automation Items

Although cyber-physical systems and the Internet of Things are equally concerned with the collection and analysis of information for the implementation of applications and services through physical objects and components, CPSs do not require the interconnection of physical components with specified addresses (Stojmenovic, 2014). In particular, the first generation of cyberphysics systems includes identification technologies, such as RFID tags, while data storage and analysis must be provided through a central service. With the second generation CPS, the systems are equipped with sensors and actuators with a limited range of functions. But the new generation of cyber-physical systems is coming to take advantage of the modern benefits of IoT by integrating CPS into the IoT-based industrial environment, which can offer “critical solutions for systems organization, programming and control” production at all levels ”(Bi et al., 2014).

CPSs control and monitor the physical infrastructure of the real world and thus, they have a gradually growing influence in the field of industrial automation. In order to effectively integrate the physical entities of the production systems with the corresponding digital entities that monitor and control the results of the former, interfaces that serve as a communication network or other intermediate elements are required. The modern production unit can be considered as a "synthesis of cyber-physical, digital and human components that uses IoT technologies as" glue "to integrate the components in terms of their cyber interfaces" (Foradis & Thramboulidis 2017). Sensing and actuation are considered useful services and in this sense, the industrial Internet is a form of IoT (Thramboulidis & Christoulakis, 2016).

Based on this vision, the "physical" part of an industrial unit is not a purely mechanical part, but is considered a mechatronic component. This is "the lowest level in the system composition hierarchy that tightly integrates the mechanical components with the electronics and software needed to transform the mechanical part into a 'smart' object that offers well-defined services in its environment." In order to integrate this cyber-physical component (CPC) with the digital component and leverage the IoT communication infrastructure, the CPC adopts a new IoT-compatible interface (IoT-compiant) to become an Industrial Automation Object (Industrial) Automation Thing, or IAT). The IoT-compiant cyber-physical components, ie IAT, can act as service providers by offering the unit functions as services. The composition of the services provides the productive processes of the industrial installation and is coordinated by the computational elements that manage the functionality of the installation. Following the solutions offered by IoT technologies, the correlation and integration of the installation processes with the offered services is achieved.

2. Background Material - Cyber-Physical Production Systems Architecture

To design the application for finding and synthesizing services of an IoT-compatible CPS, it is necessary to define the basic structural and computing components of the system as well as how the components are distributed and interacted.

2.1.The High Level Model of Cyber-Physical Production Systems

For years, production systems have been modeled on a standard five-level architectural model, the hierarchical structure of which is most commonly represented by a pyramid. As shown in the following figure, the lower level of the pyramid (field level) captures the sensors that send information to control units, and the actuators that receive pulses from the control units to perform tasks (eg to open a valve). In the second layer of the pyramid (control level), the composite parts of the system are divided into smaller manageable control units which are controlled independently, e.g. from PLCs. Supervisory control and Data Acquisition software, or SCADA (Supervisory control and Data Acquisition), refers to the level of process management in the third layer (supervisory level), which undertakes the centralized management of monitoring, data and control systems for easy monitoring and adjustment of systems from remote endpoints (eg SCADA monitors industrial networks, visualizes data from control units by creating easy-to-use and easy-to-read representations and verifies the smooth operation and integrity of systems). In the fourth layer, the Manufacturing Execution System, or MES, is used to perform complex tasks related to production processes, such as, for example, production planning. Finally, the fifth and highest layer refers to the level of enterprise resource management or ERP that undertakes business activities, such as inventory management. Multilevel architectures have many advantages, but they also place significant costs in terms of performance. In contrast, newer technologies, such as the Cloud and IoT, offer alternatives to replacing the conventional five-level architecture with a more efficient and modernized architecture.

Numerous studies have been conducted to design a model that will take full advantage of modern Cloud and Internet of Things technologies, e.g. (Harrison et al., 2016). A popular candidate approach for replacing the existing conventional model is also illustrated in the following figure. In the second figure, the input-output devices, service interactions, and distributed system functions are presented as squares, lines, and circles, respectively. Based on this model, the sensors send the data they collect directly to the Cloud and the services (eg the programming of the production processes) are automatically and in real time recorded in the data necessary for their execution.

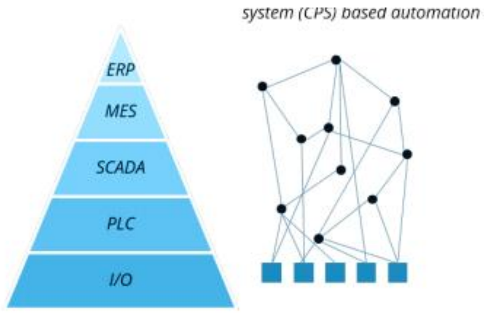


Figure 2: Hierarchical structure of the production automation system: The modern five-level conventional architecture and the future distributed CPS model (Lueth, 2015).

The systems adopting the CPS model in the above Figure collect primary data from the sensors and process it directly in the Cloud (Giang et al., 2015). Instead, the mechanism of publication, sorting and synthesis of services for the regulation of production processes was designed and implemented, with the aim of integrating it into systems based on a different architectural model. This architectural model takes advantage primarily of the features of Fog and Edge computing, and secondarily Cloud computing, ensuring that the processing of raw data takes place initially within the Industrial Automation Objects and local network level.

For this purpose, the CPS architecture depicted in the following figure was adopted. Based on this model, the sensors and actuators are part of the Cyber-Physical Element of the CPS. In this way, the data from the sensors is not immediately transferred to the Cloud, but the engineer determines the properties of the element to be exported through an IoT-compatible interface, along with the degree to which the raw data must be analyzed and filtered before being promoted to the Cloud. The adopted architecture has been selected for the implementations described in (Thramboulidis et al., 2018). Also, the same approach is followed in the MIM (Model Integrated Mechatronics) model for the development of the model of mechatronic production systems [88], which was later expanded to utilize the technologies of the Internet of Things and microservices.

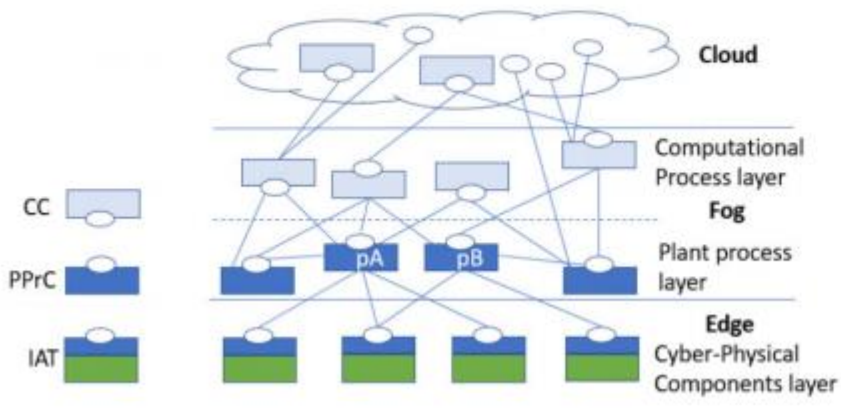


Figure 3: The distributed CPS architectural model based on Fog and Edge computing (Thramboulidis et al., 2017).

In particular, the lowest level of architecture records the Cyber-Physical Components layer, or CPCs which convert the physical units of the Cyber-Physical System into IATS. The components of the Cyber-Physical System include the sensors, actuators and control and coordination logic required by the physical part of the CPC and provide services at the following level. The CPC level corresponds to the I/O and PLC layers of the traditional pyramid of automation systems

The following Fog layer acts as a private cloud and splits into two successive sub-levels - the Production Unit Process level, or PP level and the Computational Process level, or CP level. At the PP level, production unit processes, or PPrCs (Plant Process Components), are developed and operate. The processes performed in a production unit consist of individual functions of the unit provided as services by the CPC level components. The regulation and execution of procedures at the PP level requires a clear definition of the necessary functions and activities based on the model of the production process and then the finding, sorting and synthesis of services that can perform these functions and provided by the unit IATs at CPC level, ultimately shaping the production process. At the same time, at the CP level the computing components offer computing services to the unit processes, e.g. the process generator service. The overall Fog level corresponds mainly to the SCADA layer of the traditional automation pyramid. The third and highest level of the described architecture is the Cloud layer, which shares the MES and ERP functions with the Fog level.

The above architectural model for the Cyber-Physical Production System was considered the most suitable for the implementation, as it enhances the overall performance and the advantages of the system both in relation to the conventional five-level architecture and the most modern models Dominant-based in Cloud Computing. Processing a significant amount of data locally, rather than requiring a time-consuming transmission to the Cloud, enhances the system response and prevents unnecessary network delays and increased network failure that could be caused by a Cloud-based central proxy (Thramboulidis et al., 2017). As a result, the successful and faster publication, search, commitment and interaction of the devices and their services is ensured, while at the same time, the timely and valid information on their status, operation and availability is facilitated. The processing of data and the control of IATs in real time are necessary conditions for the smooth and efficient operation of an industrial automation system. In addition, the absence of a single, cloud-based proxy provides flexibility in controlling services and processes, which can be either centralized or distributed.

At the same time, based on the architectural model, the engineer can decide which CPC level information deserves to be promoted to the Fog and Cloud levels, thus reducing communication costs and storage needs and minimizing network overhead and data redundancy to higher levels. flat. This savings in resources, serves the use of devices with limited capabilities, reducing the required complexity, energy consumption and cost of their life cycle (Chiang & Zhang, 2016).

The adopted model was applied and adapted accordingly for the design of the systems of two different work scenarios. An important element in the implementation of the model is the communication protocol that organizes the way of interaction of the elements of all levels. The following subsection is dedicated to the CoAP protocol and the reasons why it was used to set the principles governing IATs communication at the application level.

3. Background Material - Security and Protection in cyberphysical systems

3.1. Need for Security and Protection

In the field of cyberphysical systems, their safe and protected operation is a basic prerequisite especially in key areas of a country (energy management, water system management, transport systems management, military, etc.) where the effects of errors and attacks are able to significantly affect both the daily life of the citizens, but also the economy. In the past, the use of cyberphysics systems was small and not targeted, and their security revolved around the possible failure of system devices or the lack of specification and implementation of the necessary system functions, which could lead to unmanageable results and consistency in errors. An example of an error is the crash of an Airbus400M after take-off due to incorrect installation of engine control software during final assembly which may have caused the propellers to rotate too slowly (Wolf & Serpanos, 2020).

