CRANFIELD UNIVERSITY

JAVIER GRAU MARTINEZ

DEVELOPING A BLOCKCHAIN BASED CYBER SECURITY FRAMEWORK FOR CYBER PHYSICAL SYSTEMS

SCHOOL OF AEROSPACE, TRANSPORT AND MANUFACTURING
Engineering and Management of Manufacturing Systems

MSc THESIS
Academic Year: 2017 - 2018

Supervisor: Dr. He Hongmei, Professor Rajkumar Roy

September 2018

CRANFIELD UNIVERSITY

SCHOOL OF AEROSPACE, TRANSPORT AND MANUFACTURING
Engineering and Management of Manufacturing Systems

MSc THESIS

Academic Year 2017 - 2018

JAVIER GRAU MARTINEZ

DEVELOPING A BLOCKCHAIN BASED CYBER SECURITY FRAMEWORK FOR CYBER PHYSICAL SYSTEMS

Supervisor: Dr. He Hongmei, Professor Rajkumar Roy.

September 2018

This thesis is submitted in partial fulfilment of the requirements for the degree of Master of Science

ABSTRACT

The internet of Things is growing exponentially over the last years. Despite its massive use in the current industry integrating IoT with cyber physical systems, IoT systems still suffer from privacy and security vulnerabilities. The huge amount of data generated and shared by cyber physical systems is the main target for most of the cyberattacks. Sensitive data generated by thousands of sensors can be stolen or tampered causing huge damage to the companies. In addition, the data storing in data bases, is managed with a centralized server which obliges trusting in Third Party Auditors, who may not fulfill the privacy and confidentiality requirements. Many security techniques have been developed to increase the robustness of the industry control systems. This report is focused on describing and designing a blockchain framework to enhance the security of the industry control systems against cyberattacks. The current solution is based on a distributed network that brings distributed access control and data management. This framework design also enables secure data sharing providing thus security and privacy for IoT applications.

Keywords:

Internet of things, IoT architecture, cyber physical systems vulnerabilities, cyberattacks, communication protocol, blockchain architecture, decentralisation, data flow diagram, use case diagram, consensus mechanism.

ACKNOWLEDGEMENTS

First, I would like to thank my academic supervisors Dr. He Hongmei (Mary) and Professor Rajkumar Roy for allowing me to develop the current individual project. I also would like to express my gratitude for their guidance, support and direction.

I would like to thank Mary again for all the feedback given during the project and for the meetings we had during the past three months. It has been a huge contribution to achieve my objectives.

Thanks to Cranfield University for the opportunity given during this course. MSc engineering and management of manufacturing systems for its big contribution for my individual career and for granting me the opportunity to know excellent engineers from all around the world.

Finally, I would like to thank my family and my girlfriend who always have supported me.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABREVIATIONS

IoT	Internet of things
CPS	Cyber physical systems
BC	Blockchain
CH	Cluster Head
FM	Framework
I/O	Input/output
UML	Unified Modelling Language
LN	Local Network
OL	Overlay Network
CS	Cloud Storage
RFID	Radio frequency identification
WSN	Wireless sensor network

1 Introduction

The current individual project focuses on the protection of a cyber physical system against cyber threats using blockchain techniques. The aim of this research is to develop a block chain framework able to prevent cyber-attacks and build a trustworthy working environment within the cyber physical systems and the industrial infrastructure. Nowadays this is a crucial step because of the huge amount of data generated and stored in data bases managed by third parties. Availability, confidentiality and integrity of the data must be the main priority.

1.1. Research background

To ensure the total understanding of the project, next some explanation about technical concepts.

IoT: The internet of thing comprises a network of interconnected devices, which can share, receive and control data generated in real time with other devices. Through IoT systems it is possible to control the real world remotely with a simple click. Smart objects are those connected to the internet and can share the data created in real time. This network is based on the RFID (radio frequency identification) and WSN (wireless sensor network) technology which allows the data identification and monitoring.

CPS: Cyber physical system. It is a system able to interact with humans through computer programmes. It has integrated computational and physical capabilities, so it can exchange information in real time with the user while doing a task. Industry 4.0 integrate CPS in the manufacturing processes.

1.2. Research Motivation

It is vital nowadays for the companies to protect against cyber-attacks. Currently the enterprises generate and handle huge amount of sensitive information which can be exposed and stolen very easily by expert hackers or malware.

To change the way the companies, store the master data would be a great advance. Nowadays the IoT systems are stirring up the data management, enabling to interconnect a huge devices network sharing data with a central server. The possibility of information access through decentralized block chain systems ensure the users to handle the information stored in a transparent and safety way. This is because the architecture of the blockchain prevents to modify the information stored in the system's nodes due to the verification of every transaction done within this technology creating a safety and trustworthy culture.

In the information era, it is vital to manage it in a safety, transparent and fast way. Blockchain technology allows the users to handle and manage the data in a trustworthy environment. It is also an open door to the future since many different applications and technologies will be developed supported by this incredible and powerful technology.

1.3. Aim and objectives

The aim of this research is to protect IoT enabled CPS using blockchain technologies. Following, the different objectives are explained:

- To make a thorough research about current techniques for protection of CPS, cybersecurity and blockchain CPS applications.
- To identify the main vulnerabilities in IoT enabled CP systems.
- To create a data flow chart in the cyber physical system.
- To develop a use a case diagram to identify the different stakeholders, roles and evaluate the safety concerns within the CPS.

- To develop a block chain framework that generates a trustworthy environment through the confidentiality, integrity and availability from an encryption algorithm that guarantees total transparency.
- To design a blockchain framework transaction diagrams.

1.4. Research questions

- What is the level of cyberthreats against manufacturing systems?

With the rise in the number of CPS connected to the IoT networks the opportunities of being attacked by hackers increase dramatically. In the past there have been different examples where hackers managed to break the conventional security systems and compromise the manufacturing systems, threating the operators and infrastructure security (Sturm *et al.*, 2014). Cyber-attacks can be directed very specifically, damaging concrete parts of the manufacturing processes or tampering data with the objective of cause damage without being detected and even change the ultimate quality of the product. Manufacturing systems can involve many different subsystems like control systems, quality systems, production systems etc… Hence, they can be attacked from different perspectives making it more challenging to protect the whole system. Efforts must be directed in achieving integral protection. In addition, security guarantees offered by third parties involved in the manufacturing processes e.g. CAD programmes encryption, cloud storage, etc… could be assaulted if enough computational resources are invested by the attackers (Wells *et al.*, 2013).

- What is the need of this research?

There is a need for new cyber security techniques to improve the robustness and reliability of the manufacturing systems against cyber threats and address most of the cyberattacks. Nowadays cyber attackers with enough computational resources could manage to break into any manufacturing system. To prevent cyber physical systems being attacked by conventional cyber threats, a

blockchain technique framework is integrated in the manufacturing systems. New blockchain techniques present new features like decentralization and immutability that could guarantee the confidentiality, availability and integrity of the data. Transactions could be safely stored in a private or public blockchain and available for every member of the network. Later, thorough explanation about the applications of this new technology in the cyber security field.

1.5. Thesis structure

The thesis structure is divided as follows: In the current chapter a little introduction about the project. In chapter 2 the literature review, containing a thorough research about the technologies appearing in the thesis. During chapter 3 an exhaustive explanation about the architecture of a cyber physical system and its different layers. In chapter 4 a blockchain framework is designed addressing the main vulnerabilities affecting the networks. Regarding chapter 5 a discussion of how this new technology tackles the principal threats of the cyber-attackers. Finally, in the last chapter, a conclusion and future work of the project. At the end of the thesis there is a references list.

1.6. Methodology

The project's first step is a thorough research to clearly understand the current security issues of the CPS and to have a clear picture of all the possible cyber threats that may cause a serious damage to the industrial infrastructure. Studying in deep all the aspects related to the block chain technology and techniques, and the understanding of the new applications related to these revolutionary techniques. The information must come from scientific articles, universities and organisations from this technological sector researches and specialized books. This research forms the literature review.

Once the literature review is done, the next step is the deeply study and understanding of the CPS subject functioning where the blockchain techniques will be integrated. It will be needed the help of the CPS's instructions manual, and the explanation and guidance of the operator in charge of the current cyber physical system. Apart from this, a deeply research about different examples of CPS data flow charts to make a clear picture of how these systems works, collects, extracts and shares the information through IoT systems and which parts are the most vulnerable.

After understanding how the CPS manages the data, the next step is to create a data flow chart using a diagram maker software. This diagram will explain in detail the different levels of communication within the CPS and, the information flow through the IoT systems.

It is also a part of the project to analyse and to use the case diagram of the autonomous system to identify the different stakeholders that are taking part in the project and their roles.

From this point, with a total understanding of the CPS working and data management, the last part of the project consists in the development and design of the blockchain framework which prevents and avoids any kind of cyber-attacks by applying the blockchain techniques and its benefits to the cyber physical systems. It consists on creating a valid model of the blockchain methodology which implements its advantages to tackle the safety and transparency objectives. The model designed will be thoroughly explained to understand how this framework will reach all the objectives above set.

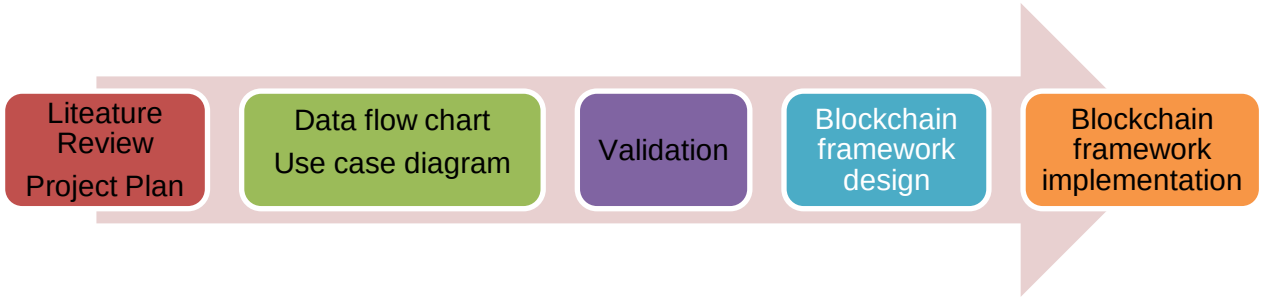

Figure 1 Methodology diagram

2 Literature review

2.1. Security vulnerabilities in IoT enabled CPS

2.1.1. Introduction

Nowadays more and more electronic devices all around the world are being connected creating a huge network. This network called internet of things (IoT) is an emerging technology which enables cyber physical systems (CPS) to identify, send, receive and share information through the working network in real time, allowing users of the network to interact, communicate and to act autonomously with minor human need. According to (Bhuvaneswari and Porkodi, 2014), the IoT provides interaction among the real and virtual world. Entities have virtual representation and the thigs become context aware as they can sense, interact, exchange data and information. The advantages behind this technology are countless and this is because the wide range of applications where IoT can successfully be implemented different domains such as society, environment and industry. Some of the main applications are: smart cities, smart farms, smart water recycling, supply chain, logistics, etc.…(Bhuvaneswari and Porkodi, 2014). It is changing our lifestyle. Now more resources are available in less time, and it is an open door for further growth and future innovation. It is expected by 2020 more than 28 billion identifiable devices will be connected through IoT network generating a 1.7$ trillion market (Jayaraman *et al.*, 2017). However, there are some other disadvantages too. This huge network will also be the main target of cyberattacks and threats, trying to reach the sensitive information circulation through the CPS network and putting all users in risk.

