Investigating An Improved Blockchain Module for IoT

Fahad A. Alkurdi

BCompSc (PWR), MIT (UC)

A Thesis Submitted for the Degree of Doctor of Philosophy of the University of Canberra

28/2/2024

Faculty of Science and Technology

UNIVERSITY OF CANBERRA

Abstract

Many systems nowadays, such as healthcare systems, are not well integrated with each other and lack the connectivity, transparency or even security. This is causing many issues in this field including transaction delays, medical errors and breach of privacy. To address these major issues, an introduction of a technology that is secure while also transparent is needed.

Blockchain technology take up has been significant in the recent past and the technology shows enormous potential for the future. It is a technology that provides the possibility of generating and sharing transaction ledgers that are tamper proof. Its use cases are expanding through multiple areas such as, Internet of Things (IoT), security and even finance. In a Blockchain, each full node must store the full history of the blockchain. This affects transaction times and limits lightweight nodes, such as IoT devices, from joining the network. As time passes, history becomes larger, and the scalability issue will be aggravated.

In this thesis we propose a novel blockchain platform with an off-chain solution for solving this storage constraint issue. We integrate a couple of security mechanisms to securely manage the IoT devices and secure the data transferred throughout the blockchain. Finally, we present simulation results and a detailed discussion scenario of the Saudi Arabian Healthcare System.

This thesis offers three main contributions to this field of research:

- A proposed blockchain platform using off-chain storage for managing IoT devices.
- A proposed security mechanism for managing IoT devices.
- An implementation of blockchain in the Saudi Arabian health sector.

The first contribution proposed an off-chain storage platform for managing IoT devices. The platform was constructed using Ethereum for its flexibility, availability and usability. A simulation script was written using python and simulations were made for different user groups to test the limitations of the platform while focusing on transaction rates and the read and write

speeds from and to the blockchain. In order to properly simulate the speed of the system, the creation of a private blockchain was necessary to remove the variables affecting the transaction speed (such as block size and transaction count) on a public network, allowing a more accurate simulation to be made.

Secondly, a security mechanism was constructed and implemented within the platform and the blockchain to securely manage all IoT devices connected to the system. Data Encryption and Data Validation were implemented and a tier level has been constructed with each user being assigned a different tier level access to avoid tampering with data. In a blockchain, public and private key play an important role in verifying the owner of the transaction as well as digital signatures. To verify if digital signature is true or false, both digital signature and private key of the user are validated using the cryptographic functions, based on the results, the transaction will be declared valid or invalid. Later we test our proposed security mechanisms against DDoS attack for validation purposes.

Finally, the system was implemented in a real time scenario. For this implementation, the Saudi Arabian Health Sector has been used as well as the Saudi Arabian Ministry of Health as the main contract deployer. A list of 50 Saudi Arabian hospitals were obtained and implemented in the platform using random generators for doctors and patients. Following that, a front end page has been designed that reads the data directly from the platform. And in the end we show why and how the Saudi Arabian Health Sector can benefit from our module implementation.

According to many real-world issues and scenarios, there is no ideal approach that could present the best comprehensive outcome. In this thesis, we took a far-reaching step by proposing and developing an off-chain storage platform to securely manage IoT devices using blockchain technology while using Bitcoin as our benchmark against our transaction rates and our read and write speed. Furthermore, we have developed our own cryptographic techniques to test and proof that our proposed solution is as secure as the traditional blockchain security mechanism. Finally, we implemented a private blockchain and integrated it within the Saudi Arabian Healthcare system which helped in clarifying the transparency and security needed within the blockchain technology for such systems. More analysis and experimentation with different ap-

proaches with real-life scenarios are needed. We believe that the effort and work presented in this thesis will assist and complement future research in the fields of blockchain technology, off-chain storage and IoT.

Acknowledgements

First and foremost, I would like to thank God for granting me endless blessings, such as the knowledge and the opportunity to complete this thesis.

I would like to acknowledge my country and my king, King Salman Bin Abdulaziz Al-Saud, for giving me the opportunity to pursue my education at one of the best universities in the world under the Saudi Arabian Scholarship Program.

It is my privilege to express my deepest appreciation to my primary supervisor Professor Kumudu Munasinghe, whose expertise was invaluable in formulating this research and sharpening my way of thinking that bought this work to a higher level. I would also like to thank my co-supervisors, Professor Dharmendra Sharma and Professor Abbas Jamalipour for their constructive advice and support during my journey.

In addition, my sincere thanks goes to my parents for their wise counsel and sympathetic ear. My spouse for believing in me along with her constant support. And all my family, they have always been there for me with support and encouragement. I could not have completed this achievement without them.

Last but not least, I would like to thank all my co-workers and friends who made this journey a joyful and memorable one.

Publications

- F. Alkurdi, I. Elgendi, K. S. Munasinghe, D. Sharma, and A. Jamalipour, "Blockchain in IoT Security: A Survey" *In Proceedings of the International Telecommunication Networks and Applications Conference (ITNAC), Sydney, Australia, November, 2018.*

Abbreviations

Amazon VPC	Amazon Virtual Private Cloud
AWS	Amazon Web Services
DoS	Denial of Service
DDoS	Distributed Denial of Service
HFA	Health for All
IDS	Intrusion Detection System
IoT	Internet of Things
ISP	internet service provider
KSA	Kingdom of Saudi Arabia
MJ	MegaJoule
MOH	Ministry of Health
QoS	Quality of Service
SHA	Secure Hashing Algorithm
UDP	User Datagram Protocol
VM	Virtual Machines
VPC	Virtual Personal Computer

Contents

List of Figures

Chapter 1

Introduction

Blockchain technology take up has been significant in the recent past and the technology shows enormous potential for the future. It is a technology that provides the possibility of generating and sharing transaction ledgers that are tamper proof. This thesis investigates an improved model for blockchain technology as used in conjunction with IoT environments.

In this chapter we introduce our research motivation, aim, research questions, thesis contributions and our thesis outline.

1.1 Motivation

With the rapid advancement in technology, blockchain is proving to be one of the greatest technological innovations both in the public sectors and the private sectors. The rising cases of cybersecurity issues have seen the wide adoption of the blockchain technology in many fields such as finance [8], security, and Internet of Things (IoT) [9]. However, many people are yet to understand how blockchain technology can be applied to IoT, and this can be seen to be a reason why many researchers focus on exploring this subject, hence the motivation for this thesis.

1.2 Background

Blockchain technology can be described as a network software protocol, which enables safe transfer of assets, information, or money through the Internet without necessarily introducing a third party [10]. Therefore, with the rise of security issues in fields like IoT, blockchain technology offers a new form of access control framework, which suits most users and enable them to control privacy [11]. The decentralized nature of the technology is the main feature of a blockchain, that many researchers attribute to it in terms of providing a secure form of conducting transactions, which goes back to the original reason of the development of blockchain to reinforce crypto-currency and transactions without a third party controlling it [12].

A notebook page is an amazing example of a blockchain block, data is written on the page exactly like data is stored on the block. The block can store any data such as medical records or property agreements. This block is chained to a previous block by embedding it from the previous one as shown in Figure 1.1. This link will obviously break if anything interfered with the data anywhere in this chain which provides security and immutability [13].

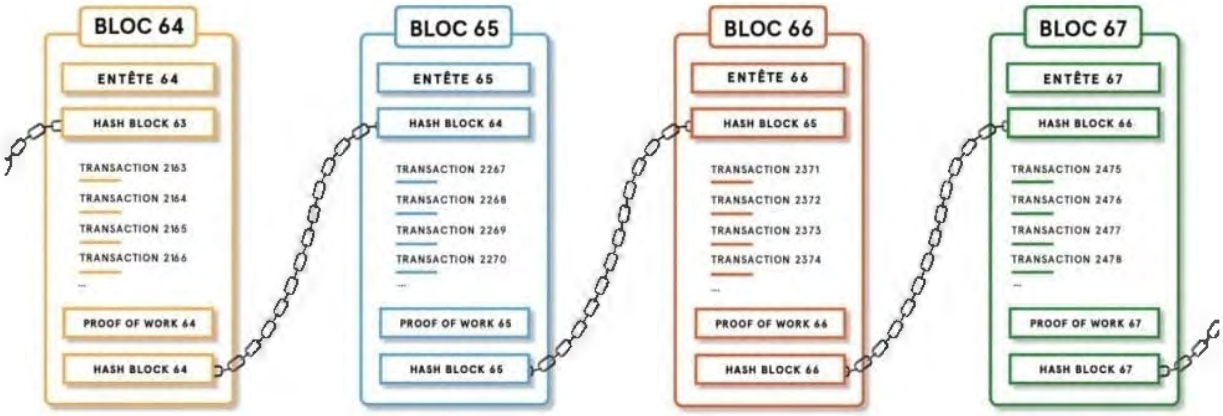


Figure 1.1: Blockchain Structure. [1]

The main advantage behind the blockchain technology is the ability of the blockchain to store approved transactions in a tamper-proof form of storage [14]. In its mode of operation and as shown in Figure 1.2, a blockchain starts with a genesis block, also known as Block 0, which is the first block in the blockchain upon which additional blocks are added and when a new block is created, the hash value of the preceding block is entered. It is effective in a

way that each individual block can trace its decent back to the genesis block since every block references the one preceding it. When a new block is created, any alterations to a previous block results in a new and different hash code, which all the participants in the blockchain can see. For IoT systems, the ability of blockchain to create or keep or transfer digital assets in a tamper-proof, decentralized, and distributed form is the aspect of the technology that presents the most practical value.

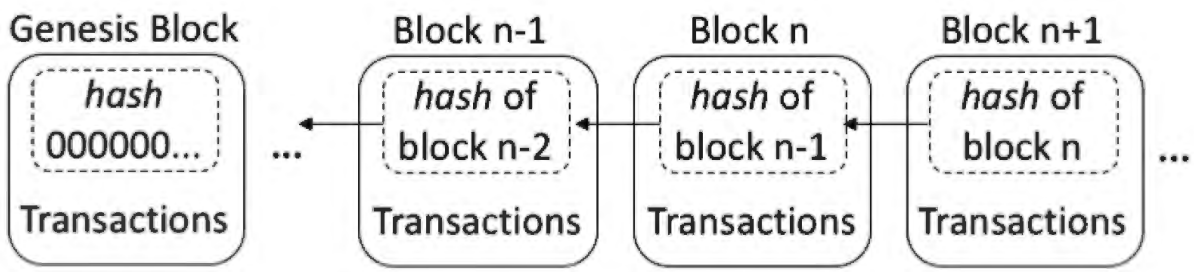


Figure 1.2: Genesis Block. [2]

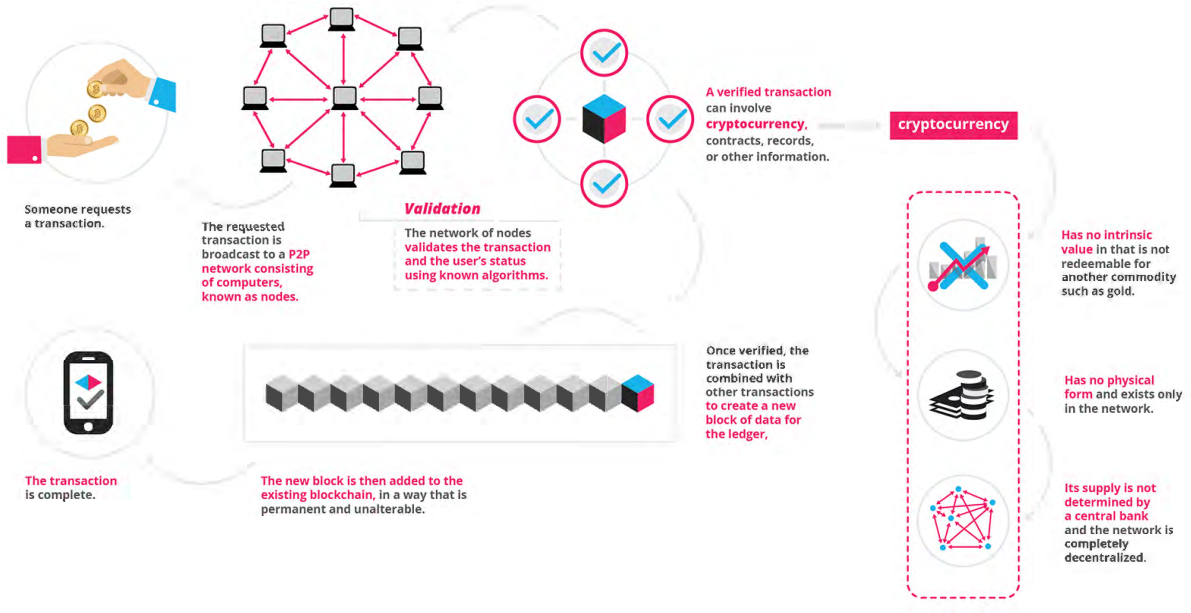


Figure 1.3: How Blockchain Works. [3]

When a transaction is being requested through a blockchain, as shown in Figure 1.3, that transaction gets broadcasted to a P2P network consisting of nodes or IoT devices. Then that transaction goes through a validation process where it gets validated by the network as well as the user's status using known algorithms (different types of information could be involved in a

verified transaction like contracts and records). After verification, the transaction is added as a new block of data on the blockchain and combined with all previous transactions. And with that, the transaction is complete.

Many systems nowadays, such as healthcare systems, are not well integrated with each other and lack the connectivity, transparency or even security. This is causing many issues in this field including transaction delays, medical errors and breach of privacy. To address these major issues, an introduction of a technology that is secure while also transparent is needed.

1.3 Main Objectives

The main objective of this thesis consist of three major parts presented as follows:

- In a Blockchain, as pointed out by [15] and [16], each full node must store the full history of the blockchain. This negatively affects time of transactions and limits most of the nodes especially lightweight ones, such as IoT devices, from joining the network. As time passes, the amount of data required to store the entire transaction history becomes larger, and the scalability issue will be aggravated. For this purpose, a platform has been constructed using an off-chain storage for managing IoT devices that will remove the load of the blockchain once the data gets larger and instead connects it to an external cloud storage.

- Blockchain technology is known for its safety and tamper-proof specification considering its transparency, integrity and connectivity features that makes it an ideal technology from a security point of view specifically for healthcare systems. On the other hand, writing data on the blockchain cost time and processing energy. Energy consumption are too high because of the consensus algorithms on blockchain. After designing the system and creating all modules, and after connecting them to each other, we need to increase the security level of the system due to the usage of an external database (off-chain storage) away from the blockchain itself. This will be achieved by implementing a few extra security mechanisms and other cryptographic techniques including data encryption, data validation and an authentication process.

- To test the proposed platform, the system needs to be implemented in a real-time scenario. For this implementation, the Saudi Arabian Health Sector will be used as an example and the Saudi Arabian Ministry of Health as our main contract deployer because of its current ongoing state of development as well as its availability to access specific data. We have obtained a list of 50 Saudi Arabian hospitals and will implement them in our platform and use a random generator for doctors and patients. Finally, a front end page will be designed that has the ability to read data directly from our platform.

1.4 Research Questions

This thesis contributes to the area of IoT, by investigating, developing and introducing blockchain technology through a novel platform built using Ethereum. The main aim of this research is to explore what could be done to increase transaction rates (Number of transactions that are successfully completed in a particular time frame) and read and write speed (Data transfer speed) using blockchain technology.

Does the capacity constraint in IoT devices negatively affect the speed of the transactions. And can we solve this issue by efficiently moving the storage off-chain?

Several sub-questions arise from the main research question as follows:

- *How to overcome the storage constraint issue when integrating blockchain with IoT while improving transaction rate performance and speed? And how can we evaluate our proposed solution?*
- *How can IoT devices be securely managed with the proposed off-chain storage constraint solution? And how can we evaluate our proposed mechanisms?*
- *How to successfully apply this solution to the Saudi Arabian Health Sector? And how can we evaluate the value of our solution in that sector?*

1.5 Thesis Contributions

The main contribution of this thesis is to build an off-chain based blockchain platform for securly managing IoT devices. This thesis contributes to the fields of Cyber security, Blockchain and IoT in the following ways:

- **A methodology to speed up blockchain transactions speed** - In a blockchain, each node must store the full history of the blockchain. This negatively affects time of transactions and limits most of the nodes especially lightweight ones, such as IoT devices, from joining the network. As time passes, the amount of data required to store the entire transaction history becomes larger, and the scalability issue will be aggravated. For this purpose, a construction of a platform using an off-chain storage for managing IoT devices has been made which will remove the load of the blockchain once the data gets larger and instead connects it to an external cloud storage. With the proposed solution, the storage constraint solution will be overcome when integrating blockchain to IoT.

- **A methodology to increase security in our off-chain blockchain platform** - After designing the system and creating all modules and connecting them to each other, and because it is a platform that uses an external database (off-chain storage) away from the blockchain itself, the need of increasing the security level of the system was needed by implementing a few extra security mechanism and other cryptographic techniques including data encryption, data validation and an authentication process) to avoid any tampering attempts to the data.

- **A methodology to simulate our platform in a real-time scenario** - An implementation has been made by using the Saudi Arabian Health Sector as an example and the Saudi Arabian Ministry of Health as the main contract deployer. A list of 50 Saudi Arabian hospitals have been obtained and implemented in the platform and a random generator for doctors and patients have been used. After that, a front end page has been designed which reads the data directly from the blockchain platform.

1.6 Thesis Outline

The remainder of this thesis has been organized as follows:

In Chapter 2, we provide the necessary background and a summary of the related work. The first part of this chapter provides the background of blockchain and IoT with an overview of both technologies. The second part goes deep into IoT technologies pointing out its insecurity as well as addressing its capacity constraint. The last part covers the benefits IoT technology can obtain from implementing blockchain technology as well as a current literature of the related work to the proposed methodologies with a summary of the gaps.

In Chapter 3, a blockchain platform with an off-chain storage is proposed for managing IoT devices. All the system modules, system structure and system tools are deeply presented. This is followed by the experimental setups, simulation, results, discussion, and chapter summary.

In Chapter 4, multiple security mechanisms are presented which have been implemented within the platform. All the necessary security measurements and cryptographic techniques including data encryption and data validation have been presented with their algorithms. This is followed by the experimental setups, simulation, results, discussion, and chapter summary.

In Chapter 5, we implemented our system in a real-time scenario. We used the Saudi Arabian Health Sector as well as the Saudi Arabian Ministry of Health as the main contract deployer. This is followed by the experimental setups, front end page, results, discussion, and chapter summary.

In Chapter 6, the contributions of this thesis are concluded and summarized, and the limitations of the proposed work and the future directions are discussed.

Chapter 2

Background and Literature Work

2.1 Introduction

This chapter presents and reports on the critique of relevant technologies to blockchain and IoT devices from various research literature. At first we introduce a summary of the building blocks of blockchain technology and IoT before advancing through an analysis of relevant research to our proposed solution concluding with a gap analysis to support our previously presented research questions.