Now the integration of cyberphysical systems in a number of sectors of the economy, from personal-domestic to industrial and critical infrastructure of a country, has attracted malicious for economic, military, espionage, political and terrorist reasons. Cyberphysical systems do not operate in a controlled environment, both in the physical world and in cyberspace, so they must manage the noise generated during their measurements and transmission, be able to operate under unexpected conditions and are adaptable to system failures (Rajkumar et al., 2010). In addition, the variability of the environment in which cyberphysical systems operate, but also the connection of new devices due to their scalability increase the chances of attack (Ashibani & Mahmoud, 2017).

For the above reasons, it is necessary to implement appropriate mechanisms that will check the safe operation of the system from accidental errors and will protect it from deliberate attacks, to ensure its integrity, availability and confidentiality throughout the operation of the system (Yaacoub et al., 2020). The safe operation and protection of cyberphysical systems is a demanding process, therefore the basic principles of safe design are used for their implementation, as well as protection mechanisms related to the software and the hardware of the system (Yaacoub et al., 2020). The following are the basic principles of safe design of cyberphysical systems and their protection mechanisms.

3.2.Principles of safe design

3.2.1. Economy of Mechanism

This principle states that the greater the number and complexity of the mechanisms used by a cyberphysical system, the more likely it is that some mechanisms will be set incorrectly resulting in the inability to perform the expected protection to the system. For this reason, it is proposed to design as concentrated and simple mechanisms as possible, but always with the primary goal of protecting the system (Loukas, 2015).

3.2.2. Least Privilege

Limiting the privilege of the system to what is absolutely necessary to perform a function by a program or a user. When performing a function, it will be accessible only to users and programs that are absolutely necessary and only for the period of time required until its completion (Fink et al., 2017; Loukas, 2015).

3.2.3. Separation of Privilege

Permission to perform a system operation based on a single condition must not be granted. Especially for performing critical operations or accessing critical information, there must be more than one approval control of the execution or access conditions (Loukas, 2015).

3.2.4. Minimization of Attack Surface

It aims to reduce the number of attacks that a CPS (attack surface) can receive by minimizing access points such as the number of users with administrator privileges or the number of networks that can communicate with the external system environment. , but with the aim of maintaining the necessary functionality. However, due to the increasing functionality of most cyberphysics systems, this principle is at odds with the needs for new capabilities demanded by users and industry (Loukas, 2015).

3.2.5. Isolation

As the sharing of system resources causes security problems, it is recommended to isolate the various subsystems of the cyberphysical system. More specifically, the data of each user, as well as the critical data and the functions to be isolated from the external environment and not accessible from it. Most cyberphysics systems due to the need for real-time communication or access to data do not implement complete isolation in their subsystems except in the most critical for achieving functionality and security (Loukas, 2015).

3.2.6. Open Design

It is argued that the design of a security system is more reliable when it becomes publicly available to be tested by a number of different people and organizations. In this way new vulnerabilities of the system are discovered and corrected and its security is generally checked more extensively (Loukas, 2015).

3.2.7. Segmentation

A physical or computational barrier is constructed for the elements of the cyberphysical system by segmenting them based on characteristics such as their function, their criticality, the communication between them, etc. In the event of uncontrolled access between components of different criticality, an attacker may be able to access elements of the lower criticality system to invade more critical ones. Elements that are critical to the operation of the system must be scattered, as well as elements that do not require frequent communication with each other, while elements that have a similar function must be concentrated in the same section (Loukas, 2015).

3.2.8. Defense-in-depth

It presupposes the creation of multiple levels of defense to protect the critical elements of the system so that even if an attacker manages to pass the first level of defense he will not be able to gain direct access to the elements as the next levels will at least slow down his access. and most will prevent the attack from reaching. An example is the splitting of the network of a cyberphysical system into separate subnet networks of the demilitarized zone type (DMZ) which are separated by firewalls. These subnets give access to the data they contain, only to the subnets that are directly connected, but direct communication between the other subnets is limited. In this way an attacker will have easier access to data located in the first subnets compared to the rest for which he will have to penetrate the remaining DMZ. However, the implementation of multiple levels of protection leads to an increase in the complexity of protection mechanisms, which is contrary to the principle of Economy of Mechanism (Fink et al., 2017; Loukas, 2015).

3.2.9. Defense-in-breadth

It presupposes the creation of a single level of defense which will consist of all the levels of defense of the cyberphysical system, which will cooperate with the result that they protect each other in attacks such as divide and conquer. This principle aims to protect a system from a possible failure or improper protection of a subsystem which can lead to continuous failures of the whole system. In addition, with the use of a cooperative level of defense even due to the scalability of cyberphysical systems in devices, the range of possible attacks is maintained at similar levels (Fink et al., 2017).

3.2.10. User-configurable data collection/logging

The collection of data, especially in cyberphysical personal use systems, contributes to a deeper understanding of the functions of the system, but also its more efficient use, while maintaining the privacy of users and confidentiality of the data they manage. The default data collection rule should make all user data private and then the users themselves should choose which data to share, as well as the system should inform users about which data they share (Fink et al., 2017).

3.2.11. Pattern obfuscation

Complicating the patterns of use of the functions of the cyberphysical system reduces the possibility of recognition by an attacker of system information and the possibility of imitating communication patterns in order to carry out a Replay attack type attack. In addition, through the complexity of the data, the result of the communication remains the same and the confidentiality between the system resources is maintained (Fink et al., 2017).

3.2.12. End-to-end security

It aims to maintain the security of data throughout its transmission from one CPS resource to another over the network and during storage. It is usually done through data encryption and the use of cryptographic information transmission protocols (Ashibani & Mahmoud, 2017; Fink et al., 2017).

3.2.13. Tamper detection/security

In order to prevent and identify unauthorized actions in a cyberphysical system, during the implementation of the system, the use of mechanisms resistant to violations and at a physical level is recommended, but also in cyberspace (Fink et al., 2017)

4. Background Material - Self-Sovereign Identity And Indistrial IoT

4.1.Self-sovereign Identity

Self-Sovereign Identity (SSI) enables a person to construct her own identity and have it verified by a trustworthy third party like the government. Even though SSI is not dependent on blockchain technology, it is frequently used in conjunction with it. Blockchain has grown in popularity as a system for storing data in an irreversible manner, therefore guaranteeing and confirming identification. Existing solutions include systems such as uPort and Sovrin (Sorvin,2021), as well as Hyperledger Indy (Hyperledge Indy,2021). The compliance to the General Data Protection Regulation (GDPR) is assumed as no private data is stores on the blockchain. There is still considerable skepticism about it, and authorities must issue clear guidelines.

It is feasible to record identities and verifiable claims on the blockchain utilizing the idea of self-sovereign identification that uses Decentralized Identifiers (DIDs) (Reed et al., n.d.). The DID is a globally unique identifier that does not require explanation since its DID scheme relates to a specific technique that explains how the DID is resolved and connects to a DID document that describes all the specifics. The DID document is completely self-describing and includes information on the entity that the DID is about. This contains cryptographic data as well as service endpoints. Due to GDPR compliance reasons it is critical that neither the DID nor the DID document include person-associated data.

A DID looks like: did:ethr:0xe34eac30c498d9e26865f64fcaa57dbb935b0d7a, and comprises three parts separated by a colon: Firstly, stringing “did” for the URL pattern, secondly, a DID method and, thirdly, a specific identifier.

Even though the DID represents the entity's identity, other verifiable claims define the entity's attributes or features (Otto et al., n.d.). A trustworthy party, which itself is represented by an identity (DID) should issue those claims. Verifiable claims can be stored on a blockchain to ensure their immutability and independence from the issuer's availability. An example of such an ecosystem is suggested by Shane (n.d.). While claims are often stored on a blockchain in the form of a smart contract, JSON Web Tokens (JWT) may be used to transfer and interchange verifiable claims off-chain (Faísca & Rogado, 2016).

JWT comprises three parts separated by dots (JWT, n.d.): A header, with information related to the signing algorithm, a payload, including the claim, and a signature, which is the signed header and payload. The header and the payload are Base64Url encrypted in order to minimize the size.

The claim itself comprises information on the issuer and the date of issuance, the claim's subject or entity, the target audience of the claim, and optionally an expiration date. Furthermore, additional optional fields are available. JWT examples and libraries are available at JWT website.

4.2.Self-Sovereign Identity for IoT Devices

Ever since blockchain technology has become more popular, people have started to consider its opportunities in various areas such as digital identity. The notion of digital identity has been defined and presented in a variety of names in the last three decades (Brickell et al., 2004; Wagner et al., 2018). However, in the last decade it has acquired the name of self-sovereign identity (SSI). More specifically, Kalabukhova et al. (2019) refer to the self-sovereign ecosystem.

According to Kalabukhova et al. (2019), people face the SSI challenge in many cases. For instance, sometimes personal information of the users of various devices are leaked to third parties, which actually means providing private data that do not have a specific purpose. Users are not aware of what happens to these data and third parties can manipulate and use them in order to gain benefit. In addition, there are cases where the entire database of an organization, which is created by a company that gathers and stores data from users' accounts on its servers, is stolen. Therefore, the customers are forced to face some economic or private data related issues.

Kalabukhova et al. (2019) suggest that the solution of the first problem can be found in SSI. SSI itself means that every user should be the only one who is able to create, utilize and control their sovereign data. Besides, as regards internet communication, user's identity should be verified so that users know that the person they are contacting is real, especially when it comes to official or economic matters, for instance, someone who is eligible to pay and able to afford this operation.

As regards SSI infrastructures, at the beginning the notion of SSI was not based on a blockchain. Actually, it referred to a protocol that sets the rules of interactions of independent identity users, who represent an end user, with its identifier. Nevertheless, there was no way to know if the counteragent was in danger or not. For instance, in a scenario that someone is able to substitute government public keys in an agent's storage, he would be able to use government's identity and make claims. In this case, there was a breach of trust as regards storing data.

This problem was solved by blockchain and distributed ledger technology, which created a secure storage unable be altered, which was based on a set of rules unanimously determined by participants. In this way, when a public key which is place to the blockchain, it cannot be altered, unless 51% of the attack is successful, and each one of the participants is entitled to a full copy of the state of a system.

Since the main goals of the researchers have been found, Kalabukhova et al. (2019) suggest that there can be a detailed overview of an architecture of SSI solutions and components. However, there is a variety of different implementations available which are pretty similar when it comes to the main idea around which they revolve.