As IoT is a technology based on the internet connection, all the threats existing on the internet are also propagated through the IoT network. For this reason, before deploying a vast network of interconnected devices sharing huge amounts of sensitive information within a CPS it is necessary to sort every kind of cyber

threats, to design properly a security architecture that protects, prevents and avoids cyberattacks targeting the IoT network in the CPS. It is also important to understand the architecture of the IoT network, and its different communication levels.

2.1.2. **Internet of things enabled Cyber Physical Systems**

As every day the total amount of cyber physical systems, which are systems that manage and control physical processes, provided with electronics and computational capabilities and internet connection is dramatically increasing, the IoT systems are growing up allowing the introduction of novel applications. Production systems are now more competitive because of the use of the IoT systems. Productivity has been improved because of a smart use of resources, high monitor and supply chain traceability and high flexibility enhancing the individualized production are the key improvements regarding the IoT systems production integration. Smart factories are based on CPS which organise and manage the production process because of the resources identification and labelling. Every product is monitored and controlled converting it into smart products, so it is possible to know in every moment the resources data such as cost, availability, material, etc. The data generated is also stored in a database (Sadeghi, Wachsmann and Waidner, 2015).

IoT systems brings security challenges like privacy, integrity, availability and resources challenges such as information standardization, energy management systems and scalability.

2.1.3. **IoT architecture and enabling technologies**

The IoT network is based on different layers: Perception layer, network layer, middleware layer, application layer and business layer (Khan *et al.*, 2012) (Al-Fuqaha *et al.*, 2015) (Jing *et al.*, 2014).

- Perception layer: This is the base layer, and it is comprised of the physical objects and connected devices. Its main objective is to identify and gather devices information.
- Network layer: This layer transmits the information gathered from devices to an information processing system. The information is transferred thus between the physical and middleware layer. Different technologies support the data transmission such as, 3G, Wi-Fi, Bluetooth, infrared, etc.
- Middleware layer: This layer receives the information coming from the previous layer and store it in the data base. This layer is also in charge of the service management. Every device deploys a specific kind of service, and only devices with the same service can be connected.
- Application layer: This layer manages the application based on the information processed in the middleware layer.
- Business layer: The last layer is responsible of the overall management of the IoT system. In charge of the results analysis and the business model building.

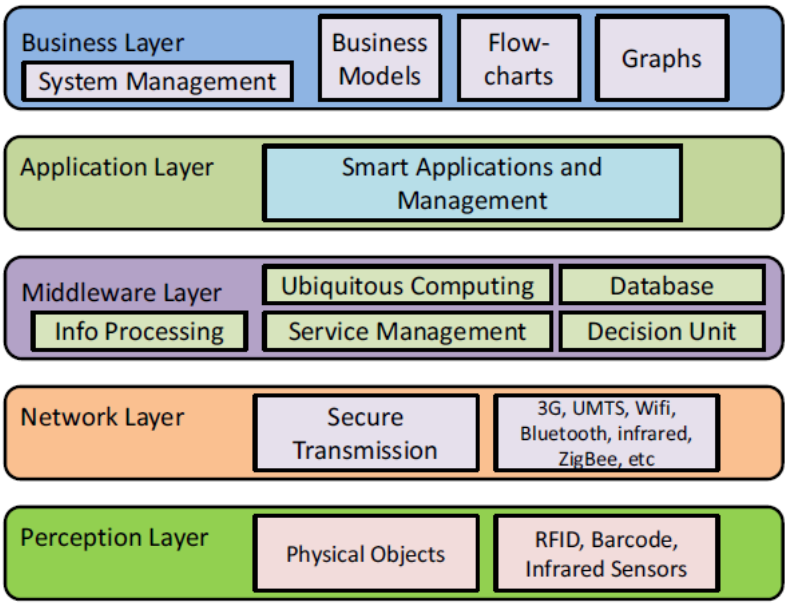

Figure 2 IoT architecture (Khan et al., 2012)

IoT systems are implemented using the next three following enabling technologies (Hadjichristofi, 2015) (Al-Fuqaha *et al.*, 2015).

- RFID (Radio frequency identification): This technology allows the data identification using labels acting like electronic barcodes. These tags are attached in microchips in the objects that are going to be identified.
- WSN (Wireless sensor network): Small devices, low powered that use sensors to monitor and track the environmental data. This system is wireless connected with the rest of nodes of the system.
- Cloud computing: enable ubiquitous powerful sensing data processing to be smart stored, enabling the access from other smart devices.

2.1.4. **Security challenges**

In the IoT system there are four elements interconnected, which are: People, object, software and hardware (Abomhara, 2014). Thus, all of them carry on associated security challenges into the IoT system such as confidentiality, open trust and privacy. There are also additional threats coming from the technologies working together and the open standards in the CPS.

The main target in terms of cyber-attacks is the data collected within the CPS. The devices network collects sensitive data from all the productive process which can be used for malicious purposes. These are the most challenging security issues to address (Abomhara, 2014):

- User privacy and data protection: Since data is collected and shared in internet and due to its ubiquitous features, the data protection is key to develop a thriving IoT network.
- Authentication and identity management: IoT network requires the authentication and identification of thousands of different devices, and all of them must be identified uniquely.
- Trust management: Trust plays an important role in terms of communication. It is vital to build a trustworthy environment to secure communication between things. There are two levels of trust: First level between entities and the second level between the system and the user.
- Authorization and access control: Authorization determines once the user, object or device is identifying whether it has access or not to the system according to previous criteria.

- End to end security: The identity of the users must be verified in both ends of the communication by implementing protocols and algorithms.
- Attack resistant security solution: Generally, the electronic devices used in the IoT systems have a low computational power, making them vulnerable to cyber-attacks. It is needed a certain level of security in every single device to mitigate this threat.

2.1.5. **IoT attacks and vulnerabilities into CPS**

IoT attacks classification is divided in four main groups which are: Physical, Network, Software and Encryption attacks. According to this classification these are the principal kind of attacks IoT systems are liable to deal with (Hadjichristofi, 2015).

A. Physical attacks: This kind of attack is targeting the hardware elements comprising the IoT enabled CPS system. The attacker must be close to the network to perform the attack. The most common physical attacks are listed below.

    - Node tampering: Cause damage to the node by replacing it or some parts of it to subtract sensitive data.
    - RF interface on RFID: Causing a denial of service by introducing noise in the radio frequency so it is impossible to identify the message.
    - Node jamming in WSN: Denying communication between nodes by interfering the radio frequencies of the wireless sensors.
    - Malicious node injection: Man in the middle attack, it is based on integrate a malicious node between two nodes to intercept the data.
    - Physical damage: Cause damage to the system with the aim of avoiding the availability.
    - Social engineering: IoT user's system manipulation to gain access to the sensitive data.
    - Sleep deprivation attack: Modify the battery life of the different nodes by increasing its use, causing availability issues.
    - Malicious code injection: Gaining access to the node information through virus, USB stick with malicious software, etc.

B. Network attacks: This kind of attack is targeting the network systems and they can be deploy remotely.

- Traffic analysis attack: Using sniffing applications like port scanning or packet sniffer.
- RFID spoofing: The attacker spoofs a RFID signal copying the information of the RFID tag and sending it pretending to be valid and hence, gaining access to the network.
- RFID cloning: The attacker clones a RFID tag to access the information, however the original ID is not replicated and making this attack distinguishable unlike the RFID spoofing.
- RFID unauthorised access: Because of a lack of authenticating procedures the attacker penetrates the network.
- Sinkhole attack: Traffic luring from de WSN breaking the confidentiality of the data and causing a denial of service because of the impossibility to deliver the data packages forward.
- Man in the middle: The attacker causes an interference between two nodes creating a misconnection and gaining access to all the data transferred between both nodes.
- Denial of service: Overload caused by a large amount of data input to the system.
- Routing information attacks: Tampering information routes, creating loops or allowing dropping traffic, etc.
- Sybil attack: Integration of a malicious node that identifies other nodes leading to false information acceptation by other nodes.

C. Software attacks: It is the most vulnerable part in the CPS. Attackers can tamper the information, steal data, deny service, etc.

- Phishing attacks: The attacker gains access to the system by spoofing the authentication credentials from infected e-mails or malicious websites.
- Virus, worms, trojan horse, spyware and aware: The attacker can infect a system with malicious software.
- Malicious scripts: Running executable active-x scripts to trick the user and gain access to sensitive data.
- Denial of service: The attacker can generate a DoS or DDoS into the application layer, avoiding other users to enter the system and getting control of the system.

D. Encryption attacks: Based on break the encryption scheme.

- Side channel attacks: The attacker gets the encryption key for encrypting and decrypting data.
- Cryptanalysis attack: Breaking the encryption scheme.
- Man in the middle attack: When attacker intercepts signals between two users and perform a key exchange.

2.2. Current techniques for IoT enabled CPS protection

In this section of the literature review, the most important and wide used protection techniques against cyber-attacks targeting IoT enabled cyber physical systems will be described. It is important to focus on the different layers available in the IoT systems to protect all of them against possible threats and guarantee the confidentiality, authenticity and integrity of data in the IoT systems. These techniques aim to address the main vulnerabilities of the IoT enabled CP systems before described. The main objective thus, is to design a security architecture able to achieve the fastest time to market, highest quality, lowest cost, best service, cleanest environment and high knowledge (He *et al.*, 2016), and to do so it is necessary to combine several protection techniques to cover all the different layers vulnerabilities.

- Encryption mechanism: There are many different types of encryption available in the security systems all around the world. To down select the kind of encryption that fits best with the IoT enabled CPS it is basic to be aware of the properties of the small electronic devices due to the wide variety of algorithms and its processing power capabilities. Just as an example and to be explained in the present literature review, two different encryption mechanisms are explained.
  On the one hand, the by-hop encryption mechanism is used to encrypt the information in the transmission process. This means every node must

keep plaintext from encryption and decryption operations. Within by-hop encryption only links that must be secured are encrypted. The main characteristics of the by-hop encryption are: high efficiency, low latency, low cost…etc.

On the other hand, the end to end encryption provides high security while only the two interested parts can share the information so in the transmission process the information will be encrypted. This method demands an authentication step to avoid MITM attacks. (Gan, Lu and Jiang, 2011).

- Secure routing: The fact that the processing power of the small devices comprising an IoT network is reduced, there is a big impact when it comes to address the security of the communication in the different layers of the system. However, there are different communication protocols that can be used to address the privacy challenges. These protocols are e.g. TLS/SS or IPSec. The first one is used to encrypt the link in the transportation layer, and the second one is to guarantee the security of the network layer. Both protocols address the integrity, availability and confidentiality in different layers (Suo *et al.*, 2012)(Jayaraman *et al.*, 2017)(Punia, Jaiswal and Gupta, 2017).

