T.C.
ISTANBUL GEDİK UNIVERSITY
INSTITUTE OF GRADUATE STUDIES

AN EFFICIENT COMPUTER NETWORK MANAGEMENT SYSTEM BASED MACHINE LEARNING TECHNIQUES

MASTER'S THESIS

Mohammed Nayyef Hussein HUSSEİN

Engineering Management Department

Master of Engineering Management in English

NOVEMBER 2023
ISTANBUL

T.C.
ISTANBUL GEDİK UNIVERSITY
INSTITUTE OF GRADUATE STUDIES

AN EFFICIENT COMPUTER NETWORK MANAGEMENT SYSTEM BASED MACHINE LEARNING TECHNIQUES

MASTER'S THESIS

Mohammed Nayyef Hussein HUSSEİN
(201281015)

Engineering Management Department

Master of Engineering Management in English

Thesis Advisor: Assist. Prof. Dr. Ahmet SARIKAHYA

İstanbuk 2023

T.C.
İSTANBUL GEDİK ÜNİVERSİTESİ
Lisansüstü Eğitim Enstitüsü Müdürlüğü

Jüri Tez Onay Formu

28.11.2023

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜ

Bu çalışma 28.11 2023 tarihinde aşağıdaki jüri tarafından Engineering Management Department, Engineering Management (Tezli Yüksek Lisans) Programı Yüksek Lisans Tezi olarak kabul edilmiştir.

TEZ JÜRİSİ

Dr. Öğr. Üyesi Ahmet SARIKAHYA
Danışman
İstanbul Gedik Üniversitesi

Dr. Öğr. Üyesi Tuğbay BURÇİN GÜMÜŞ
Üye (İmza)
İstanbul Gedik Üniversitesi

Doç. Dr. Mehmet Serdar GÜZEL
Üye (İmza)
Ankara Üniversitesi

DECLARATION

I, Mohammed Nayyef Hussein HUSSEİN, hereby certify that this thesis entitled "An Efficient Computer Network Management System Based Machine Learning Techniques" is my original thesis for the award of Master's Degree in Engineering Management at the Faculty of Engineering Management. I further certify that this thesis or any part thereof has not been submitted and presented for any other degree or research thesis at any other university or institution. (28/11/2023)

Mohammed Nayyef Hussein HUSSEİN

DEDICATION

I want to start by giving Allah, the Almighty, praise and thanks for giving me the knowledge, abilities, and opportunity to carry out and successfully complete my research. I genuinely thank my parents. Everything wonderful that has happened to me has been fueled by them, and their love is what makes everything possible. During this time, I'd like to express my gratitude to my sister and brother for their love and support.

TABLE OF CONTENT

Page

ABBREVIATIONS

IoT	**:** Internet of Things
BCN	**:** Block Chain Network
BCNs	**:** Body-Worn Communication Networks
PoS	**:** Proof of Stake
PoC	**:** proof of capacity
PoA	**:** proof of authority
PoI	**:** proof of significance
AES	**:** Advanced Encryption Standards
DES	**:** Data Encryption Standard
ECDSA	**:** Elliptic Curve Digital Signature Algorithm
RSA	**:** Rivest-Shamir-Adleman
WWAN	**:** Wireless Wide Area Network
WMAN	**:** Wireless Metropolitan Area Networks
WLAN	**:** Wireless Local Area Networks
WPAN	**:** Wireless Personal Area Networks
LoRa	**:** Long Range
CSS	**:** Chirp Spread Spectrum

LIST OF FIGURES

Page

AN EFFICIENT COMPUTER NETWORK MANAGEMENT SYSTEM BASED MACHINE LEARNING TECHNIQUES

ABSTRACT

It spreads out the authentication procedure, making the network more secure by reducing the number of potential weak spots. An additional safeguard is provided by blockchain's immutability and transparency, which makes it simple to verify and audit authentication data. Despite the clear upsides and promise, blockchain user identification for the Internet of Things is still in its infancy and faces a number of obstacles. Scalability, interoperability, privacy, and compatibility with current IoT infrastructure are just a few of the challenges that must be overcome. The purpose of this research was to provide a workable blockchain-based solution to these problems with the objective of improving user authentication in Internet of Things (IoT) systems. The overarching goal of this study is to examine blockchain technology's viability as a safe and effective user authentication method in Internet of Things (IoT) devices. The following are the precise goals that the research aims to achieve in this regard: Analyzing the Present Scene: Identify the present state, problems, and limits of existing solutions for user identification in the Internet of Things via a thorough literature and technology assessment. Feasibility Analysis of the Blockchain: The purpose of this study is to explore the viability of using blockchain technology for user identification in IoT systems by analyzing its advantages, disadvantages, prospects, and risks. System Design Considerations for Blockchain-Based Authentication To create a cutting-edge blockchain-based user identification solution for the Internet of Things that solves the problems we've discovered and makes the most of blockchain technology.

Keywords: *Data Science, AI, ML, DL, IOT*

VERİMLİ BİR BİLGİSAYAR AĞ YÖNETİM SİSTEMİ TABANLI MAKİNE ÖĞRENME TEKNİKLERİ

ÖZET

Kimlik doğrulama prosedürünü yayarak potansiyel zayıf noktaların sayısını azaltarak ağı daha güvenli hale getirir. Kimlik doğrulama verilerinin doğrulanmasını ve denetlenmesini kolaylaştıran, blockchain'in değişmezliği ve şeffaflığı ek bir koruma sağlar. Açık avantajlara ve vaatlere rağmen, Nesnelerin İnterneti için blockchain kullanıcı kimliği henüz başlangıç aşamasındadır ve bir takım engellerle karşı karşıyadır. Ölçeklenebilirlik, birlikte çalışabilirlik, gizlilik ve mevcut IoT altyapısıyla uyumluluk, aşılması gereken zorluklardan sadece birkaçıdır. Bu araştırmanın amacı, Nesnelerin İnterneti (IoT) sistemlerinde kullanıcı kimlik doğrulamasını geliştirmek amacıyla bu sorunlara uygulanabilir bir blockchain tabanlı çözüm sunmaktı. Bu çalışmanın genel amacı, Blockchain teknolojisinin Nesnelerin İnterneti (IoT) cihazlarında güvenli ve etkili bir kullanıcı kimlik doğrulama yöntemi olarak uygulanabilirliğini incelemektir. Araştırmanın bu bağlamda ulaşmayı amaçladığı kesin hedefler şunlardır: Mevcut Durumun Analizi: Kapsamlı bir literatür ve teknoloji değerlendirmesi yoluyla Nesnelerin İnterneti'nde kullanıcı tanımlamaya yönelik mevcut durumu, sorunları ve mevcut çözümlerin sınırlarını belirleyin. Blockchain'in Fizibilite Analizi: Bu çalışmanın amacı, avantajlarını, dezavantajlarını, beklentilerini ve risklerini analiz ederek IoT sistemlerinde kullanıcı tanımlama için blockchain teknolojisinin kullanılmasının uygulanabilirliğini araştırmaktır. Blockchain Tabanlı Kimlik Doğrulama için Sistem Tasarımında Dikkat Edilecek Hususlar Nesnelerin İnterneti için keşfettiğimiz sorunları çözen ve blockchain teknolojisinden en iyi şekilde yararlanan son teknoloji blockchain tabanlı kullanıcı tanımlama çözümü oluşturmak.

Anahtar Kelimeler: *Veri Bilimi, Yapay Zeka, AI, ML, DL, IOT*

1. INTRODUCTION

1.1 Background

The Internet of Things (IoT) represents a vast network of interconnected devices, each with the capability to generate and share data. These devices range from everyday household items such as smart refrigerators, thermostats, and home security systems, to industrial machinery, healthcare devices, and transportation systems. The rapid proliferation of IoT devices has led to a paradigm shift in how we interact with technology, making our surroundings smarter, more responsive, and increasingly efficient. However, with the widespread adoption of IoT, significant challenges have also emerged, particularly in the realm of data security and user authentication. Given the vastness and the diversity of IoT devices, securing these networks from unauthorized access and data breaches has become a primary concern for users and providers alike. Traditional centralized methods of user authentication present single points of failure, making them vulnerable to a variety of attacks. Recognizing these challenges, researchers and practitioners have begun exploring novel methods to enhance the security and robustness of IoT systems.

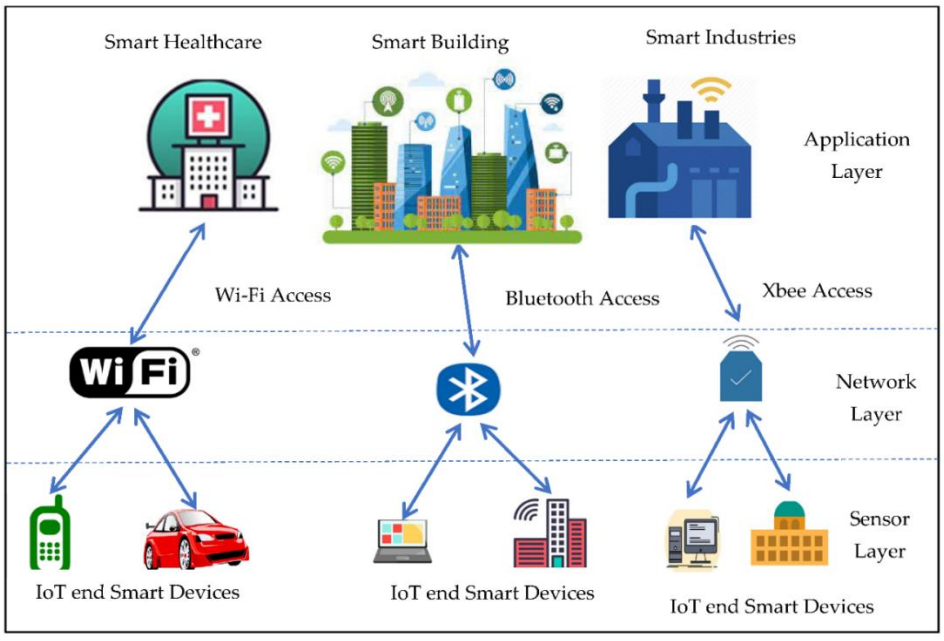

Figure 1.1: Abstract Architecture of an IOT Network [1]

One such promising solution lies in the application of blockchain technology. Originally devised for the digital currency Bitcoin, blockchain has since been identified as a potential solution to a myriad of problems beyond cryptocurrency. A blockchain is a decentralized and distributed digital ledger that records transactions across many computers in such a way that the recorded entries cannot be altered retroactively. This feature makes blockchain particularly suitable for applications where data integrity and transparency are paramount. Applying blockchain technology for user authentication in IoT networks represents a significant departure from traditional methods. It decentralizes the authentication process, eliminating single points of failure, and enhancing overall network security. Moreover, the transparent and immutable nature of blockchain enables easy verification and auditing of authentication records, providing an additional layer of security. Despite the evident benefits and potential, the application of blockchain in IoT user authentication is still a nascent field with numerous challenges to be addressed. These include but are not limited to issues pertaining to scalability, interoperability, privacy, and the integration with existing IoT infrastructure. This study aims to address these challenges, providing a comprehensive analysis and proposing a viable, blockchain-based solution for user authentication in IoT systems.

1.2 Problem Statement

The Internet of Things (IoT) has evolved as an essential component of the digital world, powering various sectors from healthcare to transportation. The massive and ever-growing number of interconnected devices and the voluminous data they generate present significant challenges, especially concerning data security and user authentication.

In the current landscape of IoT, most user authentication protocols are based on centralized models. These models are susceptible to various security risks, including single-point failures, cyber-attacks, and unauthorized data access. Furthermore, the diverse nature of IoT devices and the lack of standard protocols for interoperability pose significant issues in designing an effective, universal authentication mechanism [2].

The decentralized, transparent, and immutable nature of blockchain technology offers a potential solution to these issues. However, integrating

blockchain technology for user authentication in IoT systems is not a straightforward process. It presents its own set of challenges [3]:

Scalability: How can a blockchain-based authentication system be designed to efficiently handle the vast number of transactions in large-scale IoT networks?

Interoperability: How can a blockchain solution ensure seamless operation across diverse IoT devices from different manufacturers, each with their own unique software and hardware configurations?

Privacy: How can the system leverage blockchain's transparency for security while also ensuring privacy, given the sensitive nature of data that IoT devices often handle?

Integration with Existing Systems: How can blockchain technology be effectively integrated with existing IoT systems without causing significant disruption?

This research aims to address these challenges by developing a novel blockchain-based approach for user authentication in IoT systems. It seeks to design a system that not only enhances security but is also scalable, promotes interoperability, maintains privacy, and can be smoothly integrated with existing IoT infrastructures.

1.3 Thesis Objectives

The overall aim of this research is to investigate the potential of blockchain technology as a secure and efficient user authentication mechanism in IoT systems. To accomplish this, the study sets out the following specific objectives: Exploration of Current Landscape: To carry out a comprehensive review of existing literature and technologies regarding user authentication in IoT and understand the current status, challenges, and limitations of existing solutions. Blockchain Feasibility Study: To investigate the feasibility of applying blockchain technology for user authentication in IoT systems, examining its strengths, weaknesses, opportunities, and threats. Design of a Blockchain-based Authentication System: To design a novel, blockchain-based user authentication system for IoT that addresses the identified challenges and exploits the potential of blockchain technology. Development of a Prototype: To develop a working prototype of the proposed blockchain-based user

authentication system, thereby demonstrating the practical implementation of the design. Evaluation of the Prototype: To thoroughly evaluate the performance, security, scalability, interoperability, and privacy aspects of the developed prototype, comparing it with existing solutions. Identification of Future Research Directions: To identify potential challenges, improvements, and opportunities for future research in the application of blockchain technology for user authentication in IoT systems. By accomplishing these objectives, the thesis intends to contribute significantly to the field of IoT security, specifically in enhancing the security and robustness of user authentication mechanisms using blockchain technology.

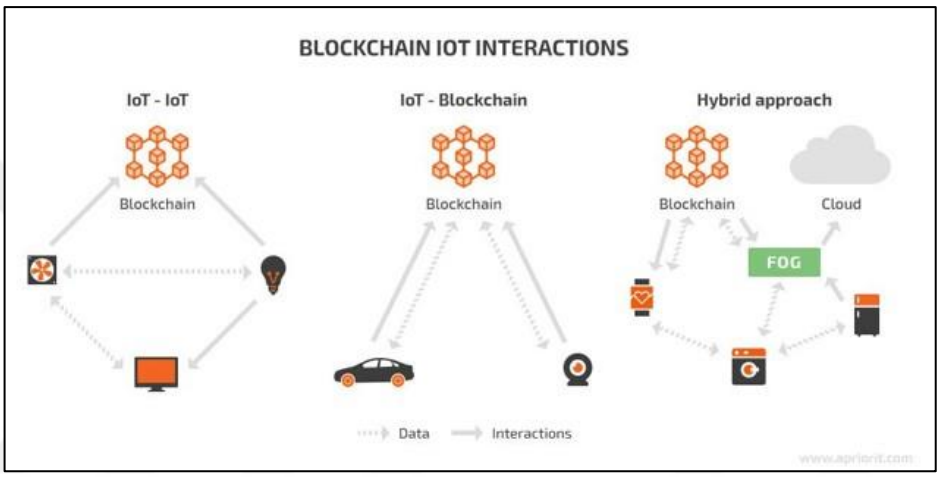

Figure 1.2: Blockchain Interactions for IOT Systems [4]

1.4 Thesis Contributions

This research contributes to the field of IoT security, specifically in user authentication, by incorporating blockchain technology. The key contributions of this thesis are as follows: Extensive Literature Review: The study offers a comprehensive review of existing literature on user authentication in IoT systems, providing an understanding of current methodologies, challenges, and limitations. It also surveys the current state of blockchain technology, shedding light on its potential use in IoT authentication. Blockchain Feasibility Analysis: This research provides an in-depth feasibility study of the application of blockchain technology in user authentication for IoT systems. It contributes to the understanding of the strengths, weaknesses, opportunities, and threats associated with such an approach. Novel Authentication System Design: A key contribution is the design of a new blockchain-based user authentication system for IoT. This system addresses the identified challenges in the

current IoT landscape and exploits the potential benefits of blockchain technology. Working Prototype: The study further extends its contributions by providing a practical implementation of the proposed design in the form of a working prototype. This prototype demonstrates the real-world applicability of a blockchain-based authentication system in IoT. Evaluation Framework: The research establishes an evaluation framework to assess the performance of the developed prototype. The evaluation considers critical factors such as security, scalability, interoperability, and privacy. Future Research Directions: Lastly, the research identifies potential areas for future work in this field, thereby contributing to the continued advancement of knowledge in the application of blockchain technology for user authentication in IoT systems. Through these contributions, this research aids in the development of more secure, efficient, and robust IoT systems by integrating blockchain technology for user authentication.

2. RELATED WORKS

2.1 Introduction

Over the course of the last ten years, the Internet has expanded to include not just the Internet of Things (IoT), but also blockchain networks (BCNs). The majority of this growth has taken place during the course of the past five years. The term "Internet of Things" (IoT) refers to a network of interconnected, internet-enabled, sensor- and software-equipped digital devices that are used for the automation of homes and buildings as well as for surveillance reasons. These devices are networked through the use of the internet. A Blockchain Network is a distributed network of computers that has the power of verifying digital transactions and permanently preserving those that are "well-formed" in a distributed ledger. Blockchain Networks are becoming increasingly popular as a secure alternative to traditional databases. The use of blockchain networks in the bitcoin sector is gaining a lot of traction recently and is expected to continue doing so. The most important feature of a blockchain network is that every node stores (ideally) its own copy of the distributed ledger and takes part in the validation of transactions. This is the feature that gives the network its most significant advantage. The Internet of Things (IoT) and body-worn communication networks (BCNs) have the potential to be of use in a wide variety of fields, including but not limited to those dealing with the environment, the economy, agriculture, and education. However, there are a great many more industries that stand to benefit from this. However, there are a number of hurdles to scaling, interoperability, and security requirements that are brought about by the fact that the processing and communication needs of IoT technologies are complex, dynamic, and diverse [6]. However, there are a lot of other difficulties in addition to these ones, and blockchain technology may be able to optionally address some of them if legislation is passed. There has been a rise in the number of suggestions, experiments, and production implementations of business models that combine blockchain networks and the Internet of Things throughout the course of the most recent few years. Investigations are being carried out right now into a wide range of

different ways in which the Internet of Things and blockchain technology could be put to use. On the other hand, a more in-depth analysis indicates that an infinitesimally small fraction of apps actually fulfill the security standards of a corporation. This is something that can only be described as "vanishingly small." It shouldn't come as much of a surprise that it is more difficult to integrate blockchain technology with an existing Internet of Things in a way that satisfies a company's requirement for a high level of data security. This chapter explores the security implications of deploying and operating IoT and BCN, as well as the possibility of merging a number of frameworks for IoT operations with blockchain technology. Specifically, the chapter focuses on the consequences of deploying and operating IoT and BCN simultaneously. In particular, the chapter focuses on the implications of putting into operation both the Internet of Things and the Blockchain. In addition, we conduct an in-depth analysis of the fundamental security challenges, and we provide some suggestions for how blockchain technology should be implemented in IoT networks.

2.2 Related Works

A blockchain network (BCN) [29] is a distributed system of computers that each hold their own copy of a distributed, shared ledger known as a blockchain. Blockchains are used in the cryptocurrency industry to record transactions. This particular kind of ledger is employed for the purpose of recording transactions as well as transactions carried out amongst users. Data on a blockchain network is preserved invariably as a result of the collective efforts of the nodes to prevent data tampering from occurring in the past, to increase visibility into operations by obtaining a consensus, and to ensure individual privacy by making transactions anonymous [16]. The phrase "immutable" ledgers has been used in previous publications such as [20,30,31] to refer to blockchains, which are essentially chains of data or records that cannot be altered in any way. This term has been used to refer to blockchains. Each new "block" that is added to a blockchain has a cryptographic reference to the preceding "block," and so on and so forth. A basic illustration of a block, a blockchain, and a blockchain network [30]. Each of the three components is linked to the other two. Each extra node in a blockchain network serves as a computer system, complete with its own local storage space, and performs the

activities that are required of it. It is recommended that each node in a BCN keep a separate and independent copy of the ledger in order to comply with best practices. A "well-formed" transaction needs to be finished first in order for a new block to be able to be added to an existing ledger that has already been created. A transaction is a data structure that represents a single, independent change to the state of a system. It is abbreviated as TXN, which stands for the transaction abbreviation. This modification is brought about as a consequence of performing an atomic operation on a collection of input values in order to bring about the desired effect. When an atomic operation is done on the input values, the transaction is considered to have been activated. The term "transaction" is used in a manner that is not entirely accurate in a lot of the writing that has been done around blockchain technology. A transaction's successful completion is defined as an atomic operation that finishes without errors and then has an effect on the state of the system once it has successfully finished. Consider the example transaction statement that follows as an illustration: "Transfer of monetary value x from Alice's wallet WA to Bob's wallet WB." Prior to the execution of the transaction, the initial state of the system, S0, is

$$WA = v1, WB = v2 \quad \textbf{(2.1)}$$

When the transaction is confirmed, which occurs when BALANCE(WA) x is greater than or equal to 0, the system transitions into the state known as S1, which can be described as follows:

$$WA = v1\ x, WB = v2 + x \quad \textbf{(2.2)}$$

Comparable to how a query such as "Balance(WA)" gives Alice's wallet balance, reading data from a storage device allows you to access the data. In contrast, the contents of Alice's wallet can be obtained using a query such as "Balance(WA)". The nodes in the network can frequently reach an agreement on the outcomes of the transaction after only one query, which means that the state of the system is not impacted in any way. Utilizing a process that is known as a consensus algorithm allows for a distributed system to arrive at a decision that is shared by all of its participants regarding the results of a transaction. Proof of work, also referred to as PoW, is a consensus method that is used by well-known blockchains like Bitcoin and Ethereum [13,14,32]. Proof of work is also abbreviated as PoW. There are several

different consensus strategies accessible now. Proof of stake (PoS), proof of capacity (PoC), proof of authority (PoA), and proof of significance (PoI) are a few examples of these. Byzantine fault tolerance is another. On the other hand, in contrast to other processes that are more efficient, such as PoS and PoC [30], the PoW mechanism has a larger cost and requires a greater amount of energy to operate. According to the level of access that each user has to the blockchain network, it is feasible to divide blockchain networks into four primary types [30]. These categories may be found below. These types of BCNs are referred to as

i. Public
ii. Private
iii. Consortium
iv. Hybrid networks.