Many research papers discuss self-sovereign identity of people (Mühle et al., 2018; van Bokkem et al., 2019). Some of them cite the ten key properties of SSI from Allen (2016): existence of the entity in the real world, the entity controlling its identity, access to the own data, transparency about the systems and algorithms used, persistence and long-liveness of the identity, portability of the identity to ensure the independence of systems, interoperability of the identity through open standards, consent of the entity to share or use its identity, reduction of the data that is disclosed through claim and protection of the entities' rights.

Al-Bassam (2017) describes a smart contract-based identity system, in which each entity is represented by an Ethereum address. His SCPKI system emphasizes on individuals or organizations as entities that control their identity via their Ethereum address's private key. In the characteristics of an identity, a proof or claim is reduced to a Boolean value.

Der et al. (2017) view SSI as one of the most important enablers for a digital revolution. The use of SSI for things is identified as a future study field in their paper's prognosis. In addition, conceptional questions are presented, such as "How can a non-human being understand and describe its own identity?"

Bartolomeu et al. (2017) present an overview about SSI for Industrial Internet of Things (IIoT). They provide a review of a number of use-cases and challenges that SSI deal with, in the context of IIoT. The verification of devices is one of the implementations mentioned. It is stated that most solutions depend on centralized instance and blockchain-based SSI is one way of addressing and solving this issue.

To function as a distinct digital twin, a device should "receive" an identity. This identity is an artificial act due to the fact that it is not connected to a physical uniqueness. Hence, this is a crucial moment security wise that should be completed during production and in a secure environment. There are numerous possibilities to include a secure environment on a chip to safely store this identity. Trusted Execution Environments (TEE) are an answer to this issue. Shepherd et al. (2016) provide a summary of actual technologies. Companies such as Intel, LEGIC, and Riddle & Code produce products that allow private keys to be stored in a secure element on a chip. Weingaertner and Camenzind (2021) they leave this to the manufacturer on purpose.

4.3.Self-Sovereign Identity And Use-Cases in Indistrial IoT

Centralized third party information systems that represent a single point of failure which can paralyze an infrastructure and cease its normal functioning all over the world, have been supporting digital identity as a component of a security framework for a long time. In addition, this type of approach may lead to the exposure of the digital identity if the main authority is violated, bringing privacy issues to the surface.

There is a challenge presented towards traditional centralized safety solutions due to the Industrial Internet of Things (IIoT) requirement as regards supporting huge numbers of heterogenous (immobile and mobile) IoT devices, especially when this type of technology is to be used in unsafe environments or need to interact with IoT devices which are establish in such environments. In this context, IoT devices might be instructed to establish infrequent or opportunistic interactions with each other, besides normal functions such as replacement and maintenance. Therefore, depending on a central authority to verify and approve these actions, not only does it constitute a single point of failure, but it also increases communication costs and the possibilities of malevolent attacks.

As Self-Sovereign Identity (SSI) is becoming more and more popular as regards digital identity, even though the term has not been clearly defined, with only a few fundamental properties defined, there has been a significant effort to disclose this notion with a large number of technologies that have been recently introduced. More specifically, SSI is an identity management system which gives users the opportunity to fully own and control their digital identity (Mühle et al., 2018). Thus, digital identity is not limited only to individuals, and it can also be used for IoT device that can own their identities according to their development process. Allen (2016) authored the ten principles of SSI according to which the user has been placed in the center of SSI with an emphasis of keeping the balance as regards clarity, justice and support of the commons accompanied by protection for the individuals.

The SSI systems promote the notion that identity artifacts can be owned by the users and be freely used when an interaction requires identification without depending on a central authority for authentication. Thus, when a device is interacting with another device for the first time, the former can provide the later with an identity artifact which reveals only the bare minimum data which is required with a view to granting access. In SSI, identity artifacts are designated Decentralized Identifiers (DIDs) and may include Claims or Credentials which can be directly provided to the requiring source, skipping the intermediate step of evaluating their validity. In addition, in SSI, as well as in many other identity management systems, there are some revoking mechanisms whose main role is to cancel credentials which have expired (e.g., driver's license expiration).

Industry's 4.0 main purpose is to merge information and communication technologies with industrial technology, focusing primarily on Cyber-Physical Systems (CPS) to build and implement intelligent factories in order to encourage the creation of a more digital, flexible, information-centered and ecological production (Zhou et al., 2015). Even though this futuristic scenario offers a number of benefits, it also introduces new problems in areas of anonymity, accessibility, verification, security and transparency, all of which should be addressed effectively.

1) *Remote Interaction:* This use-case focuses on the ways that the SSI can improve remote interaction over the IIoT. Remote interaction is defined as the direct, real-time interaction between Users/ Devices at specific moments without the need for everyone or everything to be in the same place. In order to boost the productivity and the effectiveness of the communications between Users/Devices while reducing the costs of the production, and to help people avoid dangerous workspaces, the contemporary industry utilizes remote interactions (Goodrich & Schultz, 2008). Remote interaction gives these devices the opportunity to collaborate and interact with their system operators and surrounding devices.
2) *Automatic Procurement:* In the context of industry, Automatic Procurement, often known as Electronic Procurement (EP or E-procurement), is the business of controlling the purchase orders, purchase order modification notices and other similar information which enhance the budget and contract administration. EP comprises of extra automated processes and operations (Schoenherr & Tummala, 2007). IIoT will assist the industrial EP in bettering expenditure management, catalog content, the increase in expenditure visibility and it will, also, provide a better understanding of the consumption of supplies and equipment by knowing what is necessary and what is being used (Glas & Kleemann, 2016).

   SSI has the ability to dramatically expand the range of E-procurement applications, by means of:

   a) Smart Contracts

      Smart contracts may automatically carry out the provisions of multiparty agreements, self-authorize their own terms, and self-execute by directing payments to the appropriate section (Cong & He, 2019).

      Some examples of SSI-based smart contract implementations are:

      - *Ethereum* Foundation (Abraham, 2017), which applied a cryptocurrency alongside a platform for decentralized applications which brought in smart contracts. SSI is not the direct purpose of Ethereum. However, the latter could be used as a platform in order to implement such a system.

- *Jolocom* (Fei et al., 2018) which is a decentralized infrastructure for SSI that supports the smart contracts.
- *DID-claims* (GitHub, n.d.), which is an application that carries out smart contracts (Selfkey implementation of ERC725 identity standard - Ethereum Identity Standard).

b) Purchase Order (PO) / Supply Chain Visibility (SCV)

Purchase order is still considered a very significant resource and it gives purchasers the ability to convey their intentions to the sellers clearly. Every modification at any part of the order and real-time processing, controlling of sales and purchase transactions, monitor expenditures and pay vendors, can be traced by the PO applications supply. In addition, SCV allows the buyer to confirm the authenticity and traceability of all items via product orders and physical product shipments from the manufacturing source to the final destination (buyer). SCV's goal is to better the supply chain by making data easily accessible to all stakeholders, including customers.

There are not fully SSI applications for these objectives yet, however, there are SSI-based solutions and applications for purchasing, order management, and authorization. For instance, *Peer Mountain* (Peer Mountain, 2021) is a decentralized peer-to-peer trust marketplace, which connects SSI owners with service providers that comply to the rules. Businesses can transact data safely without any interruption in order to make the efficiency of their commercial operation better by utilizing SSI-based solutions.

3) *Authentication, Authorization and Trust of IIoT User/Devices*: Many different identity management solutions have been deployed by several public and private companies with a view to managing Users/Device authentication and authorization privileges within and across system and enterprise. These solutions utilize many different methods based on (Cpałka et al., 2016):

a) Physical Segment: Devices like chip-card are used for authentication. Esfahani et al. (2017) introduced a lightweight authentication mechanism for Machine to Machine (M2M) communication in IIoT environment that uses this method.

b) Knowledge: This method utilizes data such as password and token. Huang et al. (2019) demonstrated a blockchain system with credit-based consensus mechanism and data authority administration technique to control the access to sensor data for IIoT.

c) Inherent features: Biometric features are used by this method to achieve authentication. Yang et al. (2019) suggested a lightweight biometric system that preserves privacy, which is specifically designed for resource limited IIoT devices.

The majority of these solutions depend on verification and identity network services, which are provided by a centralized server. With these solutions, end Users/Devices can use third-party digital credentials to verify or provide their identity data claims. Furthermore, the majority of the existing solutions can also be applied in the IIoT sector, providing security mechanisms which are based on asymmetric cryptography, resulting in high computational cost (Esfahani et al., 2017). To overcome these constraints, the most apparent solution is to rely on a trusted third party or a blockchain, or simply to refrain from exposing the data, so prohibiting manipulations that would reveal the nature of the data or the identity of the target.

4) *Part life-cycle support*: The life-cycles of industrial automation are very long. There are now assembly lines and process industry facilities that have been in continuous operation for more than 20 years, and this trend is expected to continue as it is with IIoT. Parts, components, and machines in the factories of the future will need to be fixed, replaced, and re-configured during these extremely lengthy life-cycles. In this context, it is critical to ensure that new components, whether from original OEMs or other sources, are genuine, non-malicious, and completely compatible with the existing parts.

5) *Big Data and Artificial Intelligence*: To boost the productivity and produce new products, industrial IoT integrates smart objects and devices, big data analytics, and

artificial intelligence (AI). These new devices produce a huge quantity of data, both structured and unstructured, that must be stored. Storing this data in the IIoT is problematic due to storage, security, and administration issues with current centralized database technologies (Zhou et al., 2015). Some firms, such as Sia , Filecoin (Protocol Labs, 2017), and Tardigrade, established a decentralized blockchain-based storage network where industrial enterprises may store their data and create a specific balance between redundancy, cost, and speed of retrieval with a view to avoiding reliance on a centralized database. These businesses aren't specifically focused on the SSI, but the concept can be used to various parts of the authentication, storage, and encryption.

4.4.SSI And Solutions for Securing Communications

4.4.1. Authorized data exchange between devices

Users can, for example, contact diabetes and Alzheimer organizations and use a service which allows them to store their private data on their phone and use a digital wallet in order to establish secure communications with a digital wallet of some other user. In this environment, users can give permission to the other party to access their data wit confidence that the other user was who he claimed to be. However, users do not know if other users -except from the doctor-have access to the third party’s data from his glucose meter.

A user’s glucose meter can connect safely to a smartphone by using DIDcomm and Peer DID connections. Peer DIDs are used to generate secure identifiers that are only known to the glucose meter and the smartphone. DIDcomm is a protocol that operates established industrial transport protocols (BLE, NFC, HTTPS, etc.) and provides a secure communication layer for the exchange of DIDs and Verifiable Credentials. Encrypted messages pass between the two agent endpoints during the DIDcomm exchange (smartphone & glucose meter). Each message is encrypted using the other party's public key and decoded by the other party using their private key. Since the shared keys are stored only in the glucose meter and the smartphone, no one can impersonate a user.