- Sensor data protection: Nowadays sensors generate huge amount of data. For this reason, it is necessary to develop different procedures to protect the data generated within the sensing systems to protect the objects and people identity and to prevent this data to be leaked and so guarantee the privacy.

- Cryptographic algorithms: There are many different algorithms applied to address the security challenges of internet networks. Next, the most important algorithms are named as follows: 1 Symmetric encryption algorithm is used to guarantee the confidentiality. 2 Asymmetric encryption algorithm is used to digital signatures and key transport. 3 The Diffie-hellman asymmetric key agreement. 4 Secure hash algorithms to guarantee the integrity (Suo *et al.*, 2012).

  The main problem related to this technique is the low computational power of the small devices and sensors integrating the IoT enabled CP system

and its low capability to process a highly complex algorithm. Currently many exhaustive researches are being made in this field.

- Authentication: These techniques are used to identify a user by applying biometrical methods alongside the development of specific algorithms that enable the individual recognition such as, finger prints or facial scanners. (He *et al.*, 2016)

- RFID security protocols: In terms of radio frequency identification there are already many different security protocols existing. Again, the down selection of the appropriate security protocol depends on the properties of the electronic devices and their computational capabilities. As an example, two different protocols are named: EMAP (efficient mutual authentication protocol) guarantees pseudonymise of the data of the tag stored. ASRAC (advanced semi randomized access control) uses random number generation in tags to prevent replay attacks (Daou, Kayssi and Chehab, 2008).

2.3. **Research on blockchain.**

2.3.1. **Introduction**

Blockchain has many different valid definitions depending on the application perspective. Some of them are shown next.

Blockchain is a peer to peer distributed shared ledger of transactions. Those transactions are gathered in blocks via consensus among peers. The blockchain is immutable and cryptographically secure (Crosby *et al.*, 2016).

Blockchain is a decentralized consensus mechanism. All peers in a blockchain need to come to an agreement to validate a transaction (Imran Bashir, 2017).

2.3.2. **Blockchain Network**

Blockchain constitute a peer to peer distributed network layer running on top of the internet. As it is shown in the image below, internet is the base of the blockchain network.

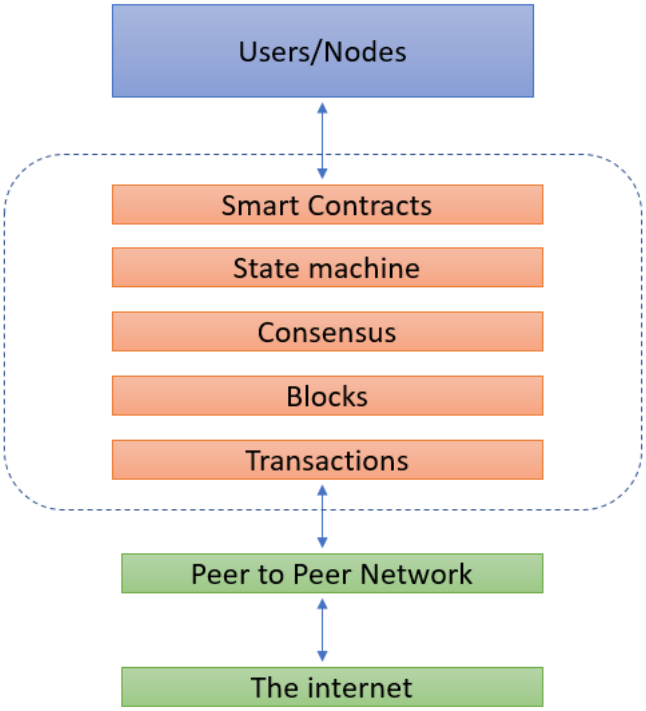

Figure 3 Blockchain network

2.3.3. **Blockchain structure**

As the name itself indicates, the blockchain structure is comprised of different blocks chained together. A block is simply a number of transactions gathered forming a transactions group. The size of each block depends on the blockchain design. The first block of the blockchain is called genesis block and it is hardcoded in the very moment the new blockchain starts. From this point beyond all the blocks add a reference to the previous block called hash pointer. Generally,

the basic structure of a single block is comprised of elements such as: timestamp, nonce and hash pointer. The following image shows the general structure of a blockchain (Imran Bashir, 2017).

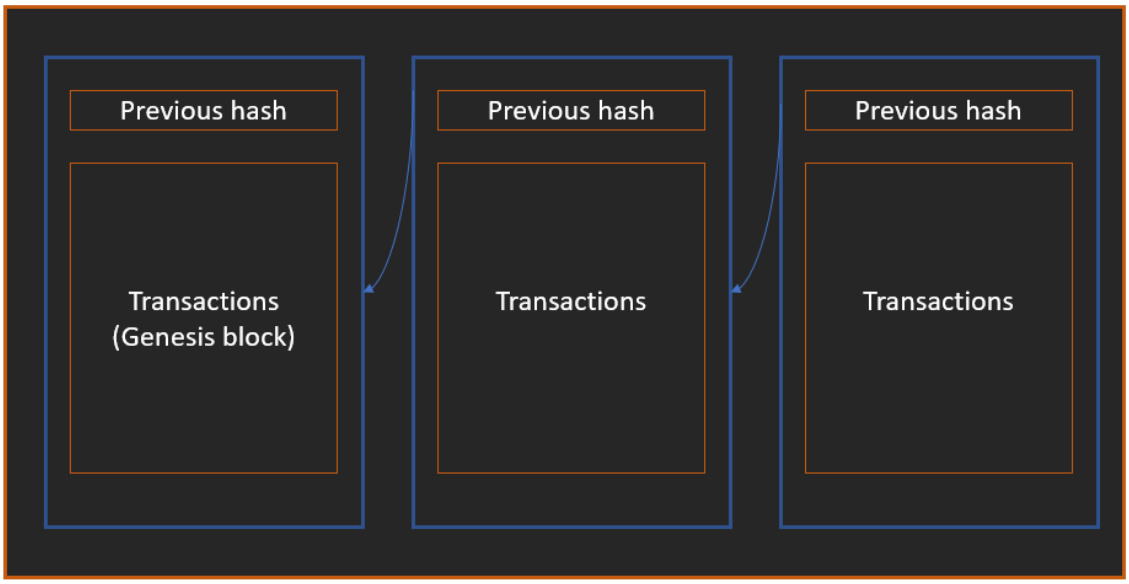

Figure 4 Blockchain structure

2.3.4. **Adding blocks procedure**

1. A transaction is first started by signing it with its node private key.

2. Through a consensus peer to peer mechanism, normally PoW (proof of work) the created transaction is validated. It takes more than one node to validate the transaction.

3. After the validating process is completed, the transaction is added into the block, generating a copy of the current block in every node participating in the current blockchain network.

4. Further blocks added into the chain are linked cryptographically back to the previous block through what is called the hash pointer.

2.3.5. **Advantages and limitations**

Blockchain is a revolutionary technology which is called to change the transactions method. Nowadays it is required a third party to guarantee the compliance of the any transaction, with all the inconvenience associated to it. Next, some of the main advantages of the blockchain technology are cited (Wright and Filippi, no date).

- Decentralization: As was mentioned above, decentralization is the main feature underpinned by the blockchain technology. It means that the third party is not required anymore to validate and guarantee that all the requirements are met. Instead a consensus mechanism validates the transactions. In the case of Bitcoin, which is the most popular blockchain network, the consensus mechanism used is called Proof of Work.

- Transparency and trust: As every node has a copy of the blockchain, transactions are easily available from every different node of the network. This allows the system to be trustworthy and transparent.

- Immutability: To modify a transaction already validated, the attacker must tamper data from huge amount of different interconnected nodes, due to the shareable feature. Moreover, this would demand a huge energy and resources consumption, making it almost impossible in large blockchain networks.

- High availability: Blockchain is based on thousands of nodes peer to peer connected, and every single node possesses its own copy making the whole system highly available.

- Highly secure: Blockchain transactions are cryptographically secured providing thus, integrity.

- Simplification of business model: The possibility of sharing a common ledger among different entities and thus, offering the availability of the blockchain technology supported by the same system represents an excellent improvement spot rather than the current disorganized systems

deployed in many industries such as finance or health, where different entities must handle their own data bases created in their own systems.

- Faster transactions: The only requirement to validate the transaction is the consensus mechanism between two different nodes, making it faster.

- Cost saving: The fact that blockchain allows to eliminate the third party to guarantee and validate the transaction requirement, eliminates the involved costs in the form of fees demanded by the third party.

On the other hand, this new technology, thus still immature present different challenges that must be tackled and currently they are under investigation. Some of them are (Imran Bashir, 2017):

- Scalability: Blockchain is a rigid system making it difficult to adapt new specifications.
- Regulation: Currently there is a lack of regulation regarding the blockchain application, especially the financial ones.
- New technology: It is still an immature technology whether there is still a lot of upgrading potential regarding blockchain networks.

2.3.6. **Types of blockchain**

Due to the nature of the blockchain it can be used in different ways according to the specific requirements of the final users. Next the main blockchain types are described (Zheng *et al.*, 2017).

- Public blockchain: These are open to the public, it means that the blockchain is not owned by anyone. Anyone can access and make regular transactions. After the validation process every node has an own copy of the blockchain.

- Private blockchain: Only a group of people or specific entities have access to the private blockchain.

- Semi-private blockchains: The private part is controlled by an organization or a group of individuals while the public part has an open access.

- Sidechains: Coins can be moved from one blockchain to other and move back. Commonly used to create new altcoins. Coins are used as a consensus mechanism.

- Permission ledger: The participants are already known and trusted, so it is not necessary a consensus mechanism. Instead an agreement protocol is used.

- Distributed ledger: Distributed ledger within the participants and organizations. The transactions are stored contiguously instead of into blocks.
- Tokenized blockchains: Generate cryptocurrency out of the mining process or initial distribution.

2.4. The applications of blockchain in IoT enabled CPS and cybersecurity

2.4.1. Introduction

Due to the blockchain nature this revolutionary technology can be implemented in very different business models and applications. Because of the high availability, integrity and decentralized management, many different applications can be underpinned by the blockchain systems, specially, those that generates huge amount of data such as IoT systems, health, finance sectors, supply chains, etc. Sharing data in a secure and fast way with a large variety of partners in real time is now more feasible than ever and a lot of scientific research is being carried on nowadays in this matter.

2.4.2. **Blockchain applications**

Coming next, some of the most important blockchain applications are introduced:

- Currency: Nowadays it is possible to realize payments with what is called cryptocurrency which is supported by the blockchain technology. In fact, Bitcoin, is the first blockchain ever, deployed in 2008 and invented by Satoshi Nakamoto. Nowadays there are thousands of different cryptos. Ethereum, Ripple, Litecoin, Bitcoin Cash, ADA, Eos, Iota, are some examples of them. They have become very popular recently increasing their value in some cases x10, x30, x100 or even more than x1000. Of course, cryptos are an open door in the financial revolution due to the fees elimination (Herbert and Litchfield, 2015) (Paper, 2016).

- Financial services: Because of the low efficiency of the current systems in terms of payment and transactions processing, blockchain stands for substituting the conventional financial services, more specifically in assets management by encrypting the records, making transactions easier and without a third party. Also payments (specially cross-border) would become much faster under this new technology (Crosby *et al.*, 2016).