As long as they don't break the rules, participants in a blockchain network that is open, public, or global are free to join, quit, and do other actions according to their own whims, as long as the network's rules are followed. Participants are not restricted from acting on their own volition at any point during the event. In the world of public blockchain networks, two of the most well-known instances are Bitcoin and Ethereum. On the other hand, approved nodes are the only ones who are able to participate in a private BCN, which is also known as a permissioned BCN. Both of these terms refer to the same thing. Handling the authentication and authorisation of nodes in a network is a responsibility that falls on the network's management or whoever owns the network. One component of network administration is controlling the identities of nodes that are permitted to participate in the network. Consortium business computer networks are a specific kind of private business computer network in which all of the users are linked with the same firm or organization, or with a collection of businesses that cooperate together on projects. These networks are also known as "cooperative" business computer networks. There is a possibility that a hybrid network will have BCN components that are of a public or private nature respectively. They protect the data's privacy by allowing only approved nodes to join the network and by relying on the agreement established by the public nodes to authenticate transactions that do not involve the data's private nature. This ensures that only authorized nodes can access the data. A hybrid

blockchain community network is an ideal alternative for supply chain management and other Internet of Things systems [16] because it ensures the confidentiality of data and the authorization of transactions. A blockchain network is composed of two basic categories of computer nodes, which are known as verifiers and ordinary nodes respectively. Verifier nodes are the ones in charge of determining whether or not a transaction is legitimate. These nodes are responsible for storing an accurate copy of the blockchain's data structure. These nodes have a few different names, one of which being "complete nodes," which is also one of their names. Their processing power as well as the amount of memory they have available has improved. They help ensure that the data is accurate, that smart contracts are carried out as expected, that the network is secure, and that consensus is reached. Through the use of communication protocols such as Gossip and Kademlia [16], they are able to speak with one another and perform financial transactions. Heavy nodes, on the other hand, have significantly higher requirements for both memory and processing performance, whereas normal nodes have lower requirements in both of these areas. They are able to gain some information about the current status of the blockchain, despite the fact that they do not hold a copy of the blockchain ledger. This information can be acquired from the full nodes. Despite the fact that they do not have access to the ledger itself, they have managed to accomplish this. The components of blockchain systems that are generally agreed upon as holding the highest significance are outlined in Table 1, which can be found here. A distributed ledger and a network of computers located in different parts of the world are the two main components that make up the blockchain technology. The technology has many more possible applications than are now being studied, some of which include digital currencies like Bitcoin and Ethereum, although this is not a complete list of the technology's applications. In this section, we will focus on the applications of the technology that are used the most frequently. The traditional ways of conducting digital payments involve a third party (often a bank, other financial institution, or credit card company) that acts as a trusted party between the payee and the payer [33]. This third party sits between the payee and the payer and facilitates the transaction. This process consists of more than one step; nevertheless, the steps that are most significant include validating the transaction, verifying the recipient's bank balance, and confirming the payment. Automating the procedures of verification and validation all throughout the network is something that is made possible by

blockchain-based payment systems like Bitcoin and Ethereum. The amount of time needed to complete a transaction is cut in half, which is one of the primary benefits it provides. Other benefits include a reduction in the costs that are associated with the employment of intermediaries [30]. There is a chance that so-called "smart contracts" can be carried out on blockchain networks, which would open the door to the potential of automating business procedures. The only distinction that can be made between traditional business contracts and smart contracts is that the former are written in computer code, whereas the latter are performed automatically and in real time on the nodes of a blockchain network [10]. As a consequence of this, smart contracts are the appropriate option for the management of complex financial transactions. The validity of the results of the execution will be validated by the miners that participate in the blockchain. Using smart contracts to assure compliance with contractual commitments not only reduces the amount of time and money spent on corporate operations, but also ensures that contractual obligations are met. They have a greater ability to automate financial transactions, audits, online trades, document approval, and the management of supply chain administration [10]. E-governance is the process of issuing citizenship certificates, collecting taxes, delivering social securities, holding elections, and making use of crowdsourcing all through the utilization of information and communication technology [34,35]. The phrase "e-governance" refers to the process that is referred to by the term "e-governance." Putting blockchain technology to use in e-governance has the potential to streamline and improve a significant portion of the administrative labor that occurs behind the scenes. Researchers from a variety of countries, including Estonia and China, have been awarded funds to research how blockchain technology could be incorporated into e-governance systems in order to improve the effectiveness and dependability of the provision of public services [36,37]. Data Redundancy: The distributed data storage that a blockchain network utilizes is one of its most significant components [16]. It is necessary for the compute nodes that make up a public or private blockchain network to keep an encrypted copy of the data that is vital to the apps running on the network. The best option to restore data that has been lost or damaged in a repository is to import it from other users who are connected to the same network. This may be done by selecting peers from the network and clicking the "Import" button. One application of blockchain technology is the creation of a decentralized database by the DokChain project. This database has the

potential to be utilized for the management of both medical and financial records. This program improves the data integrity, auditability, and overall efficiency of healthcare transactions and procedures, as well as other transactions and procedures connected to healthcare. The blockchain is a digital ledger that is openly distributed and keeps transactions recorded in a permanent chronological order [60]. This ledger is also known as the blockchain. A peer-to-peer network is being utilized to keep this order in tact. When a new batch of transactions is added to the chain, a new block is generated and added to the chain. This happens whenever the chain is updated with the new transactions. It is possible to define a blockchain in its most fundamental form as an effort made by a network of computers that are not managed by a single controlling authority to construct a series of data entries that cannot be updated. This is the definition of a blockchain in its most fundamental form. Through the use of cryptography, each individual data block is first encrypted, and then that encrypted block is linked to the one that comes after it in the chain. Because blockchain technology eliminates the need to rely on a centralized system, it paves the way for untrustworthy entities that share shared interests to establish a reliable, immutable, and transparent trading and distribution history [61,62]. Blockchain technology also makes it possible for untrustworthy groups to work together. In spite of the fact that blockchain consists of a large number of moving parts and is based on cryptography and distributed networks, it is possible to gain a deeper comprehension of the technology. In addition, you are able to construct your understanding of the complicated overall system by using the subcomponents that have been explicitly presented as a foundation. Implementations of the blockchain technology can be seen in both public and private spheres [63]. Because the blockchain data is stored in a public ledger, every user can take part in the operation of the blockchain network. Each user contributes to the upkeep of the distributed ledger and helps ensure that it will continue to be reliable by confirming transactions and providing correct services. Transactions involving cryptocurrencies are almost exclusively recorded on public blockchains at this time. The private blockchain is secure, and the only people who are allowed access to it are those who have been verified. It is entirely up to the creator of the private blockchain to decide whether or not to make any modifications to pre-existing entries or even to delete them entirely. The utilization of blockchain technology within the company's internal systems was backed by a variety of various business models. Chain blocks are transactions that have been digitally signed and

are stored in a decentralized electronic database [13]. [Note: chain blocks are not to be confused with blockchain blocks]. After the verification process and the reaching of a consensus, each block is given a cryptographic connection to the records that came before it in the chain. When a new brick is added to the construction, it becomes a great deal more difficult to rearrange the blocks that are already there. This is because each new brick adds another layer of complexity to the structure. When we talk about the confidentiality (or, privacy) [38] of data (or, a message) that is stored on a storage device (like a hard disk, RAM) or transmitted through a transmission channel (like an Ethernet cable, fiber optics, radio signal), what we mean is to keep information secret from anyone other than the person who is legally entitled to the information or the person who is intended to receive it. Examples of storage devices include hard disks, RAM, and fiber optic cables. When one person, let's call her Alice, sends a message to another user, let's call him Bob, on the other side, the secrecy of the message ensures that no third party, not even an intermediary like Eve, can read the message because it is delivered through a public channel (medium). When one user, let's call her Eve, sends a message to another user, let's call him Bob, on the other side. It is conceivable for the sender and recipient of an electronic mail or other digital or analog communication to wish for their dialogue to remain private. This is because both digital and analog messages can be encrypted. This could be done out of respect for the sender's right to privacy or because it is required by law [39]. Both of these reasons are valid. Since the Middle Ages up until the present day, when information travels at the speed of light, it has been an imperative necessity to keep the anonymity of one's data [40]. Other encryption methods, such as Advanced Encryption Standards (AES), Data Encryption Standard (DES), Blowfish, Rivest-Shamir-Adleman (RSA), and Elliptic Curve Digital Signature Algorithm (ECDSA), can also be used to preserve the confidentiality of data or communications [41,42]. Some of these algorithms are listed below. Figure 4 provides an outline of the process that can be followed to encrypt and decrypt data in a format that is simple to understand. When information (or messages) are encrypted, they are first jumbled up in such a way that it is hard for unauthorized parties to decrypt them. This process is known as encryption. Encryption methods that are known as symmetric encryption (i) and asymmetric encryption (ii) are the two that are utilized the majority of the time to safeguard and secure data. When employing symmetric encryption techniques, both the process of encrypting and decrypting data

must make use of the same private key in order to be successful. [41,42] Some algorithms that adhere to symmetric encryption approaches are Blowfish, Advanced Encryption Standards (AES), and Data Encryption Standards (DES). These are just a few examples. When employing asymmetric encryption methods, the enciphering and decoding processes each make use of their own unique keys in order to successfully perform their respective tasks. This is because symmetric encryption methods share a key between the two processes. Each individual and organization generates their own unique set of public and private keys, which are connected to one another mathematically. Before transmitting the message, the sender encrypts it with the recipient's public key so that it cannot be read by anyone else. Authentication is the process of determining if a user or communication party is a valid human user as opposed to a non-human user [41,42]. Authentication refers to the act of verifying whether a user or communication party is a legitimate human user. If Bob employs this strategy, he will know without a doubt that the person he is chatting with is Alice and not Eve. Over the course of time, Bob will acquire the ability to utilize this technique to verify that messages are coming from Alice and not Eve. This capacity will grow over the course of time. The procedure by which a person or organization is given control over certain items of data or hardware is referred to as a "authorization," and the term "authorization" refers to that operation itself. The term "authorization" also refers to the operation itself. Alice and Bob, who are both users of the system, might have read, write, and execute permissions over a file, while Eve, who is also a user, might not have any of these permissions [41]. Message (or data) integrity [38] assures that a message has not been altered in any manner while it was being stored or sent. This can refer to either the integrity of the message or the integrity of the data. Many different kinds of digital communication, such as e-mail and instant messaging, amongst others, rely on the fact that digital messages are completely authentic in order to function properly. Message integrity guarantees that Bob will receive a copy of message m0 whenever Alice gives Bob a copy of message m. In this particular setting, the value of m will be identical to that of m0. In the context of the Internet of Things (IoT), the term "data integrity" refers to the assurance that information that is being sent between any two devices that are part of an IoT network has not been altered while it was in transit. This can apply to any two devices that are connected to the same IoT network. If the locations, routes, or timing of IoT sensors are changed in any manner, even slightly, the dependability and

usability of the entire system will suffer as a direct result. Users, computing nodes, processes, or other entities that require or request a service (such as a web server, email server, data server, telephone, power, or network bandwidth, etc.) must have immediate access to both the service and its associated resources (such as data, storage engine, computational engine). Web servers, email servers, data servers, and telephones are a few examples of the several sorts of resources that fall under this category.

2.3 Chapter Conclusions

Because of the availability feature of the Internet of Things, the numerous nodes that comprise an IoT network are able to interact with one another as well as with the people who own or make use of them. This makes it possible for IoT networks to fulfill their primary purpose of providing information and control over physical objects. Temperature sensors, for example, need to be accessible in order for measurements to be taken across an industrial IoT's full of operations. Loss of sensors that monitor factors such as humidity and pesticide levels can put agricultural IoT production and supply chains in a potentially dangerous position [43]. The effect of proprietary lock-in software is another factor that can restrict users' access to data generated by the Internet of Things. This effect may compel manufacturers or suppliers to employ dated Internet of Things equipment or services, and it may even restrict them from exporting data collected by Internet of Things devices in some scenarios.

3. INTERNET OF THINGS IOT (ARCHITECTURE AND SECURITY PROTOCOLS)

3.1 Introduction

Depending on the range, throughput, power consumption, and application domain, these technologies can be classified into 4 main categories (see Figure3.1):

Figure 3.1: Categories of Communication Technologies [18]

Wireless Wide Area Networks (WirelessWideAreaNetwork (WWAN)): these networks are considered to be the most extensive networks. They generally represent networks with low power consumption wireless links (Low Power Wide Area Network (LPWAN)) such as LoRaWAN [124] and Sigfox [18] (with a theoretical throughput of 0.3 Kbits/S up to 50 Kbits/S), and cellular networks such as GSM, UMTS, and LTE They can have a theoretical speed of 2 Mbits/S (case of 2G) up to 100 Mbits (case of 4G*). WWANs also include satellite networks such as the Global Positioning System (GPS) [65].

Wireless Metropolitan Area Networks (WMAN): are based on the IEEE 802.16 standard. This category can have a range of 4 to 10 km and offers a useful throughput of 1 to 70 Mbits/S. The best known WMAN technology is WiMax

Wireless Local Area Networks (WLAN): these networks have a range of one hundred meters, the equivalent of a business premises. In theory, they can

provide a speed of more than 50 Mbits/s. The best-known technologies are Wi-Fi (see

Wireless Personal Area Networks (WPAN): relate to short-range wireless networks, of the order of a few tens of meters. Just as the range varies from one WPAN technology to another, the throughput also varies. The latter can be at 250 Kbits/S (ZigBee) up to 1 Mbits/S (case of Bluetooth). These technologies follow the IEEE 802.15 family, the best known those of the IEEE 802.15.1 (Bluetooth) sub-standard, and those used in the field of wireless sensor networks (WSN for Wireless Sensor Networks) which mainly follow the sub-standard. IEEE 802.15.4 standard such as ZigBee, OCARI, ISA100, 6LoWPAN, etc. These technologies are known for their optimal energy and resistance to interference in industrial areas.

Wireless networks represent data transport mechanisms between objects, and between objects and conventional wired networks. These technologies are used to receive and transmit information using electromagnetic waves. Wireless networks allow devices to be moved in different degrees of freedom while maintaining communication with each other. They also offer greater flexibility than wired networks and greatly reduce the time and resources needed to set up new networks and make it easier to create, modify or tear down networks [65].

These technologies are very varied, they differ according to their ranges, their speeds, and their use cases. In what follows, we will cite the best-known technologies, starting with the most extensive up to personal networks. We are mainly interested in WPAN networks, more precisely in wireless sensor networks (Wireless Sensor Networks WSN) which represents a sub-domain of the IoT mainly using objects with low computing and storage power, and constrained in energy. WSN communication technologies use the IEEE 802.15.4 standard.

The objective of this chapter is to provide a state of the art on different communication technologies and domains used by the IoT and to explain their architectures and mode of operation. We will mainly deal with the security aspects, in particular the authentication and key management mechanisms.

3.2 Wireless Networks And Their Security Mechanisms

3.2.1 Wireless wide area networks (WWAN)

Wide-area networks make it possible to cover very large areas (on a scale of several kilometres), and encompass different technologies such as low-energy wireless links (Low-Power Wide-Area Network (LPWAN)) (e.g. LoRaWAN), cellular technologies (eg 1G, 2G, 3G, 4G, etc.), and satellite networks (eg GPS).

3.2.1.1 LoRaWAN

Long Range (LoRa) is a modulation technique for delivering a very long range signal. This modulation technique is based on spread spectrum techniques and a variation of Chirp Spread Spectrum (CSS) [47] with built-in Forward Error Correction (FEC) mechanisms. In order to broadcast a signal, LoRa uses an entire channel of bandwidth, which makes the signal more reliable and robust against noise. LoRa represents the physical layer. It can be used by different higher level protocols, and deployed under different topologies (mesh, star, etc).

*LoRaWAN*is the protocol of the Media Access Control (MAC) sublayer which is standardized and normalized for low power wide area networks (LPWAN) thanks to the LoRa Alliance [124]. The latter also aims to make LoRaWAN interoperable with other communication technologies. LoRaWAN is fully bidirectional. It has an architecture totally adapted to the IoT, allowing it to easily locate mobile objects. It is deployed for national networks by major telecommunications operators (eg Orange). LoRaWAN networks are generally presented by a star-of-star topology in which gateways connect terminals (eg sensors, computers, etc.) to a central network server, which is in turn connected to an application server. Communication between gateways and terminals is done using one-hop Long Range modulation technique (LoRaTM), or Frequency Shift Keying modulation technique (FSK) [124]. Whereas communication between gateways and network server, and between the latter and the application server, is carried out via the IP standard. The figure3.2shows the architecture used and deployed in LoRaWAN.

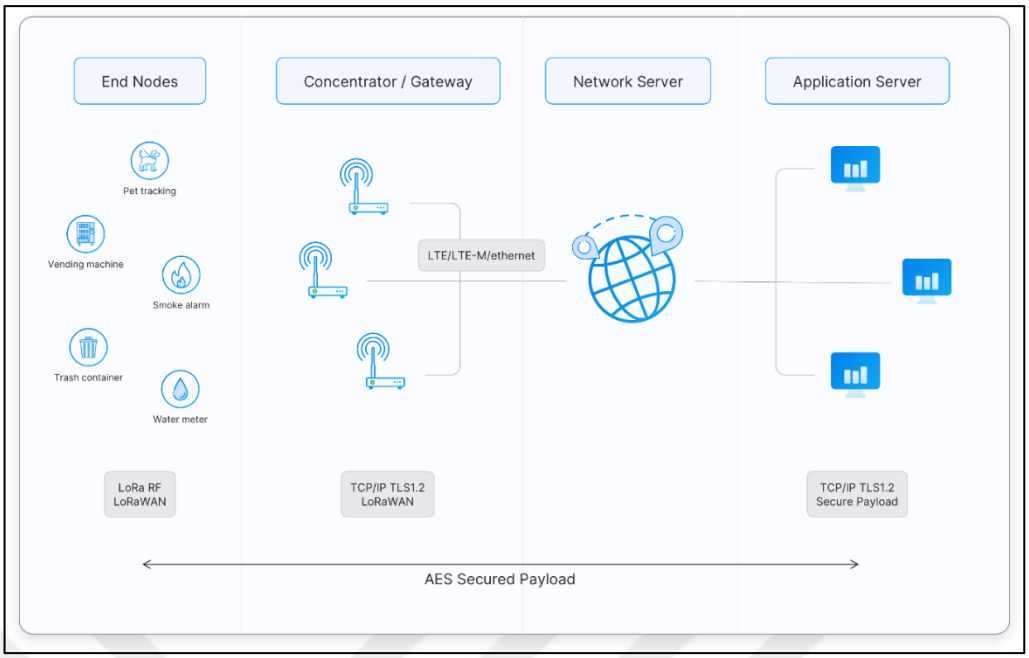

Figure 3.2: The LoRaWAN Architecture [34]

In order to optimize the trade-off between network latency and battery life, the LoRaWAN protocol uses 3 classes (A,B, and C) of objects. Each object implements at least the functionalities of class A. Classes B and C are optional, but remain compatible with class A (see [124] for more details).

a) Security in LoRaWAN

The LoRaWAN security policy ensures the basic mechanisms which are object authentication, confidentiality and data integrity. This policy also defines key sharing techniques.

According to the LoRaWAN specification [124], (1) Over-the-air authentication and key exchange (also known as OTAA) is the first approach that is being put into action. Between the LoRaWAN network server and each device, an application key, also known as an AppKey, is used to send a one-of-a-kind symmetric key that is 128 bits in length. This key is transmitted using an application key. In order for a device to become part of a LoRaWAN network, it must first transmit what is known as a "join request." This is a mandatory step in the process. This request must include the AppEUI, the DevEUI, and a random nonce of the object with a length of two bytes that is referred to as the DevNonce. This is required to prevent any attempts at cryptanalysis. In addition, a message integrity code, abbreviated as MIC and also known as a Message Integrity Code, must be included

in the request. The four-byte encoding of the message's AppKey signature is what's known as the "Message Integrity Code," or "MIC".

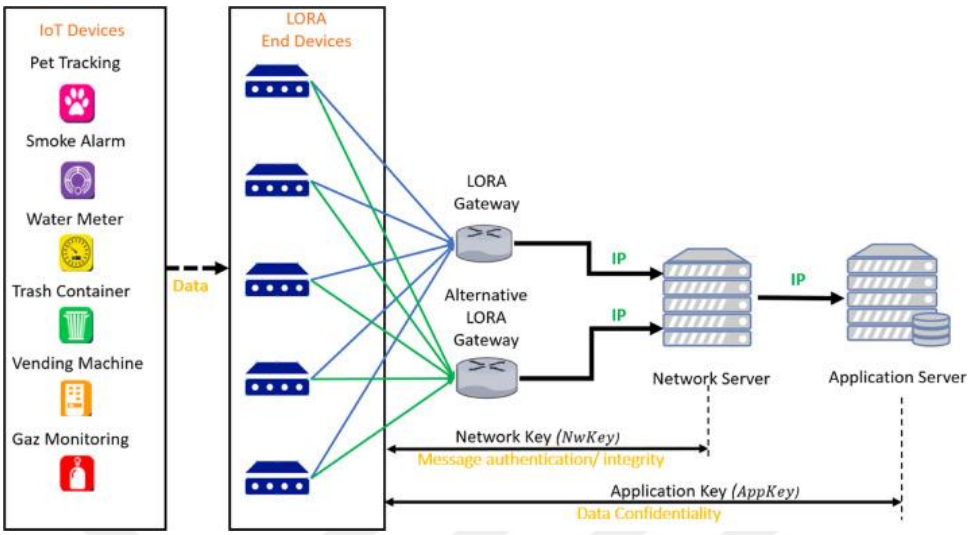

Figure 3.3: The LoRaWAN Security Protocol [124]

3.2.1.2 Technologiescellular

They represent mobile radio systems. These technologies have gone through 4 generations and the 5th is under development. The first (1G) appeared around the 1970s. It was based on an analog mobile communication system. 1G exploited two great technical inventions: the microprocessor and the transport of data between mobile phones and the base station. This technology was very expensive, and it used very large devices. This analog system was replaced as soon as another more efficient digital system appeared (the 2nd generation, or 2G). 2G was invented at the end of the 1980s, it allows voice signals to be transported and data to be exchanged digitally. This technology ensures better quality and greater capacity at a lower cost to the user. The Global System for Mobile Communication (GSM) represents the 2G standard. This generation represents an evolution towards an enriched and diversified offer of services such as the launch of the Short Message Service (SMS) short message market. It was also the beginning of mobile Internet services by creating the Wireless Application Protocol (WAP). Then, at the end of the 90s, the third generation (3G) came out - labeled IMT 2000 by the International Telecommunications Union (ITU) [This generation represents an evolution towards an enriched and diversified offer of services such as the launch of the Short Message Service (SMS) short message market. It was also the beginning of mobile Internet services by creating the Wireless Application Protocol (WAP). Then, at the end of

the 90s, the third generation (3G) came out - labeled IMT 2000 by the International Telecommunications Union (ITU) [This generation represents an evolution towards an enriched and diversified offer of services such as the launch of the Short Message Service (SMS) short message market. It was also the beginning of mobile Internet services by creating the Wireless Application Protocol (WAP). Then, at the end of the 90s, the third generation (3G) came out - labeled IMT 2000 by the International Telecommunications Union (ITU) [134]- it offers more efficient communications services for voice transport and data transfer. The 3G standard is called the Universal Mobile Telecommunications System (UMTS). Compared to 2G, UMTS is characterized by its high speed, it offers additional services such as mobile payment, localization, multimedia (video telephony and multimedia messages), international roaming, etc. In December 2010, the ITU granted the Long Term Evolution (LTE) and Worldwide Interoperability for Microwave Access (WiMAX) standards the commercial possibility of being considered 4G technologies. We will explain the WiMAX technology From the 3GPP (3rd Generation Partnership Project), which is a coordination body between telecom standardization institutes such as the European Telecommunications Standards Institute (ETSI), the Association of Radio Industries and Businesses/Telecommunication Technology Committee (ARIB/TTC, au Japan), the China Communications Standards Association (CCSA), and the Alliance for Telecommunications Industry Solutions (ATIS), LTE aims to have very high speed (around 40 Mbits), a cell size of (1) 5 km with optimal performance, (2) 30 km with reasonable performance, and (3) 100 km with acceptable performance. It also aims to allow co-existence with current standards, in other words to ensure that customers switch from one standard to another in a completely transparent way, without interruption of communication or manual intervention. And to finish, [14] explains that 5th generation (5G) will have to be a paradigm shift that includes massive bandwidths, extreme densities of base stations and devices, and an unprecedented number of antennas. Unlike the previous four generations, 5G will also be highly integrative, i.e., it will link any new 5G interface and spectrum with LTE and Wi-Fi to deliver universal high-speed coverage and a seamless user experience.

a. Security in LTE networks

In this part, we are only interested in LTE, because from the year 2012, the latter has become the most deployed technology. According to [23], more than 85%

of subscribers use this technology. The 3rd Generation Partnership Project (3GPP) specification TS36.300 [122] shows a simplified LTE architecture (see Figure3.4). The UEs communicate with the eNBs in the E-UTRAN, which in turn communicate with the MMEs - passing through gateways if necessary - which are connected to the HSS / HLR. According [120] LTE provides the main security services, which are object authentication, confidentiality and data integrity. Authentication and key exchange: In order to ensure mutual authentication between a terminal (e.g. Subscriber Identity Module (SIM) card) and an HLR or HSS through eNBs and gateways, and to secure access to mobile networks, LTE opts for the 3GPP protocol. Authentication and Key Agreement (3GPP AKA). In addition to authentication, the latter also serves as a key exchange mechanism. The Authentication part of the AKA protocol makes it possible to verify the identity of the user while the Key Agreement part allows the generation of session keys which ensure the confidentiality and integrity of the data exchanged on a user's network traffic. AKA represents a protocol that uses a challenge/response mechanism based on symmetric cryptographic keys. The scheme in Figure3.5explains the AKA protocol.