2.2 Blockchain Technology

Blockchain allows for the interchange and electronic storage of assets without the involvement of third parties. In using this technology, systems that receive and configure files from centralized servers must trust such authorities, but if that trust is broken, the gadgets become vulnerable. However, there is no need for centralized management in blockchain technologies. For instance, peer-to-peer exchanges allow systems to trade assets instantly with one another. As such, blockchain technology has a few essential characteristics that set it apart from other databases. Smart contracts or chain codes are used by blockchain technology to ensure that preset organizational guidelines are enforced correctly [17]. For automated processes, a smart contract is a computer software or protocol that is executed by nodes on the blockchain system. Smart contracts are used in Internet of Things (IoT) settings to manage configurations.

Many systems nowadays, such as healthcare systems, are not well integrated with each other and lack the connectivity, transparency or even security. This is causing many issues in this field including transaction delays, medical errors and breach of privacy. To address these major issues, an introduction of a technology that is secure while also transparent is needed.

The blockchain is a distributed platfrom operating without a centralized power which does not need a third-party authentication. As such, blockchain technology comprises blocks, each of which includes hashes of the block before it, forming a chain of frames starting from the parent node to the block header [18]. The initial block in a blockchain is the genesis block as presented in Figure 1.2. Most often, the genesis block is preloaded into the system. Since it is unrelated to any earlier block, the genesis block is a one-of-a-kind occurrence. Every block on the blockchain system can only be accessed in one method, according to the genesis block.

Forks are formed when two blocks are constructed within a few seconds of each other. However, forks coming from the genesis block are possible. Typically, the most recent block in the longest genuine chain is chosen [18]. The longest feasible chain is determined by the total intricacy of the chain rather than the number of blocks. Because they are considered invalid links, the blocks in the shorter chain systems are known as orphan blocks.

In simplistic words, blockchain is a decentralized ledger that holds an organized list of different entries that are linked together by linkages known as chains [19] [20]. Usually, authorized personnel have access to the information stored in such blocks about individual interactions. Client authorization is preserved by a complicated series of self-managed cryptographic algorithms: authenticated people receive a time-sensitive personal identifier that autoblocks the platform once the decoding timer runs out. Without a centralized authority requirement, blockchain innovation provides a decentralized computing platform [21]. Blockchain is a new technology that allows for more dispersed processing to take place [22]. Bitcoin's popularity increased with its spectacular rise as a cryptocurrency in 2017–2018 [23]. However, cryptocurrency is not the only implementation or application of blockchain. It has a wide range of applications in the corporate world, including data storage and exchange in a variety of situations.

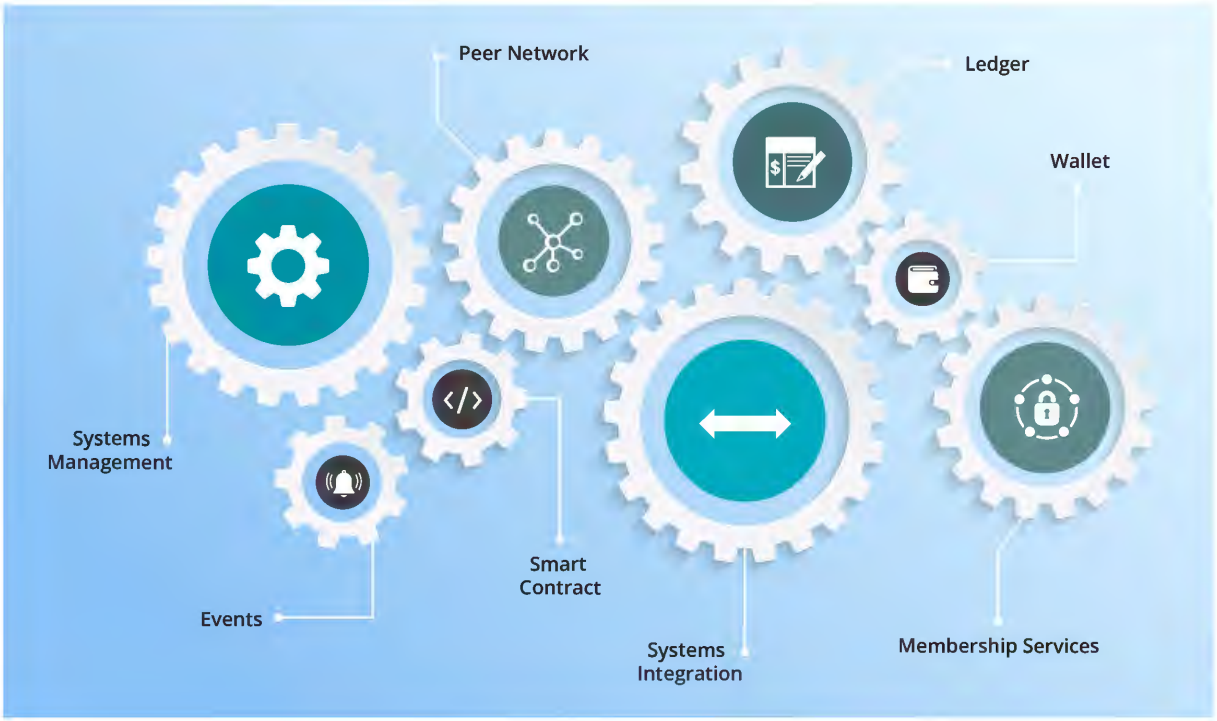


Figure 2.1: Blockchain Components. [4]

2.2.1 Blockchain Components

The Blockchain consists of eight different components as shown in Figure 2.1, each component has its own precise performance. The ledger is a historical record that is immutable and distributed and the blockchains goal is to create this ledger [24]. A peer network stores the ledger, updates it, and maintains it. A copy of this ledger is maintained by each node of this network. Coming to an agreed harmony on each update content is the job of this network. This guarantees the identicality of all copies of the ledger without the necessity of an official ”centralized” ledger copy [25]. Membership Services are responsible for authorization, authentication, and identity management of user. Anyone can join a public blockchain’s peer network and all members have equivalent authority and power. A permissioned blockchain needs authorization for joining. This membership service is responsible for authorisation, authentication, identity management of blockchain users [26].

A Smart Contract is a blockchain running program. The design of the original blockchain was as simple as allowing the performance of financial transactions on a historical ledger and storing them there with restricted allowed configurations. Nowadays, the evolution of

blockchain made some entirely fully functional computers distributed everywhere. Smart contracts are blockchain running programs that allow user interactions in a similar way as any other program on any standard computer [25]. The Wallet Stores credentials of users and track their digital assets along with any information related to the user's account [27]. Events are actions and updates notifications. The ledger and the peer network are constantly updated by events. Events such as a new transactions creation throughout the peer network and the connection of a new block as well as smart contract notifications [24]. System Management are responsible for Creation, monitoring, and modification of components. To meet the user's needs, the system management can create, monitor and modify the components of a blockchain [28]. And finally, System Integration, they are external systems of blockchain. Due to the evolution of blockchain and the constant functionality expansion, it became more convenient to integrate blockchain "usually using smart contracts" with further external systems [24].

2.2.2 Blockchain Types

Typically, there are two types of blockchains, a public blockchain and a private one. A Public blockchain is a permission-less blockchain. Anyone can join it successfully and productively. They can engage by viewing or inputting within the blockchain [29]. This public chain does not have a single unit controlling it over the network because they are decentralized which means once the data on the blockchain is validated it can't be changed. This public blockchain is beneficial because within it the user can openly input and view data, the ledger is not centralized, and it is distributed, it is immutable to avoid any tampering with data attempts, and it is secure because of the 51% rule which states that no one can obtain dominant power on this network and control more than half of the blockchain [30].

On the other hand, a private blockchain: is a permissioned blockchain. Only someone permissioned can join it and each member has restricted participations depending on the authorisations given by the network. This private chain is beneficial because within it the resources, data, and access are controlled by the enterprise, performance can be much faster with less participants on a ledger. The ability to add services and nodes when needed gives a better scalability to the enterprise, the option of having compliance support "adhere requirements" while

having infrastructure control, and more efficient consensus “less nodes” [30].

They are both similar in the way they are structured and how they function, yet they differ in the authorization point. As shown in Table 2.1.

Table 2.1: Blockchain Types

<table>
<tr><th>Private Blockchain</th><th>Public Blockchain</th></tr>
<tr><td colspan="2">Both peer-to-peer networks that are decentralized. Each maintaining a shared ledger of transactions with digital signatures.</td></tr>
<tr><td colspan="2">Both maintaining duplicates of transactions synchronized through consensus.</td></tr>
<tr><td colspan="2">Both provide definite guarantees that the ledger is unchangeable.</td></tr>
<tr><td>Only someone permissioned can join it and each member has restricted participations depending on the authorizations given by the network.</td><td>Anyone can join it successfully and productively.</td></tr>
</table>

2.2.3 Blockchain Security

Blockchain is a technology that uses a distributed ledger on a peer-to- peer network and it approaches processing and data storages exceedingly different. In fact, as presented in Table 2.2, one of the main differences between cybersecurity on blockchain and in an environment of traditional computing is the environment itself as well as its capabilities of what is it designed to do and not to do. A traditional computing environment network of an organization for the most part is administrated by staff of computer security within that organization. Even though a lot of corporations are switching to environments that are cloud based, they still acquire the majority of configurations and security throughout their systems. These traditional networks are greatly centralized, and their cybersecurity is mainly concentrated on permissions. The entire system along with users who acquire authorities on such a network are semi trusted if not fully

trusted, that leads to the main goal of eliminating external attackers from tampering with the network [31].

Table 2.2: Standard Security Vs. Blockchain Security

Standard Cyber Security	Blockchain Security
The computer security staff of a company are controlling all or most of the company network.	The design is concentrated on decentralization, and system distribution that runs on untrusted devices.
Traditional networks are greatly centralized, and their cybersecurity is mainly concentrated on permissions.	Availability and integrity is provided according to its design. On the other hand, the infrastructure of a traditional environment is based on integrity and confidentiality.
The entire system along with users who acquire authorities on such a network are semi trusted if not fully trusted, that leads to the main goal of eliminating external attackers from tampering with the network.	Blockchain security is based on protecting data from tamper by distributing copies of that data to as many possible locations for infeasibility.

The design of blockchain is concentrated on decentralization, and system distribution that runs on untrusted devices. Traditional environment's security is designed to put data in a place and barricade it by walls, while blockchain security is based on protecting data from tamper by distributing copies of that data to as many possible locations for infeasibility against tamper attempts and attacks. Availability and integrity are what blockchains provide according to its design. On the other hand, the infrastructure of a traditional environment is based on integrity and confidentiality [31] [32].

Of course, both environments have their own considerations when it comes to security. In numerous scenarios, the possibility of having the same attack on both environments occur, but it differs in the implementation details. For example, when the system becomes unable to serve the users as it is originally designed to due to an attack, such as Denial-of-Service (DoS). This can be triggered by utilizing a system's defect and is achieved by executing legal

actions rapidly faster and higher than the system can normally handle. DoS usually targets the weakest spot of the system. In a traditional environment, DoS attacks focus on an enterprise's web server denying users from services and access. This could be triggered by overloading the server with more connection requests than the capability of the server to support. Same as in blockchain, a DoS attack requires overloading the blockchain by executing more transactions than its capability. And since most of blockchains have blocks created with a predefined rate and size before being distributed, the attacker can overload and exceed the maximum predefined storage of the blockchain which then makes it unusable [33] [34].

When it comes to endpoint security, blockchain and traditional infrastructure have their differences as well. Endpoints in a blockchain are nodes and could be totally equivalent. Endpoints in a traditional cyber are all under the enterprise's control and the level of authority differs from one another. This difference between endpoints could be a risk because it gives an attacker further possibility in finding a weak vulnerable point to utilize, while the equivalency between users means a defect in one point of the system is a defect in the whole system [34].

Blockchain also differs from traditional cyber in the trust level of the company's application code. In blockchain, smart contracts can be written by anyone and anyone can make a flaw in a smart contract or in the base platform code which could lead to huge distributed consequences. In traditional cyber, the code is written by the enterprise and the exposure could be originated only from the company-controlled code. To date, the single hack ever done against Bitcoin network was exploited by overflowing integers which was a defect in its protocol. An attacker managed to assign so many Bitcoins to himself, more than the intended amount to ever be created. Bitcoin had to overcome this situation by disregarding the fundamentals and creating a hard fork and editing the historical ledger through it. If they haven't done that, the value of Bitcoin would have dropped and became valueless. A code has to be included in the application before it can be edited and such hacks makes it a big risk which any Bitcoin user has to accept [35].

Both environments are susceptible to intentional misuse attacks. In blockchain, Proof of Work systems encourage miners to do a lot. The primary defect of Proof of Work is the inse-

curity of a blockchain when a group controls more than half ”51%” of the processing power to the mining network. Proof of Work encourages miners to obtain control of as much as they can of processing power for rewards but obtaining everything is something they don’t want. In traditional cyber, DoS is an exact form of intentional misuse [36].

Each of these environments has a different goal than the other. In blockchain, data is shared and distributed, and everyone relies on the blockchain to grant availability and integrity. In traditional cyber, data is contained and siloed, with owner controlled restricted access, which puts the availability, integrity, and confidentiality of the data on them [37].

2.3 Internet of Things (IoT)

The Internet of Things (IoT) is a term used in information technology to describe the link between built-in devices and the internet. Such devices are connected wirelessly, opening up new opportunities for interactions across systems and additional management options, surveillance, and the provision of improved service features. Research demonstrates the challenge of obtaining a consistent definition [38]. Researchers propose that two unique interpretations be used, each based on an individual situation. Another research believes that the Internet of Things is ”a worldwide architecture for the information age, empowering innovative capabilities through interconnections (physical and simulated) ideas based on, established and developing, integrated information and communication technologies,” according to the Telecommunication Standardization Sector of the International Telecommunication Union [39].

The actual or digital entities must communicate, identify themselves, and engage with their surroundings. Computers and cellphones are only a few examples of such physical products, including furnishings and plays. People or creatures can provide IoT data. Such devices must be linked via the internet instead of other forms of communication [40]. The diverse nature of gadgets, their sensing, and their connectivity and communication effectiveness are all essential parts of the IoT’s definition and interpretation that influence technological advancement in IoT.

When contrasted to connected devices in enterprise networks, IoT devices are constrained by design, limiting available performance and profitability. While creating a management and monitoring system for IoT devices, available resources and implementation of IoT devices must

be taken into account [41]. Multiple configurations and levels of monitoring are used by the heterogeneity of IoT devices for diverse goals. Since enterprise network settings include comparable heterogeneity of devices, current network monitoring and management tools can be adapted for IoT implementation.

As a component of the ”Future Internet,” the IoT has evolved into a dynamic architecture influenced by a diverse number of shareholders. Although there is widespread awareness of the Internet of Things, a consistent definition is still necessary, as formulations are offered based on various interpretations and views. As a result, many elements are addressed. Three main statements are identified by [42]:

1. Internet-oriented, with an emphasis on network-based connection and features like networking devices.

2. Thing-oriented, with an emphasis on the identification and functioning of interconnected devices.

3. Semantic-oriented, with an emphasis on the complexities of managing IoT data.

Different traits are emphasized depending on the viewpoint. The most basic IoT properties are connection, diversity, adaptability, compatibility, and security or safety. Another way to appreciate the critical aspects of the Internet of Things is to examine its infrastructure [43]. There is no common IoT architectural framework. The majority of suggested architecture, on the other hand, is focused on specific service categories. On the other hand, a proposed research claim that an IoT infrastructure is made up of three strands [44]:

1. A sensory or mechanical stratum that facilitates data gathering and sensory.

2. An implementation phase that delivers programs and applications for evaluating and synthesizing data received.

3. A network phase that serves as a link between these two phases to exchange information.

Correspondingly, the Casagras proposal differentiates three levels:

1. A physical level for recognizing physical stuff.

2. A data management, implementation, and venture level issuing a framework for software and systems.

3. An intelligence analyst level providing the needed limits between these two levels [45].

A service phase is added to more service-based IoT systems that administer the necessary services by users and devices.

The Internet of Things is altering and refining manual operations to bring them into the digital world, resulting in massive amounts of data that supply information at previously unimaginable levels. The understanding assists in creating innovative technologies like improving city administration and resident quality of life through the digitalization of operations [46]. Cloud computing technologies have helped provide the IoT with the essential capabilities to evaluate and interpret data and turn it into meaningful action and information during the last several years. Because of the IoT's remarkable expansion, new community possibilities like systems to access and exchange information have emerged. The public data concept is at the forefront of these efforts.

Nevertheless, as has happened in many cases, one of the most significant vulnerabilities of such projects is data protection [47]. The growth of IoT has been aided by centralized systems such as those utilized in cloud computing. Unfortunately, they act as black boxes for data openness, and participating nodes have no idea where or how the data they contribute will be used.

The incorporation of innovative technologies like IoT and cloud computing have shown to be quite beneficial. Similarly, blockchain has enormous potential in changing IoT. Blockchain can enhance the Internet of Things by providing a trustworthy sharing service that is secure and verifiable. Data sources may be recognized at any time, and data is unchangeable throughout time, enhancing security [48]. The collaboration would be a game-changer in scenarios when IoT data needs to be discreetly transmitted among many people [49]). For example, ensur-

ing food safety requires extensive provenance across numerous packaged foods. As a result, blockchain can provide reliable and secure data to the Internet of Things. It has begun to be acknowledged as it identifies blockchain solutions as the key to solving sustainability, safety, and stability issues associated with the IoT vision.

The use of blockchain technology and smart contracts together with IoT systems in goods supply chain management is the most researched strategy. Researchers also looked at real-world examples of how blockchain and IoT sensors were used to track raw materials [50], components in supply chains in the culinary, pharmaceuticals, and other sectors. The author points out that, despite some regulatory and technological limitations, the universality and adaptability of blockchain can improve supply chain integrity and expedite management.

IoT and blockchain principles can improve supply chain administration in services, including transmission and monitoring. An example of IoT technology and blockchain applications is intelligent homes and communities. A framework was presented for allowing reliable resources management of services for all residents of an innovative grid system. Participants of intelligent cities can more effectively monitor and manage resource utilization securely and reliably

Another option to use blockchain is to supplement IoT infrastructure to improve its sustainability and administration. In terms of assessment and tracking, gadgets in an IoT context are comparable to network elements, but there are significant differences [51]. To begin with, IoT device connectivity is frequently capped given the relative complexity and protracted installation with few capabilities, and the gadget may not always be online to preserve the scarce resources. Identification of data integrity and security were presented as two major IoT concerns that can be addressed with implementing a blockchain [51].