- Smart contracts: It consists on a virtual contract created from programming language where previous conditions are established between the two interested parties so when those real-life conditions are accomplished and the data is analysed by the smart contract it gets executed (Foroglou and Tsilidou, 2015). Smart contracts are underpinned by the second generation of blockchain, and represent an advantage to authenticate users and transactions and validate payments, identities, transactions etc… (Christidis and Devetsikiotis, 2016)

- Smart property: Every property that has embedded smart technology can be stored in a private or public shared ledger, showing property details and relevant information. IoT are a supporting technology for smart properties combined along with the blockchain, connecting thus, every smart device in a huge peer to peer network sharing data in real time in a decentralized way. A good example of IoT is found in the supply chain where thousands of sensors are working together and uploading data constantly.

- Health sector: Personal patients' records can be stored in a decentralized way, leading to a total information sharing and allowing doctors to access the patients records from everywhere due to the peer to peer features (Mettler, 2016) (Xia *et al.*, 2017).

- Cyber security: Blockchain techniques can be applied to store sensitive information in a safe chain of transactions, allowing only the right users to gain access and preventing to modify the information already stored in the blockchain. A vital part of the safety improvement is the introduction of the smart contracts, to guarantee that all the requirements needed to execute a command or an action are fulfilled in advance. Decentralisation provides high availability, so every single node connected to the network and with the previous authentication possess an immutable copy of the blockchain. Data management is easier to control and tampering transactions is highly improbable. To penetrate a blockchain successfully the attacker must gain control over the major part of the blockchain, which is practically impossible due to the large number of nodes belonging to the same chain, requiring thus, huge amount of computational power (Liang *et al.*, 2018).

2.4.3. **Blockchain in IoT enabled CPS**

As IoT systems are increasing the number of interconnected devices year by year and thus, the amount of data uploaded and shared, it is contributing to strengthen the weaknesses such as privacy, security and data management. With the blockchain implementation within the IoT enabled CPS some of the main current challenges such as transparency, availability, trustworthiness and cybersecurity can be tackled.

Thanks to the tools provided by the blockchain technology it is possible to upgrade the IoT systems by turning them into decentralized systems. This is a key benefit though. This allows the electronic devices and sensors to share and upload the data in real time with every partner or entity participating directly in the blockchain network combined with a peer to peer storage system. The need of a central management is not required anymore. The data uploaded to the system is copied in all the different nodes all around the network, making it accessible and available for everyone involved in. Of course, to do so, first step is to validate

all the transactions stored into the blocks. Then, it is necessary to make use of consensus mechanisms where different nodes validate the transactions commonly through the Proof of work (there are other mechanisms, specially, in private networks). The consensus mechanism is preventing attacks such as DoS or data tampering. On top of that, with the smart contracts, which give the ability to set external conditions within a programming language it is possible to manage the IoT devices and the data produced as it is better for every different business e.g. triggering actions whenever a meter is recording any kind of values that require a corrective or preventive action.

Now it is possible to control and monitor everything. Smart contracts along with smart devices are now changing the current rules. Interconnecting this whole network of IoT within the direct benefits of the blockchain is the industry future (Huh, Cho and Kim, 2017) (Gantait, Patra and Mukherjee, 2017).

2.4.4. Blockchain protection against cyberattacks targeting IoT enabled CPS

In the final section of the literature review, the security benefits of the blockchain technology are discussed. In an overall view, given a large CP system where interconnected device are constantly generating, sending and receiving data in a conventional centralized management security threatens come up. Data tampering, DDoS or false data injection attack are some of the current cyber threats centralized data management is exposed to (Puthal *et al.*, 2018).

In terms of addressing the security issues regarding the conventional systems, blockchain techniques show up revolutionary security measurements.

The most important advantage in terms of cyber security, is the architecture of the blockchain. The fact that blockchain is a distributed ledger means that every record and every transaction recorded is automatically shared in a peer to peer

network, where every node gets a copy of the block where the transactions are stored (MATANOVIĆ, 2017).

The main idea is to build a private blockchain within the CPS. All data generated by sensors flows between nodes in a decentralized way, eliminating the DoS, FDIA and so forth threats. Trusting methods and consensus mechanisms are required to validate the transactions between nodes and to verify that the information is secure. The data collected by the different authorized nodes is encrypted and broadcasted to other nodes. A private key of every node is used to encrypt the message digest forming a signature. After the information arrives to another node, the message is decrypted by using the public key (Liang *et al.*, 2018). In this case as the data measured is done by the authorized and proposed node it is no longer necessary to check previous blocks of the chain, improving and increasing the efficiency and the speed of the system.

Moreover, the double spending attack would not be a threat in this kind of system, due to the automatic transactions between nodes. It means that the interaction of humans would not be necessary. However, what is called ‘51% attack’ is more likely to happen because of the smaller number of nodes belonging to the network.

There are some disadvantages with this kind of systems:

The first one is the big amount of time required to install all the sensors (which must have a certain degree of computational power) and setting new communication networks.

The second disadvantage is the physical attacks threaten. This kind of danger is described in the previous sections and it is the hardest to fully control or eliminate.

The third disadvantage is the redundancy of the data because of the blockchain architecture and the automatic data node copies. However, this disadvantage can be addressed or mitigated by restricting the read-permission or allowing to certain nodes the self-destruction of data to release space enough for further data flow.

This feature is highly important due to the limited computational capabilities of the small electronic sensors integrating a CPS.

3 Cyber Physical System data flow chart and use case

3.1. Introduction

In this section the main objective is based on describing both the data itinerary across a cyber physical system and the data structure of the system used to apply the blockchain framework taken as a reference model. A CP system has been taken as a model in the laboratory to make a thorough study of its internal structure and its communication system. Blockchain techniques will be applied to protect the data stored and generated by the sensors against cyber threats and cyberattacks.

To do so, it is vital firstly to understand the different communication layers within the system and thus, map the internal structure of the CPS communication with the different IoT layers and stakeholders. This overall view allows to identify vulnerable spots and match the different layers with different security techniques that fits best with each one.

3.2. CPS description and internal structure

To understand the data flow and the communication structure followed by the current CPS study, it is important firstly to define the different electronic devices that form the whole system. Next, a little introduction of the different parts used in the CPS will be given.

- Process control machine: It is a computer with a programming language software installed. This code is developed and sent to the PLC which is processing the code.

- PLC: This is a programmable logic controller. It is used to control the connected machine directly off server. The program is developed in TIA software.
- External I/O module: Scalable and flexible system that enables the connection of process signals through an interface module. It oversees the processing of the input/output signals of the controlled machine through a CPU module.
- Ethernet Industrial switch: This device allows the internet connection. Basic for IoT networks. The data generated by the CPS can be uploaded and shared online.
- HMI: Touch screen interface for operation control. This allows the operator e.g. to easily start or stop the system. The functions controlled by the HMI can be programmed with the TIA software.
- Industrial robot: Fischertechnik 96785 Punching machine with conveyor belt. This machine is equipped with two light sensors to detect initial and final conveyor belt position, and two actuators, one for punching task and other to move the conveyor.

3.3. **Data communication protocol**

To better understand how the internal communication of the cyber physical system works, it is necessary firstly to know the protocol followed to complete the internal communication among the different modules within the cyber physical system successfully.

Profinet is an industrial communication system used in all levels of an industrial automation system, (field-level networks, control-level networks and information-level networks). Its functionalities allow the data transaction in real time between different levels and modules and provides direct access also in a wireless configuration.

At the field level the distributed devices can communicate and transfer data with the autonomous system in real time. Devices such as sensors, actuators, I/O modules belong to the field level.

Regarding the control level, controllers like PLCs and IPCs communicate each other and with the IT systems through TCP/IP and Ethernet standards. Those are supported by the Profinet functionalities.

The plant level controller manages the whole automation system after gathering and analysing the information from the lower levels.

The Profinet protocol defines a vendor-independent standard to allow the communication through Ethernet with IT systems, providing direct access from the office world to the automation system levels (Belai and Drahoš, 2009)((PNO), 2014)(Sa *et al.*, 1822) .

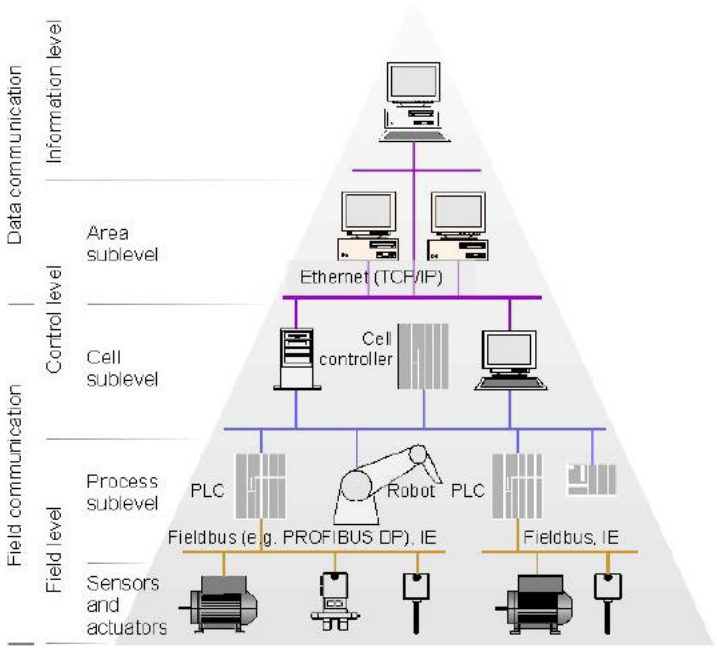

Figure 5 Autonomous system communication hierarchy.

3.4. Data itinerary & UML data flow diagram

After understanding the data transmission and communication between the different modules and levels within the cyber physical system based on the Profinet protocol, it is time to explain the data itinerary across the system.

The process starts in the process machine control, where using the TIA software (totally integrated automation software by Siemens) a code is developed according to the needs required by the manufacturing process. The process is totally designed in this step, but it can be modified easily in case there is a requirement modification. Next, an example of the programming language used to implement the manufacturing process.