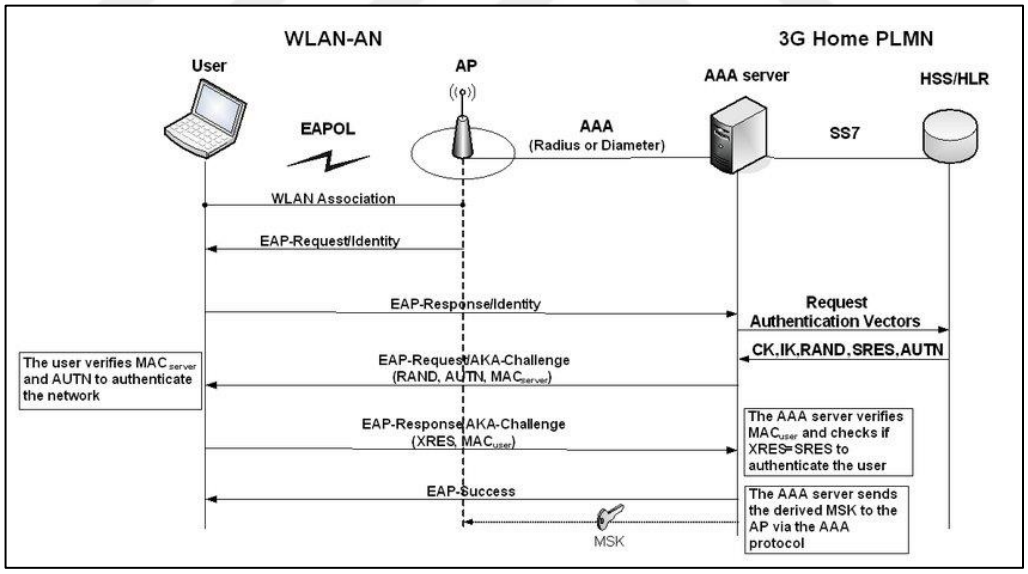

Figure 3.4: A Simplified Presentation of the AKA Authentication and Key Exchange Protocol [56]

Authentication is based on a secret and unique symmetric key K, pre-shared between the UE and the HLR. First the UE sends an association request to the HLR via an MME, which in turn transforms the association request into a request for authentication information (request of the vector d authentication) and sends it to the HLR. These vectors are:

i. RAND (challenge): a random number with a size of 128 bits generated by the HLR, which serves as an input parameter for the generation of other parameters;

ii. XRES: the expected response (compared to the challenge), it will be compared with the RES value generated by the UE;

iii. AUTN: a token that allows network authentication to the UE. This token includes an encrypted sequence number (SQN) (SQN $\oplus$ K), and a Message Authentication Code (MAC) generated from a hash function using SQN and K, which allows authentication of the HLR to the UE;

iv. KASME: is the key derived from CK and IK which are derived from K. CK and IK respectively represent an encryption key and an integrity key between the UE and the HLR. Table3.1 summarizes and shows the hierarchy of all the keys generated to ensure confidentiality and integrity services between the different entities in the LTE network architecture.

After, upon receipt of the quadruplet (RAND, AUTN, XRES and KASME), the MME keeps XRES and KASME (used to generate other keys see Table3.1), transmits RAND and AUTN to the UE (via an authentication and encryption request), and waits for a RES response from the latter. the UE verifies the received AUTN, then calculates the RES (a result TABLE 3.1 – Confidentiality and integrity keys used between the different LTE entities generated from K and the challenge) and sends it to the MME. The UE is authenticated if RES and XRES are identical. Once authenticated, the UE generates CK and IK and derived keys to ensure secure data exchange. The process of generating parameters and keys is summarized in Figure3.6.

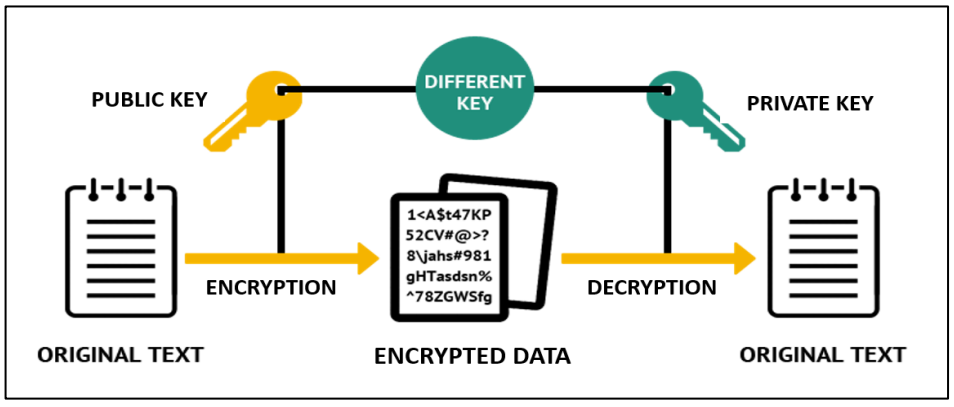

Figure 3.5: Generating Parameters and Keys [23]

Once mutual authentication and association are established, confidentiality and data integrity are ensured using the generated keys. LTE uses a privacy standard called the Evolved Packet System Encryption Algorithm (128-EEA3) and another for integrity called the Evolved Packet System Integrity Algorithm (128-EIA3) [60]. Both standards are based on the SNOW 3G encryption stream [5]. There is a version that uses the AES standard [60]

The 128-EEA3 privacy algorithm provides a stream cipher used to encrypt/decrypt blocks of data via a symmetric key (ex. CK). The data block can have a length between 1 and 232 bits [6]. The 128-EEA3 standard makes it possible to generate a keystream of L words. Each of the words is written on 32 bits, therefore we obtain a binary string

$$Z = L \times (Z[0]\, k\, Z[1] \,..\, k\, Z[31] \quad \textbf{(3.1)}$$

Where Z [0] is the most significant bit (Most significant bit (MSB)) of the first generated word, Z [31] is the least significant bit (Least Significant Bit (LSB)), and k is the operator which expresses the concatenation.

3.2.1.3 Satellite Technologies

The phrase "communication satellite" refers to a man-made spacecraft that is equipped with a transponder for the purpose of relaying and amplifying radio communications. This spacecraft is referred to as a "communication satellite." Because of the satellite that was launched into orbit, it is now possible to create a line of communication between two locations on Earth that are physically separated by significant distances from one another. Satellites used for communication have a wide range of purposes, some of which include but are not limited to television, telephone, radio, the global positioning system (GPS), the internet, and even specific applications in the military. The utilization of electromagnetic waves as a medium for the transfer of data in terrestrial wireless communications is the primary method utilized. These waves can only travel in a straight line because of the spherical form of the Earth, which causes them to encounter impediments along their path as they move over the ocean. Satellites are utilized in the field of communication due to their capacity to reflect a signal off of the earth's curvature and then transmit it back to the location where it was originally intended to be received. Radio and microwave frequencies are utilized by satellites that have been purpose-built for the purpose of

communication. Only a limited number of companies are permitted access to specific frequency ranges (frequency bands) by international organizations. This is done to reduce the likelihood of signals becoming muddled or otherwise disrupted. The probability of signal interference has been reduced as a result of the manner in which this band has been assigned its frequencies [89]. On April 6, 1965, Intelsat [54] launched the first commercial telecommunications satellite, called Intelsat I. This satellite allowed the transfer of images and voice, thus providing telephony applications, the broadcasting of television programs, and communication to planes and ships. At first, research and development of space communication technologies was restricted to international organizations such as Intelsat and Inmarsat [22]. Afterwards, in the early 2000s, thanks to technical progress and the strong growth of activity in this sector, many spatial groupings such as Globalstar Group [46], Iridium [106] and SpaceX [142] appeared. Today, satellite services no longer only concern large organizations, but also communication companies such as SigFox [101]. The objective of these companies is to adapt satellite technology to the increase in the number of intelligent objects, and to ensure a reliable connection between them, even those which are in the most remote areas of the globe. Satellites can be classified into two categories, satellites in geostationary orbit (Geostationary satellites that are located in geosynchronous orbit, which is also referred to as GEO, and satellites that are located in low Earth orbit, which is referred to as LEO. The first type of satellite communication system is the conventional sort, and it is the one that is stationed in geostationary orbit around the Earth. This particular variety of satellite communication technology always has the same orientation toward the sky. There is a delay in the transmission of signals between the GEO and the Earth because of the great distance that separates the two locations. As a direct result of this, GEO is not an ideal choice for a company that offers one-on-one communications as an option to their customers. A Low Earth Orbit (LEO) network is the second type of satellite network that exists. There are exactly 66 spacecraft that operate in low Earth orbit, and this relatively new LEO satellite communication system uses them to provide a global mobile satellite communication system [79]. The Low Earth Orbit (GEO) satellite orbits the globe at a far greater distance than the GEO satellite, allowing for a greater degree of precise control over its trajectory. The most significant advantages that LEO satellite systems have over GEO satellite systems are (1) low signal communication attenuation, (2) short signal communication latency, and (3)

large data communication channels that are narrower than those that are provided by GEO satellites.

a. Security in satellite networks

There are several works that aim to secure satellite communication networks. [84] studies the service of confidentiality in a two-way satellite network composed of two mobile users who wish to exchange messages via a multi-beam satellite. Other works [140] offer the use of the Satellite Secure Sockets Layer (SSL) protocol [59] which represents the use of the SSL protocol in satellite networks to ensure user authentication, confidentiality and data integrity. [79] offers an interesting security protocol, designed mainly for LEO satellite communication systems. The Figure 3.7 shows a simplified network architecture. This architecture includes LEO satellites (SatLEO), gateways, mobile users (UM) and a network control center (Network Control Center (NCC)). The satellite manages communications between a mobile user and a gateway, a user

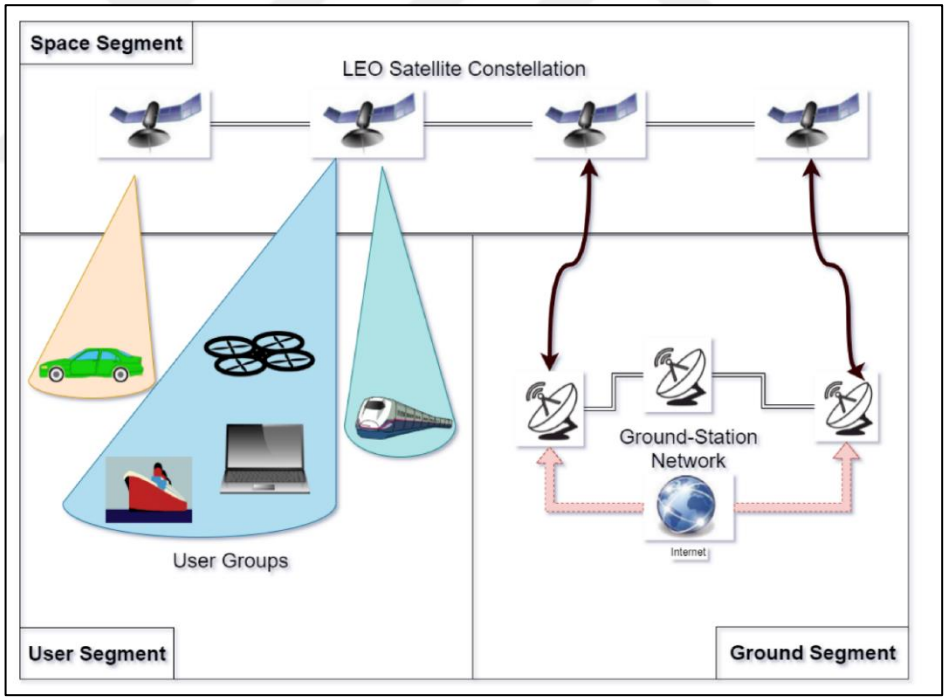

Figure 3.6: A Satellite Communication System (LEO) [37]

Mobile receiver and other mobile users, a gateway and other gateways, a gateway and the NCC, or a satellite and other satellites. The gateways represent relay points for the communication between the NCC and the satellites. In addition, they are connected to local networks to produce a diversified communication system.

b. Registration and authentication:

In order to be able to communicate, a mobile user must first (1) register, then -during its association- (2) authenticate. In the registration phase, the gateway assigns a permanent identity Uid, a secret key Kmd, and a temporary identity Tid to the user, then sends a copy of this information, associated with the appropriate LEO identifier (LEOid) to the NCC. The latter stores, in a secure manner, the quadruplet

Uid, Kmd, Tid and LEOid of each user.

Before each communication, a user must be authenticated. The authentication operation is depicted in Figure3.8as following:

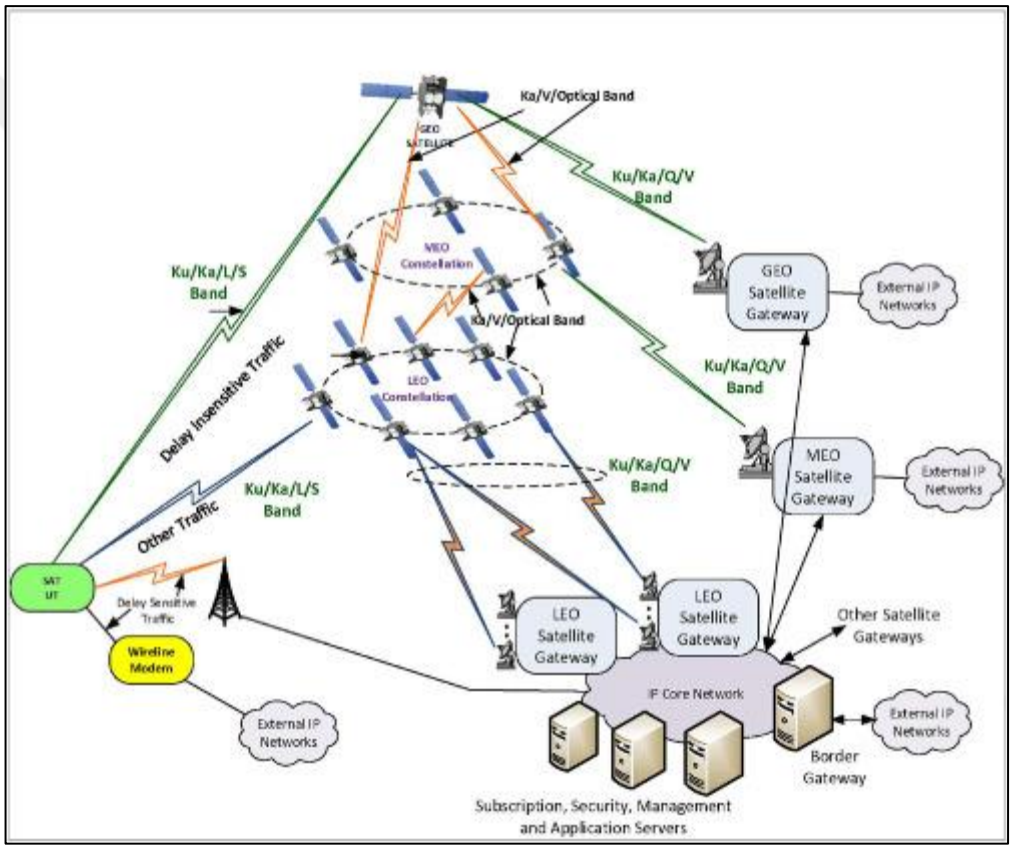

Figure 3.7: Authentication Mechanism of a Satellite System (LEO) [37]

The expression "{}_key", means encrypted with the key key. In this mechanism, encryption is established by the Data Encryption Standard (DES) [149]. First, the LEO satellite (SatLEO) sends an authentication request to the user. By receiving the request, the user creates and sends a message which contains the cipher of his identifiers (Uid and Tid) using Kmd associated with the Tid in clear. Then, this message is concatenated by the LEOid and then transferred to the NCC by the satellite. The NCC checks the validity of the LEOid then uses the Tid as an index to

search -in its database- for the Kmd session key (pre-shared with the user). With this key, he decrypts the message and obtains the Uid and the Tid. Afterwards, it checks the validity of the Uid, and makes sure that the two Tids (the one that is sent directly in clear with the decrypted one) are identical. If the data checks pass, then the NCC randomly generates a new Tid0 and a new session key K0id for the user and updates its database with this information. The fact that the decryption operation is successful, proves that the user is legitimate and it allows the authentication of the latter, because the Kmd key which is secret is only shared between the NCC and the user. The NCC in turn sends a response which contains the old Tid in clear with an encrypted part (by Kmd) composed of the triplet (Tid, Tid0 and K0id), the message is also associated by the LEOid. Finally, the LEO validates its identifier and forwards the rest of the message to the user. The latter decrypts the message with the old Kmd, checks the value of the Tid, and finally, stores (K0md and Tid0) to use them in a future authentication.

a. *Data Privacy:*

In [79], the data protection mechanism used is not explained, but they use the Data Encryption Standard (DES) for other operations such as authentication. DES is a symmetric encryption algorithm (block cipher), based on operations of permutation, substitution and the operator exclusive or ($\oplus$).

3.2.2 Wireless metropolitan area networks (WMAN)

Wireless metropolitan networks allow the coverage of very large geographical areas (on a scale of several kilometres), while ensuring very high speeds. They are based on the IEEE 802.16 standard, and the best known technology is WiMAX.

3.2.2.1 WiFiMax

*WiFiMAX*is a family of wireless communication standards based on the IEEE 802.16 set of standards This family defines several options of (1) physical layers (PHY) and (2) sub-layers of media access control (Media Access Control (MAC) of the data link layer This technology was created by the WiMAX Forum [161]. The latter represents a consortium created in 2001 which includes more than 100

members including major suppliers such as AT&T [119], Fujitsu [165] and Intel [62].

*WiFiMAX*can be deployed in a mesh network topology, but typically it uses a topology called point-to-multipoint [125]. The latter is composed of central base stations, each covering an area with a radius of less than 3.5 km, and connecting several users (see Figure3.9). One or more base stations can be connected to the Internet.

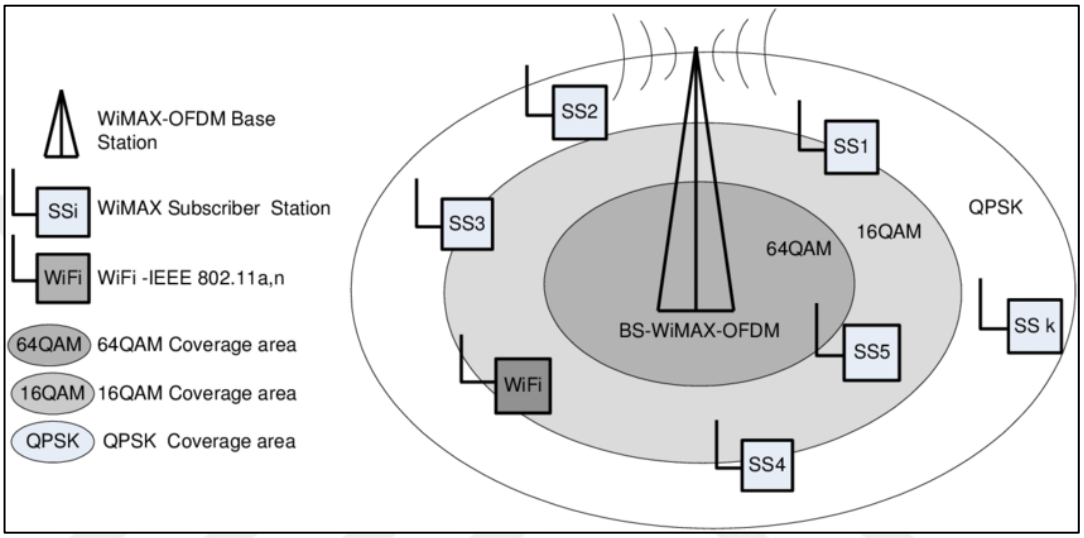

Figure 3.8: The Point-To-Multipoint Topology of WiMAX [38]

WiMAX is classified into two categories: (1) Mobile WiMAX (IEEE 802.16e) and (2) Fixed WiMAX (IEEE 802.16, IEEE 802.16c, IEEE 802.16a, IEEE 802.16f, IEEE 802.16m). In what follows, we are only interested in the first category, because it supports the mobility of objects, allows a transparent transition from one relay to another, and it is more suitable than the second category to be used as a technology of IoT communications.

At the physical layer, Mobile WiMAX uses Scalable Orthogonal Frequency-Division Multiple Access (SOFDMA) modulation. This technique allows the sharing of radio resources in time and bandwidth, and adapts a quality of service (Quality of Service (QoS)) for each user [125]. WiMAX also supports Multiple Input, Multiple Output (MIMO) technology.

At the MAC sublayer, in wireless systems that use non-QoS access methods such as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA))[169], each user's traffic may be disrupted by other users at any time.