4.4.2. Ensuring authorized data exchange between devices

If a user is searching for insulin monitor manufacturers, he can find many reliable ones, even though he does not have enough knowledge on technology in order to be sure of his choice. For example, IMX describes how they interoperate with client pumps. IMX states that their relationship with their clients has change due to the fact that clients can control the data that have been produced by their insulin monitor. IMX collaborates with PeaceOfMind, which is a trustworthy credential service company that distributes credentials to IMX on behalf of the client. With this credential, IMX gains access to the monitor's data since it is stored in a special online data container. IMX's monitor creates rich datasets and the use of valid credentials for access and rich data semantics for data capture, give IMX the ability to improve the services that they provide to their clients. IMX can send artificial intelligence models to the client's phone that can process the data and provide feedback to the client.

In addition, PeaceOfMind is a company that provides services to patients and their families dealing with potentially life-threatening medical conditions, by issuing and controlling Verifiable Credentials. PeaceOfMind is the only manufacturer that provides this kind of control and utility.

Another example is shoe inserts. If a user conducts regular research, he can find out that there is only one credential-based product by the Boot.id company. Boot.id sells shoe inserts which include computer and communication devices that stream data about the user's biometrics, including an analysis of his gait, to the user's smartphone. Boot.id, like IMX, depends on the user to verify PeaceOfMind to issue Boot.id a credentials that grants their access to the data from user's insoles.

As previously stated, only Boot.id is capable of securely transmitting data from the user's insoles due to the use of DIDcomm and Peer DIDs for identification and connection. According to this process, the data created by the insoles is provenanced using the insoles' public key and encrypted using Boot.id's public key, guaranteeing that only Boot.id can decode the data. It is conceivable to create a defense in depth strategy for the devices keeping the user safe, by developing a secure high assurance identity for the insoles in the user's shoes.

4.4.3. Ensuring data privacy

The fact that the user is able to control his data has true value to him only when he can securely share tat data with known entities. Another concerning thing is which data gets shared with others. The user needs to protect his privacy by limiting which data is visible, to whom and how. For instance, if user's age is significant, user's credential should have a data point for age rather than date of birth. Overall, the user needs to reduce the risk to his privacy and increase the value of his data that he is sharing.

VCs were created to serve the purpose of sharing, revocation and delegation. The holder of the credential has the authority to grant temporary permission to another person or organization to access the entire credential or some subgroup of the claims which are included in the credential. For example, a user who is the legal guardian of a person can authorize PeaceOfMind to issue credential to law enforcement giving them permission to access this person's location data if he goes missing for as long as the search operation lasts. Law enforcement agency would give this credential to Boot.id and IMX during the search and rescue operation. Nevertheless, once this person is found, the user can revoke the credential and fully restore this person's privacy. The most important thing in this situation is that this person's guardian has full control when it comes to granting and revoking access to this person's data.

4.4.4. Number of devices & networks to manage

To Authorize and Authenticate IoT Devices, the system currently depends on pre-shared keys or self-signed certificates, as well as public key infrastructure (PKI). While existing methods provide some protection, as the number and variety of devices deployed grows, so does the risk of a security breach as the complexity and overhead of device administration increase. The Infrastructure Manager is aware that not all devices in the facility have been granted with certificates, while some of them may have expired certificates.

DIDs can be both public and private. In the scenario above there is a value of using both. The unchangeable nature of the blockchain and the ability to connect this DID to the manufacturer boosts Infrastructure Manager's trust and assurance that updates and credentials on the device are valid and not compromised, in a case that the manufacturer has a public DID that is encoded into the device.

When the Infrastructure Manager connects the device to his network, private DIDs (or Peer DIDs) will be exchanged between the controller and the device. These peer DIDs serve two purposes: first, they verify the identity of the devices on both sides, and second, they establish a secure communication channel between them.

DIDs and VCs are used to establish the identity of IoT devices, individuals, and organizations on a worldwide scale. This allows the Infrastructure Manager to standardize the administration of both Machine-to-Machine (for example, CCTV cameras sending their footage to a server) and Machine to Person interactions (for example, doorways controlling entering and exiting of restricted areas).

By making sure that all IoT devices can definitively self-identify and authenticate, the use of DIDs and VCs in the asset management platform and wider IT ecosystem will boost security. When the process of issuing DIDs and credentials is centralized, device management procedures are improved and simplified, while errors like expired certificates are minimized.

4.5.SSI and its usage

Finally, the use of blockchain in SSI systems is not required. This adds to the entire system's complexity by introducing protocols and procedures for which there is yet no accurate data on their security and for which standardization procedures have not yet been finished. However, if we decide to use the blockchain solution, we must guarantee that no personal data is saved there, and that no conclusions are drawn about the sensitive content of the credentials. This occurs, because information is maintained on the blockchain indefinitely and there is no technical way to delete it.

Blockchain technology and how it works

Blockchain is a sequence of blocks, each containing a complete transaction file such as a public book. This indicates the order in which the transactions took place. Figure 1 represents a Blockchain, where the most recent block contains information indicating the previous one. Each block in the chain confirms the integrity of the previous one, up to the first block, called the Genesis Block (Chuen, 2015). No one may corrupt the information contained in a block. To do this, you need a lot of computing power, which makes it nearly impossible.

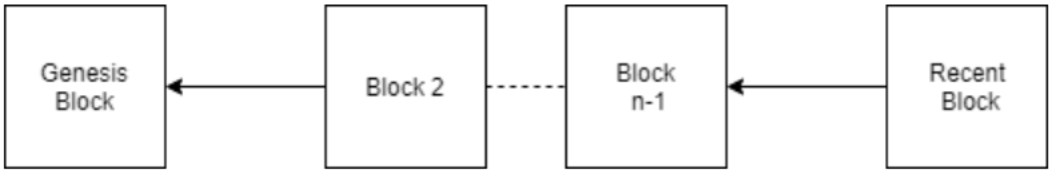


Figure 4: A blockchain (Chuen, 2015).

Blockchain is a peer-to-peer (P2P) network that is decentralized. There is control by the organization in the sense that there is no authority to control the network (unless the network is private). Because the authority that controls the chain is all of the members who engage in it, the idea of P2P relates to the fact that each member possesses a copy of the chain. The participants will decide whether a block is right, and if the majority agrees, that block will be given among the participants, and each member will add that block to the chain. There are two types of Blockchain: Public and Private Blockchain. Both of them are P2P networks, where each participant maintains a copy of the chain which stores the digital transactions. This chain can only be updated. Participants keep the chain in sync through a consent protocol. This ensures the integrity of the chain, even if there are malicious participants.

1. Public Blockchain: Public Blockchains are open networks that anyone can join as long as they have an Internet connection. Because the success and safety of such a network are dependent on the number of users, an incentive mechanism is used to entice potential participants. Bitcoin is the best example of a public Blockchain, in which those who engage in the network, known as miners, are rewarded with Bitcoin (BTC).
2. Private Blockchain: Private Blochains are smaller in size and are only accessible to a limited number of people (a license is required). Private Blockchains are created by businesses to preserve anonymity while simultaneously protecting data. It is

mostly accessed by network administrators' licensed users or by a set of rules that can be enforced. An authorized network is another term for such a network. Private Blockchains may limit the activities of individual participants, allowing transactions to be done between specific participants rather than by the entire network. This adds still another degree of security to the safeguarding of personal information.

As previously stated, Blockchain is a decentralized network in which participants are ordinary consumers with Internet connection. Apart from the fact that no third-party company has control over its operations, altering its data is nearly difficult due to the high computing power required. Each Block has three elements: 1) the data within the block, 2) an identification element (Hash), and 3) the previous block's identification element (Hash of previous block). The data stored in a Block is determined by the Block's kind. Each block in the Bitcoin Blockchain, for example, comprises transaction details such as the sender, recipient, and Bitcoin units. It also has a unique identification for each block. To counteract malicious attacks, Blockchain employs the SHA-256 (PoW) Hashcash protocol, which generates a unique identifier for each block. SHA-256 transforms every input into a 256-bit message (Chuen, 2015).

The architecture of a Blockchain may be shown in Figure 2, which consists of the Datastore, which is the blockchain data structure that holds everything in the chain. The Consensus Mechanism, i.e., the agreement that maintains data integrity and Transaction Validation, which is a distributed network (Peer to-Peer). Finally, there's cryptography, which assures that the data in the chain is secure and private.

In addition, and to delve deeper into a blockchain architecture, we can also take a look at the structure of a block. A block consists of the header and the body, as shown in Figure 3. The block header includes the following:

- Block Version: indicates which set of validation rules to follow.
- Merkle tree root hash: the hash value of all transactions in the block.
- Timestamp: current time in seconds.
- nBits: target limit for the valid hash value of a block.

- Nonce: a 4-byte field, usually starting at 0 and increasing a hash value for each calculation.
- Parent block hash: A 256-bit hash value that indicates the previous block. The body of the block consists of the counter number of transactions and trades.

The maximum number of transactions that a block can contain, depends on the size of the block and the size of each transaction (Zheng et al., 2017).

4.6.SSI for IoT And Challenges

The use of the innovative SSI paradigm in IoT contexts is fraught with difficulties that may need a "period of maturation and technological affirmation" (Bartolomeu et al., 2019). There are some non-technical issues that need considerable effort such as standardization, best practices and organizational.

- **Constrained devices:** To fully implement SSI, devices have to be capable of running asymmetric cryptography and dealing with the communication overhead of transmitting metadata like DID Documents and Verifiable Credentials.
- **Asymmetric Cryptography:** SSI requires execution of encryption algorithms that are based on asymmetric keys, which can be proven difficult for devices with restricted processing and energy resources. While authors suggest that restricted processors like the 32-bit Cortex M0 are capable of executing Elliptic Curve Cryptography (ECC) (Kortesniemi et al., 2019), the number of operations must be limited to minimize battery loss. Using long-lived session keys that are updated less regularly, such as once a day, is a typical strategy.
- **Communication overhead:** The size of DDos and VCs might pose an obstacle, depending on the communication protocol. For instance, low-energy protocols like LoRA and BLE have maximum packet sizes of 222 and 244 bytes, respectively. In contrast, DDoS and VCs often exceed 500 bytes. Hence, compression, fragmentation and infrequent document transmission are tactics that will be

necessary. In extreme contexts, SSI may not be achievable at all, which will create the need for proxy approaches (Lagutin et al., 2019).