Patch Transporter is one way to disseminate software upgrades in an IoT setting using blockchain technology. Patches are exchanged between IoT devices in a peer-to-peer manner, according to [52]. A blockchain-based program is utilized to validate the conveyance of accurate fixes and induce the operation. Self-interested gadgets may be enticed to engage in the transmission of updates to different systems. A private blockchain is utilized in network administration to distribute configuration updates to endpoints in a timely and safe manner. Unlike

the more robust conventional approach to system administration, the decentralized nature of blockchain allows for higher flexibility. It boosts dependability and accessibility by eradicating a single source point of failure [52]. Furthermore, when adjustments are stored in a blockchain system, there are no ways to interfere with such records. For example, rollback to the past working arrangement is simple in the instance of misconfigurations.

The Internet of Things (IoT) is a centralized system consisting of a global network of networked devices that communicate via a unique hardware recognition mechanism [53]. IoT mainly relies on centralized servers for security and performance. As a result, IoT may be limited to a particular range of devices in some circumstances. The centralized servers must be used to relay all interactions among devices. As a result, it has been determined that a distributed server will improve IoT capacity.

If centralized servers fail, all operations fail, according to [54]; centralized servers' incapability to have a comprehensive data encryption framework; and eventually, the functional capacity of a single central server is constrained by gadgets which can be connected and the server's processing and data transfer capacity. As a result, according to the research, a decentralized system would be favorable to the overall expansion of IoT.

Because it manages a public ledger of data flow, a blockchain-based distributed database system overcomes the problem of computational limits and encryption techniques. A poll was done to establish the significance of a blockchain-based architecture for security and privacy issues in IoT platforms [55]. The authors supported their assertion by noting that the International Telecommunication Union's Telecommunication Standardization Sectors architecture enables the convergence of IoT with blockchain, allowing for the usage of blockchain in IoT to create a resilient, distributed system.

The e-business model might be hampered by a lack of openness among the many actors [56]. Whenever the Internet of Things (IoT) is introduced, the e-business model gets difficult since IoT includes physical items and people easily connected to the communications system. Each component of the e-business model is incompatible with the IoT platform. As a result, a decentralized infrastructure is required; nevertheless, transactional authorization will be a

problem. This kind of circumstance can be facilitated by a blockchain-based platform, in which a decentralized IoT platform can self-authenticate its transactions in an e-business paradigm. It is referred to as decentralized autonomous corporations by the writers [56]. The problem with decentralized independent corporations is that they cannot deal with nodes obstructing the data transfer mechanism.

A more comprehensive protocol is needed. Beekeeper is the name given to a developed protocol [54]. BeeKeeper is a blockchain-based Time Synchronized Mesh Protocol for multi-party computation. Hosts execute algorithms on data sharing and provide answers in the procedure. It is simple to record and verify the total number of data exchanges and responses to eliminate the challenge of unauthorized harmful devices intruding on the network's privacy protection. The Beekeeper was built on an Ethereum private blockchain with four monitoring nodes, according to the researchers. The data created by the manager, server, and gadgets are collected using replicated transactions. The transaction blocks in this system contains the hash, node numbers, sequence, duration, originator, recipient, signatures, and contents, making up the actual block [54]. According to the researchers, because all of the data is stored in the blockchain and administrators assist in processing the data, gadgets do not require a lot of storage or processing capacity.

2.3.1 Security inadequacy in IoT

The modern world is more connected to web-based digital devices in the current cutting-edge advantaged position. IoT refers to objects outfitted with detectors, controllers, and a microprocessor connected to meet a specific need [57]. The internet has progressed toward being pervasive, profoundly impacting human life by watching and regulating a wide range of hand-held devices and causing massive change by introducing features such as collaboration with current reality and consciousness to nonliving entities. IoT devices have already been interconnected to the actual world and collaborate to complete complex tasks that demand high intelligence levels [57]. The digital world utilizes actuators and detectors to interconnect with the physical realm.

Intelligent and interconnectedness in many businesses and settings, IoT devices provide many methods to improve operations and efficiency, improve user experience, and lower expenses. Although IoT devices offer advantages in industries, healthcare, automobiles, residences, and municipalities, their inherent vulnerabilities pose additional security threats and concerns [58]. Because of these flaws, networks are vulnerable to cyberattacks, which can seriously disrupt enterprises and civilizations.

Threats and risks related to the IoT infrastructure in this perspective were addressed [59]. A comprehensive comparison of different IoT security procedures have been made. They developed a classification for security procedures utilized in IoT systems during this procedure, which included device verification, access management, and privacy protection, among other things. On the other hand, an establishment of a classification of IoT security risks following perceptions, conveyance, and implementation was proposed [60] [61] and an evaluation of the categorization of multiple security problems was presented [62].

In contrast, a development of an IoT security framework which composed of five stages was made (notably data processing, storage, synthesis of security models, display of security models, security assessment, and model upgrades) [63]. Depending on the properly-outlined security parameters, this model can analyze IoT security measures. another development was made as a class-based syntax for structural programming language and a system for switching among such languages [64]. From the perspective of observation layers security, the different components of an IoT ecosystem were addressed [65]. They analyzed and classified potential threats at various tiers in their design. A suggestion of a framework for remote security control of IoT devices was made to anticipate and avoid multiple risks [66].

IoT devices are unable to execute multiple complex authentication mechanisms due to a lack of processing power. As a result, endpoint authentication is a security flaw in the IoT ecosystem. For example, the Mirai malware software took use of these gadgets to conduct a DDoS assault against the rest of the network. An analysis of the various authentication systems using a multi-criteria categorization system was presented [41]. They studied and contrasted established authentication schemes to determine their comparative benefits and drawbacks. A

development of a trustworthy system authentication technique by combining physical security protocols and cryptographic innovations has been introduced [67]. The cryptographic key is created by calculating device characteristics, including relay node and radio waves. The test results reveal that a more efficient defense against a variety of typical cyberattacks is possible. A token-based verification system following the MQTT system for resource-constrained systems has been suggested [39] . The proposed method comprises four parts (notably publishers, subscribers, MQTT brokers, and token authentication servers). To obtain the credential, publishers or subscribers first present their credentials to the authentication mechanism. It can save and utilize a validated certification for further verification after getting one.

Complementary authentication protocols following multiple keys were described by [68]. The keys are shared across numerous IoT devices via a secure vault. The keys to the secure vault are given out at first, but they are changed following a successful message flow. A signature-based authentication approach for IoT gadgets has been proposed in which NS2 is used to trigger the mechanism, which is then examined through Burrows–Abadi–Needham logic [69]. A system in which IoT gadgets can only connect to a plan once they meet a multi-factor authentication threshold was suggested [70]. Such a system would help mitigate the conventional cyber threats, including replay and man in the middle through nonce and timestamps.

A thoroughly verified authentication protocol is frequently referred to as a prohibitively expensive method of guaranteeing security systems for IoT devices. To counteract the limitations, one might use technologies including imposing several lines of protection, isolating gadgets into distinct networks utilizing firewalls, and protecting the system's security. An investigation of the security problems in the communication elements of IoT-based smart houses in this setting has been established [71] . While an introduction of the CyberShip-IoT architecture was presented, which uses the software-defined network (SDN) architecture to minimize network flow assaults. For safe communications among IoT systems [72], a proposed multi-hop routing system was presented [73]. The method validates a gadget using multilayered characteristics while building a new network to improve secure communication. Security vulnerabilities with network functions virtualization (NFV) and software-defined networking (SDN) were addressed from the

standpoint of the Internet of Things [74]. They also showed the significant security issues that SDN and NFV-based security procedures will face once implemented by the Internet of things architecture. An establishment of a credible network infrastructure following self-certifying ID (SCID) has been proccessed [75], while a development of a new procedure for tackling different security challenges built on trust among Proxy Mobile IPv6 (PMIPv6) domain or IoT devices has been presented [76]. The standard supports handoffs administration, authentication mechanisms, key distribution, and other functions. An investigation of IoT capillaries networks for various IP and non-IP IoT systems has been made and a proposition of a safe critical renewing mechanism-based method for improved network integrity has been presented [77]. Even though these methods improve the integrity of IoT networks, they frequently come with a lot of installation complexities and IoT execution costs that can slow down data flow across secure network connections.

In IoT devices, sensor data is frequently used to influence the structure and behavior of different gadgets. As a result, the protection of transmitted signals in the IoT infrastructure is critical for avoiding cyberattacks. Conventional cryptographic techniques, on the other hand, are not ideal for IoT systems with limited resources. An establishment of a system was presented for transferring data with low encryption latency by employing proxy re-encryption [78]. By inventing a methodology for identifying rogue nodes susceptible to firmware version threats, while another research paper has halted the transmission of fraudulent information in the network [72].

On the other hand, A three-dimensional study was devised and designed to examine IoT system protection by integrating the concepts of IoT infrastructure and data lifespans [79]. A blockchain infrastructure was introduced along with its application in IoT security [80], while another research leveraged MySQL's Mobius architecture to create a revolutionary IoT server architecture for safe storing and retrieving of sensor information [81], which is backed by a blockchain. Furthermore, from the standpoint of IoT privacy protection needs, and the contradictions in the gathering, utilization, and administration of huge volumes of data was broached [82]. Like most other protection enforcing algorithms, the techniques examine data

stream from IoT end-point systems across the Internet to a central cloud at execution time to guarantee secure IoT data consumption. Still, they fail to monitor how such data moves across various software components dynamically.

Static system analyses can be valuable in this scenario for evaluating the erroneous data traveling through multiple IoT levels (for example, sensitive and consumers' usage information). Static code evaluation, according to [83], can be used to discover most of these errors. Taint analysis, specifically, monitors whether something at a supply (for example, methods for receiving user input and confidential material) streams into a sink (for example, techniques for transmitting data to the Internet and running SQL statements) without being cleaned (such as encrypted or escaped). The method has been frequently used to identify SQL injections in Web-based applications and delicate data leaks. An attempt to deploy such a method was displayed to a situation akin to IoT in a technique used to find leaks and inject flaws in Android automobile applications [84] [85].

On the other hand, Security and privacy flaws in five IoT systems were presented by using current static analysts to detect such vulnerabilities [86]. A portfolio of analytic techniques and methodologies aimed at various IoT systems is mostly nonexistent according to these techniques. As a result, the present IoT security environment necessitates a framework for examining the IoT state's security weaknesses while also allowing for cross-interface data transmission. Current taint analysis approaches can be quite helpful in this area, but they can only study a system in isolation [86]. Furthermore, because IoT devices are made up of several interacting parts that run separately, taint assessment must be conducted across various programs. Therefore, the taint assessment should be improved to study many interactive applications operating in parallel.

The significance of integrating interconnected systems with a security-by-design technique is based by the priority of such systems and the repercussions of attacks. Most IoT devices are insecure since they lack the requisite built-in security safeguards to protect them from attackers following the gadgets' limited computing capabilities and confined surroundings. IoT applications are generally limited-capability devices that can only execute a few operations [87]. As

a result, IoT devices cannot withstand security systems and standards, and also data security procedures. Security flaws in IoT systems could be used by cybercriminals to infiltrate and attack critical infrastructure. Cyber criminals are usually ready to exploit known weaknesses in IoT devices and turn them into IoT botnets. In 2016, the Mirai botnet hacked dozens of compromised home IoT devices, taking down marginally raised web services (after a DDoS attack) [87]. IoT weaknesses and security intrusions are at the root of several data breaches, leading in severe legal consequences for infractions of the General Data Protection Regulation (GDPR), The California Consumer Privacy Act (CCPA), Health Insurance Portability and Accountability (HIPAA), and Payment Card Industry Data Security Standards (PCI-DSS) regulations.

A deep dive was made into the revolutionary privacy and security solutions accessible for sustainable IoT-based agribusiness [88]. They provided a four-tier green IoT-based agribusiness system overview. They categorized the threat models in comparison to green IoT-dependent agribusiness into five categories, comprising authenticating, cyberattacks on confidentiality, availability, security, and authenticity, based on significant analytical work. They also looked at consensus methods and privacy-focused BC-based solutions for green IoT-based agribusiness. Another research has presented findings that machine learning algorithms, vulnerability scanning data sets, choosing effective consensus protocol, scalability assessment of BC-based solutions, and the schematization of innovative and consistent cryptography algorithms are just a few of the daunting research areas that should be investigated soon [88]. Another research was thorough, but it was limited to the realm of agribusiness [88]. IoT security is essential for the effectiveness of IoT applications and infrastructure. The data is collected via the Internet of Things (IoT) from a vast geographical area utilizing controllers and detectors. As a result, the Internet of Things (IoT) can be identified as a collection of physical gadgets, vehicular connections, domestic appliances, and other connected devices that are equipped with peripherals, electronic controls, and detectors, as well as network interconnection, that allows machines to assemble, gather and exchange data and information [26]. IoT functions as a massive network that is filtered out and assigned to those acquired assets based on their use and their understand-

ing of the surrounding circumstances.

A systematic literature search has been conducted on the present studies relating to the use of blockchain innovations in IoT cybersecurity [89]. Because of the decentralized blockchain concept, the network's inherent confidentiality and untrustworthy parties were protected. The issues of security considerations in IoT are receiving more attention than ever before. Another research paper revealed that the cryptography used in blockchain-based approaches is time and effort-intensive [89]. Their results, however, demonstrated that IoT devices have varying computational power. As such, IoT devices were not capable of performing cryptographic techniques at the required speed. Due to the decentralized state of blockchain, scalability is a crucial challenge. After some time, the capacity of the ledger could increase, and the content size is usually more significant than the limits of most IoT networks. Following the presence of multiple nodes in IoT networks, there is a considerable demand for a substantial percentage. As a result, a research reviewed the current literature on blockchain innovation's use in IoT safety and support rather than a comprehensive assessment found in the literature [89].

Furthermore, an investigation was conducted into using blockchain to ensure IoT networks' protection, trustworthiness, and privacy [90]. According to their findings, the blockchain offers solutions to particular failure spots, dependability, trustworthiness, time-stepping, and confidentiality. Blockchain also has several notable features, including improved fault-tolerant capacities adaption, faster and more effective operations, and adaptability. A finding was presented about blockchain facing challenges that require solutions to be fully utilized [90]. To meet security requirements, more functional strength is required. To enable blockchain's use in various cultures, standards and legal requirements need to be established. Excessive data storage is among the blockchain's downsides. The requirement for a certain quantity of bandwidth raises the accounting of data overload. An additional consideration is IoT performance. Data retention on an expansive blockchain is costly, as it is in other architectures; even the execution of a single program on blockchain technology has a cost. The blockchain innovation is only for the valued key pair, not for large documents [90]. Addressing the capacity problem without revealing decentralization is a significant step forward in blockchain technology.

A revision of blockchain and IoT was made, focusing on difficulties related to an IoT environment [91]. According to their literature evaluation, the Internet of Things is the next technology that will improve high-speed networks and intelligent network equipment. Unfortunately, IoT technologies are increasingly vulnerable to threats and unable to defend themselves. Their research focused on different aspects and characteristics of the blockchain network, like resolving IoT issues [91]. Furthermore, issues that remain unresolved after blockchain implementation are identified.

A blockchain-based analysis of IoT applications was conducted while addressing their associated security issues [92]. They examined the expanded category of blockchain-based IoT applications through several components based on the academic literature's governed, analyzed, and usable notion study. Advanced health care, corporate, smart home and city, innovative vehicle networking, e- commerce model, and supply chain management were the components utilizing IoT devices. [92] also illustrated the stated IoT devices' security challenges, which are essentially IoT technology limitations.

Additionally, an investigation of the solutions that improve IoT security was presented [93], such as data security and privacy, identification and authenticating administration, scalability, reliability, and anonymity, all of which are enhanced by using blockchain. The author also mentioned end-to-end foodstuff provenance, which is enabled by various technologies like IoT and blockchain. A research and analysis of the IoT's fundamental security issues has been conducted [94]. They divided the problems into three categories: transitional, elevated, and minimal IoT levels. They briefly reviewed the approaches available in the existing studies to leverage IoT security at various levels.

Due to climatic changes, population growth, and resources depletion, the world has experienced remarkable urban expansion over the last ten years. A smart city uses information technology to combine and monitor sociological, environmental, and commercial foundations to provide better help to its residents while ensuring efficient and optimal use of available resources [95]. Despite its many potential benefits, enhanced disruption has several risks associated with data protection and security. The healthcare sector is one example of a conventional

enterprise striving to reap the benefits of IoT. Application-specific requirements, like network and communication capability of devices, have posed new challenges for IoT devices [95]. Professionals are increasingly adopting IoT-based wearable technologies concurrently with the IoT wave; there are opportunities for blockchain infrastructure in the financial sector and in various relevant fields, including healthcare. Even though IoT offers significant advantages over traditional communication networks for innovative home systems, IoT installations are currently infrequent.

A distributed security framework for IoT in the smart city has been presented based on software-defined networking and blockchain technology [96]. Detecting IoT infrastructure attacks relies on three key developments: blockchain, software-defined networking, and smartphone and peripheral cloud computing. As a result, the suggested architecture requires software-defined networking to monitor and analyze traffic data throughout the entire IoT network to provide an optimum intrusion detection protocol. Blockchain enables distributed attack detection, which supports its intrusion problem, and that is the main aim of its current architecture. Attack identification at the cloud environment is aided by mobility and cloud edge processing, resulting in attack reduction at the network edge [96]. As a result, it facilitates early detection and alleviation by reducing capacity constraints, lowering calculation costs, and reducing idle time. To validate the suggested architecture's representation, it was subjected to a trial evaluation, the results of which revealed that it outperforms both combined and standardized models in terms of accuracy and localization duration.

How blockchain innovations can be utilized to handle IoT security challenges was also looked into in the context of the 5G cell structure [97]. They presented a multilayered security organization paradigm for the IoT based on blockchain technology. By separating the IoT infrastructure into a multilayered and distributed system, the suggested methodology addressed challenges associated with blockchain technology's practical transmission. They used developmental computations, including particle swarm optimization and evolutionary algorithms, to divide the ecosystem into K-unknown groups in the suggested model. Every cluster heaver selects a local verification element for inspection and certification reasons within each batch [97].

Blockchain technology helps provide a validation system to clustered head communications among each other and a foundation solution via localized blockchain utilization with no focal position due to its high confidentiality and trustworthiness verification.

The Internet of Things is entrusted with addressing objects that may be severely limited by design [47]. Given that the Internet of Things will be in charge of overseeing vital infrastructures like traffic control systems, patient health monitoring programs and domestic security systems, it is clear to see how inefficient IoT equipment might have a significant or catastrophic influence on the system's judgment [46]. The IoT capacity challenges do not stop at the gadget and equipment layers; the data link layer must also be considered. Following the heterogeneous nature of connected systems and how such devices transfer data, usually wirelessly through lossy lines, this might be hard to verify. Then there is the question of activation to address in addition to data transfer. Procedures must be set to check the correctness of the decision-making frameworks that govern the platform's actuators. Poor decision-making could jeopardize end-users' lives, rendering it a critical research topic [48]. IoT device vulnerability has become a significant concern in the commercial and state sectors.