This poses a problem for certain sensitive applications (eg real-time monitoring application). The MAC sublayer of mobile WiMAX is designed specifically to solve this problem through (1) its connection-oriented communication. Indeed, before each communication, users must establish an end-to-end connection, therefore this allows a reliable transfer of data. Furthermore, this sub-layer deploys (2) a network access scheduling algorithm. This algorithm dynamically allocates resources to any user wishing to communicate. On the other hand, depending on the priority of the services, these radio resources can be increased or decreased. Consequently, this generates an optimization of the bandwidth,

a. Security in Mobile WiMAX (IEEE 802.16e)

The IEEE 802.16e standard uses a mutual authentication method called (Pairwise Master Key (PKMv2)), which can deploy (1) the Extensible Authentication Protocol (EAP) [8] or (2) Rivest Shamir Adelman Protocol (RSA) [138] with the use of X509 digital certificates [76]. This standard opts for a variety of strong cryptographic algorithms. It also ensures confidentiality services, data integrity, and protects against replay attacks.

b. Mutual authentication and key management:

First the base station (SB) authenticates the user and verifies his legitimacy. And then the user also in turn authenticates the SB to ensure that he is not connecting to a fake network (eg a network created by a malicious station). The SB sends an authorization key (Authorization Key (AK)) to the user with a set of security information (Security Association (SA)) which defines the security profiles supported.

This mutual authentication is achieved through one of two methods:

The first represents authentication based on the RSA asymmetric cryptographic algorithm [39]. This method is based on a pair of keys (private/public). A communicating entity wishing to authenticate itself must sign a piece of data (generally a hash) with its private key, which is secret and is known only by the entity which possesses it. RSA ensures that signature verification can only be done with the associated public key, and that there can only be one public key associated with the private one and vice versa. Consequently, this operation proves that it is the owner of the private key who made the signature. However, this public key does not

prove the identity of its owner, hence the X509 certificates. A digital certificate is a data structure containing information on the validity date, the issuer of the certificate, and information on the identity of the entity concerned. This certificate also contains the entity's public key. All certificate information is hashed (to protect its integrity) and signed by the private key of a certification authority, which the entities in question trust. In other words, the certificate allows a reliable association of the public key and the identity.

The second is authentication based on the EAP protocol. This protocol - described in [8]- does not specify any cryptographic algorithm, but rather uses different security policies and tools (e.g. password, token, etc). For example [35] offers EAP Password Authenticated Exchange, which is an extension of EAP based on pre-shared keys. These criteria relate to key generation requirements, the robustness of the keys used, mutual authentication requirements, protection measures against Man In The Midle (MITM) attacks and replay attacks, etc

After authentication, the standard requires an Authorization Key (AK) Management mechanism.

First when receiving an authorization request, coming from a user who is not yet authorized, the SB generates a new AK, then associates it with a value which indicates the lifetime of the AK, and sends this data to the user via an authorization response. The AK key represents a symmetric key allowing the exchange and generation of encryption keys. AK remains active until its time expires (it remains valid until the end of the grace period). If a user fails to re-request authorization before their current AK expires, the SB considers that user to be unauthorized, and no longer holds an active AK for that user. The user is responsible for re-requesting authorization from the SB and keeping their AK active. For each Key Request, the SB regenerates a new AK, assigns it a lifetime that is equal to the remaining lifetime for the old AK plus the base lifetime, and sends the response to the user. This operation is repeated each time the AK comes close to exhaling. As long as the period of one AK has not yet expired, the SB can support the exchange of the same user using two valid AKs. The exchanges of its messages are secured by (1) RSA (asymmetric encryption/signature) or (2) by EAP (explained previously). As long as the period of one AK has not yet expired, the SB can support the exchange of the same user using two valid AKs. The exchanges of its messages are secured by (1)

RSA (asymmetric encryption/signature) or (2) by EAP (explained previously). As long as the period of one AK has not yet expired, the SB can support the exchange of the same user using two valid AKs. The exchanges of its messages are secured by (1) RSA (asymmetric encryption/signature) or (2) by EAP (explained previously).

The figure3.10 summarizes the authorization mechanisms.

c. Confidentiality and data integrity:

Confidentiality and data integrity services are established at the MAC sub-layer level thanks to the AES encryption standard with the CCM mode of operation

Indeed, the encryption of the packets is carried out at the level of the MAC sub-layer via the AES-CCM encryption algorithm, using one of the keys derived from AK (one key for unicast mode, another for boradcast mode, etc.). These keys are 128 bits in size. Before encrypting the packet, a 4-byte sequence number is associated with the plain text. The sequence number is incremented after each packet transfer to protect against replay attacks. Each sequence number received more than once must be discarded. The AES-CCM can also generate a MAC, calculated from the plain text, to protect the integrity of the packets.

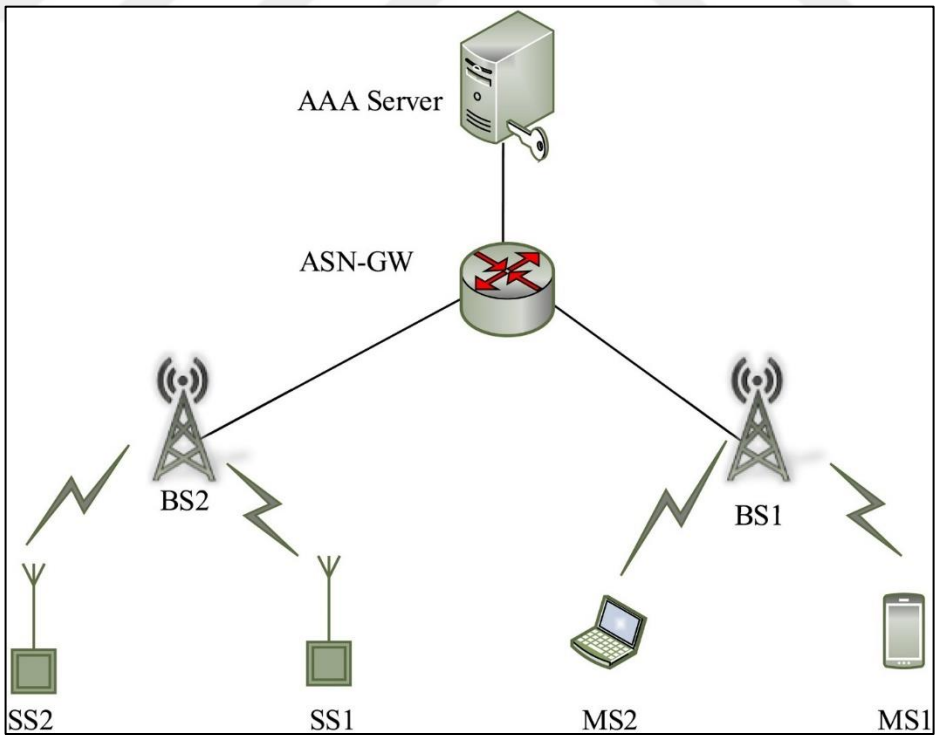

Figure 3.9: WiMAX Authorization Operation [39]

3.2.3 Wireless local area networks (WLANs)

Wireless local area networks represent networks on which an object can connect to a local area network (LAN) via wireless radio waves. WLANs - which follow the IEEE 802.11 standard - have a range equivalent to a building or campus network (one hundred meters). Wi-Fi is arguably the most widely used WLAN technology by businesses and individuals. In the following we will describe this technology, thus focusing on the security protocols that this technology deploys.

3.2.3.1 Wireless

Craig J. Mathias [112] [111] -director of Farpoint Group (a consulting firm specializing in the field of mobile networks and wireless networks)- believes that Wi-Fi will be the most suitable technology for the Internet of Things, and that it is this technology who is going to lead the revolution of this paradigm. This is explained by the fact that Wi-Fi offers several advantages, which are:

*Exploitation of an existing infrastructure:*today, most organizations have a Wi-Fi infrastructure. This technology offers major advantages in terms of capacity, coverage and ease of use. Adding more and more clients and applications has become a daily activity. Since IoT applications are often optimal (few transmissions and limited amount of data), an additional load of IoT data does not influence the performance of Wi-Fi, and in most cases it does not cause any problems. . Also note that many Internet of Things applications used by enterprises will simply be new applications running on smartphones and other devices that already use Wi-Fi networks.

*A compact size:*this technology can be deployed in tiny equipment (chip, module, etc.).

*Scalability:*expanding the coverage area and improving the capacity of Wi-Fi will be needed after a while, but in the short term, the IEEE 802.11ac standard [130] and the diversity of Wi-Fi modules already largely meet these needs.

*Fast connection establishment:*work currently being done by IEEE 802.11ai [129] Working Group, aims to improve setup time and connection establishment.

*IP-based communication:*as the IoT still requires the use of unique identifiers, then Wi-Fi already uses IP addressing, including IPv6, and all related protocols, in

this context, according to [112] “Wi-Fi technology is perfect for the Internet of Things”.

*Wireless*is a set of wireless communication protocols managed by the standards of the IEEE 802.11 group. It provides a network that allows several objects to be linked via radio waves. The Wi-Fi trademark initially corresponds to the name given to the certification issued by the Wi-Fi Alliance (formerly Wireless Ethernet Compatibility Alliance (WECA)) [13], an organization whose mission is to certify equipment that complies with the 802.11 standard, thus ensuring interoperability between them. The range of a Wi-Fi network can cover areas of several tens of meters.

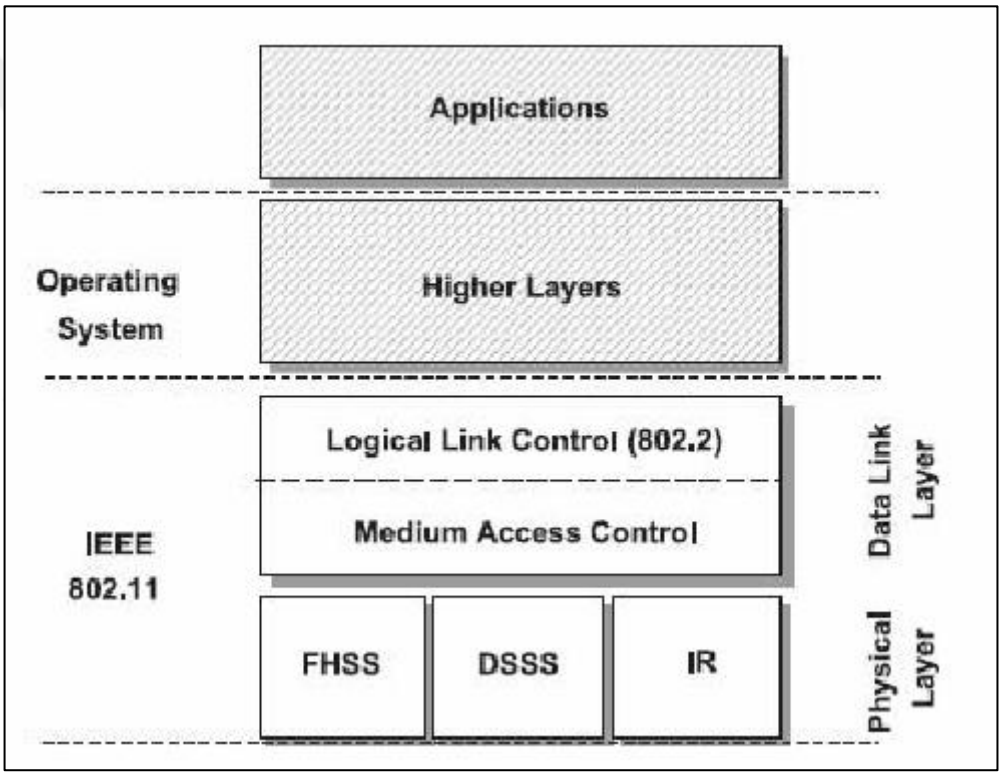

Figure 3.10: Layered Model of IEEE 802.11 [112]

*IEEE 802.11n:*802.11n was designed to be able to use the 2.4 GHz or 5 GHz frequency bands. The theoretical throughput reaches 450 Mbit/S (actual throughput up to 200 Mbit/S within a radius of 100 meters) thanks to MIMO and Orthogonal Frequency Division Multiplexing (OFDM) technologies. This standard can combine up to 2 non-overlapping 20 MHz channels, which in theory makes it possible to reach a theoretical total capacity of 600 Mbit/S in the 5 GHz band.

*IEEE 802.11ac:*it allows a high-speed wireless connection in the frequency band below 6 GHz (commonly known as the 5 GHz band). 802.11ac offers up to 1300 Mbps of theoretical throughput, using 80 MHz channels, or up to 7 Gbps of overall throughput in the 5 GHz band (5170 MHz to 5835 MHz).

The IEEE 802.11 standard defines the first and second lower layers of the OSI model, in other words, the physical layer and the MAC sublayer. The figure3.11illustrates the architecture of the model proposed by the 802.11 working group compared to that of the OSI model. In addition to the standards seen above which concern network throughput, there are other 802.11 standards which are used to ensure other functionalities such as interoperability (e.g. IEEE 802.11f), improved quality of service (IEEE 802.11e), security (IEEE 802.11i), etc.

d. Interconnection of Wi-Fi equipment

To connect the elements of a Wi-Fi network, there are generally two modes, the so-called Infrastructure mode, and the Ad-Hoc mode. The first is based on an access point (AP) allowing wireless devices to connect to each other and/or to the Internet. Stations within radio range with an AP form a Basic Service Set (BSS). Each BBS is provided with an identifier (BSSID) which is in the form of a sequence of 6 bytes corresponding to the MAC address of the PA.

The second mode works in a fully distributed way, it allows communication between two devices without there being an infrastructure. Stations within radio range form what is called an Independent Basic Service Set (IBSS).

It is possible to compose a network with several BSSs -thanks to a distribution system connected to their access points- to form an extended set of services (Extended Service Set (ESS)). An ESS is identified by an ESSID (or SSID) which is a sequence of 32 characters, which represents the name of the network. An ESS may also include an IBSS.

The figure3.12 summarizes the different modes of Wi-Fi interconnection.

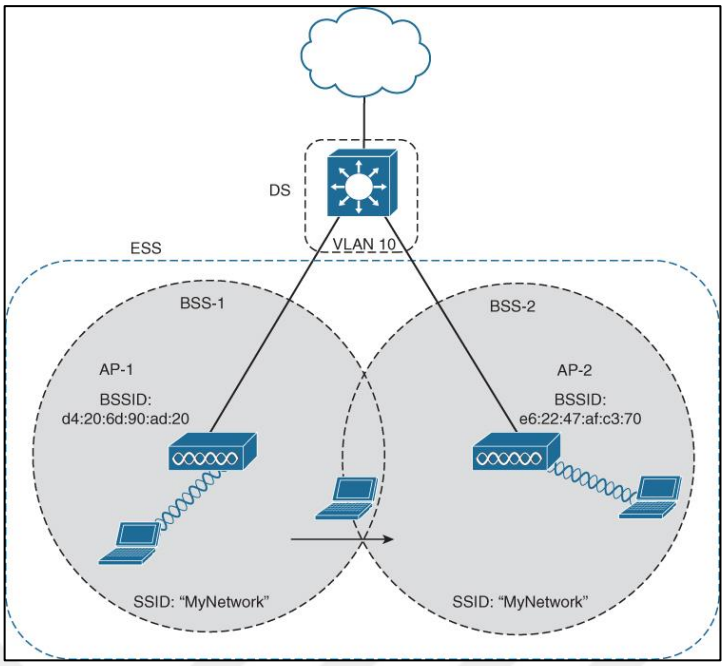

Figure 3.11: Wi-Fi Interconnect Modes [113]

i. Wi-Fi security

According to [18], Wi-Fi networks are relatively easy to hack. A hacker can easily exploit its vulnerabilities to gain access to wired networks considered to be protected. The most popular security mechanisms and protocols for Wi-Fi are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). The WEP standard is known for its weakness. According [25], the passwords used by this protocol can be cracked in minutes using only a basic laptop computer and a few widely available applications. This prompted the creation of the WPA1 and WPA2 standards (WPA version 1 and 2). WPA1 was a quick alternative to improve the security of WEP. The current standard is WPA2. In the following we will explain the WEP, WPA1 and WPA2 standards.

The WEP standard:

WEP is a protocol used to secure IEEE 802.11 frames, it uses the Rivest Cipher 4 (RC4) stream cipher algorithm [56] to ensure confidentiality, and the Cyclic Redundancy Check (CRC) algorithm [16] to ensure integrity. According [27], WEP relies on a pre-shared secret key between the communicating parties. Securing the data frame is done as follows:

First, to ensure integrity using the CRC algorithm, we calculate the checksum c(M) (4 bytes) of the message M, then we concatenate the two to get the plaintext P

= (M, c(M)). Then to ensure confidentiality, the plaintext P obtained in the previous step is encrypted with the RC4 algorithm. First, an initialization vector IV is chosen. Then, the RC4 generates what is called a keystream (keystream) according to the initialization vector IV and a key K. This keystream is represented by RC4(IV,K). Then we calculate the exclusive-or ($\oplus$) between the plaintext P and the keystream RC4(IV,K) to obtain the ciphertext (ciphertext) C = P$\oplus$RC4(IV,K). Finally, the initialization vector IV and the ciphertext C are transmitted via the radio transmission channel.

Noticed:control frames, and management frames are always in clear text [25].

For frame decryption, the recipient just reverses the encryption process.

Then, in order to verify the integrity of the frame, it separates the message M from the checksum c(M), recalculates a checksum c(M0) and compares it with c(M). In the end, only frames with valid checksums will be accepted by the receiver.

64-bit WEP uses a 40-bit encryption key to which is concatenated a 24-bit initialization vector. The key and the initialization vector thus form a 64-bit RC4 key. At the time the WEP standard was written, restrictions imposed by the United States government on the export of cryptographic means limited the size of keys. After these restrictions were removed, major manufacturers extended WEP to 128 bits using a 104-bit key [30]. Indeed, a 128-bit WEP key is entered as a sequence of 13 ASCII characters or 26 hexadecimal characters. Each hexadecimal doublet represents 8 bits of the WEP key (8 × 13 = 104 bits). Adding the 24-bit initialization vector results in a 128-bit WEP key. Today you can also use 256-bit and 512-bit WEP keys (24 bits reserved for the initialization vector and the rest for the encryption key).

One of the major weaknesses of WEP is that it does not include a key management protocol, so if the shared keys are not renewed regularly by users or administrators, then it is possible that they will be hacked (e.g. using cryptanalysis attacks). If an attacker gains control of a legitimate key, they can compromise the entire network.

The initialization vector is sent in clear text, and has a size of 24 bits (too small), this makes it possible to reproduce the same keystream in a short time (between 5 and 7 hours in an active network). This makes breaking keystreams a simple task for hackers (in less than 17 million combinations).

On the other hand, [17] believes that although WEP was not fully released and did not have a good technical design, it is considered a success because it provided significant protection for Wi-Fi when there were no other alternatives.

The WPA v1 and v2 standard:

To correct the weaknesses of WEP, the IEEE 802.11 Task Group I (TGi) created WPA (version 1 and 2). The latter operates in two modes: the first is called WPA-PSK (or WPA Personal). It is based on pre-shared keys, and designed for small networks (home network, office network, etc.) and does not require an authentication server such as Remote Authentication Dial-In User Service RADIUS or Authentication, Authorization, Accounting/Auditing (AAA)[136]. As for the second - which is called WPA-802.1X [12] (or WPA Enterprise)- is intended for corporate networks and requires the use of an authentication server. WPA-802.1X is more complex to install than WPA-PSK but it provides more security [110]. Both modes (WPA-PSK and WPA-802.1X) are available in both versions of the WPA standard.

WPA1:

WPA1 is based on a protocol called Temporal Key Integrity Protocol (TKIP), which represents a set of security mechanisms to ensure confidentiality and integrity [127]. From a main key, pre-shared or managed by the authentication server, WPA1 generates two types of keys: (1) the first named mK (64 bits) ensures data integrity by generating /checking the Message Integrity Code (MIC). (2) The second, called K (128 bits), ensures the confidentiality of data [128]. WPA1 also includes a sequence counter (a sequence number.

48-bit sequence) for initialization vectors to avoid replay attacks [110]. In the following, we will explain the secure message exchange mechanism in WPA1.

Sending a message: when sending a message, and to ensure its integrity, the sender calculates a MIC (64 bits) from mK and a Mac Service Data Unit (MSDU) using the Michael [31]. The MSDU is concatenated to the MICthe result is fragmented as a Mac Protocol Data Unit (MPDU). Next, a 32-bit checksum (CRC) is calculated for each MPDU (using the CRC32 [42]) to ensure its integrity.

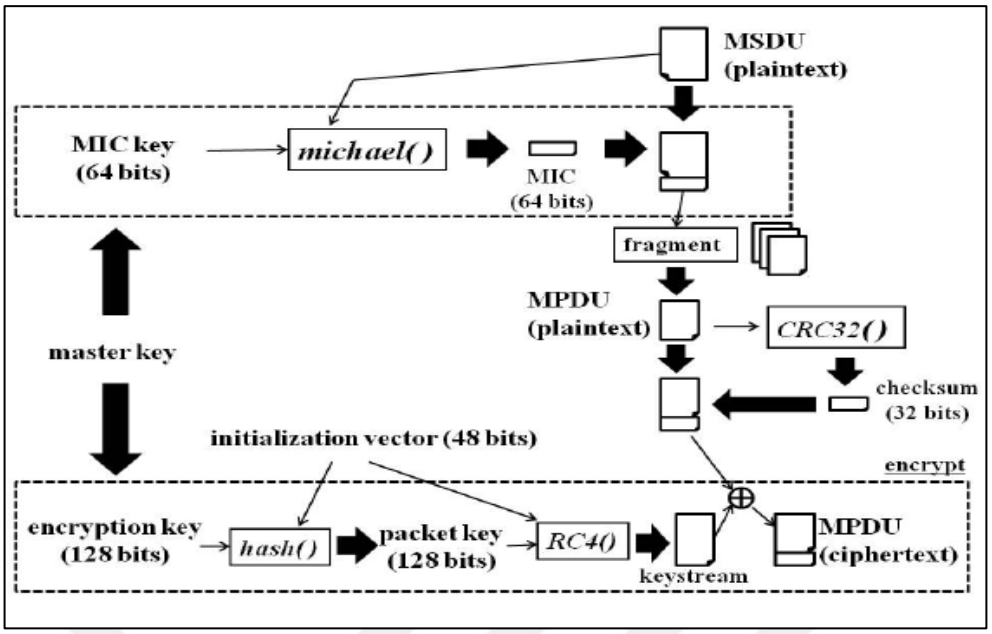

Figure 3.12: Process of Sending Secure Messages in WPA1 [42]

To ensure data confidentiality, WPA1 encryption is applied to all MPDUs associated with their checksums.

Encrypted MPDUs are associated with their plaintext IVs, and the result is sent to the recipient. The WPA1 send message preparation process is detailed in Figure3.13. k means the concatenation operation.

Receiving a message: The recipient receives an encrypted MPDU concatenated to a clear IV. The IV is compared with the IV value of the last MPDU received and accepted. If the new IV is less than or equal to the old, then the MPDU will be deleted. When the MSDU is accepted, the value of the IV is updated, and replaced with the largest IVs found in MPDUs. The process of receiving WPA1 is detailed in Figure3.14.

WPA2:

WPA2 is the successor to WPA1 which was ratified in June 2004 [16].

WPA2 makes it possible to establish a secure connection between two or more communicating entities thanks to a protocol called Counter Mode Cipher CBC-MAC Protocol (CCMP) defined in the IEEE 802.11i standard. It represents an alternative considered safer than TKIP. This standard is based on AES. The latter, compared to RC4 which is used by WEP and WPA1, provides robust security, with better performance. In order to create a secure communication channel, WPA2 requires the

completion of 4 phases [15]. (1) An entity wishing to communicate must first negotiate the security policy (authentication method, traffic management, etc.) with the access point. (2) Once they agree on parameters supported by both parties, they need to authenticate each other and (3) generate session keys using two types of negotiation, which are 4 way Handshake and the Group Key Handshake.