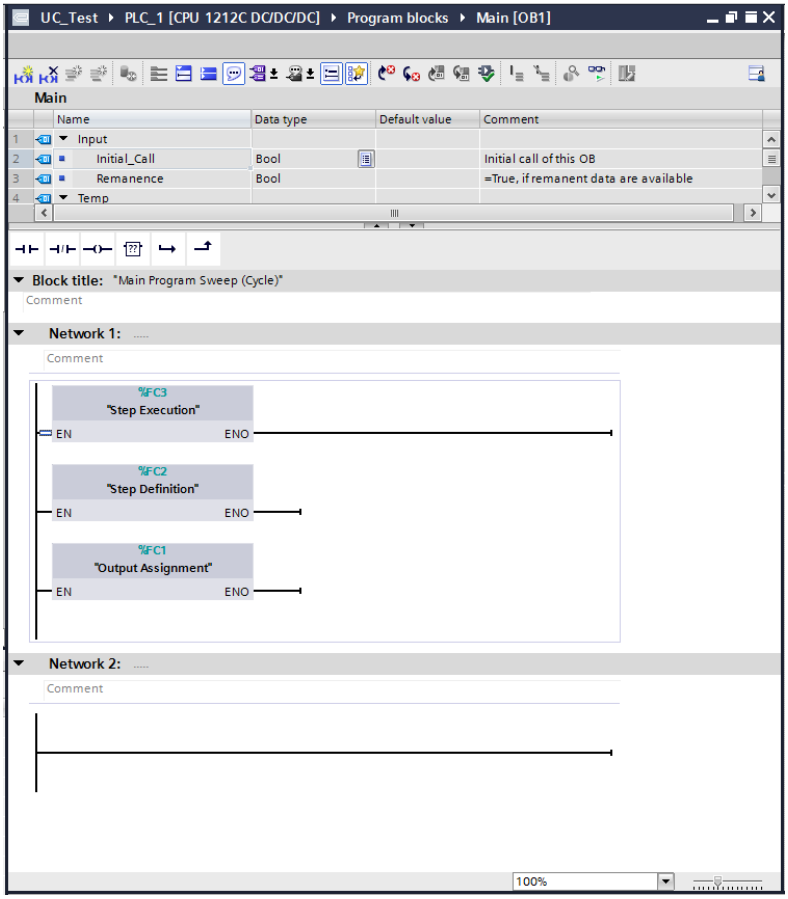

Figure 6 TIA software program.

Once the code is ready to be used, it is sent to the PLC through the Ethernet switch via online, where it will be processed. The programmable logic controller can run the program offline once it is received, processed and stored in the internal memory.

The HMI device allows to control the manufacturing process through the touch screen. The operator can start/stop the manufacturing process and trigger other options available in the interface of the device, which are easily programmed with the before mentioned TIA software. It is connected to the PLC which processes the commands coming from the HMI and with the Ethernet switch.

The PLC in turn, is connected to the I/O module. This module manages the processing of the input and output signals sent to the manufacturing machine. The working process is very simple. The I/O module sends the input signals to start the actuators when the item is in a determinate position. The position of the item is tracked and controlled with sensors at the beginning and at the end of the conveyor belt. Once the sensor records the position of the item an output (process signal) is sent to the I/O module and processed in the PLC. Depending on the position registered the PLC gives back the input signal through the I/O module to activate the right actuator of the system. The I/O module is also connected to the Ethernet switch.

As it is explained previously, all data collected by the system (sensors, actuators…), the commands and the code is linked to the Ethernet switch. This device shares all the information across the system. Then, the data collected in the network is uploaded to a data base which can be accessed online.

In the image below, the UML diagram shows the data itinerary of the cyber physical system.

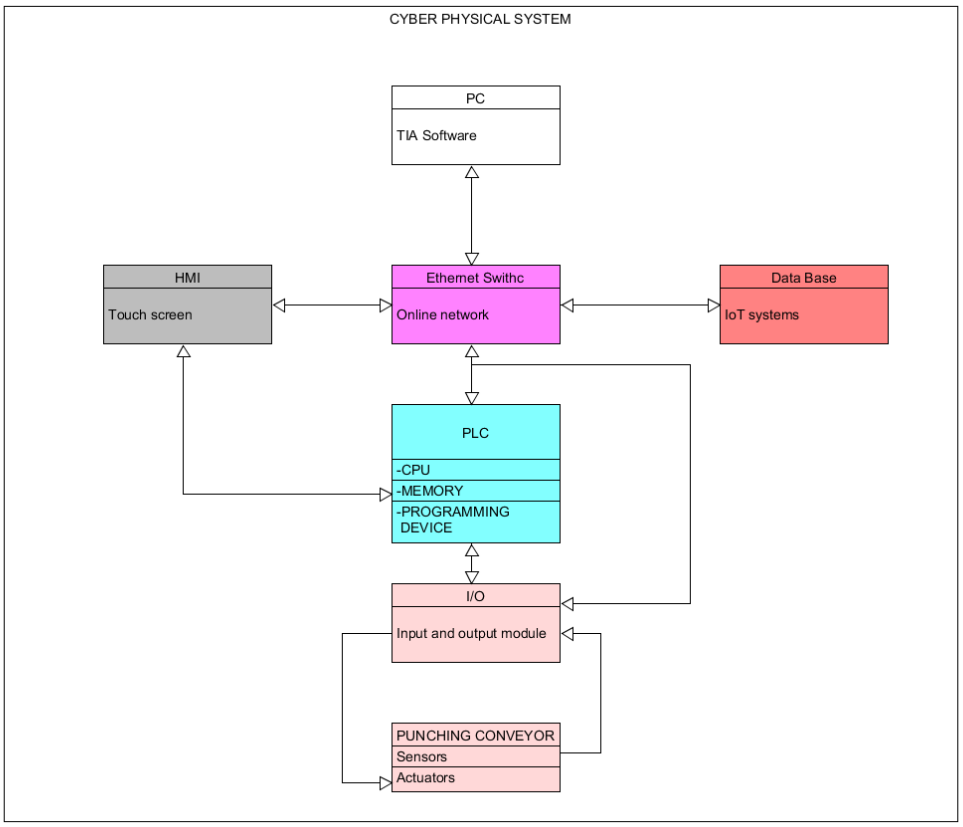

Figure 7 UML data flow diagram.

3.5. IoT CPS layers

The data transmission standard and the communication structure of the current CPS is already set. Next is to identify the different IoT layers within the structure and then apply the blockchain security techniques against cyber-attacks targeting sensitive data.

1. Perception layer: This is the base layer and it involves the physical objects and connected devices of the CPS.
2. Network layer: This is layer transmit the information gathered by the devices network such as sensors, actuators, etc. to a processing system. The transmission is completed via Wi-Fi, 3G… The information is then received and stored in a data base.
3. Application layer: This layer manages smart applications used to gain access to the network from remote places.

4. Business layer: IoT management and result analysis.

The blockchain techniques will be targeting the network layer and the application layer to ensure the data transmission of the whole system is secured with a consensus mechanism and the network access is authenticated with smart contracts.

3.6. Use case diagram

In the current cyber physical system there are different stakeholders taking part in the network management and maintenance. The next image shows the Use Case Diagram, where the different roles of the employees related to the system are specified.

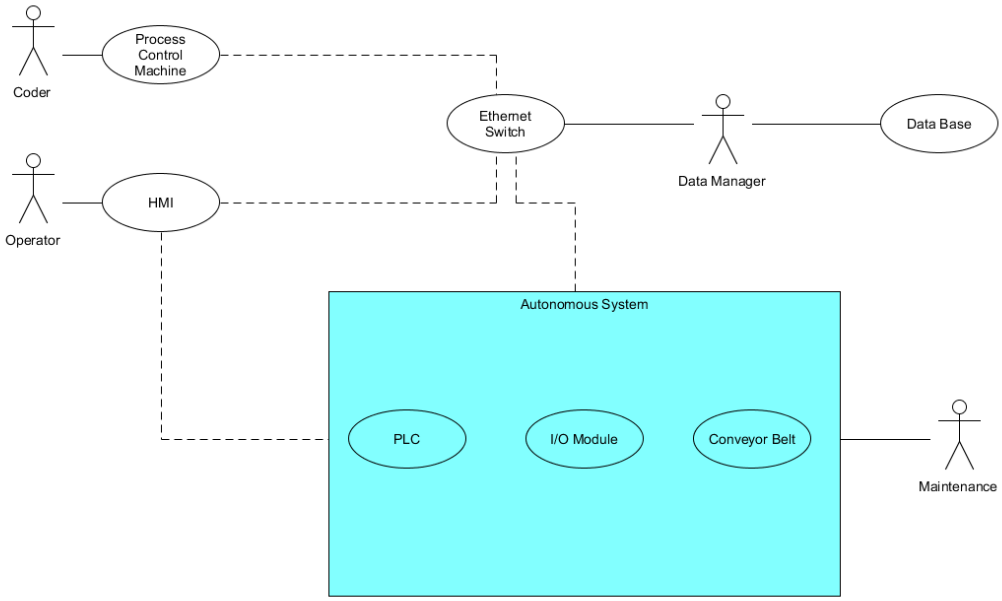

Figure 8 Use Case Diagram.

In the first place, the coder, whose main objective is to develop the program executed by the PLC. As it was mentioned before, the program used is the TIA

software. This employee is running the process control machine. It is also a task to upgrade new versions of the program in case new features are required.

In the second place there is an operator handling the HMI. The main task is to start and stop the system, track and control its functioning. There are more features available in the touch screen of the HMI that the operator must handle. This task and the programming task can be done remotely if required.

Maintenance is also a key part of the process. This employee guarantees the perfect functioning of the system, especially of the autonomous part which has not an employee assigned as the process control machine.

To conclude, there is an operator in charge of the data management. The main task is to supervise that the data generated by the CPS is transmitted and uploaded to the data base successfully.

3.6.1. **The validation of the use case diagram**

The development of the CPS data flow and use case diagrams have been completed through different visits to the laboratory in building 30. During those visits a series of interviews were done with the laboratory technician, and information was collected through individual research. The total understanding of the system used as a model in the current thesis to represent the blockchain security techniques was the first step to start the upcoming research. Technical mechanisms and properties of the system were explained in detail and instruction manuals were given too to extract the maximum information possible. Once the information collected is examined, next step is the model building. With the system manuals, the physical parts of the system can be presented and described and then linked together in a data communication perspective to build the data flow diagram. The objective was to define a data path through the whole system, from the data generation until the data management, representing the different steps the data transmission between the computational elements inside

the cyber physical system. The data flow is represented in a UML diagram to easily understand the internal procedures of the model CP system and the used to implement the blockchain framework. On the other hand, regarding the use case diagram, after knowing the different operators and their roles taking part in the CPS process to make the system run successfully, the use case diagram is developed. The objective is to define a visual map where every operator is located within the system and their roles are specified. When it comes to apply the blockchain framework solution it is very important to use this tool, as the authentication of the user and its commands will be a compulsory requirement. This section is vital so blockchain framework can be well implemented according to the current data management. Once the data flow chart and the use case diagrams are completed next step is to validate it. The procedure to do so is through meetings with the laboratory technician and the supervisor. After this step the diagrams are ready to be taken as a base to implement the blockchain framework.

4 Proposed cybersecurity Blockchain framework for CPS

4.1. Introduction

In the current section, a blockchain framework will be designed and explained. The main objective by using this new technology, is to address the security vulnerabilities that as was explained previously in the literature review, represent a threat to the current cyber physical systems integrity (Liu *et al.*, 2017).

The data constantly generated by the IoT system is uploaded and stored in a Data Base. It implies that the users willing to access and store the information through this kind of service, must trust in what is called a Third-Party Auditor (TPA). It is because usually, users have not control over the Cloud servers, assuming TPA performs a responsible behaviour despite somehow may not be as reliable as it was expected in the first place, incurring in confidentiality, integrity and availability risks, which are also present with the cyberattacks. Current CPS are vulnerable and the framework design needs to tackle main threats.

4.2. Solution requirements

As the main advantage of the blockchain technology is that it is a decentralized system, the need of trusting a Third-Party Auditor is no longer required. Data management thus, is decentralized, underpinned by the blockchain features.