2.3.2 Capacity Constraint in IoT

The fundamental challenge with Internet of Things revolves around the system's inability to support multiple devices with varying memory, computation, capacity, and bandwidth. It is considered scalable when additional services, hardware, or gadgets can be added to a system without decreasing its functionality. The availability of resources is another significant factor to consider [98]. In the multilayered architecture of IoT, scalability and availability must be implemented jointly. Cloud-based IoT applications are a perfect example of scalability since they allow users to grow IoT infrastructure by introducing new sensors, memory, and processing capabilities as needed [98].

Nonetheless, following the global decentralisation of IoT ecosystem, the establishment of a seamless IoT protocol that fulfills universal requirements demands a new research technique. Another key challenge is to ensure that authorized entities have access to resources regardless of their geographical locations and the time of such need. Numerous IoT systems are inter-

connected to the global IoT infrastructure in a decentralized approach, utilising their numerous resources and abilities. As a result, accessibility is a major problem [98]. The use of external data transport channels, like communication satellites, may disrupt different activities and resource accessibility.

Another major factor in IoT is quality of service (QoS). QoS is a protocol for evaluating the quality, efficiency, and effectiveness of IoT systems, networks, and infrastructure. Consistency, affordability, energy utilization, cybersecurity, and processing times are significant and require QoS criteria for IoT systems [99]. A more innovative IoT network must meet the needs of QoS criteria. In addition, IoT services and devices' QoS measures should be outlined initially for their integrity verification.

There are various ways that can be used to analyze QoS; however, as indicated by [100], there is a trade-off among quality variables and methodologies. As a result, to address such trade-offs, high-quality simulations must be used. Several high-quality frameworks, including ISO/IEC25010 and OASIS-WSQM, are accessible in the research and can be utilized to analyze the methodologies employed for QoS evaluation [100]. The models include a large number of quality parameters that are adequate for determining QoS for IoT applications. Furthermore, users can specify their specific demands and expectations.

Congestion happens when several devices send data simultaneously, resulting in a severe overload condition on the system, which significantly impacts system performance and can lead to network problems. Overload can also develop as a result of servers or program failure. Gadgets can access the network without overloading, so when the network is congested, all other communications are disabled. Data is being generated exponentially by the vast and quickly expanding number of linked items. For instance, a connected vehicle can generate megabytes of data in each millisecond. This would contain information on

1. The vehicle's mobility, including itineraries and velocity.

2. The vehicle's mechanical properties, including part depreciation.

3. The vehicle's surroundings, like road and meteorological changes.

4. Films captured by the vehicle's safety devices.

A self-driving car would produce considerably more data, projected to be one gigabit every second.

The smart grid in the United States is estimated to create 1000 petabytes of data annually. In 2010, the United States Library of Congress produced approximately 2.4 petabytes of data monthly, Google generated nearly one petabyte monthly, and AT&T's network used around 200 petabytes annually [101]. To transmit all data to the cloud, significant network capacity is required [102]. Due to restrictions and data privacy issues, it is frequently unneeded or even forbidden. According to ABI Research, endpoint data can be stored and processed locally instead of in the cloud for 90% of the time.

The cost of data storing is rapidly reducing, allowing users to save data produced once for an indefinite period. It also includes the fact that consumers' attitudes toward electronic files are changing. By combining all of this digital data into a global network, the IoT ultimately creates an environment that poses a significant risk to privacy and security following capacity constraints [98]. Only when a person has complete control over their data can privacy and security be guaranteed. Moreover, only approved service providers, such as certified organizations, should have access to personal data.

Furthermore, data must only be kept for a short period if necessary; otherwise, it should be discarded promptly. However, this approach is practically tricky in sensing devices, and the administrator for this kind of control is similarly hard to define. Following technical limits in connectivity and infrastructure, information transmission methods cannot handle such high levels of security vulnerabilities [98]. As a result, there is a need to develop data transmission systems that can manage high levels of security while still ensuring authentication and encryption consistency.

The first issue observed from a hardware standpoint is that sensors and actuators are the highly limited by design of IoT systems [103]. The limitations apply to battery, memory, and processing capabilities [104]. The battery capacity is an issue for IoT systems since the application server is usually uninformed of how much battery is available on the device, making it

hard to decide when to replace it [105]. The concern about battery life is exacerbated when considering that appliances may be situated in challenging and dangerous locations to replace. Because memory and CPU limitations restrict the devices' capacity to hold elaborate encryption algorithms, IoT systems need to rely on minimal encryption to safeguard signals transmission by the gadget [49] [106].

An additional problem emerges from the gadgets' confined nature when installing the low-powered detectors' restricted architecture. Connecting to a cloud service regularly to examine whether the latest update has to be implemented on the gadget is problematic owing to the lack of power and ramifications for the gadgets' battery capacity [47] [107] [108]. As a result, devices could run on obsolete firmware, exposing them to security vulnerabilities and limited operational capacities.

Sensor nodes used throughout the Internet of Things are frequently installed in isolated and far-flung places. They are often exposed to adverse climatic conditions, including heat, cold temperatures, abrasive wear, vibrations, and dampness [109]. It is necessary to assess a device's "useful life" duration to establish when it should be discontinued. If the device is used in a severe environment, its usable life will be reduced. As a result, significant differences in device lifespan and capacity for identical gadgets used in different conditions, making system reliability and performance challenging to maintain.

Most researchers looking at IoT device performance used traditional reliability measurements in IoT-based solutions. Measurments of performance, rate of failure, and accessibilities have been calculated [110]. The study suggested a statistical framework for predicting viability in interconnected IoT Systems, assuming that IoT device breakdown mechanisms follow a given distribution scheme. The researchers defined the consistency metric R(t) as the likelihood that the device is functioning successfully during the time interval [0, t]. The probability function can be used to estimate a device's predicted failure mode, usability, and performance.

An approach for quantifying the dependability of heterogeneity IoT systems has been presented [111], which comprised Mean Time to Repair and capacity measures. The process attempted to distinguish among trustworthy devices to gather data from trustworthy gadgets and

reject data from untrustworthy ones. Equipment identification, description categorization, validity, and dependability verification were the four components of the technique [111]. The researchers rated connected fitness gadgets depending on their dependability outcomes utilizing established reliability parameters of the method.

A weighted approach for assessing capacity and dependability in the IoT based on dependability was proposed [112], probability of failure, and reusability. Usability, dependability, effectiveness, and adaptability were the four quality requirements of the model. Within these parameters, indicators were established, and values were set so that the algorithm could produce an overall score for the IoT software's performance. The algorithm was then put through its paces in a simulated setting, yielding ratings for all parameters. The model allows for weighting, although all criteria were equally weighted [112]. The traditional indicators are an excellent place to start when it comes to quantifying IoT dependability and capacity. Still, they have not evolved enough to certify validity at all stages of the IoT ecosystem.

A comprehensive framework to manage quality and dependability has been presented [113]. The framework is intended to measure the quality and reliability of specific devices in the Internet of Things (IoT) systems. The approach extracted metadata from IoT devices from a network using Networked Smart Objects according to [114]. Transparency, authenticity, security, and verification were the variables derived from a security standpoint. Reliability, responsiveness, and thoroughness were the gathered quality criteria [114]. Every variable received an index value ranging from zero to one, indicating the node's efficacy concerning that variable.

BlockBench was proposed along with a paradigm for statistical analysis and private blockchains based on conventional blockchain [115]. The application level, which includes symmetric encryption, asset tracking, stocks clearance, among other popular usages, makes up the overarching architecture. Consent block, database schema, and implementation mechanism are all operations in the middle level. The blockchain's CPU, memory, and networking are at their most basic level. The application level is at the summit of the BlockBench, accompanied by the executable scheme, database schema, and unanimity [115]. Agreements are handled by the application level, while compilers, virtual machines, and Dockers employ the executing engine

surface, which is CPU intensive.

Meanwhile, the data model level is made up of block operations and is utilized for analytics, while the consensus overlay is used for agreements. Nevertheless, because each node in the chain must keep the transactions of all other nodes in the chain, BlockBench has been accused of being a heavy node. The researchers suggest a networking coding-based decentralized storage – to resolve the bloat challenge, which slows down the node delivery process and the storage requirement of all nodes [116].

Even while systems like NC-DS address the challenge of storage, it was pointed out that there is a trust concern to address and the issue of crucial exploitation [117]. To enable fine-grained accessibility control over data in distributed storage solutions, the researchers propose a novel model that incorporates the distributed storage solution IFS, the Ethereum blockchain, and attribute-based encryption technologies [117]. With a verified key and the capacity to give secret keys to data consumers, the data holder is the only one who has control over their data. The technique is more adaptable than the usual structure. In the same area, secure key management in IoT context was proposed by using Ethereum platform [118].

A new architecture for dealing with bloated nodes has been provided [119]. The researchers proposed an architecture that uses the aggregated signature approach to maintain privacy. The data storage capacity in all nodes is a big concern in many privacy-preserving blockchain frameworks. Because each node keeps its decentralized ledger, there is a need to be a framework to mitigate the problem of bloated nodes. With the aggregated verification process, each node would only contain the verification obtained by condensing all of the preceding nodes' signatures, resulting in a reduction in storage capacity. However, the quantity of computation required to execute encryption and decryption of a block operation with many inputs and outputs is hidden using this blockchain approach [119]. Furthermore, irrespective of the number of inputs, the size of the signatures on an operation remains unchanged, boosting transaction efficiency.

In a blockchain, storage capacity and adaptability have been heavily challenged. The chain is still expanding in this innovation, at a pace of 1MB each block per 10 minutes in Bitcoin,

and duplicates are kept amongst nodes in a system. The whole chain is stored by only complete nodes (nodes that can completely authenticate transmissions); however, the storage needs are substantial. Nodes demand more resources as their size expands, limiting the system's capacity scale [98]. Furthermore, a large chain has severe performance consequences, such as increasing its time for new users to synchronize.

As nodes in the blockchain platform are required to authenticate transactions of all blocks, transactional validation is an integral part of the decentralized consensus process [120]. The processing power needed is standardized by transactions in a blockchain system and the period between blockchains, impacting transactional confirmation timeframes. As a result, the consensus mechanism directly impacts blockchain network capacity. Bitcoin-NG presents a new Byzantine-fault-tolerant blockchain protocol that reduces agreement delay compared to Bitcoin, taking into account the security framework of Bitcoin and its scaling limits [121]. Litecoin is theoretically similar to Bitcoin, but because of a decrease in the block growth cycle and an authenticator built-on-script, a memory-intensive passcode based on a crucial derivation mechanism, it has fast processing times and better storage effectiveness [122]. GHOST strives to increase Bitcoin's scalability by altering the network selection rule.

Off-chain technologies are designed to process operations outside the blockchain, boosting bandwidth and raising the risk of data loss. Another idea involves decreasing the Bitcoin protocol's increase delay, which could jeopardize the platform's security [123]. BigchainDB provides blockchain properties to an extensive data distributed system, rather than boosting the scalability of blockchain. BigchainDB blends blockchain's preservation and distributed architecture with the maximum bandwidth and low latency qualities of large data decentralized database systems [124]. The Inter Planetary File System is another significant advancement that enables a Peer-to-peer decentralized data system to make the internet safer, quicker, and more open by storing distributed and shared data. Inter Planetary File System aims to improve the web's performance while also removing duplication and keeping track of each document's version history.

2.4 Related Literature

A blockchain is an advanced tool for providing information and transactional processes to privacy concerns and gadgets. Blockchain has recently attracted much attention due to its fundamental structure and associated security and privacy implications. Blockchain can remove IoT constraints like data security and privacy [125]. In IoT, data is exchanged, and content is verified through a centralized authority, raising privacy and security considerations. In sharing data, there is incorrect verification, reduced dependability, and gadget spoofing. Blockchain innovation has been portrayed as an IoT component to address privacy and security challenges, with no mention of a centralized server. Blockchain is a technology that allows for the capture and archiving of interactions. It is not centrally administered and has remained unchanged over time. The peer-to-peer transactional information is saved and disseminated in a public blockchain comprises of interconnected transaction blocks. Blockchain keeps data in the same way that a database does. However, it differs because it does not use the centralized control system [125]. The lack of a regulating institution occurs in the same way that a legislature or a bank does, in that a system of nodes, such as personal computers is used to locate data. Manifestly, this data is widely available; yet, its accessibility is limited, ensuring safety. In this context, blockchain is viewed as a distributed system with cryptographically enabled capabilities for data security and a decentralized information block structure with intrinsic capacity that provides secure and real-time data. Intruders believe it is challenging to gain access to data in IoT systems because they are protected by a sophisticated encryption protocol [126]. Furthermore, even when the system is filled, blockchain drastically reduces all breakdown points' potential.

A situation based on the blockchain-enabled IoT strategy has been developed to establish security and privacy of power exchange in networked MicroGrids [127]. The apprehensions of renewable power supplies and hourly energy demands were modeled using a contemporary randomized situation based on the uncompressed transformation. Compared to conventional techniques, the proposed protocol could improve network confidentiality, reliability, and transparency. How blockchain technology could help assure the IoT-enabled mini solar converters'

connectivity and data protection was also looked into [128]. The blockchain can improve data protection and connectivity in IoT-enabled photovoltaic panels [127]. However, there are several drawbacks with the current blockchain systems: the blockchain ledger grows in size, there is a delay for real-time data exchange, decreased connectivity difficulty and increased scalability, and the private keys have limited unpredictability.

The use of blockchain and smart contracts in conjunction with IoT sensors in commercial supply chain management and efficiency is the most researched strategy. Legitimate use-cases has been investigated in which blockchain and IoT devices were used to track raw materials, chemicals, and components in supply chains in the food, pharmaceuticals, and other sectors [50]. They point out that, despite some regulatory and technological limitations, the universality and adaptability of blockchain can improve supply chain integrity and administration through real-time transportation and coordination.

A further approach concentrated on addressing the privacy and robustness problems originated from using centralized identity management systems is described in [129]. The authors affirm the need for providing an automated authentication systems for IoT applications where scalability is needed and where device heterogeneity and mobility are frequent. To address such challenges, the researchers present an IoT smart home system that is blockchain-based that automatically extracts appliance signatures to identify both the appliances and their users.

Secured blockchain-based network congestion adjustment has been presented with edge processing to facilitate IoT and training [130]. Their study addressed traffic congestion by proposing a structure for location information, identifiable evidence, and verification, as well as reinforcement training for traffic congestion forecasting and anticipation. They pushed innovations to an edge computing phase using IoT and safe transactions using hyper ledger fabric blockchain due to the need for an appropriate framework [130]. In the suggested scheme, blockchain stepped in as a protection standard. Protection norms, which are necessary for large-scale implementation, are not included in the local kind of IoT. The key motive for blockchain's inclusion in their architecture design is to ensure the confidentiality of communications and consistent access management. Their mission is to reduce traffic congestion on heavily con-

gested routes and enhance the overall metropolitan traffic system without investing heavily in new communication infrastructure and city planning. The gathered experiment findings indicate that the platform's ability to discern difficulties into a more straightforward instance and proceed with projections near the actual world is limited [130]. After that, the assumptions are used as the starting point for the modeling approach and interpretation.

Blockchain provides flexible, adaptive structures and can collaborate with centers in a secure, traceable manner. A situational analysis was offered on leveraging IoT in conjunction with blockchain and big data to improve health care [131]. They could obtain varied patient data from multiple IoT nodes while also doing continuous patient monitoring and storing information more securely by merging IoT with blockchain. Because blockchain technology now lacks database qualities, the data might be stored effectively using massive information equipment or recently constructed equipment. In this approach, blockchain can save money and improve coordination across health foundations that use blockchain and prevent attackers from altering or deleting sensitive patient data [131].

Further researchs has looked into the usage of blockchain's distributed system capabilities [132]. One of the causes for blockchain's rapid increase in recent years is its distributed computing ability [133]. Many applications are built on the blockchain's capabilities, including image capture [134] and online taxi ordering systems [133]. Both writers stress the necessity of protecting the privacy and security of users' data in such services. In their image enhancement techniques, Blockchain structure was utilized to sustain data protection [134], while another research paper, in their online taxi booking system, not only uses the decentralized assets of blockchain but also integrates a perpetual perceived loudness framework in blockchain to establish personal data confidentiality [133].

Challenges to blockchain implementation in the supply chain has been investigated and identified [135]. How IoT can help improve supply chains has been looked at by providing data for data analytics and simulation [136]. How IoT can help with operational coordination and real-time logistics was also addressed [137].

IoT and blockchain principles can improve supply chain management in services, including transmission and monitoring. One example of IoT technology and blockchain implementation is intelligent homes and smart cities, where a framework for providing reliable resources management of services for all smart city residents was presented [138]. Residents of intelligent cities can more easily track and manage resource utilization securely and reliably.

Another option to use blockchain is to supplement IoT solutions to improve its sustainability and administration. In terms of control and implementation, IoT systems are comparable to wireless networks. Still, there are some significant differences following the IoT systems' simple structure and long-term performance with scarce resources. IoT systems bandwidth is typically limited, and such gadgets may not be available on the internet all of the time to preserve the available resources. Data integrity and security were identified as two major IoT concerns that can be addressed with implementing a blockchain [51]. PatchTransporter is one way to disseminate software upgrades in an IoT setting using blockchain technology. Patches are exchanged between IoT nodes in a peer-to-peer approach. Blockchain-centered smart contracts are utilized to validate the conveyance of accurate fixes and give incentives in the transaction [51]. Self-interested gadgets may be enticed to engage in the transmission of updates to other systems.

A suggestion of a phase structure was proposed following IoT systems and blockchain to stimulate diabetic follow-up and motivate patients to properly self-manage their condition [139]. Their engineering combined IoT and blockchain technology to collect patient files and communicate them among healthcare departments constantly and securely while maintaining patient privacy. As a result, the patients can ensure that their health data is collected frequently and regularly. The researchers focused on patient safety and the confidentiality of the client's devices to defend against harmful devices [139]. The authors used proof of power as a consensus procedure for a faster architecture that was affordable in terms of vigor and time.

Using blockchain-centered smart contracts was also advocated to facilitate secured inspection and management of medical devices to manage the secured health data provided by IoT systems [140]. Utilising a private blockchain infrastructure centered on the smart contracts, re-

searchers formulated a system in which the monitors can transmit data with smart devices that makes smart contracts and data documentation of all events on the blockchain platform. The aforementioned intellectual contract framework will aid continuous medical observations and healthcare measures by notifying clients and healthcare practitioners and maintain a secured documentation of individuals initiating such procedures [140]. The smart contract framework would address many security flaws linked to remote client observation while automating notifications to all parties engaged in a health provision and accountability in a compliant manner.

On the other side, an investigation was held containing the use of a blockchain to examine massive volumes of healthcare data and provide protected monitoring [141]. The previously reported challenges was examined using blockchain innovation and IoT systems [141]. They suggested a novel set of altered blockchain infrastructures appropriate for IoT gadgets relying on the dispersed structure and other system safety and defense aspects. The model's extra safety and defense measures rely on cutting-edge cryptographic techniques [141]. Over a blockchain-dependent network, the configurations have rendered IoT application data and interactions exceedingly safe and cryptic.