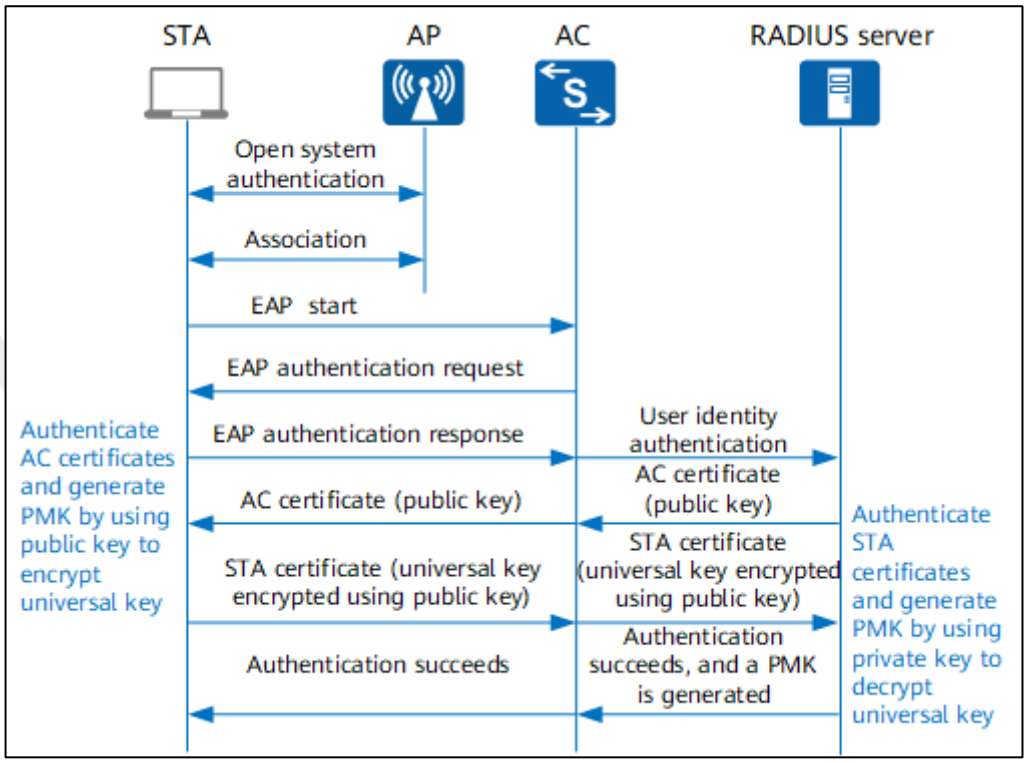

Figure 3.13: Process for receiving secure messages in WPA1 [43]

The 4 Way Handshake performs the following tasks:

i. Generation of pairwise transient keys (Pairwise Transient Key (PTK)) from the pairwise master (or master) key (Pairwise Master Key (PMK)) - which is in turn derived from the master key (MK)) in WPA Enterprise mode, or from PSK in WPA Personal mode. PTKs are used to generate other unicast keys and/or group temporary keys (Group Temporal Key (GTK), used to derive broadcast and multicast keys);

ii. From a PTK, the 4-Way Handshake can generate 128-bit confirmation keys (Key Confirmation Key (KCK), used to verify the integrity of frames during negotiation) and encryption keys of 128 bits (Key Encryption Key (KEK), used to encrypt the frames during this phase. And from

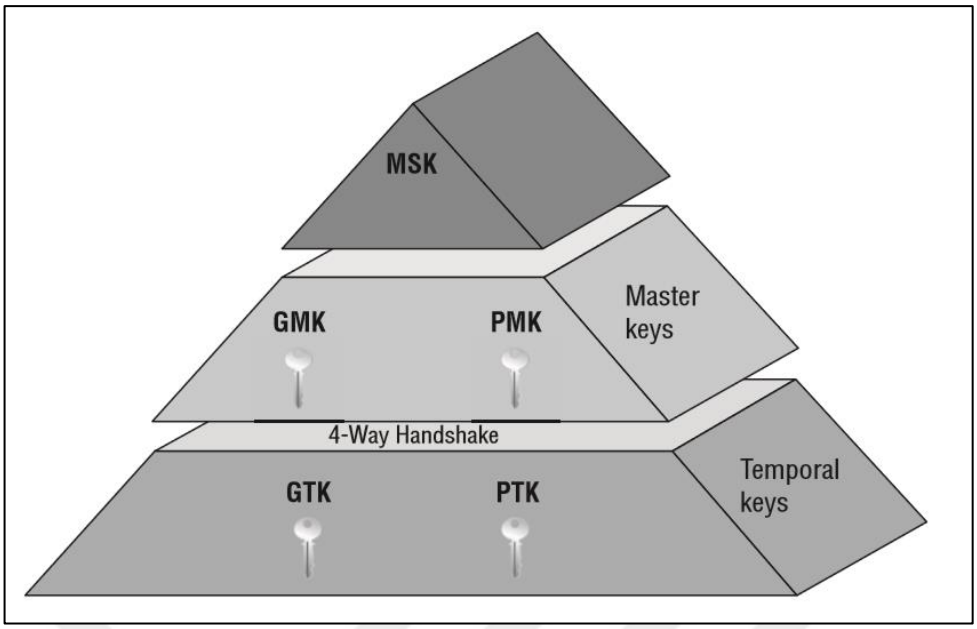

Figure 3.14: Key Hierarchy in WPA2 [44]

PTK or GTK, it allows the generation of 128-bit temporary keys (Temporal Key (TK), used to secure traffic data, and generate MICs). The figure3.15summarizes the process of generating the set of keys used;

The 4 Way Handshake confirms a ciphersuite (ciphersuite) selected from a list of suites called ciphersuites.

The Group Key Handshake is used to renew the GTK. (4) Finally, all these keys are used by the CCMP protocol, in order to ensure confidentiality and data integrity[15].

In order to ensure confidentiality and data integrity, the CCMP protocol applies the AES CCM algorithm [87]. CCM is a mode of operation which ensures both confidentiality and integrity services. For more details on AES CCM

WPA2 also introduces control traffic protection mechanisms to prevent a number of Denial of Service (Dos) or Distributed Denial of Service (DDos) attacks to which all networks are currently vulnerable.

3.2.4 Wireless personal area networks (WPAN)

Wireless personal networks represent short-range wireless networks (about ten meters) with a speed that can reach 1 Mbits/S. The most promising communication technologies used to create WPANs are those defined in the IEEE 802.15.1 standards [99] and IEEE 802.15.4 [29]. Bluetooth, defined by the IEEE

802.15.1 standard, is based on a wireless radio system designed for short-range devices to replace cables for computer peripherals, such as mice, keyboards, joysticks and printers, etc. On the other hand, the IEEE 802.15.4 standard, which is very successful thanks to its optimality, its reliability and its robustness against interference, focuses mainly on the specification of the lower layers (physical and data link) necessary for the creation of wireless sensor networks (WSN). WSNs are used to manage a given environment in real time. A WSN allows you to collect data via sensors, process it, then act if necessary

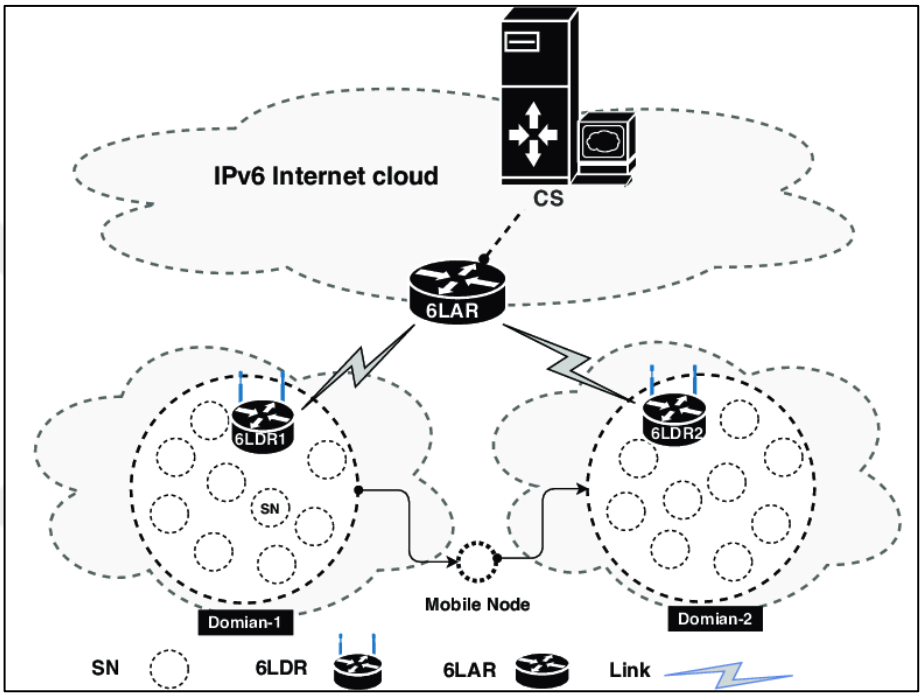

Figure 3.15: An Architecture of a 6LoWPAN Network [45]

Using actuators. WSN communication technologies generally use the ISM bands. In what follows, we are only interested in IEEE 802.15.4 technologies, because this standard is designed to support objects characterized by their low bit rate, low cost, and limitation in terms of computing capacity, storage and energy. . First we start by studying the 6LoWPAN then the ZigBee, and we end with a new innovative technology called OCARI, which we used to validate our research work and deployed our solutions in terms of security.

3.2.4.1 6LoWPAN

According to [95], 6LoWPAN is a specification of a low-power wireless personal area network. It can be deployed with a star or mesh mode topology. It is

based on the IPv6 protocol, which allows it to have several advantages, such as the possibility of using existing IP infrastructures and technologies which are tested and approved. Furthermore, IP-based objects can easily be connected to other IP networks, without the need for intermediate entities such as gateways (for more details see [95]).

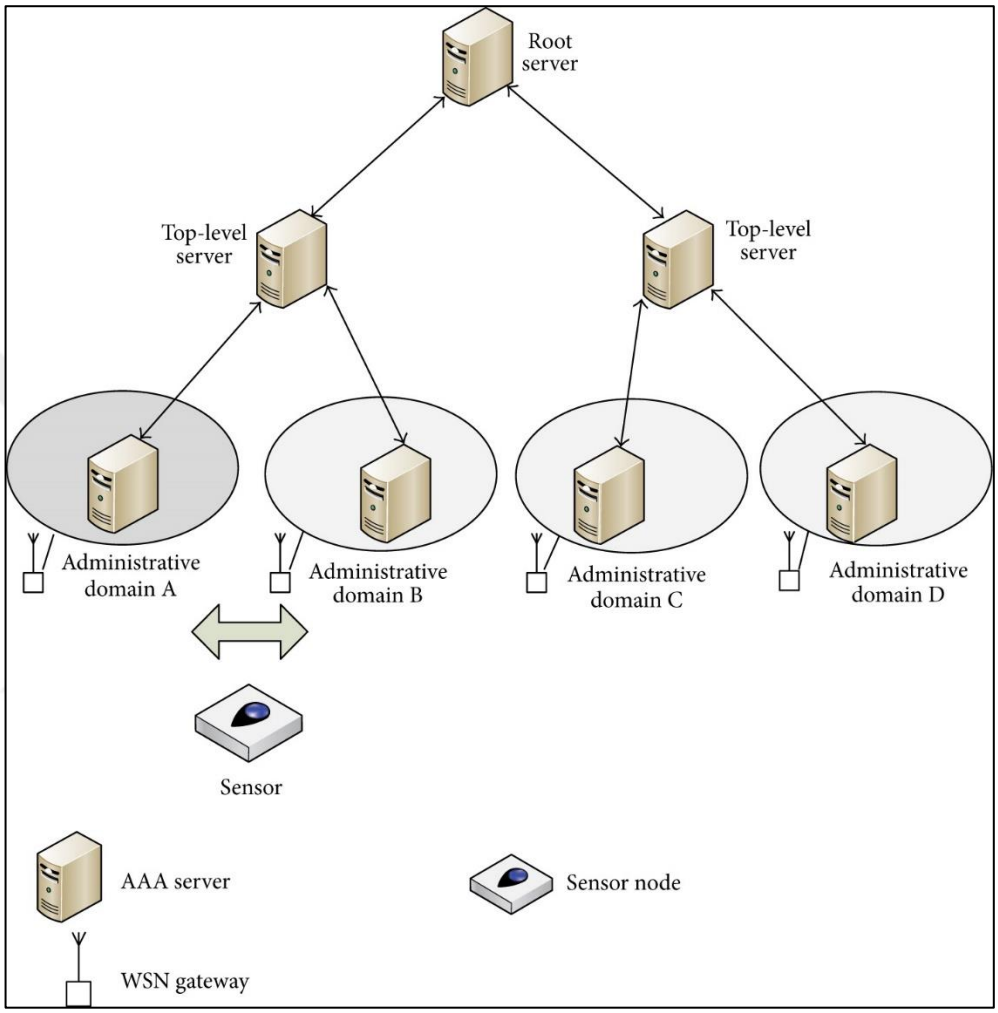

Figure 3.16: EAP-GPSK Mutual Authentication Mechanism (Proposed for 6LoWPAN) [95]

In order to protect the data exchanged, [95] recommends using the AESCCM* standard, which is an algorithm that provides both integrity and confidentiality services.

3.2.4.2 ZigBee

Zigbee is a low-speed, low-resource (power, compute, and memory) WPAN technology that can be deployed with a star or mesh topology. It was invented by the ZigBee Alliance [131], which generated the first specifications in 2004. The two

lower layers of this technology are based on the IEEE 802.15.4 standard, which allows it to exploit the ISM frequency bands for data exchange. In addition, it has other standardized bands which are 915 Mhz in the United States and 868 Mhz in Europe [147]. In order to be able to access the communication channel, at the MAC sub-layer level, ZigBee objects use the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism [55]. The latter makes it possible to optimize energy consumption by limiting the number of transmissions of lost messages due to collisions. The ZigBee Alliance also defines the network layer which is responsible for (1) routing messages and (2) joining and disjoining objects to the network, and (3) providing discovery and maintenance services [147]. And finally, the application layer provides various services including mutual authentication.

a. Security in ZigBee

Security is deployed at the application layer and the network layer. Each layer is responsible for securing the exchange of its data.

Key exchange mechanism and mutual authentication:

Key exchange:

The ZigBee security protocol is based on (1) a 16-byte data link key (link key), shared between 2 objects, and used only at the application layer to secure unicast communications (unicast). And a 16-byte network key, shared between all network objects, used both at the application layer and at the network layer to protect communication in broadcast mode.

Master key, which represent a starting point for establishing the link key. then, the key establishment protocol must follow 3 steps, which are (1) the exchange of ephemeral information, (2) the use of this information for the generation of the link key, and (3) the confirmation that the key has been calculated successfully;

Key transport: this service provides secure and non-secure means to transport a key to one or more objects. The secure means makes it possible to transport a key from a source (trust center) to an object and to protect it by cryptographic means. The insecure means is used to transfer a key in the clear.

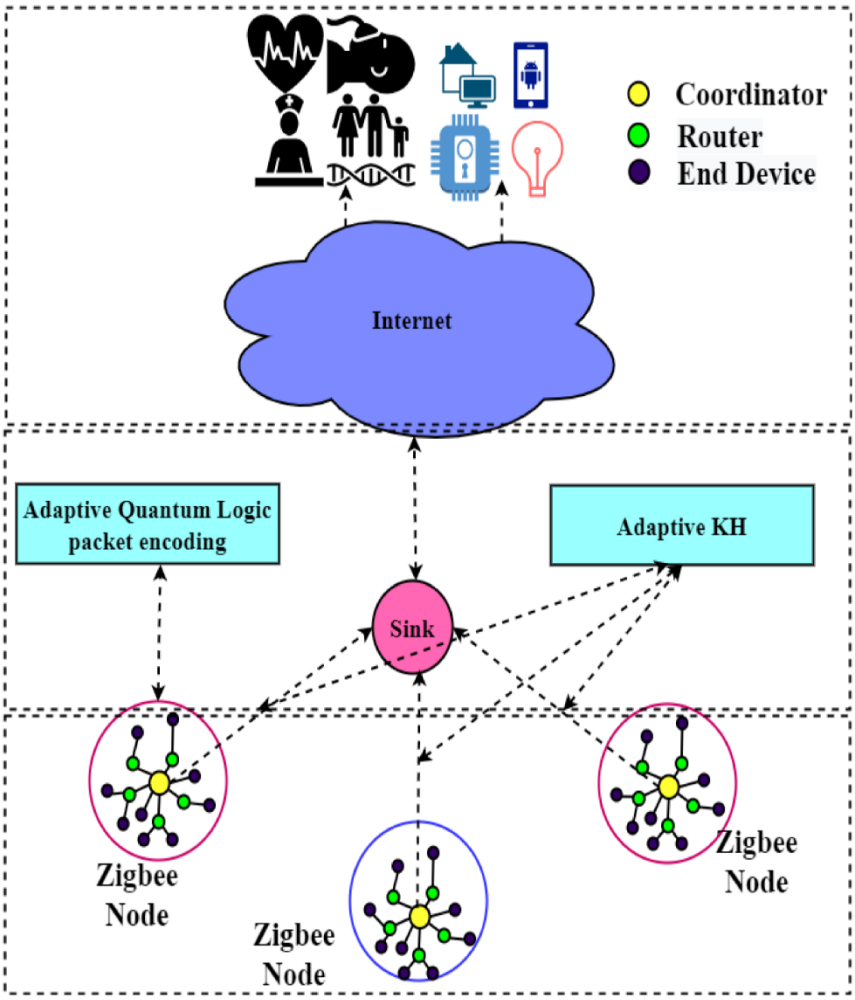

Figure 3.17: ZigBee Mutual Authentication Mechanism [55]

Mutual authentication:

According to the ZigBee Alliance [131], the mutual authentication mechanism between 2 objects (U and V) is based on a shared key and some information exchanged. The authentication operation, depicted in Figure3.18, follows these steps:

Confidentiality and data integrity:

Confidentiality and integrity services are provided through authenticated encryption.

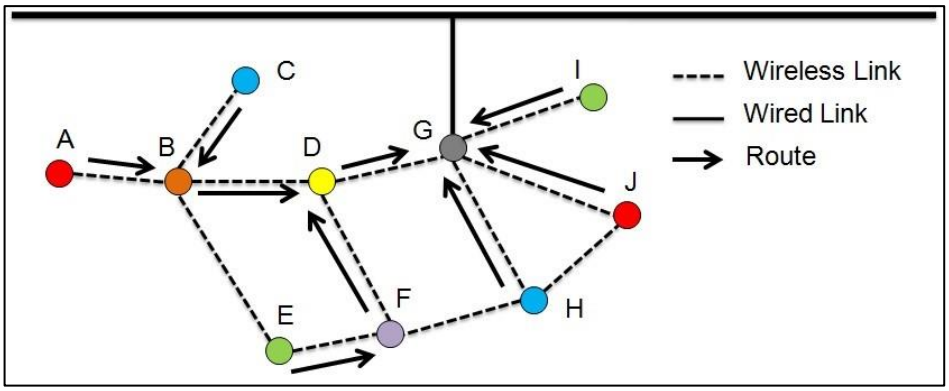

Figure 3.18: Topology of an OCARI Network[131]

Deployed at the application layer and the network layer. Indeed, the messages are doubly protected at the level of the two layers separately, using the AES-CCM* standard. A full description of how AES-CCM works.

4. PROPOSED BLOCKCHAIN SYSTEM FOR IOT DATA SECURITY

4.1 Introduction

The aim of utilizing a blockchain, which is also known as a "chain of blocks," is to record transactions in a way that cannot be altered and is incorruptible. A blockchain is a peer-to-peer network that is decentralized and does not call for the usage of a centralized server at any point in its operation. Each node in the network stores a copy of the ledger since it is duplicated across the network. This eliminates the possibility of the system having a weak spot that could cause it to fail. At the same time, the accuracy of each copy is double checked, and it is brought up to date as necessary. The issue of double spending in the area of cryptocurrencies (also known as digital currency) served as the impetus for the first creation of the technology known as blockchain. [123]. The implementation of this technology makes it possible to handle and protect all different kinds of information, including financial and other kinds. [116]. [49] [14]. Blocks are the component parts that make up the ledger in its actual form. Each block is capable of being divided into two halves that are identical in size. It is possible that the first section of the block is the most important part of the whole structure. It offers a description of the business transactions or information that the database ought to keep a record of, and it does so by providing this description. The term "data" can be used to refer to a wide range of distinct items, such as financial transactions, medical information, production records, system logs, and many other types of information. The section that follows will include the heading for the block that you are looking for. The latter includes extra information about the block, such as the date, the hash of transactions, and so on, in addition to the hash of the block that came before it. It contains the hash of the block that came before it. As a direct result of this, a series of linked and structured blocks that are produced. Each of these blocks is made up of all of the blocks that came before it in the sequence. A greater amount of work is required to produce a chain that is longer than one that is only a few links long. Because the hashes of the

individual blocks are connected to one another, it will be necessary for a malicious user to change or swap a transaction on all subsequent blocks if they wish to amend or swap a transaction on block (1). Second, it must ensure that each node's local copy of the blockchain is brought up to current in order to fulfill its role. A easy application of a blockchain, an example of which is presented in figure 4.1.

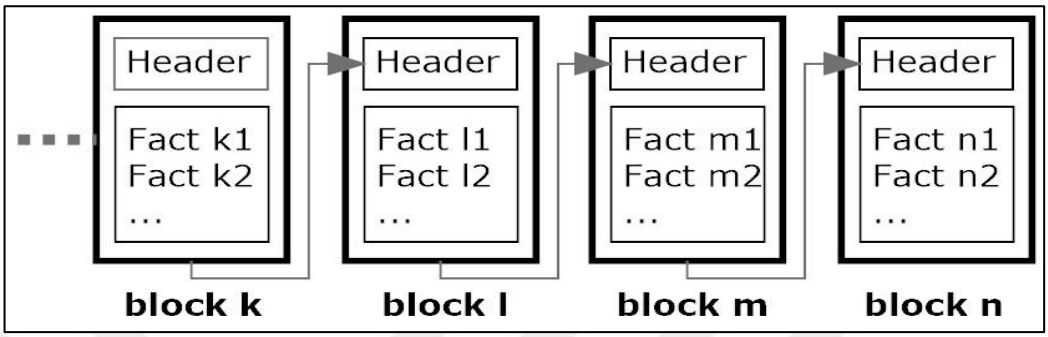

Figure 4.1: Simplified Example of a Blockchain [43]

The most used are the Proof of Work (PoW) mechanism and the Proof of Stake (PoS) mechanism.