Moreover, cyberattacks like distributed denial of service (DDoS), denial of service (DoS), Man in the middle attack, False data infection attack, etc.… can be now tackled easily due to the blockchain nature. It means that whenever a node (data generator) is tampered through a cyberattack, it can be detected by the rest of the network because every single node has a copy of the stored blockchain,

possessing the correct information in real time. It means that to succeed in a blockchain attack, the cyber attacker must gain control over at least, 51% of the nodes, which is considered practically impossible due to the high computational resources required to produce such a big attack.

For this reason, blockchain is considered an immutable ledger that provides non-repudiation of the stored data. In addition, the data is encrypted, and public and private keys are required to verify the authenticity and identity of the users and the information.

However, there are some disadvantages associated with the blockchain technology in IoT systems that must be mitigated. These are the following:

- Most of IoT devices have low computational power.
- Mining blocks is time and resource consuming while low latency in IoT systems is desirable.
- Blockchain protocols can result in overhead traffic which can affect to the IoT devices behaviour due to its low computational power.
- Limited scalability as the number of nodes in the network increases.

The objective is to maximize the advantages and mitigate the disadvantages combining both blockchain and IoT networks and achieve a trustworthy environment guaranteeing the confidentiality, availability and integrity of the data.

4.3. Blockchain framework architecture

The blockchain framework design is composed of three different layers: local network, overlay network and cloud storage.

1. **The local network** is formed by three different parts:

- Devices: This includes all the sensors, actuators and smarts devices able to generate data within the cyber physical system. Those are the nodes of the local blockchain.

- Local blockchain: In the current framework design, two different local private blockchains are integrated in the local network. Blockchains are stored in the central PC which is always online and oversees the management of the local network. It means that are managed in a centralized way. The objective is to combine both together, so it is possible to manage on the one hand the data produced by the punching machine's nodes and on the other hand, to ensure the commands of the operator through the HMI device are validated and stored in the second blockchain with the use of smart contracts. The first local blockchain is designed to manage the data generated by the nodes of the punching machine (couple of I/O, sensors and actuators) as mentioned before. Every transaction done by each device is chained together. Regarding the second blockchain, using smart contracts, which are secure and unstoppable computer programmes representing a previous agreement that is automatically executed when the requirements are met, the commands of the operator handling the HMI device (which constitute a node), and the authenticity of the user are validated, verified and considered correct because of the automatic smart contract execution. Otherwise the smart contract is not executed and the transaction (command) is not validated, preventing the machine to execute the wrong command. Those transactions are chained together in the second blockchain network. Smart contracts are written thus, in a language that a computer or a machine can read.

  The PC controller can add or remove new nodes to both blockchain networks by adding new access transactions or deleting its ledger. To do so, it is necessary to set an access control policy in the first place, which allows the owner to control all the transactions and the new node's local blockchain access. The policy is based on shared keys. Public and private keys managed by the control PC that nodes must have firstly to join the network. Once the policy is set, the following process of adding new blocks to the blockchain is called mining. As this is a local blockchain managed centrally and comprised of low computational power nodes, the Proof of Work which is a consensus mechanism previously explained in the literature review is not required, avoiding thus, overheads. The miner

adds a pointer to the previous block, set the policy access control to the current block and adds the block to the local chain.

- Local storage: There is a local backup drive in the local network.

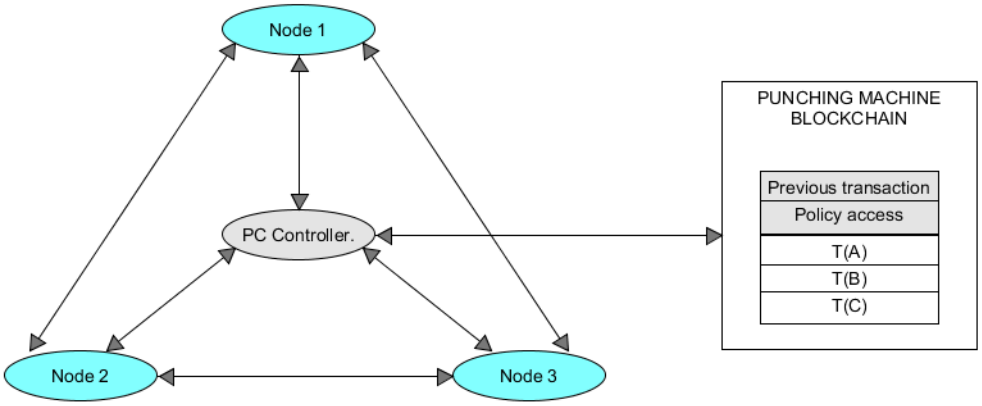

Figure 9 Local P. Machine Blockchain

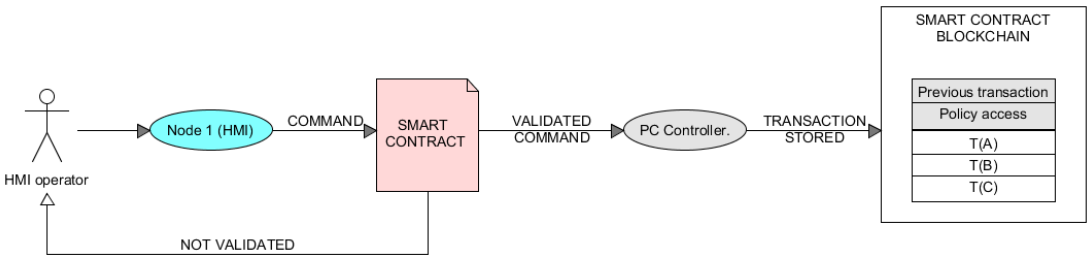

Figure 10 Local S.C blockchain

2. **Overlay network**: The nodes constituting the overlay network are the PC controllers. Every CPS existing has two local blockchains managed by the PC controller which at the same time constitute a node in the overlay network. This means that every single CPS that may be added in the future can easily join the overlay network through the PC controller. The overlay network is a distributed peer to peer ledger. To reduce the overhead and

delay of the network, the nodes are gathered in what is called clusters, and then, one node is designed as a cluster head. It is possible for every node to change the cluster in case there is too much delay. At the same time, the nodes of the cluster can also change the cluster head at any time. Every cluster head (CH) must manage the public keys. The CH has the public keys of the nodes allowed to access the data belonging to this cluster and a list of the transactions from other cluster heads. It means every single cluster head keeps a copy of the overlay blockchain.

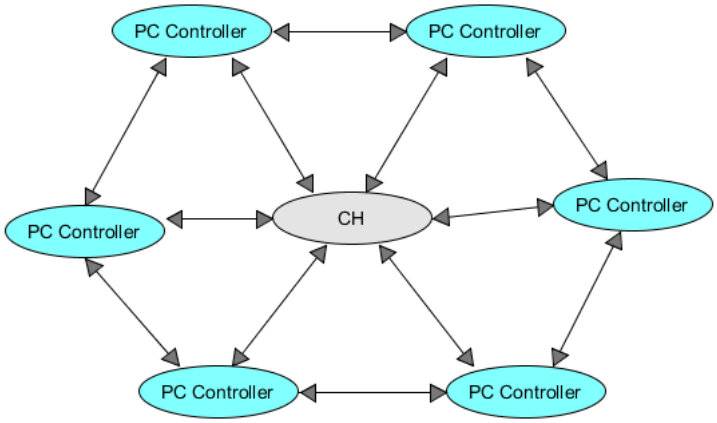

Figure 11 Overlay network

3. **Cloud storage**: The data storage gathers the data in blocks. Every block has associated a block number and a hash. A secure hash algorithm transforms a data input into a fixed length value based on the plaintext with the objective of ensure data integrity. The cloud storage then, uses the block number which is encrypted using a shared key and the hash for authentication so only the user with the appropriate key can access the data stored. If it is possible then to locate the target data using the block number and the hash the user is successfully authenticated. The way of storing data is first-in-first-out data blocks (Xu, Wang and Guo, 2018).

4.4. Blockchain framework transactions

Now that the architecture of the blockchain framework is explained next is shown how the transactions are completed. Storing and accessing data (Dorri, Kanhere and Jurdak, 2016).

1. **Storing**: Data collected from the sensors and the command transactions across the system is stored in the cloud storage. To do so, data from the sensors and the command transactions are sent to the PC controller in the local network where the policy access to chain a new block in both local blockchains is verified by the PC controller and then, the transaction is allowed. Next, the block number and hash of the previous block is extracted. With this information, the PC controller creates an ID and sends the data collected along with the created ID to the cloud storage. After verifying the transaction and checking there is space enough a new hash of the received data packet is calculated. If the hash calculated and the hash sent by the PC controller coincide, the data is stored, and the block number is encrypted with the shared key. The block number is then sent back to the PC controller and the new hash of data is sent to the distributed ledger in the overlay network layer where a new block is mined and added to the distributed blockchain. Now the data stored is completely secure because any change could be checked from the different nodes of the overlay blockchain network.

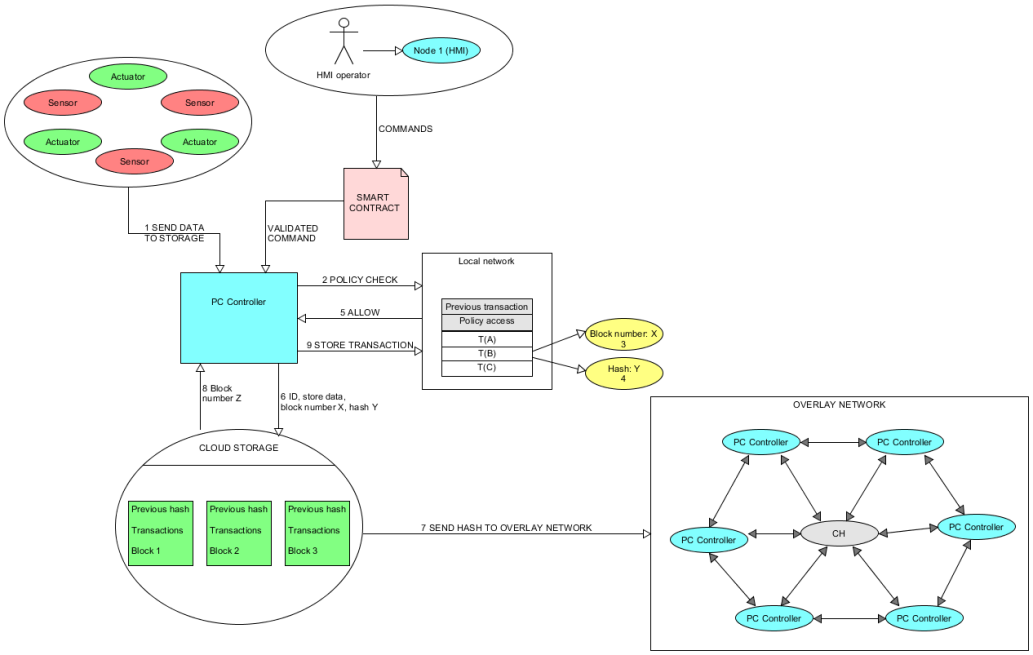

Figure 12 Storing transaction

2. **Accessing**: When any user needs to grant access to the data in the cloud storage, firstly must sign a multisignature transaction. This transaction called T.Access, is also signed by the PC controller prior to send it to the cluster head. Once sent, the CH checks both public keys lists confirming the multisignature transaction. Once the authentication is verified and the user´s access is granted, the PC controller asks for the data packet stored in the cloud service and encrypt it using the user's public key. After the data is sent to the user, the transaction is recorded in the local blockchain and in the different cluster heads of the overlay blockchain.