- **DID Resolution:** Downloading DID Documents may not be an option for highly limited devices which may not be able to connect to the Internet. The creation of a local cache of known DIDs, which may be controlled by the device or by its gateway, is a possible solution. On the contrary, the devices can easily exchange their DIDs directly, if both of them use peer DIDs, shifting the issue to securely providing the DIDs in the first place.
- **Traceability:** It is necessary to avoid global tracking. Even though a DID does not divulge sensitive information, repeated interactions with the same DID can be traced in order to identify a device. As a result, in privacy-sensitive cases, the did:peer approach should be explored. When linkability is required (for example, to identify malicious devices), this technique works effectively since it allows devices to be individually addressed without leaving the same footprints across domains.

5. Case Study: Design of a Single Pole Marine Wind Turbine in the Ionian Sea using a cybersecure system combining IoT and SSI

5.1. Problem definition

A particular problem for offshore wind turbines is the erosion of the seabed around their base. If left unattended, the problems caused by corrosion can cause serious damage, or even lead to the collapse of the plant. With this in mind, there has been an exploration of possibility of piezoelectric energy conversion into electricity (by the vibrations that are usually caused in the structure of wind turbines). This provides sufficient and reliable power to the sensors that detect and monitor friction as well as other damage. Considering the above, we propose a structural robustness monitoring system that not only ensures their proper operation but can safeguard the turbines from cyber threats as well.

To begin with, in order for this system to be properly induced and to minimize the risks, we need to have a general idea about the dangers that can occur on the Internet of Things (IoT) devices. In September 2015, the FBI issued a cyber-security warning, stating that Internet of Things (IoT) devices could be targeted by cybercriminals, endangering their users (Ceara & McCaffery, 2016). In the future, it is unlikely that the biggest security problems will be caused by similar technologies, as it will be up to the machines with Artificial Intelligence to decide for the good health (or not) of the people who use them. Security issues that may arise today in artificial intelligence technologies are related to the digital signal, and are, for example, if the signal is impairments and communication and interoperability problems arise as a result. For this it is useful to detect transmission errors through special batch grouping algorithms. It also concerns how much data is affected by transmission delays. Real time applications may be affected by delay jitter and may no longer be usable by the receiver. For security, a buffer can usually be used on the receiver so that enough video and audio data to be transferred is already stored, thus addressing a limited delay. In some cases, the tolerance of transmission of errors in the telecommunication channels does not matter so much, since for some applications it is not possible or desirable to correct them, and in the end it does not bother the end user (eg in a friendly communication via skype). For others, however, as should be the case for data in the field of health, there should be no such tolerance. The correct download of all data should be required and the destination should be prevented from recomposing the original data if even a single initial bit is wrong. It should also be noted that real-time file and data transfers are not time sensitive.

5.2. Description of the Offshore Wind Turbines

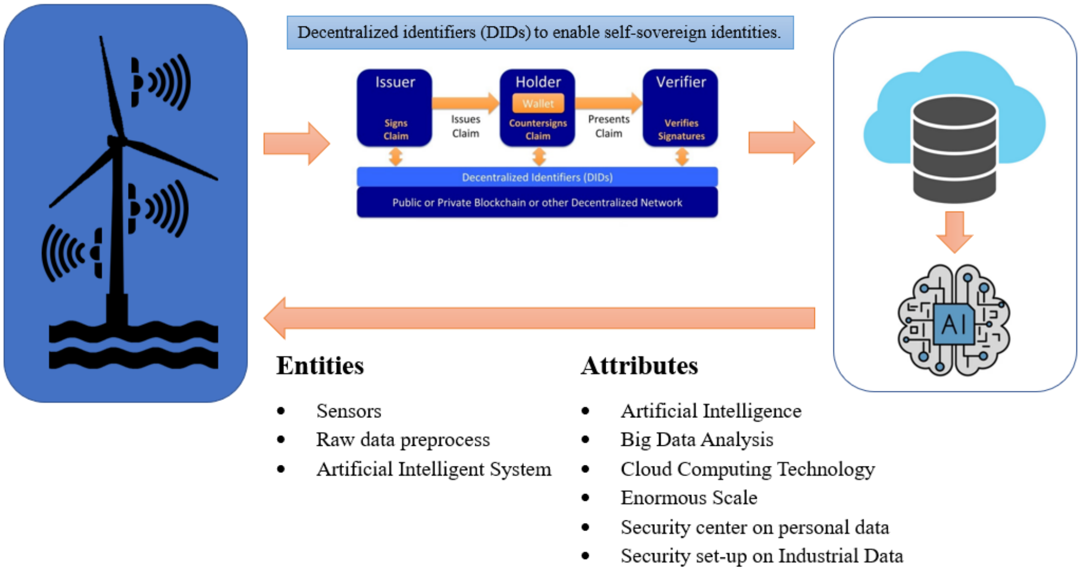
Offshore wind energy, ie the energy produced by wind farms located at sea, is almost 25 years old. However, in Greece no remarkable progress has been made in this field both in research and in development. In the case study of the present work, initially we describe the various types of marine wind turbines that can be used in the Greek seas, recording their inherent advantages and disadvantages. We will focus on the operation of a wind turbine at sea and will make a comparison with the respective land generators that are already installed in Greece. We will also analyze the process and basic design principles of offshore wind turbines, in accordance with international standards. Subsequently, a specific study of a floating offshore wind farm for the Ionian Sea will be carried out. The preliminary design of a standard single-stroke marine wind turbine will be analyzed based on the above reports. The mechanical parts of the wind turbine, its interior, the aerodynamics of the blade and its possible performance will be analyzed.

5.3. Description of the sensors-based IoT system

For our system we suggest many sensors that will collect data and will be connected to an intelligent system that will decide according to the situations. Temperature sensors, motion sensors, humidity sensors, air quality sensors, light sensors, sensors that detect and monitor friction, as well as other damage will be installed. These sensors, together with a connection, will allow us to automatically collect information from the wind turbines, which, in turn, allow us to make smarter decisions, which will be related to the optimal operation of the machines for better performance.

Connecting them to the internet and transferring this data to a server will allow machine learning algorithms to train different models and make various decisions about the operation of wind turbines. It could receive weather information from its internet connection, can also know when it will rain and decides not to water the crops that day because they will be watered by the rain anyway. For example, if one day there are no strong winds or there are enough waves and there are frictions, the wind turbine can be adjusted to its operation automatically without human intervention.

Our proposal concerns a device-to-cloud communication model (device to cloud, D2C), the IoT device connecting directly to a cloud Internet service, such as an application service provider, for data exchange and control message traffic. This approach often leverages existing communication mechanisms such as traditional wired Ethernet or Wi-Fi connections to establish a connection between the device and the IP network, which eventually connects to the cloud service, but may also use cellular technology.


Decentralized identifiers (DIDs) to enable self-sovereign identities.
Issuer
Signs Claim
Issues Claim
Holder
Wallet
Countersigns Claim
Presents Claim
Verifier
Verifies Signatures
Decentralized Identifiers (DIDs)
Public or Private Blockchain or other Decentralized Network
AI

Entities

- Sensors
- Raw data preprocess
- Artificial Intelligent System

Attributes

- Artificial Intelligence
- Big Data Analysis
- Cloud Computing Technology
- Enormous Scale
- Security center on personal data
- Security set-up on Industrial Data

Figure 5: Our Proposed System

5.4. IoT safety and Insecure Cloud Interface

Our proposed framework focuses in depth on the security of the data that will be derived from sensors through the cloud server. The security provided by IoT technologies is the most crucial factor in the widespread adoption of such technologies by end users. If there are no guarantees regarding system-level confidentiality, identification and privacy of the members concerned, no IoT solution will work. In the early stages of IoT solution development, which relied solely on RFID, security solutions were provided only when needed and were not integrated from the outset. This is due to the fact that such solutions were developed in a vertical manner, where all elements were under the control of a single administrative entity. In the case of an open IoT ecosystem, where the stakeholders have different roles, for example one group of stakeholders has sensors or actuators, another group manages and processes the data collected by previous stakeholders and finally, a different group of people will provide services to the end users, which will be based on the data collected and processed. Such a model raises a number of security issues that need to be addressed in order for IoT technologies to prevail. The key factors that need to be addressed are data confidentiality, privacy and trust.

Another crucial aspect is the Insecure Cloud Interface. In the event of a failure, attackers can take advantage of the following to gain relatively easy access to data access or cloud governance policies through cloud websites: 1) inadequate authentication, 2) lack of encryption data transfer and 3) non-listing of accounts. Those who could carry out such an attack could be those who have access to the internet. Insecure Cloud Interface is a security vulnerability that is common and easily detectable. This is what happens when one can easily guess the credentials used or list accounts. Such a security problem can be easily detected if the SSL protocol is used or not when connecting to the cloud interface. A password recovery mechanism can also be used to find valid accounts to determine if this could lead to an enumeration of accounts. The technical consequences that can be caused by such a lack of protection are serious, as it is possible to expose user data and gain full control of the device.

On the business side, they need to consider the impact they will have on their business in the event that their users' personal data is stolen or their attackers regain control of their devices. They should therefore ask themselves if their customers or their company name are affected in such a case. The checks that need to be done to see if the cloud interfaces are secure or not are as follows: a) To see if the default username and password can be changed during the initial installation of a product. b) Determine if a specific user account is locked after 3-5 failed login attempts. c) Determine if valid user accounts can be identified using password recovery mechanisms or new user pages. d) Review the interface for security issues such as cross-site scripting, cross site request forgery and sql injection. e) Review all cloud interfaces for vulnerabilities (API interfaces and cloud-based web interfaces).

Thus, in order to ensure that the cloud interfaces are secure, it is required: 1) The default passwords, and ideally the usernames, to be changed during the initial installation. 2) Ensure that user accounts cannot be listed using methods such as password reset mechanisms. 3) Lock a user's account, after 3-5 failed login attempts. 4) Ensure that cloud interfaces are not vulnerable to XSS, SQLi or CSRF attacks. 5) Ensure that credentials are not exposed online. 6) Apply authentication to two different elements (2FA-two factor authentication) if possible.

5.5. Security measures of our framework

In security matters, our system will follow the principles of IIoT security measures. The way the industrial world approaches process management and control is changing. The concept of interconnectedness of intelligent devices in the consumer world is permeating the industrial realm. The resulting interconnected industrial environment is delivering a whole set of benefits like efficiency, safety, and profitability among others. However, while Internet of Things (IoT) concepts can be applied to industrial devices, assets, and infrastructure, the Industrial IoT (IIoT) has much stricter requirements in terms of quality, security, reliability, synchronization, and so on. As such, these systems are more complex and challenging.