A development of a minimalist but extensible blockchain with tiers tailored to IoT requirements has been presented [142]. They looked into using a minimalist but extensible blockchain in an innovative home environment as a delegate architecture for larger IoT systems. Low-cost devices in an intelligent household benefit from a centralized administrator who sets up public keys for interaction and processes for all incoming and outgoing requests. Lightweight, scalable blockchain achieves decentralization by forming an overlaying structure in which high-value devices interact with an open blockchain that ensures security and anonymity from start to end [142]. To reduce overhead expenses, the overlaying is made up of a distinct cluster - head, and the cluster representatives are in charge of dealing with the open blockchain. Lightweight, scalable blockchain combines a few improvements, including computations for the lightweight agreement, allotted trust, and boards. Objective claims show that a Lightweight, scalable blockchain is adaptable to various security threats [142]. Compared to significant benchmarks, extensive reenactments reveal that lightweight, scalable blockchain reduces bundling overhead

and delay while increasing blockchain flexibility.

To separate IoT projects' security weaknesses of smartphones, researchers employed a variety of intelligent audio management and intelligent home robotics in the industry, as well as third party attacks including smart mining and data parcel grabbing [143]. Furthermore, a suggested framework was displayed for dealing with security challenges by analyzing security threats using real-life examples [143]. The framework intergrataes the existing safety threats in mobile IoT provisions and recommends a secured and divulged infrastructure of mobile IoT connectivity security framework centered on blockchain innovation to secure the said issue by depicting the massive system security risks experienced by mobile IoT following new circumstances.

Another recommendation was presented for utilizing Ethereum blockchain to tackle a prototype smart house application case situation to improve IoT security [144]. The researchers seek to combine Ethereum-based blockchain with IoT nodes to secure their protection and secrecy. Finally, their proposed idea, an Ethereum-based blockchain with IoT system combination, is still in its early stages. Further, companies' utilization was increasingly widespread than the initial stages of blockchain-based IoT advancement [144]. Ethereum blockchain is a general category and smart contracts-based cryptocurrency that can be used to improve IoT security.

The safety, confidentiality, and trustworthiness issues associated with contractually renting and leasing IoT devices-enabled homes were investigated by [145]. They recommended using blockchain-based smart contracts to eliminate the threat of confidentiality, safety, and trustworthiness from IoT-enabled monitoring gadgets within smart homes. In an intelligent home-sharing system, researchers concentrated on minimizing threats from interior monitoring Internet protocol webcams. The smart contracts improved the localization of the home-sharing system in the above technique. The researchers recommended process allows users to maintain control over the interactions and data transmission. Implementing unique hardware authentication ensures data transfer and secure transactions [146]. Additionally, it can save IoT security by facilitating encryption key modification using smart contracts.

On the other hand, an excellent lightweight, integrated blockchain architecture was created to fulfill IoT requirements [147]. The developed framework is used as an initial structure in a smart home setting to demonstrate its usability in various IoT environments. A centralized administrator, who created a public key to transfer information and all input and output requests, benefits the resource-constrained assets in home automation. The efficient, lightweight, integrated blockchain approach provided here created a network infrastructure that highly connects assets to a public blockchain that identifies dedicated safety and confidentiality [147]. A lightweight consensual method, certificate-less encryption, and a decentralized bandwidth management system are among the three improvements worked out in the proposed efficient, lightweight, integrated blockchain model. A prototype was run under several circumstances in terms of computational time, power consumption, and overhead [147]. Compared to the traditional technique, the efficient, lightweight, integrated blockchain achieved a 50% reduction in computation duration while using 0.07 mJ of electricity.

In comparison to the rapid expansion of IoT terminal accessibility, advancements in admission verification has been examined [148]. The improvements in admission verification are currently available. Researchers suggest using the blockchain to fingerprint the stations' distinguishing proof data, boosting IoT terminal cybersecurity when connecting to the cloud. In addition, the researchers presented a method for storing the endpoint fingerprint blockchain in an IoT terminal. After that, they suggested checking the obtained fingerprint data against the details in the blockchain to ensure the distinctive fingerprint data's veracity.

User protocol was also built and a security prototype for an IoT device based on blockchain technology that streamlines the data incursion and hacking procedures and constructs a multi-security blockchain framework between the IoT device and the customer device [149]. By developing a new approach, researchers addressed the cybersecurity risks faced by IoT system advantages [148]. Researchers specifically outlined a few initiatives to improve a multi-security certification methodology for IoT security that relies on blockchain technology.

A recommended structure was proposed based on enhanced safety in electronic-voting applications using IoT devices [150]. The user would create a file with proper verification per-

formed using voter identification other biometric approaches on a computing device. An inspector would authorize each transaction made with the file, which would be a vote [150]. The suggested blockchain equipment for digital voting with IoT devices is once again certified and tested using a set of variables, including response time, resource usage, and demands addressed.

An architecture was presented for gaining control in the IoT centered on blockchain innovation [28]. The researchers' initial obligation entails providing a standard model for the recommended system within the locations, modeling, architecture, and instrumentation specific to the Internet of Things. Furthermore, researchers established Fair Access, a distributed pseudonymous and protection authorization board platform enabling users to own and govern their data. Fair Access, unlike revenue-based Bitcoin exchanges, offers new types of interactions that can be used to allow for, receive, sponsor, and so forth [28]. Researchers created an underpinning execution with a Raspberry PI gadget and a local blockchain as a working prototype. Also, researchers adopted and altered the blockchain into a distributed access authorization system to make the prototype a reality.

For IoT networks, a data security architecture was presented [151]. The configuration is based on applying blockchain innovation to IoT systems to provide distributed gadget verification. Data security guarantees that resource constraints on IoT devices and the heterogeneous nature of IoT networks are considered, allowing fundamental virtual servers of blockchain extraction to be organized [151]. A prototype based on the suggested architecture demonstrates the model's ability and assurance to provide data security in the IoT system.

A blockchain-based IoT security architecture has been demonstrated [152], IoT network. Researchers demonstrated how the three-level architecture achieves proof of identity, access control, safety assurance, the lightweight component, provincial center adaptability to non-essential failures, disruption of service flexibility, and capacity dependability at that time [152]. Researchers demonstrated that IoT network bandwidth is sufficiently low for a certified implementation at that moment.

Another blockchain-based IoT security protocol was developed in which trustworthiness is established due to blockchain's changeless and distributed characteristics [153]. The blockchain

concept is delivered to make the structure increasingly intense and highly resilient to a single source of failure. Researchers developed a feature that would provide continuous protection in the architecture by regularly evaluating customers' actual proximity in a large IoT-Zone without the need for customer arbitration [153]. Every user cooperation in an IoT ecosystem is saved as an interchange in blockchain, and the order in which such interactions are stored refers to a customer's IoT history. For a customer partnership to be successful, an amazing automated crypto-token is essential. The certificate is used as an entry control element to prevent unauthorized access to the system. Tokens are pre-developed in the blockchain based on an anticipation system based on the customer's IoT history [153]. They created the blueprint more reliable, robust, and coherent by using blockchain as a core framework in IoT conditions and employing a strategic plan for long-term protection.

Additionally, a blockchain-based security solution was suggested for IoT with an outskirt toggle collecting sensor data and sending it to the blockchain [154]. Sophisticated encryption protocols encapsulate the IoT application's communication. The access control devices are made using smart contracts [154]. Finally, a theoretical analysis revealed that the suggested framework might protect against different threats as well as minimal passivity.

When developing and evaluating SPAINChain, safety, prevention, contextual insights, and the use of blockchain has been looked at as a defense for IoT, notably, security and incorporating knowledge in the framework of IoT and blockchain [155]. It has been demonstrated that IoT-blockchain mapping is possible. Following the mapping concept, finding the perfect blockchain-to-IoT connection, in which device T is paired with blockchain B, is possible. As a result, we're shifting from the architecture to polarities of B lattice and T grid. The configuration for each blockchain is determined by the preceding, and the configuration for all IoT devices is determined by the last [155].

For ensuring that IoT devices communicate, a suggestion for a decentralized and distributed communication protocol was presented [156]. The protocol is based on blockchain technology, which has been tweaked to meet the IoT's requirements. The authors depicted how blockchain technology could be revamped to meet this demand and a model simulation. They showed that

using blockchain for IoT device communication at the plan level is feasible and encouraging. The results of these tests would show whether or not the network is beneficial and the extent to which it is used (count of devices, distance traveled by devices, amount of data) [156]. The recommended standard would be presented as an interaction that would allow products to be easily used on mobile devices. If innumerable devices did not operate, they would be of little importance in today's world.

Furthermore, another research gave a point-by-point synthesis of how blockchain IoT functions [126]. They also highlighted the importance of securing an IoT - based system and presented an analysis of blockchain and other protection tactics in terms of power, setup cost, risk of failure, among others, and offered a comprehensive cybersecurity approach that could be used for IoT systems. They concluded that blockchain is the most logical option for IoT security based on their extensive discussion and investigation. They also compared traditional cybersecurity to blockchain protection, discovering that blockchain is more adaptive than conventional security [126]. The report primarily focused on three different blockchain IoT systems.

The impact of the system's load variation on blockchain execution and security was explored by [157]. They initially presented a Markov fastening model to capture the performance of the directed acyclic graph agreement process in distinctive load circumstances, taking into account the fragile system load. The suggested technique broke out the essential execution measures, such as cumulative weights and affirmations delay. They then use a stochastic approach to disintegrate the chances of a successful two-fold expenditure attack in distinct system load levels [157]. The results can provide an in-depth understanding of the directed acyclic graph agreement process, such as how system load affects the affirmation latency and the possibility of substantial cyber-attacks.

There is a lack of transparency in how user data is exchanged among third-party systems due to expert consolidation in managing information generated by IoT devices. IoT devices such as intelligent webcams, health well-being monitoring devices like pulse monitors, and glucose level monitors, for example, can reveal security data on users. Such gadgets collect and send security-related data by providing them with computing and communication capabil-

ities [158]. Due to the limited management capacities of IoT devices, they frequently force remotely operated third-party systems specialized in performing further data preparation. Customers are compelled to disclose in expert firms to allow data security and provide data security by communicating sensitive customer data to exterior administrative vendors [158]. The little flexibility given to specialized third parties is based on collaborative programming, which necessitates trust in an external architecture as a central authority to supervise client data.

An investigation of different models was conducted to design and deliver evaluation [159]. Initially, an IoT security paradigm based on blockchain and the Entomb Planetary Document Framework was developed. Many potential threats associated with traditional IoT architectures may be avoided in this architecture, and framework performance is vastly enhanced in terms of distributed massive limit accumulating simultaneity and inquiries. Average passivity and capacity were used to evaluate the proposed model's presentation, which is essential for further studying and enhancing this component [159]. The blockchain-based security paradigm was found to be adequate after examination and testing.

Multi-signature was used to guarantee data reusability and filtered via two hubs with the highest hub rating from dynamic hub's impending hubs to do two-thirds multi-signature, saving resources [160]. The above technique used Rivest Shamir Adleman to encode and mark the data transmitted, allowing recipients to double-check the data. The blockchain provides for secure data transmission. Effective propagation is demonstrated by beneficial approbation [160]. Tests revealed that the recommended approach could successfully distinguish between active and inactive hubs, increasing the difficulty of intruders' attacks while ensuring the security and safety of IoT hubs and data.

For IoT data storage and accessibility, a development of a three-layer blockchain-based creditable architecture was introduced [161]. Users, tasks, acquiesces, information items, and their linkages were all formally recognized in the platform. The definitions were used to develop smart contracts that use the job-based authorization architecture. A prototype element is also planned to collect IoT data organized by data entry and store it in documentation in the Between Planetary Record Framework. For attainability validation and performance evaluation of the

recommended network, researchers constructed an elegant chain model based on Ethereum and InterPlanetary File System (IPFS). Not only does the platform assure data trustworthiness when storing IoT data, but it also secures data privacy when the data is used [161]. Furthermore, restoration findings revealed that the conceptual model exhibits superior presentations in terms of time, space, and gas usage.

A lightweight security structure has been suggested for IoT data exchange based on blockchain technology [162]. The solution used a two-chain approach to consolidate data blockchain and interchange blockchain: circulating capability and protected data in the communication blockchain, and enhanced instrumental consensus computation using the enhanced Viable Byzantine Flaw Lenient [162]. The efficiency of data enrolment; resource and data transfers in the interchange through enhanced computations based on incomplete visual impairment marking computations, blockchain has improved interchange performance and protection coverage. A novel game method for hub cooperation has been presented to prevent the malignant behavior of neighborhood robustness. The mysterious hub situation is examined by examining the hub's organizational renown value; the high-trust reference record is used to resolve the malicious hub's heaviness in the overall discussion, and hub merging leads to Bayesian equilibrium. The reenact test office confirmed the counter cyberattack capability, dual thread preparation power, and delay [162]. The results showed that the architecture is secured, practical, and reachable and that it is possible to examine the application's location information for reliable capability devices.

To secure the individual data of IoT users, a blockchain-based approach was presented that supports general information insurance guidelines [163]. Such tasks promoted the analysis of available information insurance guideline regulations to appear as opcodes in smart contracts, in addition to their essential genuine queries. A few prepared instances were also presented to demonstrate how the ability of data security with the help of blockchain and a general information insurance policy may be incorporated into the company operations of IoT devices during application layer protocol [163]. The proposals were delivered to the Ropsten test organization. The findings revealed a direct link between the several tasks completed on near-home

data and the expense incurred on activity validation following general information insurance guideline regulations [163]. Regardless, the extraction period was devoid of the diverse nature of suggested smart contracts.

An alternative concept to the traditionally included paradigm was offered for gaining control and IoT data by incorporating smart contracts to provide a trust-free data-sharing element with no requirement for intermediaries [164]. The data owners in the suggested technique have complete control over their data. Furthermore, blockchain's distributed nature facilitates administrative access. Using the focus points of Ethereum blockchain's presently private and public key pools in imbalanced cryptography ensures data security and truthfulness while keeping a strategic distance from a man-in-the-middle attack [164].

In a service-based IoT, an approach was suggested for modeling reliability [165]. In particular, methodologies for evaluating performance in a centralized heterogeneous IoT service infrastructure were presented by [165]. The authors recommended that the presence of the software to run the service, the accessibility of inputs needed for the service to perform, and the service dependability of components linked with the network could all be evaluated. The programs were tested on a real-world fire alarm system. The systems could detect whether the software and document for each element in the IoT environment were accessible. On the other hand, the approach does not account for the possibility that IoT devices might malfunction at any time and start delivering erroneous data or that the networking could be infected with a virus or other threats [165]. It is vital to have a system that can inform the user of system problems before critical control systems represent consistency.

Approximately 90% of the data on the planet currently was generated in only the last two years (IBM, 2017). Because of

1. The Internet of Things (IoT).

2. Population expansion, the rate of growth will accelerate (Stats, 2017).

Whereas the growing potential of blockchain and IoT innovations are now immense, the symbiotic interaction between these two disciplines opens up many more opportunities. For example, decentralized wireless sensors, one of the foundations of technical and human growth despite

their flaws [166], show how blockchain infrastructure might improve IoT by minimizing its flaws and maximizing its promise.

The distributed ledger and its intrinsic characteristics are primarily driving the increased attention and expenditures for building distributed IoT systems [56] [25]. The central concept is to allow secure and traceability data sharing in diverse situationally situations with a large number of networked digital sensors [167]. Furthermore, the platform's great resilience and effective operation are enabled by functioning in an autonomous and decentralized manner [168].

Compatibility on the blockchain allows for autonomous and secured real-time payment processing, which can be used to improve conventional commercial activity, e-commerce, and formal and informal transport networks. There are various programs that combine these features, like Filecoin, a computer memory vendor, and EtherAPIs [167], that allows API calls to be monetized. As such, IoT systems could be connected with cryptocurrency-based financial institution to enable micropayments in return for financial services [25], and similar ideas can be extended to the smart-grid sector to facilitate energy sales.

Decentralized sensor networks in provenance and supply chains automate merchandise assessment in a variety of scenarios, like food supply chains, transit systems, or inventory control [169]. The data obtained by IoT devices can be timestamped as exchanges on blockchain systems. The use of blockchain-based IoT innovations can address a number of concerns, including the high costs of traditional techniques [170]. Furthermore, a decentralized and secure P2P approach can improve the security of IoT systems [171], allowing for greater management of IoT systems.

Without a doubt, some limitations, like IoT devices' low processing and storage capacities, can limit the adoption of Blockchain technologies. An alternate method was presented for implementing a decentralized ledger that overcomes such disadvantages while also improving IoT solutions [172]. Other effective layouts are provided in [142], in which the researchers offer a safe lightweight blockchain-based infrastructure for IoT in various application scenarios.

Generally, a correctly configured and centralization infrastructure in IoT systems results in higher transactions than blockchain alternatives. The issue is worsened in the context of large systems [173], because resolution processes in public blockchain architectures are expensive. To get around this constraint, the Ethereum ecosystem is contemplating to divide the blockchain into parts and retains each structure's own state and transactions record. Nodes process interactions for individual fragments in this fashion, and the blockchain is split into sub chunks, dramatically improving system performance.

2.5 Gap Analysis

Based on our findings from this chapter, we concluded the following:

1. The major issue other researchers encountered regarding IoT devices is the storage constraint. This is due to IoT devices being lightweight and idle for carrying and traveling around with.

2. Handheld devices are insecure and are susceptible to many types of cyber attacks including DDoS attacks which are very common with IoT devices.

3. Blockchain technology provides a structure of data with built-in security qualities. It is based on decentralization, consensus, and cryptography principles, which ensure tamper proof and trust within its transactions.

The advantage of these findings is that they complement our research questions and were the reason behind our motivation to proceed with this investigation for using blockchain to manage IoT devices using an off-chain storage principle. While the disadvantage is that this principle has been mentioned multiple times by other authors, but it was never implemented or even tested. Which means there are no other platform to benchmark our results against.

2.6 Chapter Summary

IoT devices are easy targets and susceptible to many cyber attacks. This is due to their insecure network services, lack of device management, insecure Data transfer and storage, and many more. many of these vaulnarabilities could be solved by introducing blockchain technology to IoT devices. The advantage this technology has to further advance the IoT field is of blockchain being secure and all data transferred through it is tamper proof.

A common issue that many researchers have brought up regarding IoT devices is its storage limitation. Blockchain stores the complete history ledger which increases in size with each new entry. A solution to solve this issue by implementing blockchain in IoT has been proposed but not focusing on the storage constraint issue. An off-chain storage blockchain solution for managing IoT devices has never been implemented which was the base of the motivation behind this research.