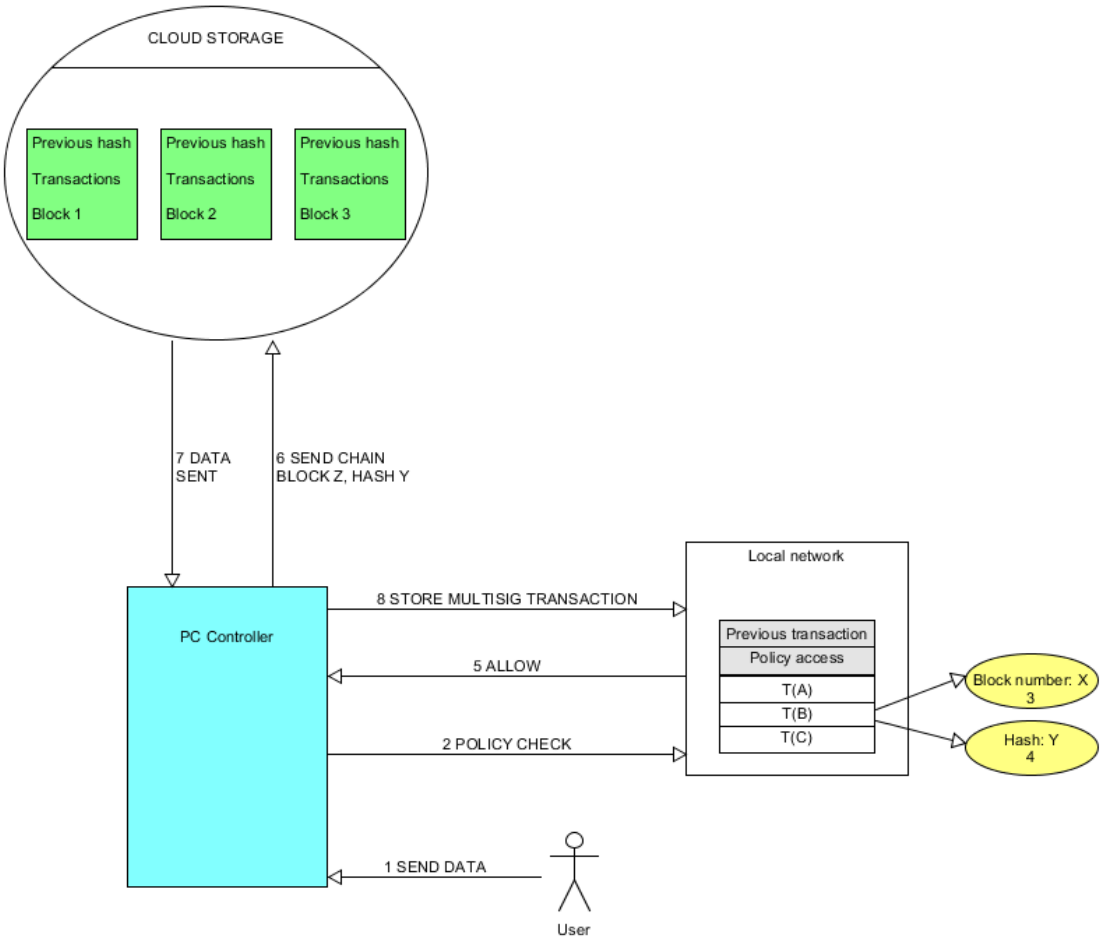

Figure 13 Access transaction

4.5. **Consensus mechanism**

In this proposed blockchain framework the distributed trust is ensured among cluster heads. Every time a new block is generated, the cluster head send the block along with the own generated multisignature transaction to the neighbour CHs. Those transactions must be validated and verified prior to accept the blockchain copy in the rest of the CHs creating direct and indirect evidence between the cluster heads. To reduce the overhead and the delay in this process, further verifications are based on the previous evidence between cluster heads, reducing the verification process. It means only a part of the total transactions are validated instead of the whole block by checking the signatures. In case there is not direct or indirect evidence between nodes, the whole block transactions are verified, creating evidence for further verifications (Zyskind, Nathan and Pentland, 2015).

5 Validation

5.1. Introduction

During this section the methodology applied to develop the blockchain framework and the results obtained from it will be validated.

5.2. Validation methodology

To complete the proposed blockchain framework developed in the present project, the methodology followed is illustrated in figure 14.

To begin with the definition of the framework, the first step was the deep study of the previous use case diagram and data flow chart, to define the data exchange path and the data management. Also define all the stakeholders taking part in the process and their defined role within the CPS. According with this information already validated in section 3, the solution requirements had to be discussed and validated through meetings with the supervisor prior to the blockchain framework development.

The development of the project required an exhaustive research. Academic articles and books, conferences and meetings were necessary to extract valid information and build the base of the framework, fulfilling the solution requirements. The proposed blockchain framework developed would be discussed with the supervisor prior to validate it.

Figure 14 validation methodology

5.3. Results validation

Several meetings with the expert supervisor were necessary to validate the whole proposed blockchain framework.

During the meetings the main features of the blockchain network were discussed to demonstrate the mechanisms to tackle the security vulnerabilities affecting IoT enabled CP systems. As it is deeply explained in section 6.4, solution requirements are met, and the proposal design can tackle the main vulnerabilities, guaranteeing the users the data availability, confidentiality and integrity.

Some disadvantages were also pointed out, associated with the blockchain technology, however easily mitigated since the blockchain framework was designed to avoid high computational power requirements. Overheads are also mitigated and avoided with the overlay network, and protocols are designed in case a node is attacked.

With the validation of the framework next step is to discuss its impact within the CPS and how it contributes to protect manufacturing systems.

6 Discussion

6.1. Introduction

The theoretical blockchain framework is fully developed in chapter 4 where the architecture is explained, and its transactions maps are deployed. To achieve the objective the methodology described in the introduction of the thesis has been followed. First carrying on a literature review in chapter 2, then with the acquired knowledge a data flow chart and a use case diagram has been designed to build the base of the data management in the cyber physical system used as a model in chapter 3.

The objective of this chapter is to discuss the results of the proposed blockchain framework design.

6.2. Discussion of research methodology

To complete the individual thesis a methodology has been followed. First a thorough literature review has been completed to explain the technologies currently used in the industry, the future technologies and its benefits and disadvantages. Security vulnerabilities, current security techniques for protection, the applications of the blockchain, an exhaustive research on the blockchain nature and a cyber security research for industry infrastructure form the first step of the methodology. From this point, with the use of the technical information the research on the laboratory cyber physical system started. The author visited the laboratory to explore the system, get information manuals and arrange meetings with the technician, so the data needed to develop the data flow chart and the use case diagram was extracted. The process of defining the diagrams required meetings with the supervisor to validate the progress done. With this part of the

project finished, the implementation of the proposed framework started with a thorough research on current blockchain applied in IoT enabled cyber physical systems. Information was selected and studied to build a theoretical framework which aims to tackle most of the cyber security vulnerabilities. Different blockchains were designed according to the local network and overlay network and defined the process of storing transactions in the cloud storage.

6.3. Discussion of the data flow chart and use case diagram

Data flow chart and use case UML diagrams constitute the intermediate step of the thesis. They define the conditions of the cyber physical system and explain and define its internal structure. Blockchains are the designed according to the data management previously defined.

Data flow chart allows to map the internal structure of the cyber physical system with the IoT layers and ultimately with the blockchain network layers. The definition of the data management constitutes a key part of this project. Data generators, both sensors and actuators, are considered the nodes of the local network which are managed by the pc controller and where all the transaction are chained together and stored. The data transmission is then predefined.

To define the first blockchain no human interaction is needed since data coming from nodes is automatically validated and authenticated, then chained to the blockchain stored in the Pc controller. On the other hand, to manage the HMI commands coming from the operator, whose role is previously defined in the use case diagram, it is necessary to define the HMI as a node of the second blockchain designed in the local network. Smart contracts execute only the valid commands as explained aforementioned and authenticate user's identity. Data coming from the HMI node goes directly to the Pc controller where is stored in a second blockchain.

The work done to develop the data flow chart and the use case diagram are then the base to develop and implement a blockchain framework according with the different communication layers.

6.4. Discussion of the blockchain framework solution

With the fully integration of the new blockchain framework, many security threats are addressed and solution requirements are tackled. As it was in the literature review there are many cyber-attacks threating the layers of the network security. The main target of the cyber-attacks are accessibility, anonymity and authentication (Liang *et al.*, 2018).

1. Accessibility: The goal is to avoid the user to access the data. Next some of the most important attacks classified in this group.

    - DoS: Denial of service caused by sending false transactions or blocks, can be successfully addressed with the use of the Public Keys lists of the requests and the requestees in the cluster head. If several unsuccessful accesses are recorded, the cluster head blocks the public key of the attacker node and ban further transactions.
    - Data tampering: Changing, modifying or deleting data stored in the cloud would be detected by the data hash comparison with the local blockchain stored hash. The fact that it is a distributed ledger makes it possible to compare the stored hash from any PC controller. The fake user access transaction could be then easily detected and banned by the cluster head.
    - Dropping attack: To make this attack possible, the attacker must have control of at least one or more cluster heads and drop the transactions and stored blocks. This kind of attack would be quickly detected since all the rest of nodes belonging to the cluster would not receive transactions anymore. In this situation a new cluster head is elected.
    - Mining attack: To complete this attack, the adversary must have control over multiple CHs and coordinate them to introduce fake blocks by signing the multisig transaction. As this framework is

based on the common trust between nodes, the attacker takes advantage and can validate a big percentage of transactions and blocks. However, this is difficult to perform due to the large amount of resources required to take control of many different cluster heads. Still, due to the decentralized features, if a cluster heads not tampered detect fake transactions, the compromised cluster heads are detected.

2. Anonymity: The attacker tries to link different transactions with the user identity. Since all the blocks mined have different IDs and block numbers and the list of PKs required are also changeable it is easy to prevent the anonymity attacks.

3. Authentication and access control: 3 cases are contemplated in this section. In the first case, the attacker tries to hack a device or a node of any of the local blockchain to access the network. In the case of the sensors blockchain, that would be easily detected because a transaction is stored in the local blockchain when an access is completed, giving the user the opportunity to check all the access transactions and thus the access record. Regarding the smart contract blockchain there is no way of completing a transaction if the smart contract is not executed first, and to do so, the user must be identified successfully in the first place, and the command through the HMI must be correct. In the second case, the attacker tries to introduce a new device in the network, but this is not possible since all the sensors or nodes of the network are previously predefined, and a non-valid starting transaction would be detected easily. The third case, and the most complicated, the attacker acts as a service provider (third party), so the block number and the data hash are sent by the user. This information can be used to verify the access as a true user and storage and manipulate the data. To prevent the block transactions tampering, the miner adds an empty block and points it back to the block that the fake user will insert, preventing thus, chain the new block to the user's block.