4.1.1 Block validation mechanisms

4.1.1.1 Proof of work

In order for this system to operate well, it is necessary for a miner to complete a certain amount of work. This work is presented in the form of a challenging mathematical puzzle or task that is tough to compute but simple to check. The difficulty of the validation challenge is automatically scaled up or down by the blockchain depending on how long it takes to validate a block. Before a block may be considered validated, a Proof-of-Work challenge pertaining to that block must first be solved. When an adversary attempts to manipulate a block, they are required to change all of the blocks that follow it and provide a new Proof-of-Work for each of these blocks. Additionally, the block that they are attempting to manipulate must remain unchanged. Additionally, in order for the new version of the chain to be reflected in all of the objects, they are necessary to update all of the objects, which is not the case. In order to achieve this goal, you will need computers with a lot of processing capability as well as a large amount of power. Despite this, PoW does have a few problems that, if left unchecked, could lead to unwanted results. [21]. Miners will be compensated an ever lower amount as time goes on, which will result

in a smaller network as transaction fees become the dominant source of income. This is because, as time goes on, miners are going to receive progressively fewer rewards for their work. As a direct result of increased competition from other systems, it is anticipated that the costs associated with these transactions would fall. When there are fewer miners participating in the ecosystem of a blockchain, that ecosystem is more susceptible to being targeted by a 51% attack [100]. The second scenario takes place when a single malicious miner (or a group of miners working together) commands 51% or more of the total computer power that is accessible across the network. This can happen while a single miner is mining alone. As a consequence of this, he is in a position to nullify the transactions that other users on the network have produced while simultaneously generating blocks of fraudulent transactions for either himself or another corporation. Last but not least, in some consensus mechanisms, such as Bitcoin's longest chain, miners who validate blocks and achieve Proof of Work are not rewarded since they do not have sufficient power to construct the longest chain. This is the case because these miners cannot construct the longest chain. Because of this, the miners are unable to construct the chain that is the longest possible, which leads to significant financial losses. Proof-of-work, also referred to as PoW, is the protocol that is utilized the majority of the time in blockchain networks (such as Bitcoin, Ethereum, and Litecoin) in order to validate blocks. It is also well known by its abbreviation, PoW.

4.1.1.2 Proof of stake

Because Proof of Work (PoW) suffers from a number of drawbacks, Proof of Stake (PoS) was developed as a potential alternative. In this approach, there is no mining that places a significant demand on the resources that are readily available. In today's business world, it's not uncommon for companies to promote younger workers into managerial positions. The amount of money that a counterfeiter has access to is directly proportional to the ability of the counterfeiter to validate blocks. To put it another way, the likelihood of someone being accepted is directly proportional to the amount of financial resources that they have available to them. If we think about Point of Sale as a type of gambling, then we can say that each counterfeiter is placing a bet on a block when they use it at the POS system. As soon as the honest blocks, which are blocks that do not include any fraudulent transactions, are added to the chain, it is easy to state that each forger is compensated

in proportion to the quantity of the wager he put. An honest block is a block that does not include any fraudulent transactions. And in Proof-of-Stake, a forger whose block turns out to be dishonest is penalized and the value of his bet is taken from his balance, whereas in Proof-of-Work, hostile miners are forgiven. In Proof-of-Stake. In Proof of Work, a forger will be punished if their or her block is found to be invalid. One of the most significant flaws in the system is the fact that the people who stand to earn the most from it are those who are engaged in counterfeiting and hoarding large amounts of money.

4.1.2 Blockchain categories

There is the potential for blockchains to exist in both a "permissioned" (private) and "permissionless" (public) format. The first class places limits on the number of participants who are permitted to take part in the process of obtaining a consensus. Only a select few individuals are permitted access to the process of validating financial transactions. It does not waste either time or resources because it does not take a large amount of computation to obtain a consensus. This means that it does not waste either time or resources. In the vast majority of instances, only objects that have been specifically permitted to inspect the particulars of a transaction are able to do so. The second type of blockchain, which is known as the public blockchain, enables users to make use of an infinite number of inconspicuous items. The use of cryptography makes it feasible for all concerned parties to have communications that are kept in strict confidence. A user's access to a blockchain's read, write, and validate capabilities for transactions is represented by a pair of keys, one of which is public and the other of which is private. If the consensus of the network can be established and at least 51% of the objects contained in the blockchain can be relied upon, then the blockchain will be regarded as trustworthy. Permissionless blockchains are inefficient and waste both time and energy due to the amount of computational power that is required to ensure the system's integrity (via the use of methods such as proof-of-work, or PoW).

4.2 Bitcoin

Bitcoin is a sort of digital currency that functions on the basis of a public record known as the blockchain. It is decentralized and operates independently from

any central authority. Because of this, the use of bitcoin, a form of digital currency, is now feasible, whereas previously it was not. A hash that is stored in the header of each block in the Bitcoin blockchain is referred to as the merkle root [115]. This hash is made up of each and every transaction that took place in the aforementioned block in question. The latter includes the hash of the header for the block that came before it in its construction as well. Every node in the Bitcoin network stores its own copy of the blockchain, independent of whether or not the nodes themselves take part in the mining process. This is true even if the nodes do not themselves mine Bitcoins. Mining is the process of creating blocks of timestamped, chronologically organised transactions. These blocks are timestamped and arranged via mining. Blocks of transactions are another name for these groups of records. After that, a process for arriving at a decision that everyone agrees on is put into action. Bitcoin, in point of fact, employs its very own set of rules in order to guarantee that transactions are legitimate. The rule sets that should be used to validate transactions are indicated to Bitcoin objects by the version numbers of the transactions [3]. In particular, the rule sets that should be used to validate transactions may be found here. One way to ensure that all Bitcoin miners are running off of the same version of the blockchain is to use the rule that dictates utilizing the blockchain version with the longest chain. When two or more miners who are competing against one another produce similar blocks at the same moment, this results in a dispute between the miners. The disagreement stems from the fact that each of these miners is of the opinion that the blockchain should incorporate their respective blocks. If A and B are both trying to make a block with the number n, then A will produce the block symbolized by the letter nA, and B will produce the block signified by the letter nB. If both A and B are attempting to produce a block with the number n, then both A and B will produce blocks. Each block includes the address of its own generator so that the latter can be compensated; also, separate sets of transactions may be included in each of the two blocks that make up the blockchain. As a direct consequence of this, nobody believes the interpretation of the blocks offered by anybody else because these interpretations aren't updated and publicized extremely quickly. Following that, it proceeds to the following block (n+1) in the sequence and performs the operation there as well. In keeping with the concept of the chain that is the longest, if miner A is slower than miner B, and miner B generates block n+1B before miner A generates block n+1A, then miner A is forced to accept miner B's chain as legitimate and delete its own

chain, which is the shorter of the two. In the case that this chain is deemed invalid, it will be referred to as the orphaned chain from that point on. Each new block in Bitcoin requires a miner to submit their Proof of Work (PoW) in order for the cryptocurrency to function properly. This is due to the fact that Bitcoin employs the Proof of Work block validation procedure in order to make its system more resistant to modification attacks. Because Bitcoin makes use of the Proof-of-Work system for validating blocks, this may be a difficult task to generate (both financially and in terms of the amount of time it takes), but it is simple for others to validate. To provide a more detailed explanation, the following is a rundown of how the Bitcoin mining process functions: (1) It is the responsibility of each miner to produce a block that includes a header with a date, the merkle root of the transactions in the block, the hash of the block that came before it, and so on, as well as a body that is comprised of transactions. This block must also include a hash of the block that came before it. (2) The Bitcoin protocol will, at that point, produce a (target) "t" with the value t]0.2 561]. (3) In order for miners' work to be validated, they need to combine the hash of their block with the hash of a number picked at random (n[0.2256 1]), and the value that results from this combination needs to be less than or equal to t. A miner will keep repeatedly changing the value of n until he finds t such that sha256(sha256(block)||n) t. This will continue until the miner has found t. This will make it possible for the miner to find a solution to the problem. The miner will append this value to the block once the equation has been solved to serve as evidence that work has been done on the block. When a node creates a block and broadcasts it to the network, all of the nodes in the network are bound to confirm the transactions and Proof of Work included inside the block. A block is created when a node generates information and then broadcasts it to the network. If the majority of network nodes concur that a block should be supported, then that block will be added to the blockchain and will be considered valid once it has been added. This causes the person who generated the block to receive a reward, and it also causes an update to be applied to the copy of the blockchain held by each of the other objects. At regular intervals of ten minutes, the blockchain receives fresh information which is then added to it. The efforts of a miner who originates from an orphaned block will not result in any reward of any kind. Blocks in a Bitcoin transaction can only be changed theoretically if at least 51% of the objects involved are stolen or hacked. This threshold must be met before a modification can be made. Which is something

that is incredibly difficult to accomplish at this moment because of how things are currently. If Google were to deploy some of its processing capacity for bitcoin mining through its cloud computing service [12], the company's contribution to the global bitcoin mining sector would amount to around 0.0019% of all mining activity. This figure is based on the assumption that Google would mine bitcoins using its cloud computing service.

4.3 Ethereum

The blockchain technology used by Ethereum functions as a public distributed ledger. The ticker symbol for the cryptocurrency that it supplies is "Ethereum (ETH)," and its name is "Ethereum." The specific blockchain in question is put to use not just for the processing of monetary transactions but also for the handling of general data. The miners for Ethereum are responsible for validating blocks as well as processing programs that are known as smart contracts. This is in addition to validating blocks. Because of this, Ethereum is able to serve as a platform for distributed application development. [4] In order to carry out the terms of smart contracts, objects use the Ethereum Virtual Machine, also known as EVM, as their operating system. The act of creating and confirming blocks is a vital component of the mining process for Bitcoin, just as it is for other cryptocurrencies like as ethereum and litecoin. This is true even if Bitcoin is the most popular cryptocurrency. The size of an Ethereum block is less than one-tenth that of a Bitcoin block, and the entire process of adding new users to the network and gaining confirmation of their addition takes roughly 14 seconds. Bitcoin blocks are approximately 10 times larger than Ethereum blocks. In addition, there is no other method that is even remotely comparable to the one that uses blocks and awards. In point of fact, Ethereum employs a method that is known as Ethereum Greedy Heaviest Observed Subtree (GHOST). This is the name given to the system by its developers. As a reward, a miner is given 5 ETH whenever they successfully verify and add a block to the main blockchain. The sender of each transaction is also obligated to pay him an additional sum in gas; the amount of this gas payment is determined by how difficult it is to carry out the conditions of the contract. The sender of each transaction is also obligated to pay him an additional sum in gas. When a miner has successfully mined a block, they will add their Proof of Work to

the end of the block that they have completed and then upload it to the network. In the course of the 14 seconds required to reach a consensus, a sizeable number of blocks are allotted to each item. As a direct result of this, it only makes use of the first block that it acquires and treats the blocks that come after it as "uncles" [63]. As a consequence of this, the major chain will be comprised of the chain that is the longest in length; this chain is also referred to as the one that carries the heaviest load; and all of the other chains will be derived from the major chain. Last but not least, Ethereum makes it possible for any uncle generator to earn a dividend that is proportional to the value of the reward that the mainchain block generator receives. This is not to say that this is the least important feature of Ethereum. This latter group, in turn, is eligible for a share of the benefits that were first conceived of as being reserved for the original creators of the uncles [37]. Ethash is the name of the proof-of-work system that Ethereum employs, and it is this protocol that is utilized to validate blocks. According to the information presented in [38], all participating objects are required to build a seed out of the block headers and utilize it in the computation of a 16MB pseudo-random cache. This requirement can be found in the document. To produce a dataset with a size of one GB, only a small number of the objects now stored in this cache are required. Miners are in charge of archiving the dataset, while thin clients are in charge of storing the cache. Both of these roles are necessary for the network to function properly. The caching functionality is handled by the thin clients themselves. In order to find a solution to this mathematical conundrum, miners employ a technique known as hashing and apply it to sections of the dataset that are selected at random. When performing a check operation, the cache is used solely for the purpose of regenerating data in discrete chunks, as this is the only purpose for which it is employed. The beta version of the Casper protocol for Ethereum can now be accessed by anyone interested in using it. A point-of-sale system is the second choice, and its name comes from its function. Picking participant objects does not require the execution of any external block validation processes (like Proof-of-Work) because of the way in which Ethereum's private blockchain operates. This is due to the fact that Proof-of-Work is not required.

5. SIMULATION AND RESULTS

5.1 Approach

In order for any two entities to be able to interact with one another, there must first be some kind of connection or association created between them. First, Object A will send an association request to Object B in order to establish a link with Object B. Object B will then respond with an association acknowledgement after receiving the association request. This is the standard procedure that is followed when attempting to create a connection between two different objects in a WSN. On the other hand, any potentially hazardous entity C is capable of acting as though it were A and behaving in the appropriate manner. In order to find a solution to this issue, it will be necessary to set up some sort of authentication procedure. Our asynchronous technique is based on the challenge-response mechanism, which is described in RFC 1994 [15]. This mechanism serves as the basis for our method. Because it does not require all of the communication organizations to reach a decision in unison, this option was selected as the one to proceed with by our team. In contrast to the synchronous mode, which requires an agreement between objects on particular parameters such as "time" (e.g., the Timebased One-Time Password algorithm TOTP [121]) or a "counter" (e.g., the HMAC-based One-Time Password method HOTP [120]), the asynchronous mode does not require any such agreement between the objects. Instead, the synchronous mode relies on the parameters to determine whether or not the objects can communicate with one another. It is sufficient for the objects to just communicate with one another, rather than for them to collaborate. There are also numerous wireless technologies that do not permit precise time, and the majority of wireless networks are unstable to the point where the counter numbers are no longer accurate if a transmission is lost. Additionally, there are many wireless technologies that do not permit precise time. It creates a considerable barrier to the synchronization of the events that are occurring. As a consequence of this, our OTP is arrived at by applying a combination of the challenge-response approach [145] and the HOTP [120], which is primarily designed for synchronous mode, as outlined in

the Algorithm. This allows us to generate a one-time password that is secure. The function that is tasked with the creation of OTP is referred to as fotp in the documentation.

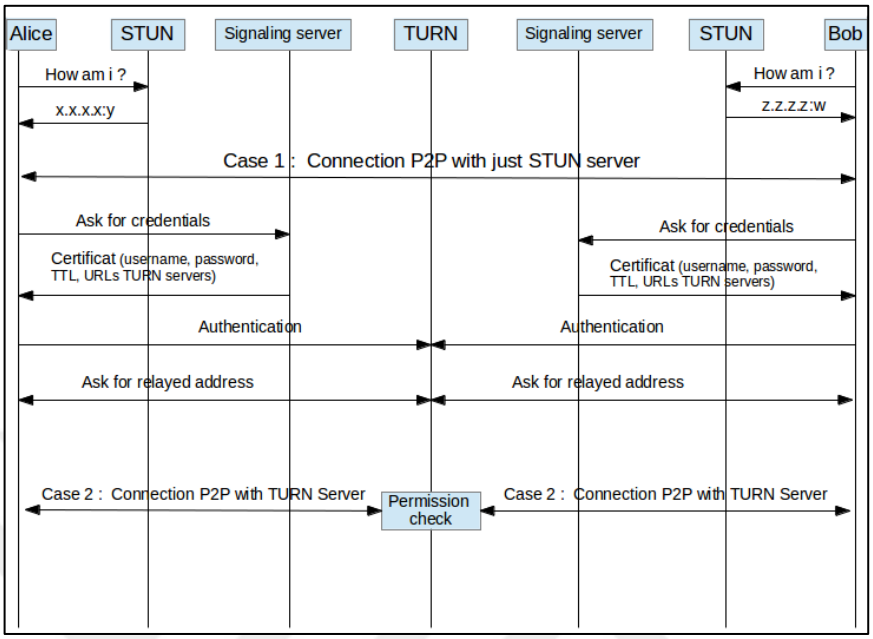

Figure 5.1: Authentication Mechanism (Case 1)

5.1.1Association

Before each data exchange, an object must first associate itself with the network, which requires its authentication. In what follows, we will show the different designs we went through before arriving at the secure and final version in relation to this chapter. In order to avoid additional processing and to ensure more transparency and flexibility at the upper layers of the Open Systems Interconnection (OSI) model [73], we deployed our authentication mechanism at the MAC sublayer. As shown in Figure5.1, to avoid the exchange of several messages and to save time and energy, we only used the two basic association messages (association request and association response). First the Device generates a challenge using the random() function. Then it calculates an otp using the fotp function with as input data the challenge and a secret key k shared with the CPAN. Then it sends an association request containing its unique identifier (UI) associated with the generated parameters. Upon receipt of the request, the CPAN generates otp0 -based on the same parameters- and compares it with otp. If the two OTPs match, then Device authentication successful

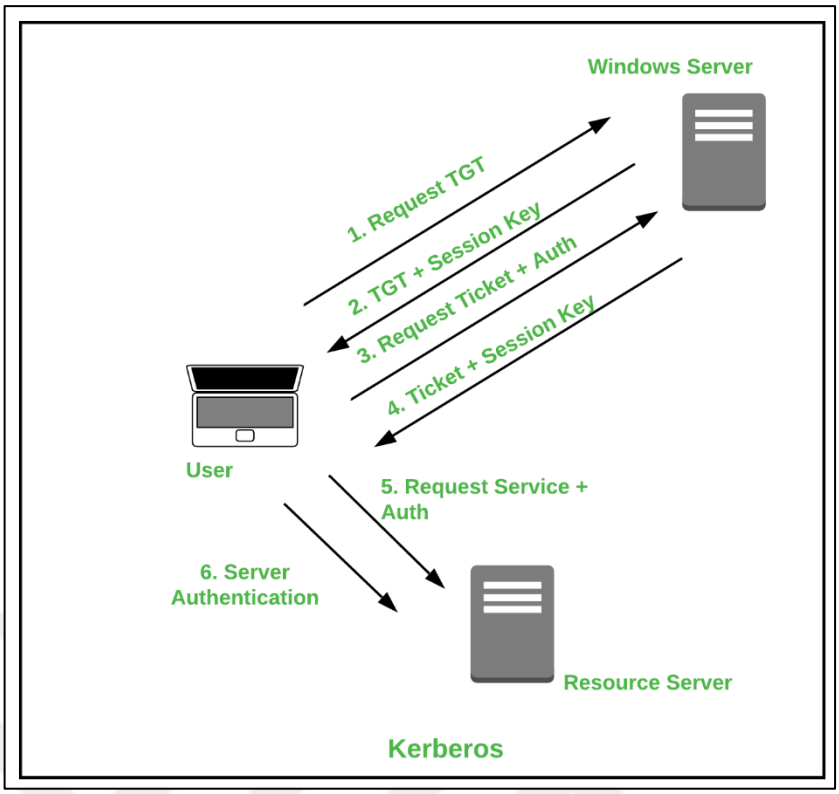

Figure 5.2: Authentication Mechanism (Case 2)

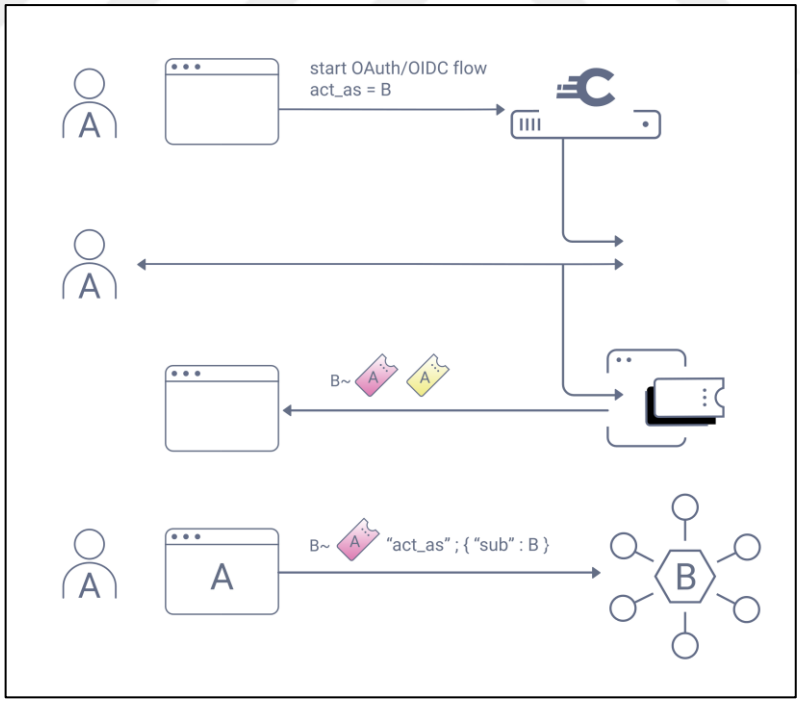

Figure 5.3: Intrusion by Internal Object

And the CPAN associates it with the network, otherwise the authentication fails and the association operation stops. To solve this, we added two more authentication request and authentication response messages (see Figure5.2). In this

new design, it is the authenticator (CPAN) which generates the challenge -after having received an association request- and sends it to the Device, so that the latter can calculate otp and send it to the CPAN via a authentication response. Finally, the CPAN authenticates the Device and associates it with the network. Our security mechanism is based on a shared secret key. This key must be unique and known only by the two communicating entities, otherwise if this key is shared between n objects (where $n \geq 3$), as is the case with the (ZigBee security protocols), this represents a security breach and generates internal attacks on authentication. As explained in Figure5.3, an internal attacker (Device 1) can impersonate Device 2 because it has the same secret key k as Device 2 and the CPAN. Thus, Device 1 can listen to, modify or falsify the messages exchanged between Device 2 and the CPAN. This problem can be solved by installing unique key pairs between the devices and the CPAN.

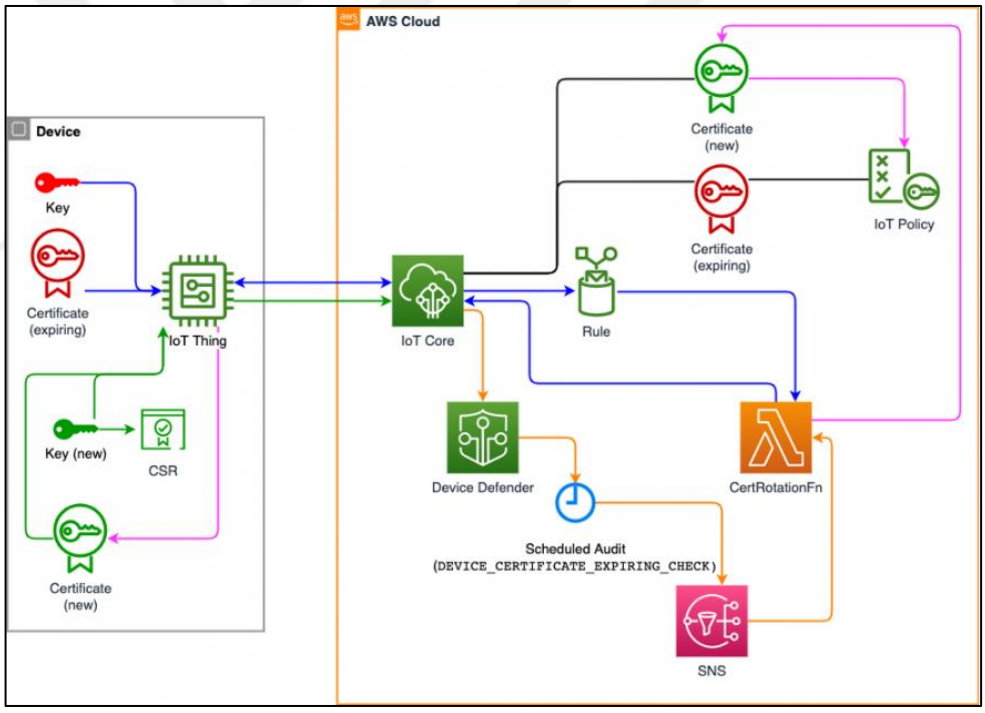

Figure 5.4: Key Customization Mechanism

The trusted authority, which is usually the provider, must install -in out-of-band mode (e.g. physical flashing)- an initial key ki in the CPAN, and generate derived keys kd(s) from it, assigned to each legitimate device belonging to the same cluster. Where hash_function is an irreversible function that generates strong keys and protects ki against deduction attacks. Once kd is created and configured in the device, it can be associated with the network. In addition to solving the problem of

impersonation by internal objects, this solution is optimal and very flexible, because the CPAN does not need to have the kd(s) of the participating objects to authenticate them, but rather, using ki it can get any kd. When adding a new device x to the network, it is not necessary to update the CPAN with the new key kdx, because based on UIx and ki, the CPAN can generate kdx.