Chapter 3

A Blockchain Platform for Managing IoT Devices

3.1 Introduction

A blockchain node must store the entire history of the blockchain. This concept affects the block's speed and time of transactions negatively and limits IoT devices from joining the network particularly when the history becomes larger. For that we have constructed a blockchain platform using Ethereum.

Ethereum is an open programmable Blockchain platform [174]. The platform is an open-source program not owned or controlled by a single entity with smart contract functionality and is powered by the peers who run the Ethereum nodes. Everyone is eligible to sign up for the platform and create an Ethereum account. Users can create and deploy smart contracts to the platform and build decentralized applications which is why we have decided to use this platform for building our blockchain.

In this chapter we introduce our own novel blockchain platform using an off-chain storage solution to manage IoT devices. We present our system structure and explain all modules constructed within our platform, system simulation including simulation script and simulation results, ending with a chapter summary.

Within the platform, we created a smart contract and managed our blockchain. We then connected some nodes (IoT devices) to it and connected it to an external database (Cloud) using Amazon Web Services (AWS) for both to remove the history load of the blockchain.

For our nodes (IoT Devices), we used Amazon Web Services. AWS represents through virtualization, a large set of computing resources, such as storing and processing capacities can be split, assigned, and dynamically sized to satisfy customers' demand. Customers are represented by companies aiming at offering their services without carrying on costs and risks of building and managing their own hardware and infrastructure [175].

3.2 System Structure

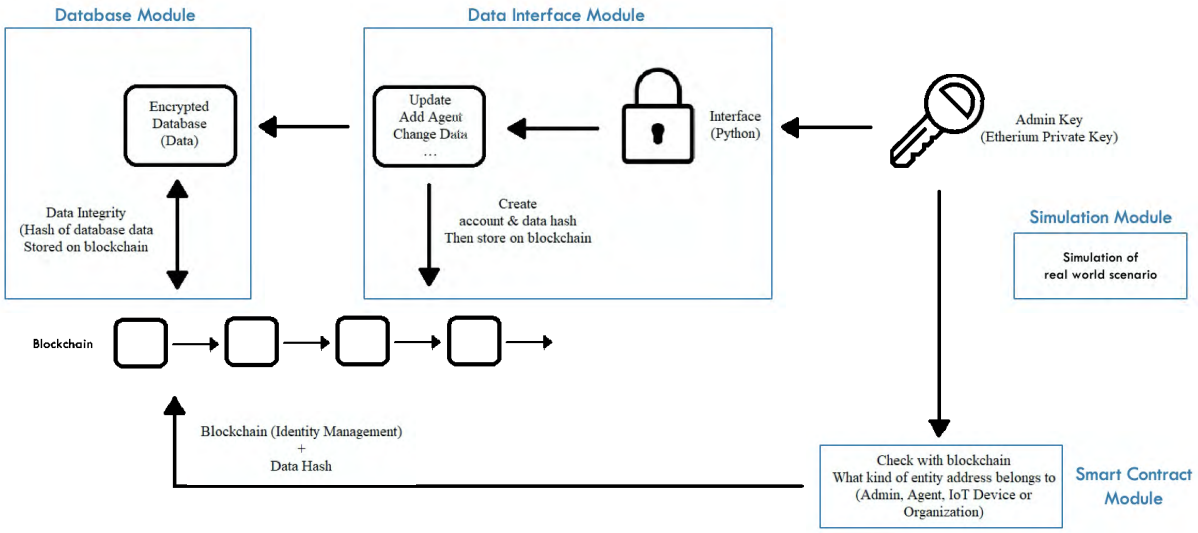


Figure 3.1: System Structures.

As shown in Figure 3.1, the proposed system comprises of four different modules represented and labeled within the blue borders of the structure. These modules are defined as Smart Contract module, Database module, Data Interface module and Simulation module. The following sections characterise each of the four modules.

3.2.1 Smart Contract Module

The Smart Contract Module defines the identity of the entities interacting within the system. It is written using the Solidity language, for the Ethereum network and defines the identity

and access rights side of this project. This contract defines the entity base-structure and three separate entities - Agent, Organization and Device. Entities interact with each other, by reading and writing data to and from one another. Entities have a tier-based levelling system, meaning that the higher their tier, the more access they have starting from tier 1 up to tier 4.

- *Entity*: An entity holds information about itself, like it's unique ID (address), tier (level within an organization), it's creator ID and it's data Hash (will talk more about it in the database and interface sections. It also contains info about other agents, like who has access to its data and what kind of access rights they have.

- *Agent (Individual)*: An agent can be simply understood as an individual. The agent's tier gives it it's status. Under any given scenario, different individuals will have different statuses.

- *Organization (Group)*: An organization is simply an entity under which a group of agents operate. A hospital as (Tier 0) might be one; or a police station. Higher-tiered organisations are entities under which both agents and lower-tiered organisations operate - such as a ministry.

- *IoT Devices*: The purpose of a device is to collect information about an agent (For example, collecting vitals of patients in a hospital setting), an organization (For example, checking the air quality in a city or factory) or any other attributes that are related to the system.

3.2.2 Database Module

The Database Module holds the data of the entities. It is a json (nosql) database using AWS which handles the data part of this project. This contains details about each agent, organization and device. Each entity has access to its own data. If one entity wants to access another entity's data, the blockchain is checked through the smart contract to see whether the accessing entity has that permission or not. The data repository is a database that can be hosted on a server, or on a local machine, and copies of only its hash are shared on all the nodes. It holds each entity's information, it's history, it's relation to other entities and its access rights.

The database is connected to the smart contract through the third module, the interface. It differs from a traditional blockchain structure in not having it within the blockchain itself but being hosted elsewhere. Data integrity of each individual entity is maintained by saving the hash of the database entries within the blockchain (data Hash field inside the Entity structure). The blockchain allows either the contract owner (the administrator who initialized this system) or the entity itself to save that data Hash, by calling a function on the smart contract which can only be called using their accounts.

3.2.3 Data Interface Module

The Data Interface Module connects the smart contract to the database and enables the secure interaction between the two and a simulation script which tests the speed and security of the entire system. Written in python, using web3.py and handles the logic part of this system. The interactions between the smart contract and the data happens through this module, such as instantiation of new entities, changing tier levels, changing access rights or changing the data in any way. When an entity tries to change the database through the interface, first the blockchain will be consulted to check whether that entity has that permission or not. Once they do, the new database hash is saved. If an entity changes the database outside of the interface, we will know that has happened and where the data was changed, and the new data won't be valid. Each read and write operation by an entity to the database module generates a new hash such that once that entity's permission/authorization level is confirmed in the blockchain, then the hash is saved as a valid entry in the database else the hash is deemed invalid.

Figure 3.2 presents the flowchart of our system. When a user inputs new data or requests to change data through an IoT device, its access rights get verified through the smart contract. After that the data is sent to the database for validating the tier level. The data can be changed only when the blockchain validates it, otherwise the request gets rejected. When the validation process is successfully completed, a copy of the data hash is saved on the blockchain and gets sent back with the new data hash through the flowchart process as a new data.

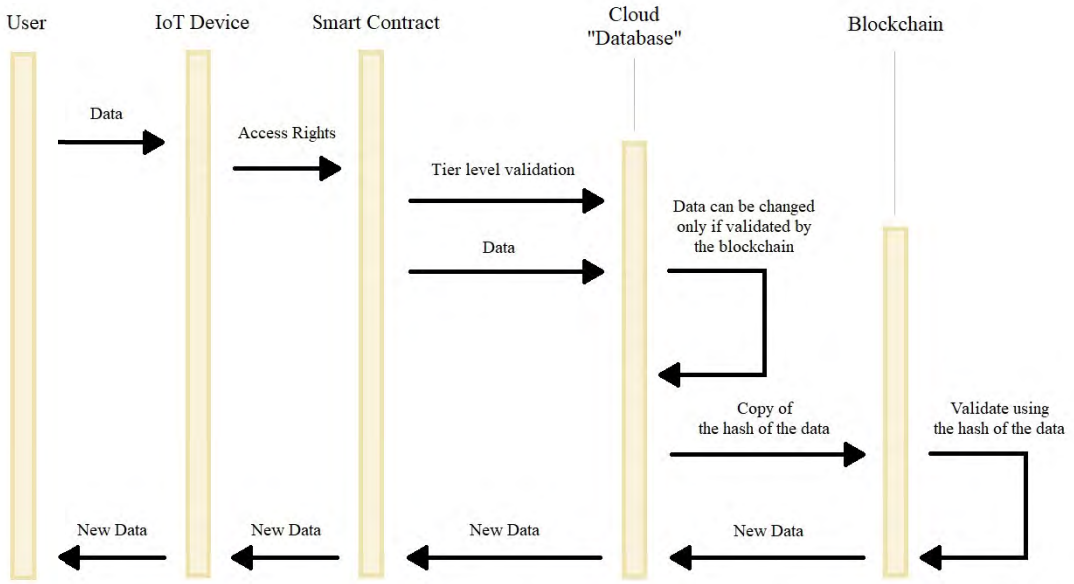


Figure 3.2: System Flowchart.

3.2.4 Simulation Module

The Simulation Module defines the simulation of a potential real-world scenario which uses our system. This module is a script written in Python, which connects to the Ethereum node which runs on the local machine and defines the simulation of a potential real-world scenario which uses our system. This determines the number of entities that exist in the simulation, how often they interact with each other and it also tests the speed at which the system runs. Parameters such as the read and write time of information from the data will be tested, or the changing of access rights of entities, which will require the use of blockchain. Since we are using cloud computing, we used wifi connection to control our virtual machines.

In order to properly simulate the speed of the system, we also need to create a private blockchain which will remove the variables affecting the transaction speed on a public network, allowing us to run a more accurate simulation. Therefore, we created a 'Genesis' file shown in the following algorithm 1 which defines certain characteristics of the blockchain, such as block speed, certain protocol implementations and whether there are any addresses with pre-allocated funds.

- *First Node*: First, we initialised the private blockchain on one of our personal computers and ran the Geth software on it, making it the first node on our blockchain. Then, we copied this node's enodeID.

- *Subsequent Nodes*: Next, we instantiated multiple AWS servers to create other nodes. Once a server was created, we installed all prerequisites, we then initialized the blockchain locally (using the same parameters as the first node) and ran the Geth node software. Then, in order to connect to the initial node we used the same enodeID.

Algorithm 1 Genesis File (specifying the settings for the network and the contents of the initial block in the blockchain)

```
”config”:
”chainId”: 13373,
”homesteadBlock”:0,
”eip150Block”:0,
”eip155Block”:10,
”eip158Block”:10,
”eip160Block”:10

”nonce”: ”0x0000000000000042”,
”alloc”:”0x0000000000000000000000000000000000000001”:

”balance”: ”1”
”0x0000000000000000000000000000000000000002”:
”balance”: ”1”
”0x0000000000000000000000000000000000000003”:
”balance”: ”1”
”0x0000000000000000000000000000000000000004”:
”balance”: ”1”

”timestamp”: ”0x00”
”parentHash”:
”0x0000000000000000000000000000000000000000 0000000000000000000000000”,
”extraData”:
”0x3535353535353535353535353535353535353535353535353535353535353535”,
”gasLimit”: ”0x1000000”,
”difficulty”: ”0x10000”,
”mixhash”:
”0x0000000000000000000000000000000000000000 0000000000000000000000000”,
”coinbase”:
”0x0000000000000000000000000000000000000000”
```

3.3 System Simulation

The Simulation was done by running the same script on the 11 different computers in parallel. Ten of the eleven computers were Virtual Personal Computers (VPCs) rented from the AWS cloud provider, which ran on Ubuntu 16.10 with 16GB RAM, 500GB disk space, 24 CPU cores and 2.3GHz processor speed. These specifications were set as they are considered average IoT specifications nowadays and simulation results may slightly change depending on the device specifications used. Later we installed all necessary software to be able to run the simulation on each machine, including Python compiler, Web3.py library, Solidity compiler, Ethereum software and Geth. The 11^{th} computer was a Macbook Running on macOs Mojave, which had the same software installed. And the process was as follows:

3.3.1 Simulation Script

We initialized the private blockchain based on the custom Genesis file, on each of the eleven machines. We, then started the node software (Geth) on each machine and using the enodeID of the first node we connected all the other nodes to it - therefore connecting all the nodes to the same network. We then created a wallet and started mining on every node in order to have some Ether to run the simulation.

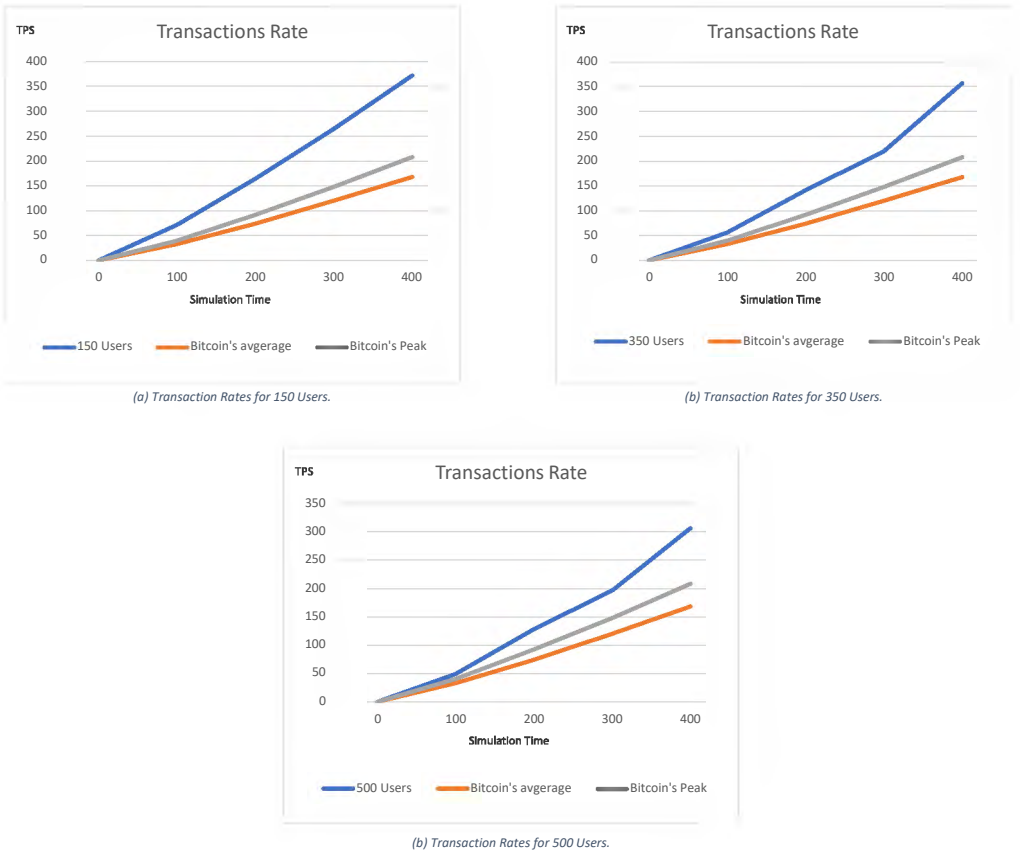
The next step was to run the simulation script. In the initialization phase, the script creates 9 agents and assigns some Ether to each of them and allows certain agents to have access to other agents' data by calling a function in the smart contract.

In the simulation phase, the script loops through the created agents, checking with the smart contract to see which other agents they have access to. If for example Agent 1 has WRITE access to a subset of Agent 2's data, then Agent 1 writes something in the database under Agent 2's data path to which it has access. The write function changes both the database and the blockchain, by changing the data hash entry under Agent 2's object on the smart contract. Since Agent 2's new data has a different hash than the previous one, and since we know it was written there non-maliciously, the program certifies it by writing its data hash on the blockchain, under Agent 2's object. The final phase consists of the script going through all the agents comparing

their database entry's hash with the one written on the blockchain, certifying the validity of the data in the database.

The simulation script described above runs on all of the eleven machines, in parallel, therefore generating a total of 99 agents which actively interact with the blockchain and the database around the same time. We did this to speed and stress test our system, to see what is the transaction throughput and whether any validity issues are detected at the end of the simulation (whereby something that is written in the database is not valid according to the blockchain).

3.3.2 Simulation Results



(a) Transaction Rates for 150 Users.

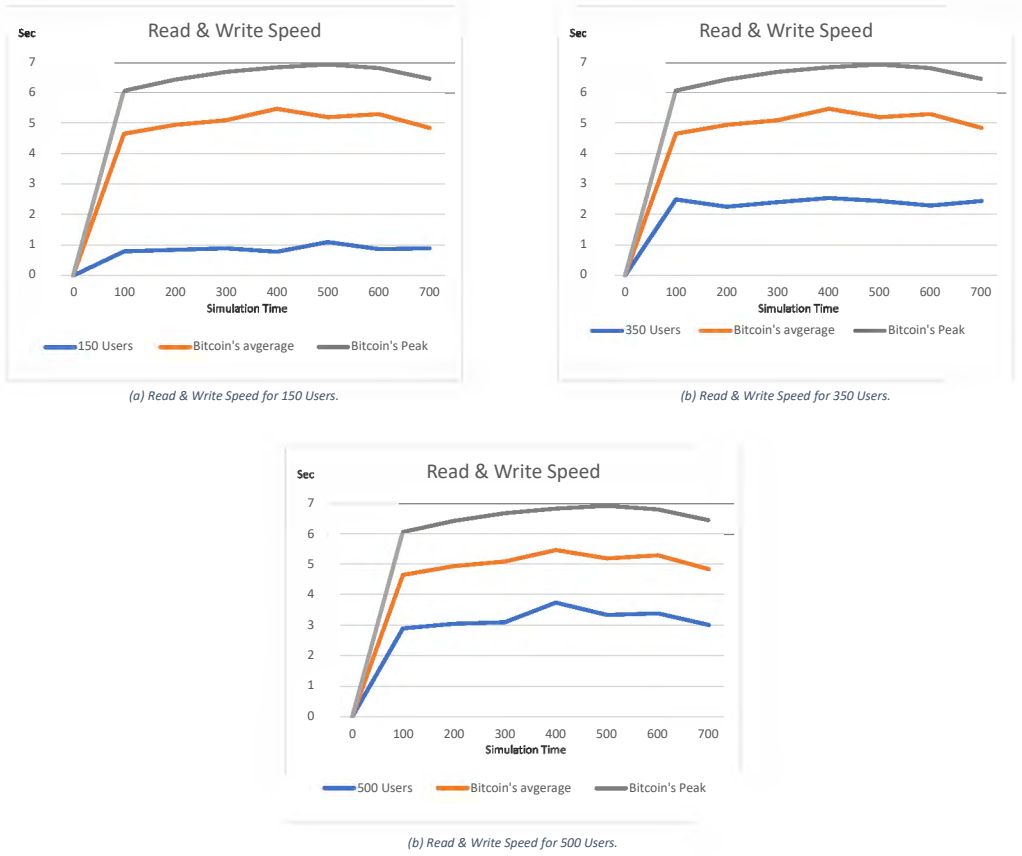
(b) Transaction Rates for 350 Users.