The proposed framework ensures the confidentiality, availability and integrity of the data generated, retrieved and stored. The encryption algorithms applied in the data packets ensure the confidentiality. Decentralisation of the blockchain nature allows very high data availability and its immutability feature grants data integrity.

6.5. Discussion of the framework implementation

The blockchain framework is based on three different levels. The local network, the overlay network and the cloud storage.

Local blockchains in the local network run in the Pc controller. From the controller it is possible to manage all the nodes forming local blockchains. It is the responsible to add or eliminate new nodes and the policy check to add new blocks to the chain is set there too. Nodes generate the data and send it to the Pc controller and then is sent to its final destiny, the cloud storage. Pc controller computational power requirements are high, however almost every modern PC would run this network.

Overlay network blockchain is also underpinned by a Pc controller, in this case called cluster head. Every cluster head possesses the whole copy of the overlay blockchain. Cluster Heads can be elected or dumped by the rest of the nodes forming the cluster.

From the Pc controller and the cluster head it is possible to verify the policy check and grant access to the cloud storage whether to store or retrieve information. Every action allowed is then recorded in the overlay network cluster heads hosting the overlay blockchain.

7 Conclusions

IoT systems enabled CPS are constantly generating and uploading data to the cloud storage service. Sensitive data is the main target for cyber-attacks. Conventional IoT systems have currently, serious security vulnerabilities that can compromise the security of the whole system. As was defined in the literature review nowadays hackers have designed a wide range of different attacks targeting different areas within the manufacturing systems and processes making it more difficult to guarantee the total protection of the systems.

To address some of the main security vulnerabilities identified in the CPS, a blockchain framework has been designed with the main objective of ensure the availability, confidentiality and integrity of the data.

The proposed framework structure was designed according to the data management of the cyber physical system used as a model. Along with the use case and the data flow diagram definition, blockchain framework was designed mapping the internal structure with the CPS structure.

The fact that blockchain is managed in a decentralized way has provided new opportunities in terms of data managing and availability. A third party is not required anymore to guarantee the validity of the transactions. Data is highly available since every single node possesses a copy of the blockchain, due to the peer to peer network attributes, making it easy to access data whenever it is required and from anywhere. In addition, it contributes to create a trustworthy and secure environment.

Data integrity is also granted because every transaction already validated cannot be changed unless the attacker gains control over most of the nodes. It is highly improbable due to the huge energy and resources consumption required. Moreover, the transactions are encrypted and only the user with the correct list of public keys can decrypt the information, providing the user high confidentiality.

All this blockchain features combined with the IoT CPS system provide a secure data management, ensuring the integrity, availability and confidentiality of the information and users of the system.

From the point of view of the computational resources and capabilities of the nodes belonging to the overlay network, the pc controllers, the framework was built with the objective of reduce the overheads by gathering nodes together. A modern pc controller can host the overlay network making it accessible for industry to implement this new technology.

7.1. Future research

Future improvements of the security blockchain framework must be dedicated to increase the computational power of the devices comprising the blockchain networks. The more computational capabilities in a single device, the more sophisticated the consensus mechanisms can be. This can ensure even more the authenticity of the nodes and the validation and verification of the transactions done. In addition, upgrading the computational power of the sensors would improve the capabilities of the local blockchain and contributing to make it safer, faster and more reliable.

Future work will explore the scalability of systems and data and investigate how blockchain are connected to the industry systems seamlessly with the final objective of integrate the new system in the 4.0 industry.

8 REFERENCES

(PNO), P. N. e. V. (2014) ‘PROFINET System Description’, p. 28. Available at: http://us.profinet.com/wp-content/uploads/2012/11/PI_PROFINET_SystemDescription_EN_2014_01.pdf.

Abomhara, M. (2014) ‘Security and Privacy in the Internet of Things : Current Status and Open Issues’, *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*, pp. 1–8. doi: 10.1109/PRISMS.2014.6970594.

Al-Fuqaha, A. *et al.* (2015) ‘Internet of things: A survey on enabling technologies, protocols, and applications’, *Ieeexplore.Ieee.Org*, 17(4), pp. 2347–2376. doi: 10.5752/P.2316-9451.2013v1n2p78.

Belai, I. and Drahoš, P. (2009) ‘The industrial communication systems Profibus and PROFInet’, *Applied Natural Sciences*, (September 2015), pp. 329–336.

Bhuvaneswari, V. and Porkodi, R. (2014) ‘The internet of things (IOT) applications and communication enabling technology standards: An overview’, *Proceedings - 2014 International Conference on Intelligent Computing Applications, ICICA 2014*, pp. 324–329. doi: 10.1109/ICICA.2014.73.

Christidis, K. and Devetsikiotis, M. (2016) ‘Blockchains and Smart Contracts for the Internet of Things’, *IEEE Access*, 4, pp. 2292–2303. doi: 10.1109/ACCESS.2016.2566339.

Crosby, M. *et al.* (2016) ‘BlockChain Technology: Beyond Bitcoin’, *Applied Innovation Review*, June(2), pp. 6–19. doi: 10.15358/0935-0381-2015-4-5-222.

Daou, H., Kayssi, A. and Chehab, A. (2008) ‘RFID security protocols’, *2008 International Conference on Innovations in Information Technology*, pp. 593–597. doi: 10.1109/INNOVATIONS.2008.4781675.

Dorri, A., Kanhere, S. S. and Jurdak, R. (2016) ‘Blockchain in internet of things: Challenges and Solutions’. doi: 10.1145/2976749.2976756.

Foroglou, G. and Tsilidou, A. L. (2015) ‘Further applications of the blockchain’, *Conference: 12th Student Conference on Managerial Science and Technology, At Athens*, (MAY), pp. 0–8. doi: 10.13140/RG.2.1.2350.8568.

Gan, G., Lu, Z. and Jiang, J. (2011) ‘Internet of Things Security Analysis’, *2011 International Conference on Internet Technology and Applications*, pp. 1–4. doi: 10.1109/ITAP.2011.6006307.

Gantait, A., Patra, J. and Mukherjee, A. (2017) ‘Implementing blockchain for cognitive IoT applications, Part 1’, *IBM DeveloperWorks*, pp. 1–10.

Hadjichristofi, G. C. (2015) ‘Internet of Things : Security vulnerabilities and challenges Internet of Things : Security Vulnerabilities and Challenges’, (August

2017), pp. 180–187. doi: 10.1109/ISCC.2015.7405513.

He, H. *et al.* (2016) 'The Security Challenges in the IoT enabled Cyber-Physical Systems and Opportunities for Evolutionary Computing & Other Computational Intelligence', pp. 1015–1021.

Herbert, J. and Litchfield, A. (2015) 'A Novel Method for Decentralised Peer - to - Peer Software License Validation Using Cryptocurrency Blockchain T echnology', *38th Australasian Computer Science Conference (ACSC 2015)*, (January), pp. 27–30.

Huh, S., Cho, S. and Kim, S. (2017) 'Managing IoT devices using blockchain platform', *International Conference on Advanced Communication Technology, ICACT*, pp. 464–467. doi: 10.23919/ICACT.2017.7890132.

Jayaraman, P. P. *et al.* (2017) 'Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation', *Future Generation Computer Systems*. Elsevier B.V., 76, pp. 540–549. doi: 10.1016/j.future.2017.03.001.

Jing, Q. *et al.* (2014) 'Security of the Internet of Things: perspectives and challenges', *Wireless Networks*, 20(8), pp. 2481–2501. doi: 10.1007/s11276-014-0761-7.

Khan, R. *et al.* (2012) 'Future internet: The internet of things architecture, possible applications and key challenges', *Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012*, pp. 257–260. doi: 10.1109/FIT.2012.53.

Liang, G. *et al.* (2018) 'Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks', *IEEE Transactions on Smart Grid*, (March). doi: 10.1109/TSG.2018.2819663.

Liu, B. *et al.* (2017) 'Blockchain Based Data Integrity Service Framework for IoT Data', *Proceedings - 2017 IEEE 24th International Conference on Web Services, ICWS 2017*, pp. 468–475. doi: 10.1109/ICWS.2017.54.

MATANOVIĆ, A. (2017) 'Blockchain/Cryptocurrencies and Cybersecurity, Threats and Opportunities', (October). Available at: http://bisec.rs/files/2017/02-a-matanovic-bisec-2017.pdf.

Mettler, M. (2016) 'Blockchain technology in healthcare: The revolution starts here', *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services, Healthcom 2016*, pp. 16–18. doi: 10.1109/HealthCom.2016.7749510.

Paper, W. (2016) 'www.econstor.eu'.

Punia, A., Jaiswal, S. and Gupta, D. (2017) 'A Perspective on Available Security Techniques in IoT', pp. 1553–1559.

Puthal, D. *et al.* (2018) ‘The Blockchain as a Decentralized Security Framework [Future Directions]’, *IEEE Consumer Electronics Magazine*, 7(2), pp. 18–21. doi: 10.1109/MCE.2017.2776459.

Sa, L. *et al.* (1822) ‘Logicbus SA de CV. Estrada Roque, José Antonio. PROFINET 1’, (33), pp. 1–5.

Sadeghi, A., Wachsmann, C. and Waidner, M. (2015) ‘Security and privacy challenges in industrial internet of things’, *Proceedings of the 52nd*. Available at: http://dl.acm.org/citation.cfm?id=2747942.

Sturm, L. D. *et al.* (2014) ‘Cyber-Physical Vunerabilities in Additive Manufacturing Systems’, *International Solid Freeform Fabrication Symposium*, pp. 951–963. Available at: http://sffsymposium.engr.utexas.edu/sites/default/files/2014-075-Sturm.pdf.

Suo, H. *et al.* (2012) ‘Security in the internet of things: A review’, *Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012*, 3, pp. 648–651. doi: 10.1109/ICCSEE.2012.373.

Wells, L. J. *et al.* (2013) ‘Cyber-physical security challenges in manufacturing systems’, *Manufacturing Letters*. Society of Manufacturing Engineers (SME), 2(1), pp. 74–77. doi: 10.1016/j.mfglet.2014.01.005.

Wright, A. and Filippi, P. De (no date) ‘SSRN-id2580664’.

Xia, Q. *et al.* (2017) ‘BBDS: Blockchain-based data sharing for electronic medical records in cloud environments’, *Information (Switzerland)*, 8(2). doi: 10.3390/info8020044.

Xu, C., Wang, K. and Guo, M. (2018) ‘Intelligent Resource Management in Blockchain-Based Cloud Datacenters’, *IEEE Cloud Computing*, 4(6), pp. 50–59. doi: 10.1109/MCC.2018.1081060.

Zheng, Z. *et al.* (2017) ‘An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends’, *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.

Zyskind, G., Nathan, O. and Pentland, A. S. (2015) ‘Decentralizing privacy: Using blockchain to protect personal data’, *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, pp. 180–184. doi: 10.1109/SPW.2015.27.

Imran Bashir (2017) ‘Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, anFird popular Blockchain frameworks’, pp. 10-31.