From the architectural point of view, IIoT embedded devices must have compelling processing capabilities to deliver significant results. Heterogeneous computing architectures that encompass a mix of general-purpose processors and massive parallel elements are suitable for advanced IIoT applications. General-purpose processors provide powerful, stand-alone execution of floating point operations, data logging, and connectivity. In addition, massive parallel elements such as FPGAs and graphics processing units are used to reduce data, customize algorithms, and quickly respond to critical events.

From the security point of view and because IIoT embedded devices operate at the edge, they also represent the last line of defense against attackers. This is often overlooked during the design cycle of such devices because more immediate issues such as lack of domain expertise, implementation costs, and time-to-market constraints relegate security to a secondary plane of importance. Consequently, the 2010 Stuxnet attack exposed the true vulnerability of these systems, demonstrated how much damage an industrial breach can cause, and publicly positioned industrial applications as potential targets.

Wind turbines, nuclear plants, oil and gas pipelines, and similar industrial assets are now the target of government and hacktivist groups that exploit vulnerabilities in industrial devices. The US Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) estimates that attacks on US industrial targets climbed from 41 in 2010 to 198 in 2011 and 245 in 2014. As this trend continues, it is paramount to consider a different approach that would introduce cyber security concepts from the early stages of embedded device design to prevent, mitigate, and predict attacks that target highly sensitive industrial operations. The problem described urges both a change in the way embedded devices are developed and a re-evaluation of security standards applicable to such devices. Integrated development platforms and standardization are required to guarantee seamless implementation of security requirements while maintaining interoperability with other IIoT entities. Initiatives such as the IIoT and Industry 4.0 provide best practices and recommendations to address these challenges. However, the integration of these recommendations into an open development platform is still a big challenge the industry must overcome.

A flexible platform with support for standardized, open security technologies would greatly reduce the expertise needed to develop IIoT applications while increasing security in industrial systems. The key to making this platform useful for the IIoT is integrating the right security features so applications can automatically benefit from them. Unfortunately, a widely applicable security standard for the IIoT is still incomplete and immature. Until this standard is ready, designers must look for commonality among existing related standards and fill in any gaps for an integrated solution. A set of widely agreed-upon security features is possible today through open technology such as Linux.

5.6. Connection of Self-Sovereign Identity (SSI) with IIoT

In our system, we propose a connection between the SSI approach and the IIoT that was described in the previous section. According to (World Bank Group, 2018), SSI is presented as a service to an individual or entity that will claim its identity without the intervention of a third party. Of course, the validity of the term is questionable, because the civil identity is confirmed by an authorized publishing authority before it is managed by the holder. Thus, more reference is made to a self-managed identity than to a self-sovereign identity. Moreover, modern technology practices include the following areas: Plans for smart cities in e-government, IoT, websites, social media, telecommunications, Industry 4.0, artificial intelligence, telemedicine, mobile telephony, electronic voting (Noizat, 2015). In addition, the technology is used for notarial deeds, birth certificates, contracts where the documents are attached to the electronic identity of the transaction party to prove his identity (Bashir, 2017). It appears that many countries around the world are already planning and programming the use of Blockchain technology for electronic identification. The idea of constructing a digital passport for each and every person in the world is not unique, but with the growing interest and progress of distributed ledgers, a new way of dealing with existing problems appeared. On the other hand, a lot of development groups are working in parallel on similar topics, but there is not a clear view of their work yet.

Another vital part of our implementation, are the Decentralized Identifiers (DIDs) which are a new type of identifiers for verifiable, “self-sovereign” digital identity. In Figure 1 below, a generalized scheme of interaction within SSI is presented and in the following section, a certain protocol with DIDs is proposed in order to facilitate the encryption process.

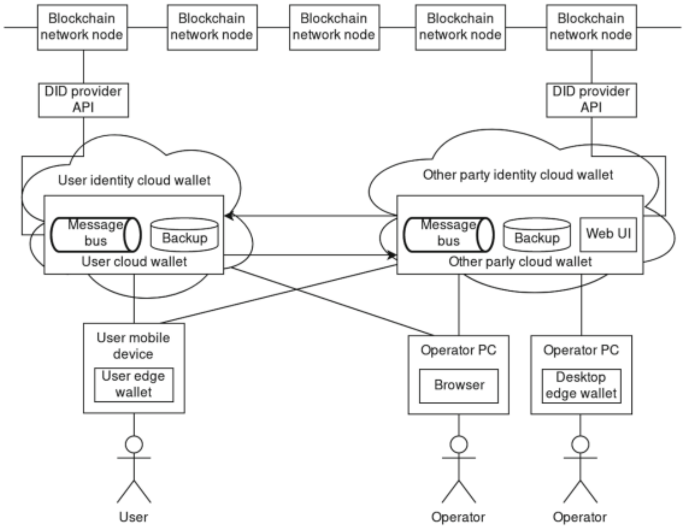


Figure 6: Generalized scheme of interaction within SSI (Kulabukhova et al., 2019).

5.7. Authentication Protocol with DIDs

In this section, a protocol for handshake between arbitrary client and server is being presented, where both are using wallets/DIDs to identify themselves on a web. The main goal here is to translate an identifier to an actual encrypted key in order to use it in a symmetric traffic encryption process, like TLS/HTTPS protocol does. Suggested steps of such a handshake are described in the following sequence diagram (Fig. 2). The wallets here could be replaced with a generalized wallet API and afterwards, both Client and Server can use it locally or remotely without the need to create an actual transaction to verify the opposite side DID on their respective hardware. DLT stands for Distributed Ledger Technology, which can be any modern ledger system, like Ethereum. At the final step, the user would be able to log into the system with the usage of SSI, and use local identity from centralized IDM to interact with a resource. This approach is not completely right from the perspective of decentralized systems, but is capable enough to easily enable DIDs for a variety of infrastructure owners using classic identity management solutions, like corporates, and also shows up a main principle of identity control.

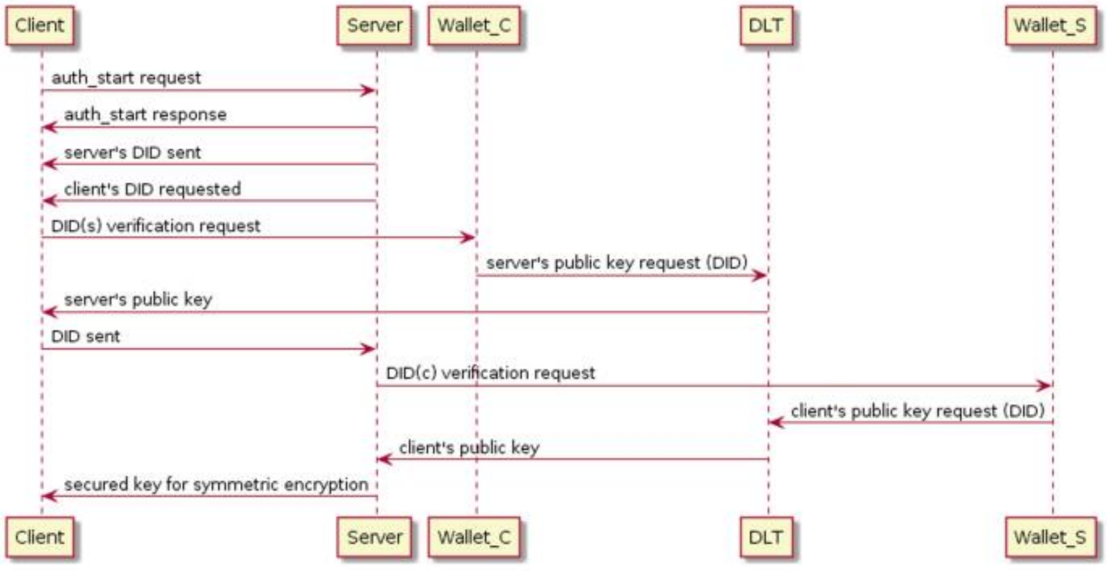


Figure 7: Authentication protocol with symmetric encryption by DIDs (Kulabukhova et al., 2019).

So far we've been describing authentication and authorization, but another interesting area where SSI/DID solution can be used is a cryptography. These appliances are quite simple and come from basic SSI principles. Blockchain already contains public keys, so it can be used as a basis for a public key infrastructure. If the user is already aware of a DID of a machine from the pool where he/she wants to have mutual relationships between nodes, it is then possible to obtain its public key and check if the machine will respond correctly to the message encrypted with that specific key. In addition to that, this process is eliminating key exchange phase at connection initialization. Another case aims at a way more global problem with certification authorities. Basically, every operating system has a package of trusted root certificates preinstalled or such a package already available. This certificate set enables secure communications over the global network. In addition to that, root authorities should store their certificates securely, issue child certificates and include them to the chain. There is no actual way to know whether the authority was compromised or not so, the user should just put his faith in the system and act accordingly.

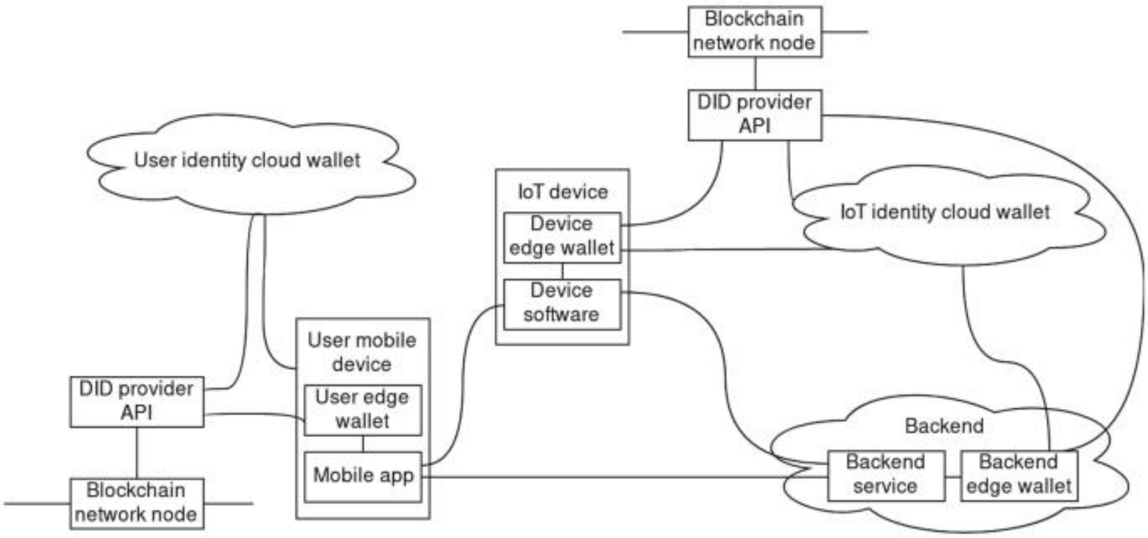


Figure 8: The general scheme of a decentralized application (Kulabukhova et al., 2019).