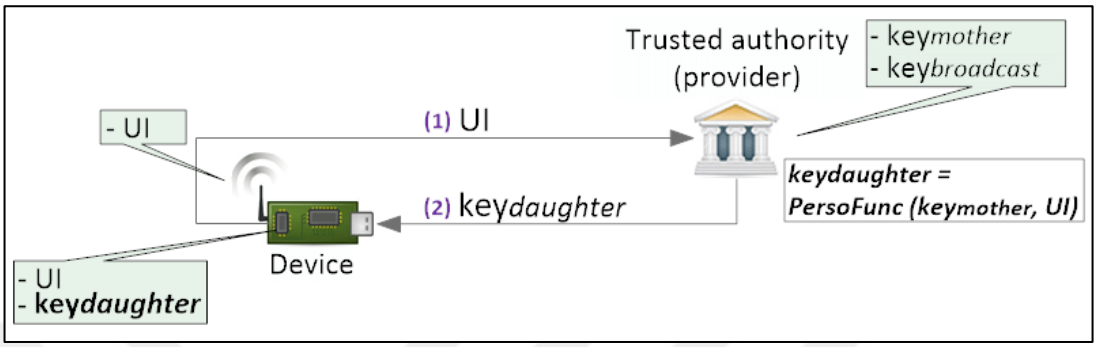

Figure 5.5: Authentication Mechanism (Corrected Design)

When a Device x having a derived key kdx wants to be associated with a network, it must first generate an association request containing its UIx identifier, the CPAN generates and sends a challenge via an authentication request. Upon receipt of the request, Device x calculates otp using the challenge received and kdx as input data, then it sends the result -associated with Uix- to CPAN via an authentication response.

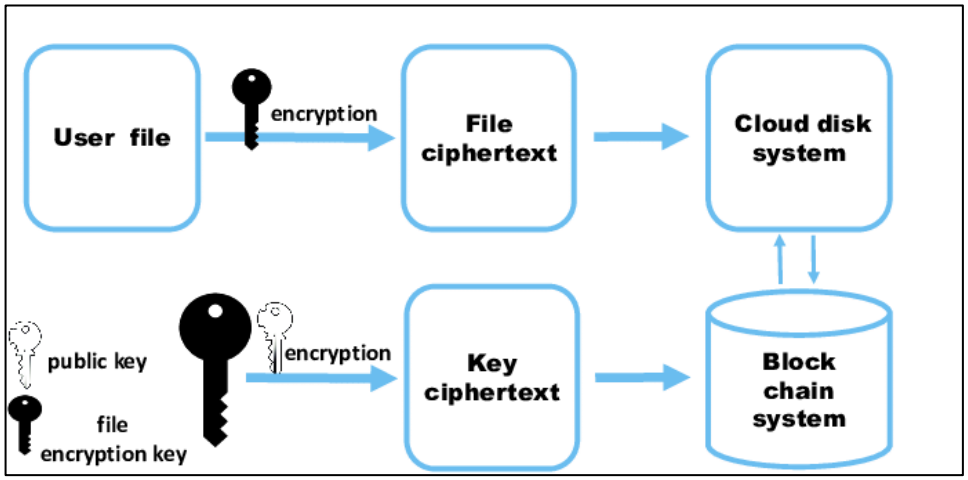

Figure 5.6: Format of a Frame (Version 1)

Finally, CPAN generates a derived key kdx0 corresponding to Device x, and calculates otp0 based on kdx0 and the challenge. If the verification succeeds, then the device will be associated, otherwise it will be rejected.

5.1.2 Communication channel

By exploiting the first 16 bytes of the hash generated during the calculation of otp, a key ku is generated which will be used to ensure the integrity of the data exchanged -in unicast mode- at the level of a communication channel (session). ku is an ephemeral key and is only valid for a single session, this protects our protocol against cryptanalysis attacks like the one applied on WEP

5.2 Evaluation and Results

In this chapter we are only interested in the time elapsed during the association phase. In order to evaluate the performance of our security protocol, we realized an implementation in C language on Dresden Elektronik deRFsam3 23M10-R3 sensors (microcontrollers), having 48 kB of RAM, 256 kB of ROM and a Cortex-M3 processor. For our experiment, we realized a small architecture composed of 3 objects which represent a CPAN and two devices.

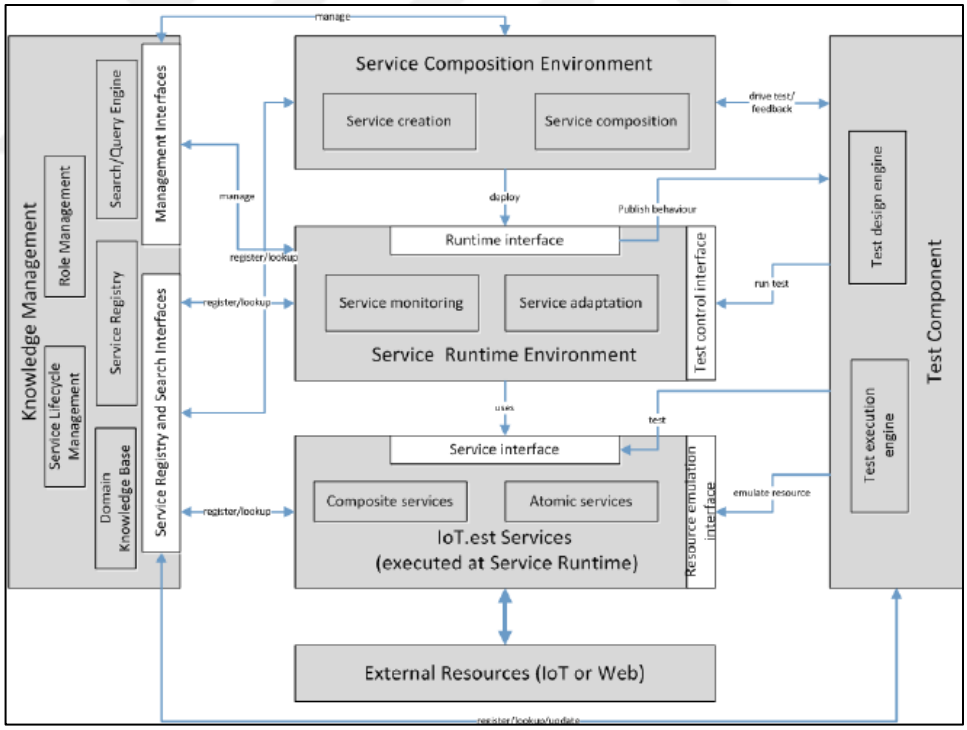

Figure 5.7: Test Architecture

As shown in Figure 5.7, first via a trusted authority (e.g. the manufacturer), we install an initial key ki at the CPAN level and we personalize the devices (Device 1 and Device 2) with the derived keys kd1 and kd2. During the association phase, Device 1 requests its association to the network by communicating directly with the

CPAN, while Device 2 associates with the CPAN by passing its request through Device 1 (2 hops away) which is already associated and playing the role of router.

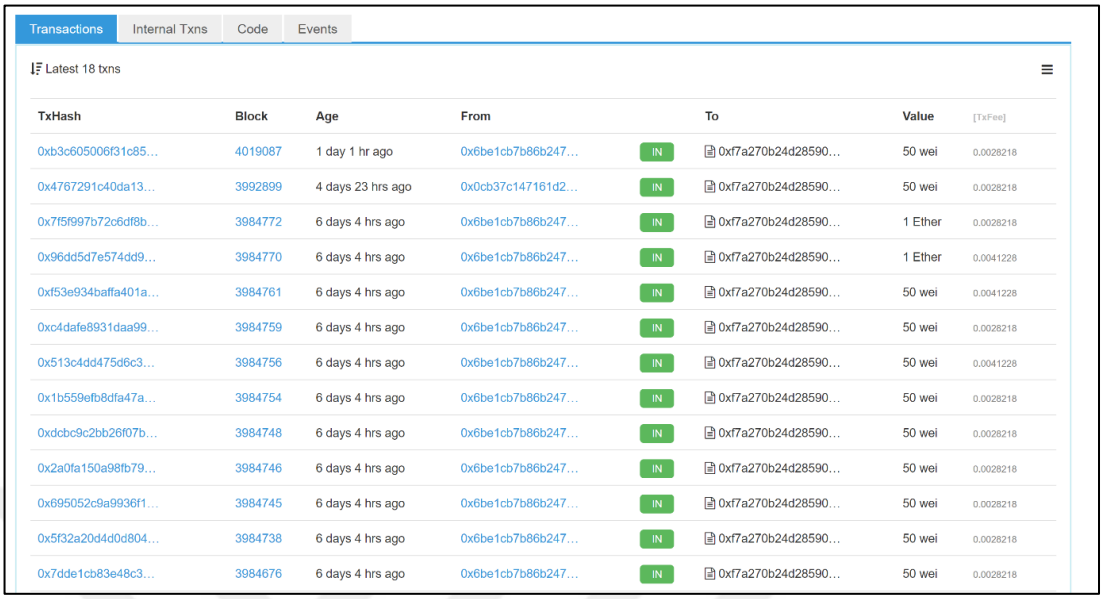

Figure 5.8: IOT Dataset Used for Blockchain Encryption

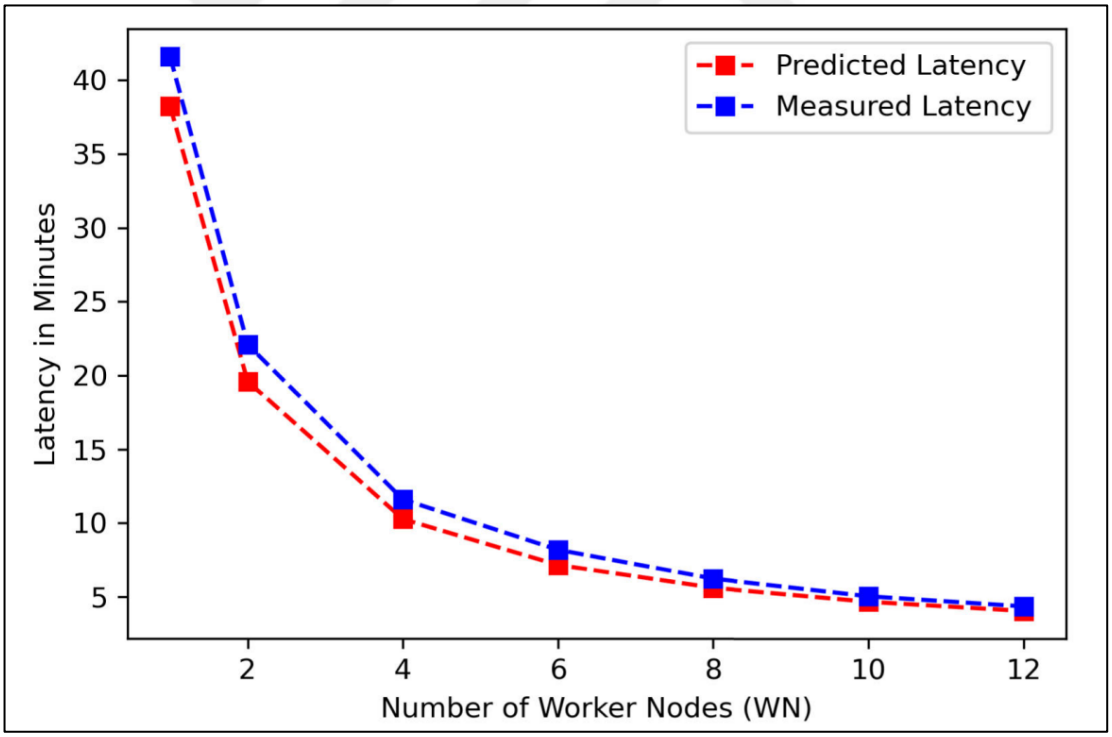

Figure 5.9: Latency in the Proposed IOT-Blockchain System

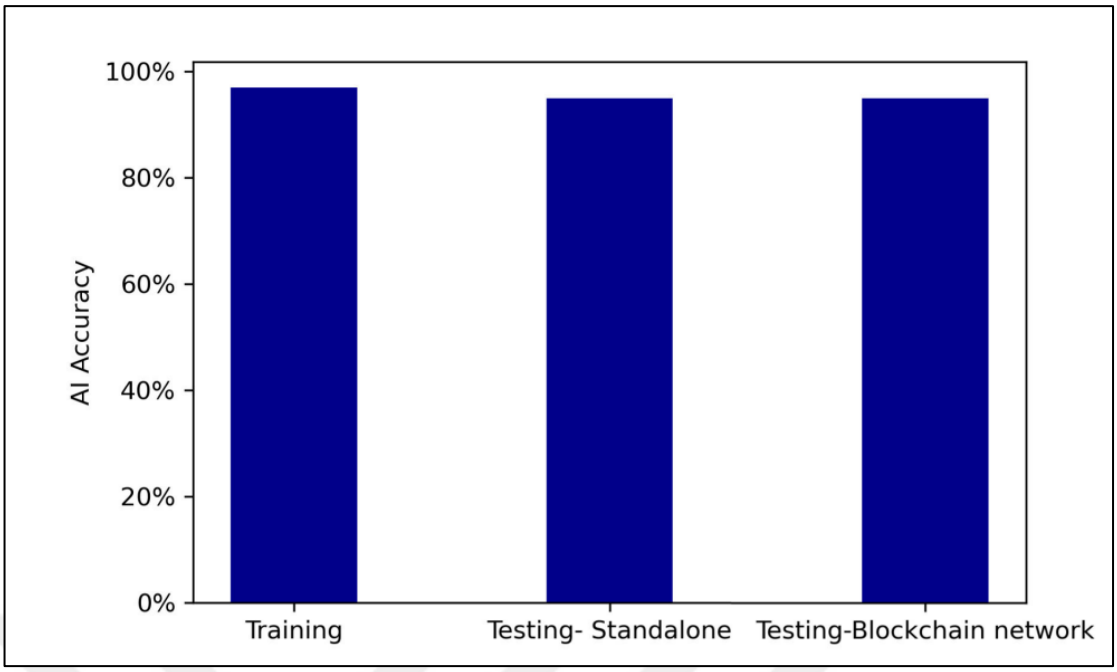

Figure 5.10: Accuracy in Key Generation for the Proposed Method

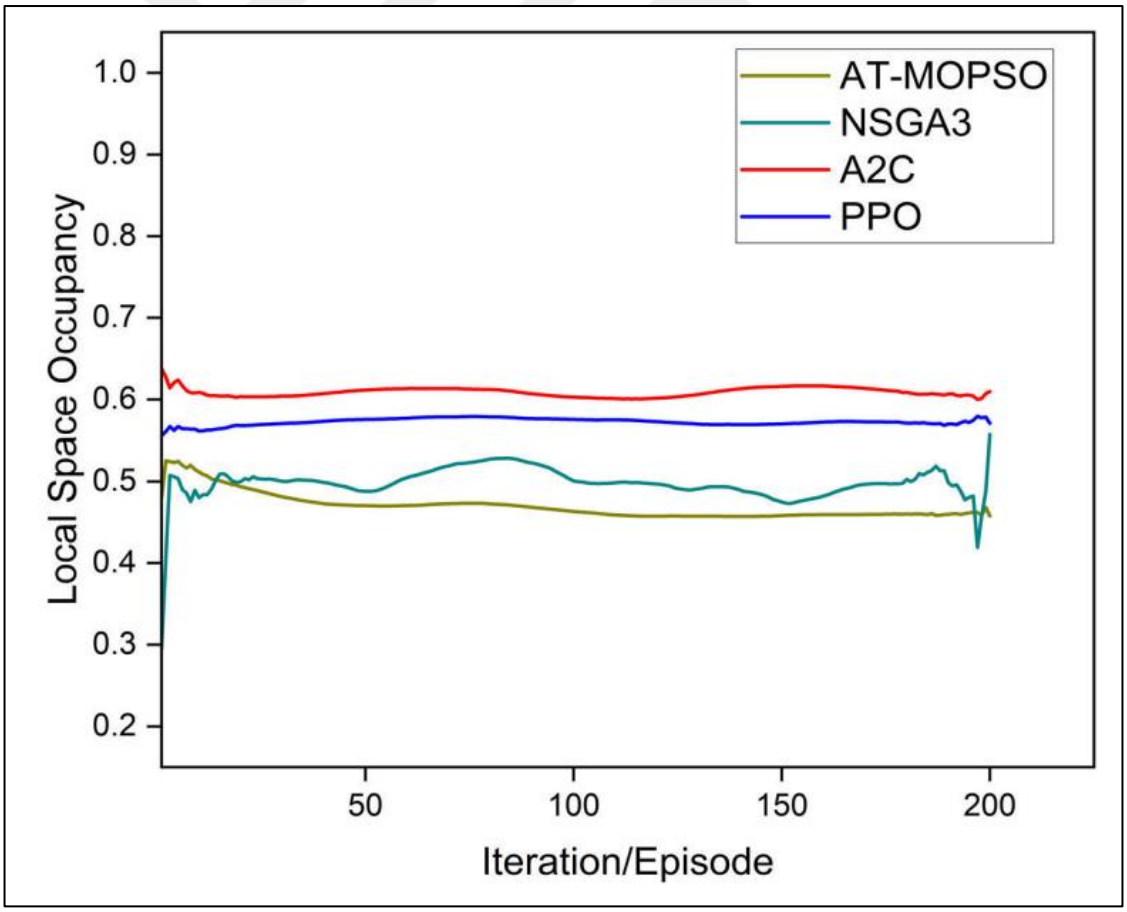

Figure 5.11: Space Management in the Proposed System

6. CONCLUSIONS AND FUTURE WORK

6.1 Conclusions

This research focused on the implementation of blockchain technology as a mechanism for authenticating users in IoT systems. The work provides a comprehensive analysis of how blockchain, as a distributed and immutable ledger, can significantly enhance the security and privacy of data in IoT networks. The study established that blockchain's decentralization nature has the potential to eliminate single points of failure in IoT systems, increasing the robustness and resilience of these systems. Blockchain's transparent and immutable nature was found to be highly beneficial in preventing unauthorized access and data tampering, as every transaction (or authentication) was recorded and easily verifiable. The conducted experiments and the developed prototype illustrated that blockchain-based authentication in IoT systems not only offers enhanced security but also presents a feasible and efficient solution. Despite the computational and storage challenges that IoT devices may face, the architecture proposed in this research proved capable of managing these limitations effectively.

6.2 Future Work

While the study has yielded promising results, the incorporation of blockchain technology into IoT systems is still in its infancy and leaves room for several exciting research opportunities. Scalability and Efficiency: Future research should focus on addressing the scalability issues of blockchain in IoT. While this study has successfully implemented a prototype that works efficiently with a small network, the scalability of such a system in a larger IoT network remains an open question.

Interoperability: The study highlighted the importance of interoperability in blockchain-based IoT systems. As IoT networks often comprise a diverse array of

devices from different manufacturers, ensuring seamless interoperability is crucial. Future work could explore standardization approaches or protocols to facilitate this.

Privacy: Though blockchain enhances security, it could potentially expose some privacy concerns due to its transparent nature. The development of privacy-preserving techniques or models for blockchain-based IoT systems is a fertile ground for future research.

Edge and Fog Computing Integration: Another promising direction is the integration of edge and fog computing with blockchain-based IoT systems. Such integration could effectively address latency issues and further enhance system efficiency and scalability.

Smart Contracts: Further exploration into the integration of smart contracts with blockchain for IoT can lead to more autonomous, secure, and efficient systems. Smart contracts could automate many processes, making the system even more secure and efficient.

In conclusion, this research has demonstrated the potential of blockchain in improving the security of IoT systems through effective user authentication. However, there are several challenges yet to be addressed, which opens up various avenues for future research.

REFERENCES

[1] **P. Lade, R. Ghosh, and S. Srinivasan**, (2017). "Manufacturing Analytics and Industrial Internet of Things," *IEEE Intelligent Systems*, vol. 32, no. 3, pp. 74–79, May

[2] **A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram**, (March 2017) "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 618–623.

[3] **Y. Zhang and J. Wen, (Jul 2017).** "The IoT electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983–994, [Online]. Available: https://doi.org/10.1007/s12083-016-0456-1

[4] **M. Conoscenti, A. Vetro, and J. C. De Martin**, (Nov 2016). "Blockchain for the` internet of things: A systematic literature review," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, pp. 1–6.

[5] **M. Banerjee, J. Lee, and K.-K. R. Choo**, (2018). "A blockchain future for internet-of-things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149 – 160.

[6] **A. Reyna, C. Martn, J. Chen, E. Soler, and M. Daz,** (2018). "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173 – 190.

[7] **T. M. Fernandez-Caramˆ es and P. Fraga-Lamas**, (2018). "A review on the use of` blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32979–33001.

[8] **M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani**, (2019). "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1676 – 1717,. [Online]. Available: https://doi.org/10.1109/COMST.2018.2886932

[9] **A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito,** (2018). "Blockchain and iot integration: A systematic survey," *Sensors*, vol. 18, no. 8. [Online]. Available: http://www.mdpi.com/ 1424-8220/18/8/2575

[10] **S. Petersen and S. Carlsen**, (Dec 2011). "WirelessHART Versus ISA100.11a: The Format War Hits the Factory Floor," *IEEE Industrial Electronics Magazine*, vol. 5, no. 4, pp. 23–34.

[11] **K. Mekki, E. Bajic, F. Chaxel, and F. Meyer,** (2018). "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Express*.

[12] **M. Chen, Y. Miao, Y. Hao, and K. Hwang**, (2017). "Narrow Band Internet of Things," *IEEE Access*, vol. 5, pp. 20557–20577.

[13] **O. Khutsoane, B. Isong, and A. M. Abu-Mahfouz,** (Oct 2017). "IoT devices and applications based on LoRa/LoRaWAN," in *IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, pp. 6107–6112.

[14] **H.-N. Dai, H. Wang, G. Xu, J. Wan, and M. Imran**, "Big data analytics for manufacturing internet of things: Opportunities, challenges and enabling technologies," *Enterprise Information Systems*, 2019.

[15] **X. Lu, D. Niyato, H. Jiang, D. I. Kim, Y. Xiao, and Z. Han**,"Ambient Backscatter Assisted Wireless Powered Communications," *IEEE Wireless Communications*, vol. 25, no. 2, pp. 170–177, April 2018.