(b) Transaction Rates for 500 Users.

Figure 3.3: Transaction Rates for 150, 350 and 500 Users.

The simulation, as presented in Figure 3.3, ran for 400 seconds for 500 users in the network using 11 VM's, during which the scripts generated an average of 306 transactions each. $306 \times 11 = 3366$ transactions were minted in total over those 400 seconds, or 8.4 transactions

per second. We simulated for 350 and 150 users and achieved an average of 357 and 372 transactions each, generating an average between 9.8 and 10.23 transactions per second. At the end of the simulation, there were no inconsistencies between the database and the blockchain. We then benchmarked our results with Bitcoin's average transaction rate per second (3.8 transactions per second) and with the highest Bitcoin's transaction rate of all time (4.7 transactions per second) [176]. Which was almost half the transaction rate recorded by our proposed module.



(a) Read & Write Speed for 150 Users.

(b) Read & Write Speed for 350 Users.

(b) Read & Write Speed for 500 Users.

Figure 3.4: Read and Write Speed for 150, 350 and 500 Users.

Read and write operations as presented in Figure 3.4, were simulated for 700 seconds with the cloud database and blockchain validation, to check if a specific agent has access to a path within the database. It took an average of 0.9 seconds for 150 users, an average of 2.4 seconds for 350 users and an average of 3.3 seconds for 500 users. Public and private keys were generated in 2.3 seconds when the agent registered with the blockchain for the first time. After that, we benchmarked our results with Bitcoin's average read and write speed (5.06 seconds)

and with the highest Bitcoin's read and write speed of all time (6.71 seconds) [176]. Which was more than double the time recorded by our proposed module.

An observation has been recorded that our obtained results are being affected with the number of users being simulated. But given our simulation outcome, if we increase the number of users to 1000 users, our proposed platform will continue to perform better results than Bitcoin's average and peak records.

3.4 Chapter Summary

Bitcoin is a cryptocurrency which is just a Blockchain use case. However, Bitcoin still remains the most common Blockchain application used up to date [177]. Hence the reason of our benchmark choice in our previous results. And a major reason of our achieved results was based on the Block Propagation Theory which states that the more number of nodes you have, the more time it takes for the block propagation hence less nodes means higher transaction speed.

As blockchain technology represents low costs of usage to users, it still holds high implementation costs for companies, which delays its spread of adoption and implementation. It is also inefficient to have multiple network users validating the same transaction, since only one user is granted the reward derived from this mining process. This process, also involves a massive waste of energy, which makes makes this technology not environmentally friendly [178].

Based on the simulation results presented in this chapter, we conclude that it is more efficient to move the storage away from the blockchain as presented in our proposed platform, especially when using IoT devices due to their small capacity nature. And because the blockchain storage keeps expanding in size with each transaction made similar to how Bitcoin is currently structured. Which will eventually lower the performance and speed by time.

Chapter 4

Security Mechanisms Implemented in the Platform

4.1 Introduction

Blockchain is not immune to hacking, but being decentralized gives the technology a superior line of defense. To alter a chain, an attacker or a criminal would need to gain control of 51% (which more than half) of all the computers in the same distributed ledger. Each new block connects to all the blocks before it in a cryptographic chain in such a way that it's nearly impossible to tamper with. All transactions within the blocks are validated and agreed upon by a consensus mechanism, ensuring that each transaction is true and correct.

This technology is known for its safety and tamper-proof specification that makes it an ideal technology from a security point of view. After designing the system and creating all modules, and after connecting them to each other, we had to increase the security level of the system because we are using an external database (off-chain storage) away from the blockchain itself. We did that by implementing a few extra security mechanism and other cryptographic techniques.

In this chapter we introduce our own cryptographic techniques and algorithms that we proposed to help further secure our platform and test it against an attack for verification purposes.

4.2 Cryptographic Techniques

In blockchain technology, public and private key play an important role in verifying the owner of the transaction. The digital signature is required to sign the transaction from the agent. Digital signature is a function of signature of message and private key. To verify if digital signature is true or false the message, digital signature and private key of the owner will be validated using cryptographic functions, based on the result the transaction will be declared valid or invalid.

Blockchain uses secure hashing algorithm (SHA) which is a 256-bit cryptographic hash function used for digital signature. It will require 2^{256} guesses to get the private key of the agent right. For example, the word goodbye will have a certain bit pattern of 0 and 1's even manipulating a letter will completely change the bit pattern. This is one of the reasons it is almost impossible to be reversed given the time limit to crack the cryptographic puzzle.

4.2.1 Data Encryption

To protect the privacy of all participants involved in a blockchain, both a symmetric or an asymmetric encryption could be used to encrypt data before introducing the data into the blockchain itself as transactions. A possible design for distributing encrypted data among numerous participants is shown in the following Figure 4.1 and discribed as follows.

In the beginning, one of the participants involved generates a secret key for the purpose of data encryption and shares it off-chain during a fundamental key exchange. Neither the key nor its generating seed are suposed to be shared on the blockchain. In the situation where an involved participant has the need to input new data into the blockchain, they have to symmetrically encrypt it first using the secret key. Only after that should the transaction with the encrypted data be submitted to the blockchain. Based on that, only the participating individuals which have access to the secret key have the ability to decrypt the data embedded in the transaction [5].

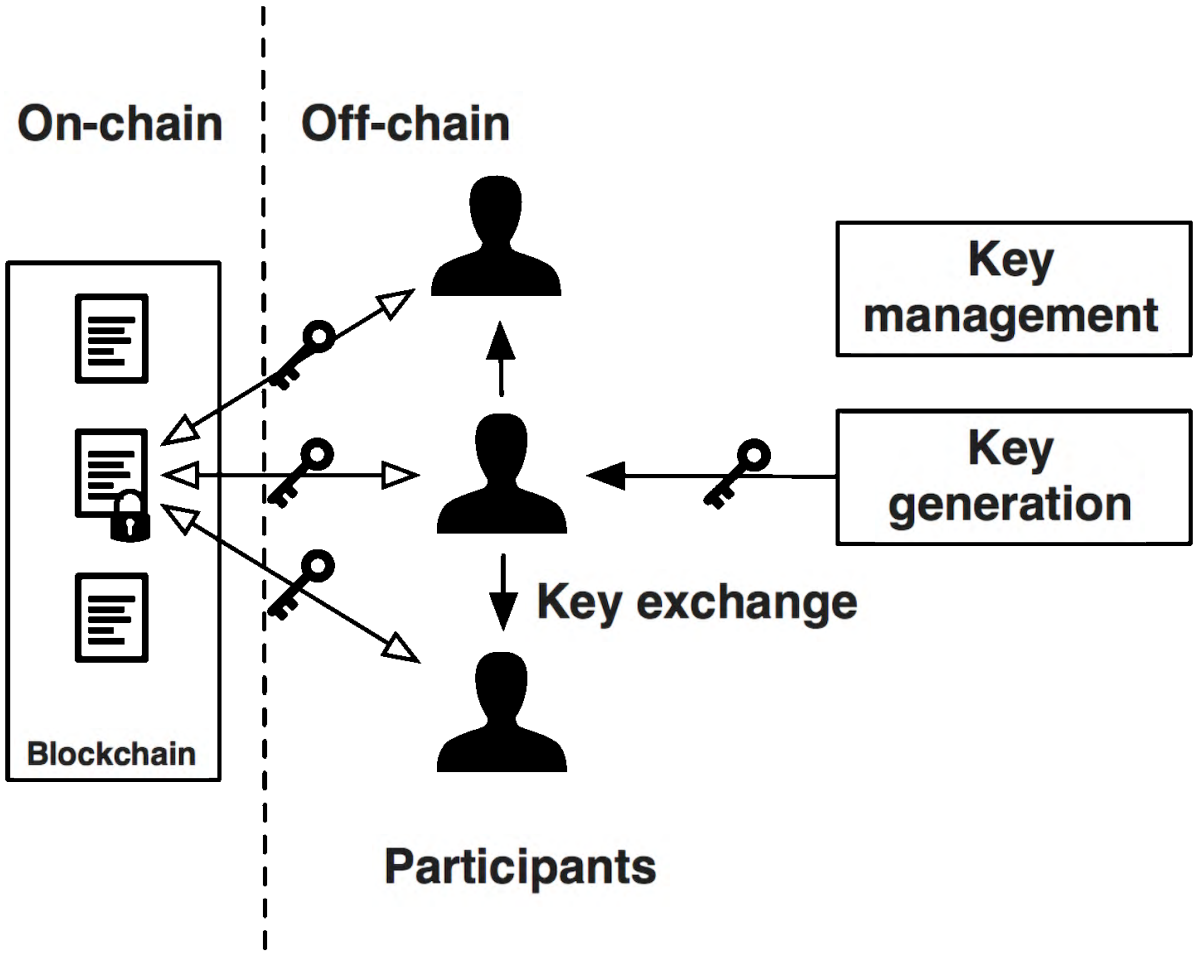


Figure 4.1: Blockchain Data Encryption Pattern. [5]

Algorithm 2 Data Encryption

function **ENCRYPTION** (data)

if user confirm data preservation over blockchain **then**

Generate a symmetric key S_k

$C_t \leftarrow E_s$ (data,S_k)

$C_k \leftarrow E_(as)$ (S_k,$R_(pk)$)

else

Do nothing

end if

end function

In the above algorithm 2, we implemented a similar pattern by using a symmetric key S_k to encrypt the data E_s and produce a cipher text file C_t. After that, we used a public key cryptography to encrypt the symmetric key S_k (double encryption technique). We encrypted the symmetric key S_k by using the receiver's public key $R_(pk)$ and send the cipher text file C_t and denote the encrypted symmetric key $E_(as)$ by using the cipher key C_k.

4.2.2 Data Validation

During the validating process and as shown in the following algorithm 3, the validator uses the same hash function to generate the hash value $H_(vc)$ of the received cipher text data (C_t). As well as, the validator supplies the validation algorithm with the validation key and the digital signature and extract the original plain text data's hash value $H_(vp)$. If both hash values are identical, that verifies that the data file has not been tampered with during the transfer process between both ends of this message (sender and receiver).

Algorithm 3 Data Validation

Input: Encrypted file C_t, Validators Public Key $V_(pk)$

function **VALIDATION** (C_t, $V_(pk)$

$H_v \leftarrow$ Calculate hash value of the received encrypted date C_t to be verified
Using public key$V_(pk)$ of signer, extract $H_(vp)$ of senders file

if H_v = $H_(vp)$ **then**

  Return C_t

else

  return "Validation Error!"

end if

end function

4.3 Authentication Process

For testing purposes, we implemented our technique using a medical organization example. When a doctor intends to update any data related to patient's records, the function presented in the following algorithm 4 combines the on-chain components with the off-chain components.

The blockchain contains authentication information about the doctor and the patient (agents), the organization they belong to, their tier levels within this organization and the hash of the data that is stored off-chain. While the off-chain storage contains the actual patient records that requires the update.

Algorithm 4 Authentication Process and Results

```
Auth onChainSystem;
Database offChainDatabase;

function ChangePatientData (doctorId, patientId, updatedRecords, doctorSignature)

if !doctorSignature was signed by (doctorId) then
   return (”Error! The signature does not seem to match the doctorId”)

   var docAuth = onChainSystem view AgentDetails (doctorId)
   var patientAuth = onChainSystem viewAgentDetails (patientId)

   if docAuth orgId == patientAuth orgId && docAuth tier > patientAuth tier then
      offChainDatabase updateData (patientId, updatedRecords)
   else
      return (”Error! Agent doctorId does not have the rights to update the records of patientId’);”)
   end if
   end function
```

When the function is called by the doctor, a signature from their private key is required for identification and authentication purposes. After confirming the authorization of that particular doctor, the function will then check the on-chain records to verify whether both the doctor and the patient are part of the same organization and whether the doctor has a higher tier level than the patient. If these two conditions were fulfilled, the off-chain component then can update the data according to the doctor’s input. Otherwise the process is denied and an error message is returned.

Algorithm 5 Agents Data

```
doctor_1 = {
id: '123qwe',
orgId: '123xyz',
tier: 3
}

patient_1 = {
id: '345ert',
orgId: '123xyz',
tier: 1
}

patient_2 = {
id: '456rty',
orgId: '123xyz',
tier: 1
}
```

Lets take a doctor and two patients as an example, with their personal details shown in the previous algorithm 5. If we call the above function shown in algorithm 4 with doctor_1['id'] as the doctorId and patient_1['id'] as the patientId, the function will proceed without any errors.

We then constructed an algorithm for testing purposes and the following algorithm 6 worked and returned the message "Changes have been made successfully".

Algorithm 6 Change Agent Data - Successful

```
changePatientData(doctor_1['id'], patient_1['id'], updatedRecords, doctorSignature);

return "Changes have been made successfully"
```

However, if we call the above function shown in algorithm 4 with patient_1['id'] as the doctorId and patient_2['id'] as the patientId, the function will not proceed and give an error message because patient_1['tier'] is not greater than patient_2['tier'].

We then constructed an algorithm for testing purposes and the following algorithm 7 worked and returned the message ”Changes cannot been made”.

Algorithm 7 Change Agent Data - Unsuccessful

```
changePatientData(patient_1['id'], patient_2['id'], updatedRecords, doctorSignature);

return ”Changes cannot been made”
```

This change can not be made because Agent ’345ert’ does not have the rights and the correct tier level to update the records of Agent ’456rty’.

4.4 Simulation of DDoS Attack

After structuring all our security mechanisms presented previously and implementing them within our proposed platform, we decided to test our platform’s security level by challenging it against an attack. DDoS attacks are one of the most common attacks against IoT networks which was a major motivation for us to specifically simulate it and choose it between all other types of attacks while some even consider it a benchmark for attacks on IoT devices.

During the latest decade, DDoS attacks have posed a dominant security risk to many ISPs, and came with it huge economic losses. In 2009, attackers induced DDoS attacks directed to some of China Telecom’s main DNS servers, this problem resulted in services disabling of hundreds of websites. Based on the survey of Arbor in 2008, Smurf attacks, DNS flooding attacks and SYN flooding attacks are three major approaches of DDoS attacks, and 76% of which are SYN flooding attacks [179] which is why we have decided to use this particular approach of DDoS attack in our scenario.

A UDP flood is a type of DDoS attack where User Datagram Protocol packets attempts to over-flood a server in an attempt to overwhelm its process ability for new requests and respond appropriately. The server receives these UDP requests and constantly checks whether currently running programs are listening for requests at specific ports and upon finding none, it responds with an unreachable destination message. With UDP requests flooding in, the targeted server becomes over-whelmed which affects its capacity to process and respond to requests. The following Figure 4.2 presents a simple diagram of a UDP flood attack.

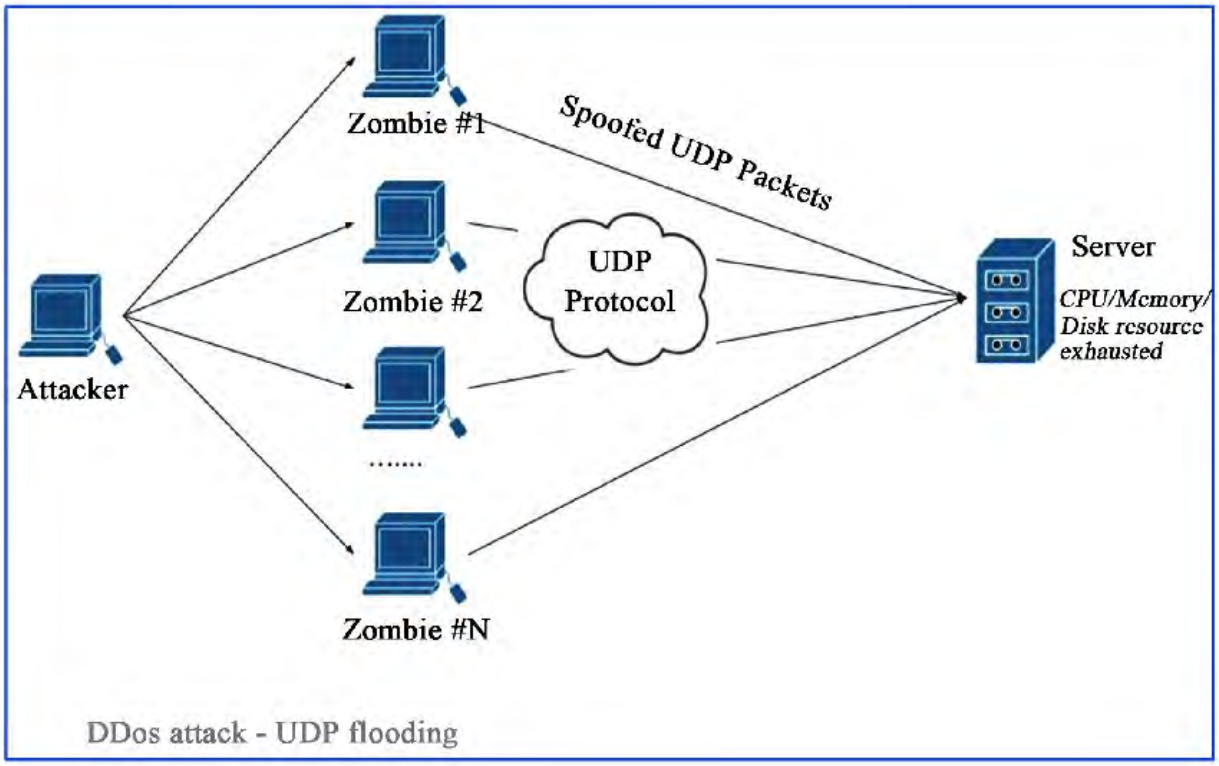


Figure 4.2: UDP Flooding Attack. [6]

For the simulation scenario, an attack server has been set up with both the VICTIM server and the UDP Echo server. Therefore, all the bad clients start the UDP flood Attack to the server. In this scenario, the intruders use a malicious UDP network traffic to deny other users access to the server service just like in other network layer attacks. The UDP Flood attacks have more effect on the UDP Echo server for time synchronization. Algorithm 8 shows the parameters of the UDP flood attack. The message size ranges between 512 to 1024 bytes and sent at an interval of 0.01 - 0.05 seconds. Therefore, all the bad clients (distributed hackers) will send 20 to 100 packets of messages per second to the victim server. The UDP attack will deny the victims' server service.