5.8. Identification of IIoT attributes and entities

In contemplation of our proposed system, an identification of both attributes and entities of the previously discussed IIoT is required. By doing so, we can perceive the concept of IIoT even more and thus, enable a safer and better connection with SSI.

IIoT Attributes

- Artificial Intelligence
- Big Data Analysis
- Cloud Computing Technology
- Enormous Scale
- Security center on personal data
- Security set-up on Industrial Data

IIoT Entities

- Sensors
- Raw data preprocess
- Artificial Intelligent System

6. Discussion

Self-sovereign identification (SSI) is the idea that people and corporations can store their own identity data on their own devices and choose which information to share with validators, rather than relying on a central repository. Nation-states, companies, and global organizations might all construct their own identities (Baars, 2016).

If a person has a complete self-sovereign identity, personal data is saved digitally on a device to which only he has access and which he controls, such as a digital wallet. The blockchain can hold the hash of this data, whether it consists of claims or digital documents. Third parties, such as the issuer or verifier, vouch for the accuracy of this information. As a result, certificates are kept alongside the rest of the individual's data on the security device and shredded into a blockchain. With this information, an individual can be securely identified in any location that the verification body trusts, simply by proving that they are the owner of the public key associated with the certificate claim and without having to reveal any personally identifiable information (including their name). For example, when a college student obtains a scholarship, he or she may be required to identify himself or herself as a scholarship recipient in other parts of the university in order to receive certain services (Crosby et al., 2016).

An SSI user has the ability to create and verify unique identities as well as store identification data. The legal and social implications of digital identity are complex and difficult to understand. However, it is simply a result of the increasing use of computers and the need to provide computers with data that can be used to identify external factors. Identifying who someone is communicating with in cyberspace, is an important issue. There are no precise means of identifying a person in the digital space using static IDs, such as passwords and emails, because this data can be compromised or used by many people behaving as one. Digital authentication can verify and validate an identity with up to 95% accuracy using dynamic entity correlations obtained from behavioral history across multiple websites and mobile applications.

Moreover, by analyzing a collection of entity relationships between a new event (e.g. link) and past occurrences, a convergence pattern can ratify or validate an identity as legitimate. Divergence, on the other hand, denotes an attempt to conceal one's identity. The data used for digital identity is anonymous in most circumstances, thanks to one-way hash fragmentation, which reduces privacy concerns. Because it is based on previous action, a digital ID is impossible to forge or steal.

Offshore wind farms have gained a significant share nowadays in the effort to use renewable energy sources and specifically to produce energy from wind exploitation. With this method, floating wind turbines are used in marine areas with a distance of more than 10 km from the shores, giving the possibility for larger areas of wind farms that can exploit the wind potential. According to our study, in recent years, this form of energy has aroused the interest of several European countries. In Greece, the interest is particularly recent with the companies Kopelouzos and R.F Energy having secured production licenses for the first offshore wind farms in the country. The company TERNA ENERGIAKI, which has signed a cooperation with Ocean Winds for the development of projects with a total capacity of over 1.5GW, is moving in the same wavelength. Ocean Winds is a partnership of the two largest RES companies in Europe, EDP Renewables and Engie.

For the construction of an offshore wind farm, it is necessary to consider the raw materials that will be used. Our study suggests that the raw materials we will use for offshore wind farms are logically different from the raw materials for onshore wind farms. Increasing the size of wind turbines makes progress in this area with the aim of increasing the energy produced and maximizing profits. The raw materials that were to be used are related to the following:

A) Types of foundation: The type of foundation and the form that the wind turbine support body m

ust have are important elements for the overall construction, which shapes the cost of the project. Marine wind turbines can be supported in two ways: the foundation and the floating system. The decision for the appropriate way of support is connected with the depth of the sea, the characteristics of the soil and the technical knowledge available.

B) Foundation system: The most widely known foundation systems for offshore wind turbines are solid systems. The preference of the type of system to be chosen depends on the depth of the sea. Specifically, for depths up to 15 meters, gravity foundations made of reinforced concrete are used. For depths between 15 meters and 90 meters, the single pile, the tripod support, and the net tower are mainly chosen.

C) Floating systems: Floating systems include floating wind turbines.

D) Connection of the offshore wind farm with the local network: One of the options is the offshore substation which connects all the wind turbines. In addition, the Automatic Interconnection Switch of the offshore wind farm is located at this point, which consists of voltage and current transformers. Load switches are, also, located here.

According to our study, unfortunately, offshore wind energy has some negative effects on the environment and people. Firstly, offshore wind farms have an impact on birds. In particular, seabirds and migratory birds have been observed to be at risk of colliding with wind turbines and resulting in death. In addition, due to the offshore wind turbines, there is a case of bird population displacement. As a result, it is recommended not to build offshore wind turbines in areas that are considered migratory bird crossings. Secondly, if the wind farm is close to areas where air lines or ship navigation are developed or to areas where military exercises are carried out or to areas that attract the interest of fishermen, the probability of accidents increases. Therefore, the characteristics of each area, which is proposed for the construction of an offshore wind farm, must be analyzed.

Finally, another negative effect of the offshore wind farms is the excessive noise. In offshore wind farms we can distinguish two different types of noise. The first one is the distinguishable noise caused by the construction of the wind farm and the second one is caused when the farm is in operation. In the first case the sound depends to a certain extent on how the core will be installed at the bottom of the sea. In this case, it is recommended that the wind turbine be assembled on land, if this is feasible, in order to protect marine organisms. In the second case, the noise that can be produced by the farm or by its maintenance, has negative consequences for the marine environment. More specifically, this noise can result in the fish being disoriented and lead to migration, as they will be unable to locate food. This will have consequences for the local economy as well, since we know that the economy in the coastal areas depends to a large extent on fishing.

In Greece, some areas of the Aegean Sea have some of the best wind potential in Europe. In Greece in 2010, the Ministry of Energy selected twelve marine areas (St. Efstratios, Alexandroupoli, Karpathos, Corfu, Thassos, Kryoneri, Kimi, Lemnos, Lefkada, Petali, Samothrace and Fanari of Rodopi) in which it would create offshore wind farms with a total capacity of 1.2 GW. In fact, in Lemnos, they wanted to create the largest offshore wind farm in the world with a total capacity of 500 MW. Unfortunately, this plan did not come true due to bureaucracy and high costs that the Greek state was unable to cover due to the economic crisis in which the country was and continues to be until now.

In order to solve the energy problem in Greece and to ensure the energy needs, it is necessary to create a legislative regulation which will define the following: the ability to use various energy resources, enhancing renewable energy sources (RES) through financial incentives (lower taxation), the creation of national objectives that will define the energy that will be produced by RES and the emission, energy saving in industries, homes and transportation, the use of environmentally friendly forms of energy, enhancing domestic forms of energy.

In our study we present the general goals set by Greece regarding energy policy, which are ensuring the country's energy supply and categorization of energy forms, protecting the environment and enhancing the renewable energy sources, enhancing productivity and competitiveness in the country and promoting development in all regions of the country. Moreover, there are some specific objectives for the sake of the environment. Firstly, it is important to improve energy efficiency in buildings. Secondly, universities should promote renewable energy through state funding. Last but not least, the reduction in energy consumption through various energy saving measures will, also, benefit the environment. As regards the measures that have to be taken for companies, the equipment they use must be environmentally friendly and they should adopt recycling for the equipment to be installed. Additionally, companies should orient their employees and customers to softer forms of energy, they should try to make rational use of energy and keep up with new technologies. Furthermore, our study suggests that Greece should take some special measures that will ensure licensing for renewable energy sources to be done within a reasonable time, since several investments in RES have been severely delayed due to bureaucracy. In addition, these measures should ensure better cooperation between stakeholders on energy policy issues.

Conclusion

Summing up, despite the multiple technologies and applications of the still evolving, global connecting system of IoT, security remains its biggest concern in terms of adaptation. Our proposed structural robustness monitoring system is capable of providing the necessary security for offshore wind turbines by connecting the Self-Sovereign Identity (SSI) with the industrial organizational application of IoT, IIoT. After an initial analysis of both IoT and cloud interface concerning the security parameters of IoT technologies, we delve into our main concept of the union. We achieve that by providing crucial information about both the SSI and IIoT, presenting an Authentication Protocol with DIDs and finally, by pointing out the major attributes and entities of IIoT itself. Our contribution here is that the proposed framework could potentially be used for the security of data generated by sensors above offshore wind turbines.

References

Abraham, A. (2017). Self-Sovereign Identity Whitepaper About the Concept of Self-Sovereign Identity Including Its Potential. *E-Government Innovationszentrum, Graz*.

Al-Bassam, M. (2017). SCPKI: A smart contract-based PKI and identity system. In *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, 35-40.

Allen, C. (2016). "The Path to Self-Sovereign Identity" http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html, [Accessed March 25, 2020]

Allen, C. (2016). The path to self-sovereign identity. *Life with Alacrity*.

Anagnostopoulos, A. G., & Papadopoulos, B. P. (1995, December). Restraint of an Active Landslide by Bored Piles. In *Bengt B Broms Symposium On Geotechnical Engineering* (p. 27). World Scientific.

Aponno, G., & Sholeh, M. (2019, November). An Evaluation of Carrying Capacity of Jack-in Piles with Base Enlargement in Soft Clay. In *IOP Conference Series: Materials Science and Engineering* (Vol. 676, No. 1, p. 012025). IOP Publishing.

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, *68*, 81-97.

Baars, D. S. (2016). *Towards self-sovereign identity using blockchain technology* (Master's thesis, University of Twente).

Bartolomeu, P. C., Vieira, E., Hosseini, S. M., & Ferreira, J. (2019). Self-sovereign identity: Use-cases, technologies, and challenges for industrial iot. In *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. 1173-1180. IEEE.

Bartolomeu, P. C., Vieira, E., Hosseini, S. M., & Ferreira, J. (2019). Self-sovereign identity: Use-cases, technologies, and challenges for industrial iot. In *2019 24th*

IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). 1173-1180

Bashir, I. (2017). *Mastering blockchain*. Packt Publishing Ltd.