[16] **J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos**, "Security and Privacy for Cloud-Based IoT: Challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, January 2017.

[17] **R. Roman, J. Zhou, and J. Lopez**, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[18] **J. He, J. Wei, K. Chen, Z. Tang, Y. Zhou, and Y. Zhang**, "Multitier fog computing with large-scale iot data analytics for smart cities," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 677–686, April 2018.

[19] **Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang**, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352 – 375, 2018.

[20] **C. Miguel and L. Barbara**, "Practical Byzantine fault tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, vol. 99, New Orleans, USA, 1999, pp. 173–186.

[21] **X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen**, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017.

[22] **M. Conti, S. K. E, C. Lal, and S. Ruj**, "A Survey on Security and Privacy Issues of Bitcoin," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2018.

[23] **B. Chase and E. MacBrough**, "Analysis of the XRP Ledger consensus protocol," *arXiv preprint arXiv:1802.07242*, 2018.

[24] **Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich**, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proceedings of the 26th Symposium on Operating Systems Principles*. ACM, 2017, pp. 51–68.

[25] **F. R. Yu, J. Liu, Y. He, P. Si, and Y. Zhang**, "Virtualization for Distributed Ledger Technology (vDLT)," *IEEE Access*, vol. 6, pp. 25019–25028, 2018.

[26] **T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan**, "Blockbench: A framework for analyzing private blockchains," in *Proceedings of the 2017 ACM International Conference on Management of Data*, ser. SIGMOD '17. New York, NY, USA: ACM, 2017, pp. 1085–1100. [Online]. Available: http://doi.acm.org/10.1145/3035918.3064033

[27] **G. Zyskind, O. Nathan, and A. Pentland,** "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in *2015 IEEE Security and Privacy Workshops*, May 2015, pp. 180–184.

[28] **S. S. Chawathe,** *Clustering Blockchain Data*. Cham: Springer International Publishing, 2019, pp. 43–72.

[29] **J. Ream, Y. Chu, and D. Schatsky**, "Upgrading blockchains: Smart contract use cases in industry," Deloitte Press, 2016. [Online].Available: https://www2.deloitte.com/insights/us/en/focus/signals-for strategists/using-blockchain-for-smart-contracts.html

[30] **N. Szabo,** "The idea of smart contracts," *Nick Szabo's Papers and Concise Tutorials*, 1997.[Online].Available:http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/ LOTwinterschool2006/szabo.best.vwh.net/smart contracts 2.html

[31] **Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran**, "An overview on smart contracts: Challenges, advances and platforms," *Future Generation Computer Systems*, vol. 105, pp. 475–491, December 2020. [Online]. Available: https://doi.org/10.1016/j.future.2019.12.019

[32] **F. Idelberger, G. Governatori, R. Riveret, and G. Sartor**, "Evaluation of logic-based smart contracts for blockchain systems," in *International Symposium on Rules and Rule Markup Languages for the Semantic Web (RuleML)*. Springer, 2016, pp. 167–183.

[33] **C. Sillaber and B. Waltl,** "Life cycle of smart contracts in blockchain ecosystems," *Datenschutz und Datensicherheit - DuD*, vol. 41, no. 8, pp. 497–500, Aug 2017.

[34] **R. Koulu**, "Blockchains and online dispute resolution: smart contracts as an alternative to enforcement," *SCRIPTed*, vol. 13, p. 40, 2016.

[35] **S. Nakamoto**, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[36] "**Ethereum: Blockchain APP Platforms**." [Online]. Available: https: //www.ethereum.org/

[37] "**GemOS: the blockchain operating system**." [Online]. Available: https://enterprise.gem.co/

[38] "**MultiChain: Open platform for building blockchains**." [Online]. Available: https://www.multichain.com/

[39] "**Hyperledger project**," 2015. [Online]. Available: https://www. hyperledger.org/

[40] **X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba**, "A taxonomy of blockchain-based systems for architecture design," in *IEEE International Conference on Software Architecture (ICSA)*, 2017, pp. 243–252.

[41] "**Consortium chain development**." [Online]. Available: https://github. com/ethereum/wiki/wiki/Consortium-Chain-Development

[42] **D. Johnson, A. Menezes, and S. Vanstone**, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[43] **K. Christidis and M. Devetsikiotis**, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[44] **Q. Lu and X. Xu**, "Adaptable blockchain-based systems: A case study for product traceability," *IEEE Software*, vol. 34, no. 6, pp. 21–27, 2017.

[45] **Y. Zhang and J. Wen**, "An IoT electric business model based on the protocol of bitcoin," in *Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN)*, 2015, pp. 184– 191.

[46] **M. Massaro,** "Next generation of radio spectrum management: Licensed shared access for 5g," *Telecommunications Policy*, vol. 41, no. 5, pp. 422 – 433, 2017, optimising Spectrum Use. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0308596117301416

[47] **J. Eggerton**, "FCC's Rosenworcel Talks Up 6G," https: //www.multichannel.com/news/fccs-rosenworcel-talks-up-6g, Tech. Rep., September 2018.

[48] **R. Saracco,** "Let's start talking about 6G!" http://sites.ieee.org/ futuredirections/2018/01/25/lets-start-talking-about-6g/, Tech. Rep., January 2018.

[49] **A. Gatherer,** "What Will 6G Be?" https://www.comsoc.org/ publications/ctn/what-will-6g-be, Tech. Rep., June 2018.

[50] **S. Yrjol¨ A,** "Analysis of blockchain use cases in the citizens broadband¨ radio service spectrum sharing concept," in *Cognitive Radio Oriented Wireless Networks*. Cham: Springer International Publishing, 2018, pp. 128–139.

[51] **K. Kotobi and S. G. Bilen,** "Secure Blockchains for Dynamic Spectrum Access: A Decentralized Database in Moving Cognitive Radio Networks Enhances Security and User Access," *IEEE Vehicular Technology Magazine*, vol. 13, no. 1, pp. 32–39, March 2018.

[52] **E. H. H. Kure, P. Engelstad, S. Maharjan, S. Gjessing, and Y. Zhang, "**Distributed uplink offloading for iot in 5g heterogeneous networks under private information constraints," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6151 – 6164, 2019. [Online]. Available: https://doi.org/10.1109/JIOT.2018.2886703

[53] **E. Langberg,** "Blockchains in Mobile Networks," https://e.huawei.com/ hk/publications/global/ict$ $insights/201703141505/, Tech. Rep. 21, March 2017.

[54] **S. He, C. Xing, and L.-J. Zhang**, "A business-oriented schema for blockchain network operation," in *Blockchain – ICBC 2018*, S. Chen, H. Wang, and L.-J. Zhang, Eds. Cham: Springer International Publishing, 2018, pp. 277–284.

[55] **H.-N. Dai, R. C.-W. Wong, H. Wang, Z. Zheng, and A. V. Vasilakos**, "Big data analytics for large scale wireless networks: Challenges and opportunities," *ACM Computing Surveys*, vol. 52, no. 5, 2019. [Online]. Available: https://doi.org/10.1145/3337065

[56] **S. Bera, S. Misra, and A. V. Vasilakos**, "Software-defined networking for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1994–2008, Dec 2017.

[57] **K. Kalkan and S. Zeadally**, "Securing internet of things with software defined networking," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 186–192, September 2018.

[58] **P. K. Sharma, S. Singh, Y. Jeong, and J. H. Park**, "Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 78–85, 2017.

[59] **I. D. Alvarenga, G. A. F. Rebello, and O. C. M. B.** Duarte, "Securing configuration management and migration of virtual network functions using blockchain," in *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, April 2018, pp. 1–9.

[60] **I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck,** "Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions," *IEEE Communications Surveys Tutorials*, vol. 20, no. 3, pp. 2429–2453, 2018.

[61] **C. Esposito, A. Castiglione, B. Martini, and K. K. R. Choo**, "Cloud manufacturing: Security, privacy, and forensic concerns," *IEEE Cloud Computing*, vol. 3, no. 4, pp. 16–22, July 2016.

[62] **V. Ortega, F. Bouchmal, and J. F. Monserrat**, "Trusted 5g vehicular networks: Blockchains and content-centric networking," *IEEE Vehicular Technology Magazine*, vol. 13, no. 2, pp. 121–127, June 2018.

[63] **K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang,** "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5g," *IET Communications*, vol. 12, no. 5, pp. 527–532, 2018.

[64] **C. Chen, M. Lin, and C. Liu**, "Edge computing gateway of the industrial internet of things using multiple collaborative microcontrollers," *IEEE Network*, vol. 32, no. 1, pp. 24–32, 2018.

[65] **N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie,** "Mobile edge computing: A survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450–465, 2018.

[66] **Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han**, "When Mobile Blockchain Meets Edge Computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, August 2018.

[67] **M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song,** "Computation offloading and content caching in wireless blockchain networks with mobile edge computing," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11008–11021, Nov 2018.

[68] **P. Yang, N. Zhang, Y. Bi, L. Yu, and X. S. Shen,** "Catalyzing cloudfog interoperation in 5g wireless networks: An sdn approach," *IEEE Network*, vol. 31, no. 5, pp. 14–20, 2017.

[69] **Y. Dai, D. Xu, S. Maharjan, and Y. Zhang,** "Joint load balancing and offloading in vehicular edge computing and networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4377 – 4387, 2019. [Online]. Available: https://doi.org/10.1109/JIOT.2018.2876298

[70] **Z. Zhou, P. Liu, J. Feng, Y. Zhang, S. Mumtaz, and J. Rodriguez**, "Computation resource allocation and task assignment optimization in vehicular fog computing: A contract-matching approach," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3113 – 3125, 2019. [Online]. Available: https://doi.org/10.1109/TVT.2019.2894851

[71] **Y. Yang, K. Wang, G. Zhang, X. Chen, X. Luo, and M. Zhou**, "Meets: Maximal energy efficient task scheduling in homogeneous fog networks," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 4076– 4087, Oct 2018.

[72] **A. Kusiak**, "Smart manufacturing," *International Journal of Production Research*, vol. 56, no. 1-2, pp. 508–517, 2018.

[73] **J. Wan, J. Li, M. Imran, D. Li, and F. e-Amin**, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3652 – 3660, 2019. [Online]. Available: https://doi.org/10.1109/TII.2019.2894573

[74] **J. Huang, L. Kong, H.-N. Dai, W. Ding, L. Cheng, G. Chen, X. Jin, and P. Zeng,** "Blockchain based mobile crowd sensing in industrial systems," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2020. [75] I. Konstantinidis, G. Siaminos, C. Timplalexis, P. Zervas, V. Peristeras, and S. Decker, "Blockchain for business applications: A systematic literature review," in *Business Information Systems*, W. Abramowicz and A. Paschke, Eds. Cham: Springer International Publishing, 2018, pp. 384–399.

[76] **H. M. Kim and M. Laskowski,** "Toward an ontology-driven blockchain design for supply-chain provenance," *Intelligent Systems in Accounting, Finance and Management*, vol. 25, no. 1, pp. 18–27, 2018.

[77] **A. Tapscott and D. Tapscott,** "How blockchain is changing finance," *Harvard Business Review*, vol. 1, 2017.

[78] **N. Kshetri,** "1 blockchains roles in meeting key supply chain management objectives," *International Journal of Information Management*, vol. 39, pp. 80 – 89, 2018.

[79] **Z. Li, H. Guo, W. M. Wang, Y. Guan, A. Vatankhah Barenji, G. Q. Huang, K. S. McFall, and X. Chen,** "A blockchain and automl approach for open and automated customer service," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3642 – 3651, 2019. [Online]. Available: https://doi.org/10.1109/TII.2019.2900987

[80] **D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu**, "Blockchain application in food supply information security," in *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, Dec 2017, pp. 1357–1361.

[81] **F. Tian,** "An agri-food supply chain traceability system for china based on rfid amp;amp; blockchain technology," in *13th International Conference on Service Systems and Service Management (ICSSSM)*, 2016, pp. 1–6.

[82] **F. Sander, J. Semeijn, and D. Mahr,** "The acceptance of blockchain technology in meat traceability and transparency," *British Food Journal*, vol. 0, no. 0, p. null, 2018.

[83] **R. Bett´ın-D´ıaz, A. E. Rojas, and C. Mej´ıa-Moncayo,** "Methodological approach to the definition of a blockchain system for the food industry supply chain traceability," in *Computational Science and Its Applications – ICCSA 2018*. Cham: Springer International Publishing, 2018, pp. 19–33.

[84] **Q. Lin, H. Wang, X. Pei, and J. Wang,** "Food safety traceability system based on blockchain and epcis," *IEEE Access*, vol. 7, pp. 20698– 20707, 2019.

[85] **C. Zhang, J. Wu, Y. Zhou, M. Cheng, and C. Long**, "Peer-to-peer energy trading in a microgrid," *Applied Energy*, vol. 220, pp. 1 – 12, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0306261918303398

[86] **Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang**, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3690– 3700, Aug 2018.

[87] **N. Z. Aitzhan and D. Svetinovic**, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, Sept 2018.

[88] **C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini**, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 1, 2018.

[89] **K. Wang, Y. Shao, L. Shu, C. Zhu, and Y. Zhang**, "Mobile big data fault-tolerant processing for ehealth networks," *IEEE Network*, vol. 30, no. 1, pp. 36–42, January 2016.

[90] **C. Esposito, A. D. Santis, G. Tortora, H. Chang, and K. R. Choo**, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, Jan 2018.

[91] **K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh**, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of Medical Systems*, vol. 42, no. 7, p. 130, Jun 2018. [Online]. Available: https://doi.org/10.1007/s10916-018-0982-x

[92] **M. Z. A. Bhuiyan, A. Zaman, T. Wang, G. Wang, H. Tao, and M. M. Hassan,** "Blockchain and big data to transform the healthcare," in *Proceedings of the International Conference on Data Processing and Applications*, ser. ICDPA. ACM, 2018, pp. 62–68.

[93] **Y. Sun, R. Zhang, X. Wang, K. Gao, and L. Liu**, "A decentralizing attribute-based signature for healthcare blockchain," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, 2018, pp. 1–9.

[94] **M. A. Rahman, M. S. Hossain, G. Loukas, E. Hassanain, S. S. Rahman, M. F. Alhamid, and M. Guizani,** "Blockchain-based mobile edge computing framework for secure therapy applications," *IEEE Access*, vol. 6, pp. 72469–72478, 2018.

[95] **F. Wu *et al.***, "A new coronavirus associated with human respiratory disease in china," *Nature*, 2020. [Online]. Available: https://doi.org/10.1038/s41586-020-2008-3

[96] **Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung,** "Blockchainbased decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495 – 1505, May 2018. [Online]. Available: https://doi.org/10.1109/JIOT.2018.2836144

[97] **H. Liu, Y. Zhang, and T. Yang,** "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Network*, vol. 32, no. 3, pp. 78–83, May 2018.

[98] **J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain**, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, Dec 2017.

[99] **J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "**Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660 – 4670, 2019.

[100] **Y. Dai, D. Xu, S. Maharjan, G. Qiao, and Y. Zhang**, "Artificial Intelligence Empowered Edge Computing and Caching for Internet of Vehicles," *IEEE Wireless Communications Magazine*, vol. 26, no. 3, pp. 12 – 18, 2019.

[101] **Y. Zeng, R. Zhang, and T. J. Lim**, "Wireless communications with unmanned aerial vehicles: opportunities and challenges," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 36–42, May 2016.

[102] **G. Kimchi, D. Buchmueller, S. A. Green, B. C. Beckman, S. Isaacs, A. Navot, F. Hensel, A. Bar-Zeev, and S. S. J.-M. Rault**, "Unmanned aerial vehicle delivery system," 2017, uS Patent 9,573,684.

[103] **L. Wang, F. Chen, and H. Yin**, "Detecting and tracking vehicles in traffic by unmanned aerial vehicles," *Automation in Construction*, vol. 72, pp. 294 – 308, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0926580516300887

[104] **N. Cheng, W. Xu, W. Shi, Y. Zhou, N. Lu, H. Zhou, and X. Shen**, "Airground integrated mobile edge networks: Architecture, challenges, and opportunities," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 26–32, August 2018.

[105] **A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. Berman**, "Blockchain-based protocol of autonomous business activity for multiagent systems consisting of uavs," in *2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS)*, 2017, pp. 84–89.

[106] **A. Kumar, A. Kundu, C. A. Pickover, and K. Weldemariam,** "Unmanned aerial vehicle data management," 2018, uS Patent App. 15/463,147.

[107] **B. Li, Z. Fei, and Y. Zhang**, "Uav communications for 5g and beyond: Recent advances and future trends," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2241 – 2263, 2019. [Online]. Available: https://doi.org/10.1109/JIOT.2018.2887086

[108] **Y. Dai, D. Xu, S. Maharjan, and Y. Zhang**, "Joint Computation Offloading and User Association in Multi-Task Mobile Edge Computing," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 12313–12325, Dec 2018.

[109] **T. X. Tran, A. Hajisami, P. Pandey, and D. Pompili,** "Collaborative mobile edge computing in 5g networks: New paradigms, scenarios, and challenges," *IEEE Communications Magazine*, vol. 55, no. 4, pp. 54–61, April 2017.

[110] **X. Li, H. Wang, H.-N. Dai, Y. Wang, and Q. Zhao**, "An analytical study on eavesdropping attacks in wireless nets of things," *Mobile Information Systems*, vol. 2016, 2016.

[111] **J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao**, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[112] **Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao**, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[113] **M. Apostolaki, A. Zohar, and L. Vanbever**, "Hijacking Bitcoin: Routing attacks on cryptocurrencies," in *Security and Privacy (SP), IEEE Symposium on*. IEEE, 2017, pp. 375–392.

[114] **S. Adhami, G. Giudici, and S. Martinazzi,** "Why do businesses go crypto? an empirical analysis of initial coin offerings," *Journal of Economics and Business*, vol. 100, pp. 64 – 75, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/ S0148619517302308

[115] **L. Hu, H. Wen, B. Wu, F. Pan, R. Liao, H. Song, J. Tang, and X. Wang,** "Cooperative jamming for physical layer security enhancement in internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 219–228, Feb 2018.

[116] **W. Xu, S. Jha, and W. Hu,** "LoRa-Key: Secure Key Generation System for LoRa-based Network," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6404 – 6416, 2019.

[117] **M. Apostolaki, G. Marti, J. Mller, and L. Vanbever,** "SABRE: Protecting Bitcoin against Routing Attacks," in *Proceedings of the Network and Distributed System Security Symposium*, 2019, pp. 1–15.

[118] **T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang**, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, July 2018.

[119] **A. Dorri, S. S. Kanhere, and R. Jurdak,** "MOF-BC: A memory optimized and flexible blockchain for large scale networks," *Future Generation Computer Systems*, vol. 92, pp. 357 – 373, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/ S0167739X17329552

[120] **M. Moser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan *et al.*,** "An Empirical Analysis of Traceability in the Monero Blockchain," *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 3, pp. 143–163, 2018.

[121] **K. Saito and M. Iwamura,** "How to make a digital currency on a blockchain stable," *arXiv preprint arXiv:1801.06771*, 2018.

[122] **A. Yasin and L. Liu,** "An online identity and smart contract management system," in *Proceedings of 40th Annual Computer Software and Applications Conference (COMPSAC)*, vol. 2, 2016, pp. 192–198.

[123] **A. Bogner, M. Chanson, and A. Meeuw,** "A decentralised sharing app running a smart contract on the ethereum blockchain," in *Proceedings of the 6th International Conference on the Internet of Things*, 2016, pp. 177–178.

[124] **X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla,** "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, 2017, pp. 468–477.

[125] **D. G. Glover and J. Hermans**, "Improving the traceability of the clinical trial supply chain," *Applied Clinical Trials*, vol. 26, no. 11, pp. 36–38, November 2017. [Online]. Available: https: //search.proquest.com/docview/1984377517?accountid=28120

[126] **C. Huang, Z. Wang, H. Chen, Q. Hu, Q. Zhang, W. Wang, and X. Guan,** "Repchain: A reputation based secure, fast and high incentive blockchain system via sharding," 2019.

[127] **P. Wang, R. X. Gao, and Z. Fan**, "Cloud computing for cloud manufacturing: benefits and limitations," *Journal of Manufacturing Science and Engineering*, vol. 137, no. 4, pp. 1–9, 2015.

[128] **N. Wang, X. Xiao, Y. Yang, T. D. Hoang, H. Shin, J. Shin, and G. Yu,** Privtrie: Effective frequent term discovery under local differential privacy," in *IEEE International Conference on Data Engineering (ICDE)*, 2018.

[129] **Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y.** Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5g beyond," *IEEE Network Magazine*, 2019 (in press).

[130] **C. Remy, B. Rym, and L. Matthieu**, "Tracking bitcoin users activity using community detection on a network of weak signals," in *Complex Networks & Their Applications VI*. Cham: Springer International Publishing, 2018, pp. 166–177.

[131] **P. Tasca, A. Hayes, and S. Liu**, "The evolution of the bitcoin economy: Extracting and analyzing the network of payment relationships," *The Journal of Risk Finance*, vol. 19, no. 2, pp. 94–126, 2018.

[132] **W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, and Y. Zhou**, "Detecting ponzi schemes on ethereum: Towards healthier blockchain technology," in *Proceedings of the 2018 World Wide Web Conference*, ser. WWW '18. Republic and Canton of Geneva, Switzerland: International World Wide Web Conferences Steering Committee, 2018, pp. 1409–1418. [Online]. Available: https://doi.org/10.1145/3178876.3186046

[133] **K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer *et al.***, "On scaling decentralized

blockchains," in *International Conference on Financial Cryptography and Data Security*. Springer, 2016, pp. 106–125.

[134] J. **Vermeulen**, "Bitcoin and Ethereum vs Visa and PayPal Transactions per second," *Altcoin Today*, April 2017. [Online]. Available: http://www.altcointoday.com/ bitcoin-ethereum-vs-visa-paypal-transactions-per-second/

[135] **S. Albrecht, S. Reichert, J. Schmid, J. Struker, D. Neumann, and¨ G. Fridgen,** "Dynamics of blockchain implementation-a case study from the energy sector," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

[136] **Y. Lewenberg, Y. Sompolinsky, and A. Zohar**, "Inclusive block chain protocols," in *International Conference on Financial Cryptography and Data Security*. Springer, 2015, pp. 528–547.

[137] **L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena**, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16. New York, NY, USA: ACM, 2016, pp. 17–30. [Online]. Available: http://doi.acm.org/10.1145/2976749.2978389

RESUME

Mohammed NAYEF

EDUCATION:

- Master 2022 – 2023 : Istanbul Gedik University, Engineering Management Master's Degree.
- Bachelor 2012– 2013: Almaarif University College –Al-Anbar \Iraq Computer Engineering BSC Full B.sc in this field

LANGUGES:

- Arabic : Mother Tongue
- English: Proficient in Speaking and Writing.

SKILLS:

Ability to work under pressure, work with a team, positive attitude, self- directed and confident decision maker, strong work ethic, ability to prioritize, multitasked and exceptional management.

COMPUTER SKILLS:

- Computer Use
- Internet User
- Emails
- Microsoft Word
- Microsoft access
- Microsoft PowerPoint

WORK AND EXPERIENCE:

- Ministry of Industry and Minerals
- From 1991 to noew