Bekken, L. (2009). Lateral behavior of large diameter offshore monopile foundations for wind turbines.

Bi, Z., Da Xu, L., & Wang, C. (2014). Internet of things for enterprise systems of modern manufacturing. *IEEE Transactions on industrial informatics*, *10*(2), 1537-1546.

Brickell, E., Camenisch, J., & Chen, L. (2004). Direct anonymous attestation. In *Proceedings of the 11th ACM conference on Computer and communications security*, 132-145.

Carvalho, N., Chaim, O., Cazarini, E., & Gerolamo, M. (2018). Manufacturing in the fourth industrial revolution: A positive prospect in sustainable manufacturing. *Procedia Manufacturing*, *21*, 671-678.

Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. *IEEE Internet of things journal*, *3*(6), 854-864.

Chuen, D. L. K. (Ed.). (2015). *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data*. Academic Press.

Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies*, *32*(5), 1754-1797.

Cpałka, K., Zalasiński, M., & Rutkowski, L. (2016). A new algorithm for identity verification based on the analysis of a handwritten dynamic signature. *Applied soft computing*, *43*, 47-56.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.

Der, U., Jähnichen, S., & Sürmeli, J. (2017). Self-sovereign identity $-$ opportunities and challenges for the digital revolution. *arXiv preprint arXiv:1712.01767*.

Esfahani A., Mantas G., Matischek R., Saghezchi F. B., Rodriguez J., Bicaku A., Maksuti S., Tauber M., Schmittner C., Bastos J.. (2017). “A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment”, doi: 10.1109/JIOT.2017.2737630.

Faísca, J. G. and Rogado, J. Q.. (2016). “Decentralized semantic identity” in Proceedings of the 12th International Conference on Semantic Systems, 177-180.

Fei, C., Lohkamp, J., Rusu, E., Szawan, K., Wagner, K., & Wittenberg, N. (2018). Jolocom: Self-sovereign and decentralised identity by design. *White paper*.

Fink, G. A., Edgar, T. W., Rice, T. R., MacDonald, D. G., & Crawford, C. E. (2017). Overview of security and privacy in cyber-physical systems. *Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications*, 1-23.

Foradis, T., & Thramboulidis, K. (2017). From mechatronic components to industrial automation things: An IoT model for cyber-physical manufacturing systems. *Journal of Software Engineering and Applications*, *10*(08), 734.

Giang, N. K., Blackstock, M., Lea, R., & Leung, V. C. (2015, October). Developing iot applications in the fog: A distributed dataflow approach. In *2015 5th International Conference on the Internet of Things (IOT)* (pp. 155-162). IEEE.

Glas, A. H., & Kleemann, F. C. (2016). The impact of industry 4.0 on procurement and supply management: A conceptual and qualitative analysis. *International Journal of Business and Management Invention*, *5*(6), 55-66.

Goodrich, M. A., & Schultz, A. C. (2008). *Human-robot interaction: a survey*. Now Publishers Inc.

Harrison, R., Vera, D., & Ahmad, B. (2016). Engineering methods and tools for cyber–physical automation systems. *Proceedings of the IEEE*, *104*(5), 973-985.

Huang, J., Kong, L., Chen, G., Wu, M. Y., Liu, X., & Zeng, P. (2019). Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. *IEEE Transactions on Industrial Informatics*, *15*(6), 3680-3689.

Hyperledger Indy. (2021).Type: Distributed ledger software. https://www.hyperledger.org/use/hyperledger-indy

Jazdi, N. (2014, May). Cyber physical systems in the context of Industry 4.0. In *2014 IEEE international conference on automation, quality and testing, robotics* (pp. 1-4). IEEE.

JWT. (n.d.). "Introduction to JSON Web Tokens" https://jwt.io/introduction/ [Accessed November 9, 2021]

Kortesniemi, Y., Lagutin, D., Elo, T., & Fotiou, N. (2019). Improving the privacy of iot with decentralised identifiers (dids). *Journal of Computer Networks and Communications*.

Kulabukhova, N., Ivashchenko, A., Tipikin, I., & Minin, I. (2019). Self-Sovereign Identity for IoT Devices. In *International Conference on Computational Science and Its Applications,* 472-484. Springer, Cham.

Kulabukhova, N., Ivashchenko, A., Tipikin, I., & Minin, I. (2019, July). Self-Sovereign Identity for IoT Devices. In *International Conference on Computational Science and Its Applications* (pp. 472-484). Springer, Cham.

Kurzweil, R. (2004). The law of accelerating returns. In *Alan Turing: Life and legacy of a great thinker* (pp. 381-416). Springer, Berlin, Heidelberg.

Lagutin, D., Kortesniemi, Y., Fotiou, N., & Siris, V. A. (2019). Enabling decentralised identifiers and verifiable credentials for constrained IoT devices using OAuth-based delegation. In *Proceedings of the Workshop on Decentralized IoT Systems and Security (DISS 2019), in Conjunction with the NDSS Symposium, San Diego, CA, USA* (Vol. 24).

Lee, E. A. (2006, October). Cyber-physical systems-are computing foundations adequate. In *Position paper for NSF workshop on cyber-physical systems: research motivation, techniques and roadmap* (Vol. 2, pp. 1-9).

Lee, E. A. (2008, May). Cyber physical systems: Design challenges. In *2008 11th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC)* (pp. 363-369). IEEE.

Loukas, G. (2015). *Cyber-physical attacks: A growing invisible threat*. Butterworth-Heinemann.

Lozano, C. V., & Vijayan, K. K. (2020). Literature review on Cyber Physical Systems Design. *Procedia Manufacturing*, *45*, 295-300.

Lueth, K. L. (2015). Will the industrial internet disrupt the smart factory of the future. *IoT Analytics, available online: https://iot-analytics. com/industrial-internet-disrupt-smart-factory/, accessed*, *3*, 2017.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80-86.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80-86.

Muzammal, M., Qu, Q., & Nasrulin, B. (2019). Renovating blockchain with distributed databases: An open source system. *Future generation computer systems*, *90*, 105-117.

Noizat, P. (2015). Blockchain electronic vote. In *Handbook of digital currency* (pp. 453-461). Academic Press.

Otto, N., Lee S., Sletten, B., Burnett, D., Sporny, M. and Ebert, K. "Verifiable Credentials Use Cases; W3C Working Group Note 24 September 2019" https://www.w3.org/TR/vc-use-cases/ [Accessed November 9, 2021]

Peer Mountain. 2021. This is Peer Mountain. https://peermountain.com/

Pivoto, D. G., de Almeida, L. F., da Rosa Righi, R., Rodrigues, J. J., Lugli, A. B., & Alberti, A. M. (2021). Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. *Journal of Manufacturing Systems*, *58*, 176-192.

Protocol Labs. (2017). “Filecoin: A Decentralized Storage Network”.

Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010, June). Cyber-physical systems: the next computing revolution. In *Design automation conference* (pp. 731-736). IEEE.

Reed, D., Sporny, M., Longley, D., Allen, C., Grand, R. and Sabadello, M.. (n.d.).“Decentralized Identifiers DID (v1.0)” https://w3c.github.io/did-core/ [Accessed November 9, 2021]

Schoenherr, T., & Tummala, V. R. (2007). Electronic procurement: a structured literature review and directions for future research. *International Journal of Procurement Management*, *1*(1-2), 8-37.

Shane, J. “Welcome to uPortlandia!” https://medium.com/ uport/welcome-to-uportlandia-2302e0d2ceb1 [Accessed December 30, 2020]

Shepherd, C., Arfaoui, G., Gurulian, I., Lee, R. P., Markantonakis, K., Akram, R. N., ... & Conchon, E. (2016). Secure and trusted execution: Past, present, and future-a critical review in the context of the internet of things and cyber-physical systems. In *2016 IEEE Trustcom/BigDataSE/ISPA*, 168-177.

Sorvin. (2021). Home Page. https://sovrin.org/

Stojmenovic, I. (2014). Machine-to-machine communications with in-network data aggregation, processing, and actuation for large-scale cyber-physical systems. *IEEE Internet of Things Journal*, *1*(2), 122-128.

Thramboulidis, K., & Christoulakis, F. (2016). UML4IoT—A UML-based approach to exploit IoT in cyber-physical manufacturing systems. *Computers in Industry*, *82*, 259-272.

Thramboulidis, K., Bochalis, P., & Bouloumpasis, J. (2017, October). A framework for MDE of IoT-based manufacturing cyber-physical systems. In *Proceedings of the seventh international conference on the internet of things* (pp. 1-8).

Thramboulidis, K., Vachtsevanou, D. C., & Solanos, A. (2018, May). Cyber-physical microservices: An IoT-based framework for manufacturing systems. In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)* (pp. 232-239). IEEE.

Treacy, C., & McCaffery, F. (2016). Data security overview for medical mobile apps assuring the confidentiality, integrity and availability of data in transmission. *International Journal on Advances in Security*, *9*(3 & 4), 146-157.

van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. (2019). Self-sovereign identity solutions: The necessity of blockchain technology. *arXiv preprint arXiv:1904.12816*.

Wagner, K., Némethi, B., Renieris, E., Lang, P., Brunet, E., & Holst, E. (2018). Self-sovereign identity: A position paper on blockchain enabled identity and the road ahead. *Identity Working Group of the German Blockchain Association (https://jolocom. io/wp-content/uploads/2018/10/Self-sovereign-Identity-_-Blockchain-Bundesverband-2018. pdf*.

Wan, J., Cai, H., & Zhou, K. (2015, January). Industrie 4.0: enabling technologies. In *Proceedings of 2015 international conference on intelligent computing and internet of things* (pp. 135-140). IEEE.

Weingaertner, T., & Camenzind, O. (2021). Identity of Things: Applying concepts from Self Sovereign Identity to IoT devices. *The Journal of The British Blockchain Association*, 21244.

Wolf, M., & Serpanos, D. N. (2020). *Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems*. Springer.

World Bank Group, & Global Partnership for Financial Inclusion. (2018). G20 Digital Identity Onboarding.

Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, *77*, 103201.

Yang, W., Wang, S., Zheng, G., Yang, J., & Valli, C. (2019). A privacy-preserving lightweight biometric system for internet of things security. *IEEE Communications Magazine*, *57*(3), 84-89.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). Ieee.

Zhou, K., Liu, T., & Zhou, L. (2015). August. Industry 4.0: Towards future industrial opportunities and challenges. In *Fuzzy Systems and Knowledge Discovery (FSKD), 2015 12th International Conference on*, 2147-2152.