Algorithm 8 Configuration Parameters for UDP Attack

```
description = ”UDP Flood Attack”

**.NIDS.dataset-name = ”dataset-udp-flood.txt”
**.client[*].numUdpApps = 1
**.client[*].udpApps[0].typename = ”UDPBasicApp”
**.client[*].udpApps[0].destAddresses = ”attack.server”
**.client[*].udpApps[0].destport = 1000
**.client[*].udpApps[0].messageLength = uniform(512B, 1024B)
**.client[*].udpApps[0].sendIntervals = uniform(0.01s, 0.05s)

**.server.numUdpApps = 1
**.server.udpApps[0].typename = ”UDPEchoApp”
**.server.udpApps[0].localPort = 1000
```

The Simulation Tool used for this test is Trinoo which is a set of computer programs written using C language to execute a DDoS attack. UDP is the protocol chosen for this simulation as well as UDP flood for its attack. We have chosen this specific simulation tool for the following reasons:

- Highly used by the research community.
- Bandwidth depletion tool that launches coordinated UDP floods against IP addresses.
- Does not spoof source address.

After the simulation was created and set up, the traffic generator was ready for normal and attack data generation. We ran the generator for as long as we could to retrieve the largest amount of data possible which will then be increased as much as we need based on running the generator.

Table 4.1: DDOS Attack Result

No.	Description	Value	Comment
1	SRC ADD	176.45.32.176	Source IP Address
2	DES ADD	176.45.32.104	Destination IP Address
3	PKT ID	464	Identify of Packet
4	FROM NODE	322	Identify of Low Layer (if it is −1, unknown layer)
5	TO NODE	307	Identify of High Layer (if it is −1, unknown layer)
6	PKT TYPE	17	Type of Packet (17: UDP, 6: TCP.....)
7	PKT SIZE	503	Packet size
8	FLAGS	Null	Flags (SYN, ACK, FIN...) of Packet. This is not used in UDP. It is only used in TCP
9	FID	Null	Identify of Transfer Layer (It is only used in TCP)
10	SEQ Number	Null	Sequence Number (It is only used in TCP)
11	NUMBER OF PKT	3	Number of Received Packet
12	NUMBER OF BYTE	2158	Number of Received Bytes
13	NODE NAME FROM	encap	Name of Low Layer
14	NODE NAME TO	ip	Name of High Layer
15	PKT IN	1	Input Packet or not (1: INPUT, 0: NOT)
16	PKT OUT	0	Output Packet or not (1: OUTPUT, 0: NOT)
17	PKTR	0	Routing Packet or not (1: ROUTING, 0: NOT)
18	PKT DELAY NODE	0	Delay is occurred at this host? (1: YES, 0: NO)
19	PKT RATE	180.181	Rate for packet receive (number of received packet per second)
20	BYTE RATE	144,405	Rate for bytes receive (number of received bytes per second)
21	PKT AVG SIZE	706.14	Average Received Packet Size ($= \frac{Total\ Received\ Bytes}{Number\ of\ Received\ Packets}$)
22	UTILIZATION	1	This packet is used? (1: YES, 0: NO)

Table 4.1 summarizes our simulation results. As it is shown, 180,181 packets were received per second which was translated to 144,405 bytes per second with an average packet size of 706.14 bytes. This simulated DDoS attack did not affect our platform services as it was up and running during the whole attack simulation. The features of the data can be used for developing an IDS and evaluation.

4.5 Chapter Summary

Blockchain is not hack resistant, even though it is known for its safety and tamper-proof specification that makes it an ideal technology from a security point of view, we have used a public blockchain and moved its storage off-chain which made our platform more vulnerable to attacks. For that reason we have developed the security mechanisms and algorithms presented in this chapter and tested it against an attack for verification purposes.

Based on the simulation and testing results presented in this chapter, we conclude that our module can withstand against a DDoS attack securely. And this type of attack was chosen due to it being a very common type of attack usually used against IoT devices.

Chapter 5

Blockchain in Saudi Arabian Health Sector

5.1 Introduction

Numerous nations presently battle to supply cost-effective, quality healthcare administrations and services to their citizens [180]. The real transformation of the Saudi Arabian health sector began with the establishment of the Saudi Arabian Ministry of Health (MOH) in 1954. Saudi healthcare facilities, both public and private sectors, are supervised overall by the Ministry of Health. In 1970, the Saudi Arabian government initiated it's first five-year development plan promoting with that massive developments in multiple sectors including the health sector [181].

In this chapter we present a brief introduction of the Saudi Arabian health sector and its structure, as well as the health sector transformation program that has been launched under the Saudi Vison 2030 program. We then introduce our platform to this sector and present our solution's value in developing the transactions and data security in the Saudi Arabian health sector

The Saudi Arabian health sector system endorsed consecutive succeeding development plans and complete system transformations. With those continuing development and adaptability, the necessary infrastructure was well-established and developments have been implemented

since. These developments have improved primary healthcare, research facilities as well as private and public hospitals [181].

The Kingdom of Saudi Arabia (KSA) has experienced an issue of high cost at the side of concerns regarding quality of care in its public facilities. To attend these issues, the kingdom is currently reconstructing their healthcare framework in public hospitals and medical facilities in a transformation sense for the purpose of complying with the Saudi Arabian program of Vision 2030.

5.2 Saudi Arabian Health Sector

The Kingdom of Saudi Arabia is a welfare state. And according to the Saudi constitution, its government has the obligation to provide free healthcare services to all Saudi citizens. Citizens have access to free healthcare services by rights, which is and has been provided for through the constant development of the Saudi Arabian health policy. This policy is committed to a "Health for All (HFA)" goal.

The Saudi Arabian Ministry of Health has the responsibility of managing the country's health system. It has a well-defined, decentralised administrative and organisational structure. Its operations contain strategic planning, specific health policies formulating, delivery programs supervision of all health services, as well as controlling and monitoring all other activities related to health [182].

Health services in Saudi Arabia, as shown in Figure 5.1, are provided by the healthcare system as follows [7]:

- *60% of the Saudi health services are provided through the Saudi Arabian Ministry of Health.*
- *20% of the Saudi health services are provided through other government sectors and agencies.*
- *20% of the Saudi health services are provided through private and non-government sectors.*

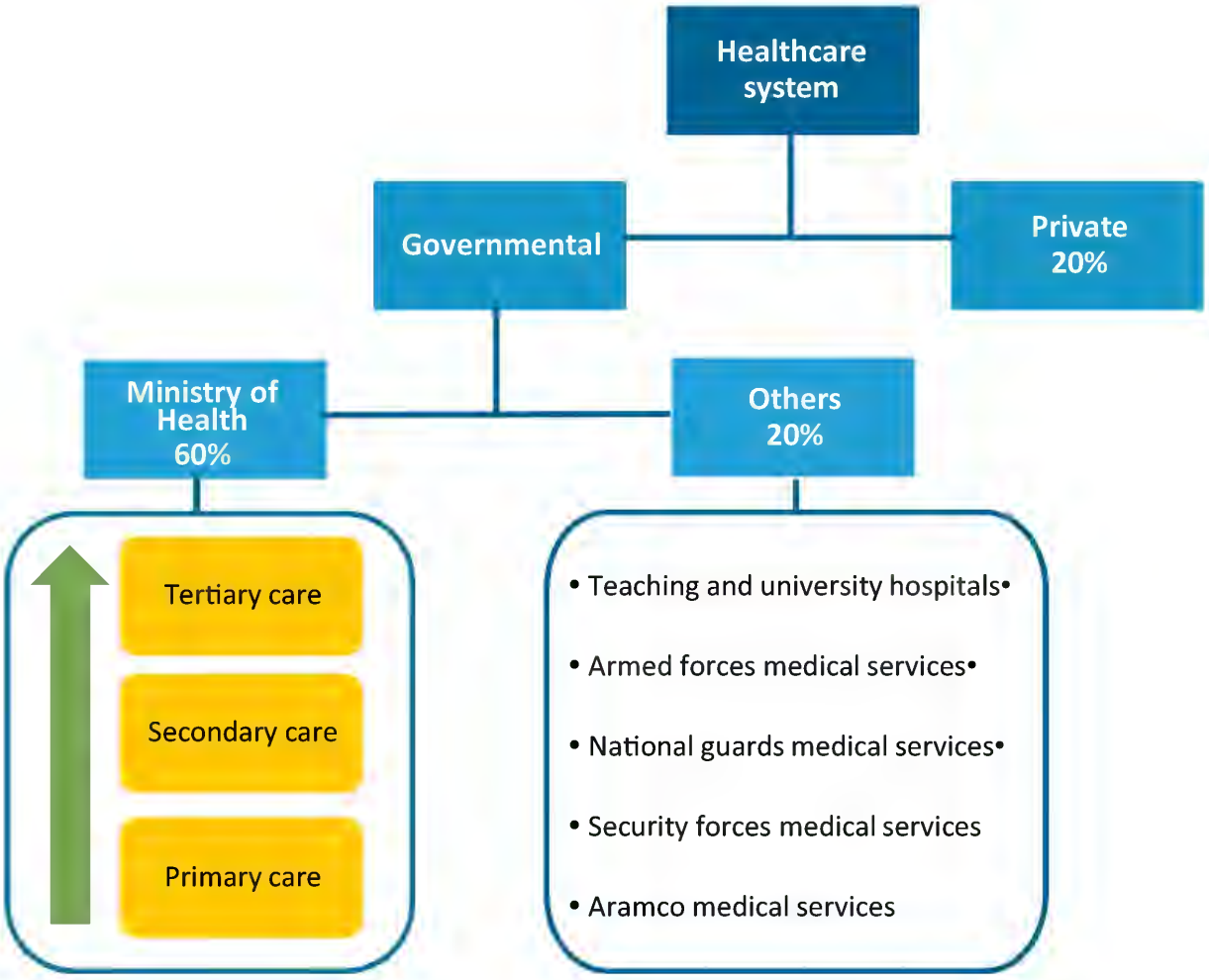


Figure 5.1: Saudi Arabian Health System Structure. [7]

5.3 Health Sector Transformation Program (Vision 2030)

The Health Sector Transformation Program was recently launched for the Kingdom of Saudi Arabia's Vision 2030 and will be launched by the end of 2021 to ensure extended and regular development of healthcare services in the Saudi Arabia and focus efforts in this crucial sector. This came right after the strategic targets and the accomplishment achievement of the National Transformation Program which managed to upgrade the health sector by improving and increasing efficiency and quality of health services as well as the level of health risk's protection level [183].

The main aim of the program is to improve the kingdom's health sector by rebuilding its structure to become an integrated, effective and an overall comprehensive health system that is based on the health of the society as well as individuals (including citizens, residents and visi-

tors). It is built upon a value-based care fundamental, which provides and assure transparency and financial sustainability by exhibiting public health as well as applying the recent care model related to disease prevention. This program also aims to advance and improve health services access through optimal coverage and an extensive and fair geographical distribution by broadening health services, digital solutions and e-health services as well as improving their quality of Service (QoS). The Health Sector Transformation Program works as well on improving connection and coordination between all entities of the health sector and other related government entities, it addition to linking this transformation and aligning it with other national transformations and goals [183].

Addressed as one of the main strategic sectors of the National Transformation Program, a huge amount of effort were applied in developing the health sector in general and specifically in response to the novel coronavirus (COVID-19) pandemic. Technology have also played a major role in Saudi Arabia's response to the social, economic and health impacts of the COVID-19 pandemic as well as the successful overcome of the crisis and its challenges [183].

Before the current stage, the Saudi health sector has achieved many achievements and accomplishments, such as improving the quality of health services and its efficiency and simplifying access to it and focusing on digitizing and automating the health sector and launching a couple of applications (Mawid and Sehhaty), and with that, increased the service coverage all around The Kingdom of Saudi Arabia regions [183].

In light of the world-wide development of health system, the Health Transformation Program is focusing its work on enabling broad transformation in the health sector and restructuring into an effective, broad and integrated system, based on the health of the society in general and the individual in particular. The organization is adopting the fundamentals of value-based care that provides and ensures transparency and develops health services to contribute to increase the beneficiaries' satisfaction. This program will focus on extending and improving prevention of diseases, public health, and health services accessibility [183].

The Saudi Arabian Health Sector will gain a huge benefit from adapting blockchain technology into its systems. This will defiantly proceed the development that is currently ongoing

and eventually succeed in reaching all the goals and meeting all milestones pointed out by the program.

5.4 Off-Chain Storage Blockchain in Saudi Arabian Health Sector

To integrate our off-chain storage blockchain platform, we have used the Saudi Arabian Health Sector as our use case scenario. And based on how the Saudi Arabian Health System is structured and presented in Figure 5.1, we have used the Saudi Arabian Ministry of Health as our main contract deployer on the network. We have also obtained a list of 50 Saudi Arabian hospitals and implemented them into our platform [Appendix B].

5.4.1 Front End

Our front end is written using JavaScript and is directly linked to our off-chain storage blockchain platform on Ethereum via the web3.js JavaScript library, which is bundled with the front end resources and served to a browser by a web server via an extension. In our case we used MetaMask extension.

For this implementation, we have developed a front end page that reads the data directly from our platform and presents it in a live feed manner. As shown in the following Figure 5.2, the Ministry of Health is presented on top as the deployer of contract which has the authority over the blockchain network and holds the highest tier in the authorisation hierarchy. Followed by the list of hospitals with each individual hospital specification presented next to it including the number of doctors, nurses and patients belonging to that particular hospital. We also have a line graph plot at the bottom of the page that reads the data directly from the platform and displays the amount of transactions made in the last 50 blocks and next to it is a speedometer indicator that displays the blockchain's transaction rate per second.

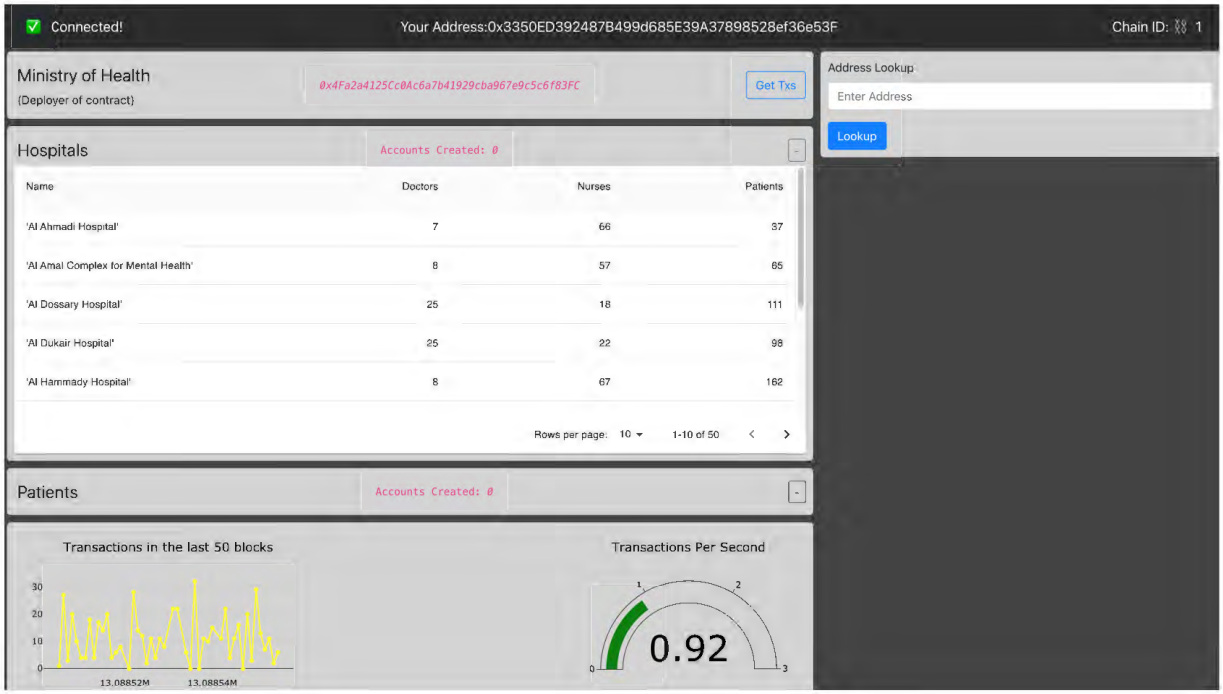


Figure 5.2: Implementation Front End.

After that, we used a random generator for agents (doctors, nurses, and patients) and integrated random number of each agent into each hospital as shown in the following Figure 5.3. These doctors, nurses, and patients are all directly interacting with the blockchain and the front end system is only reading and displaying the results directly from our built platform.

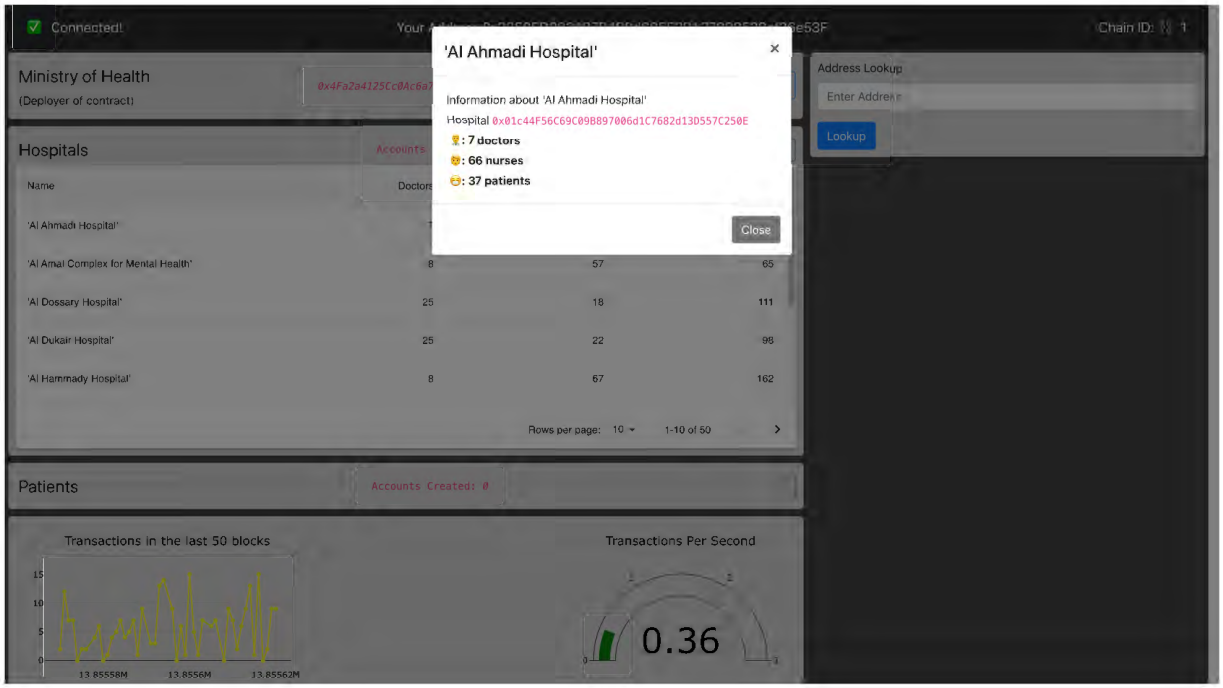


Figure 5.3: Hospital Details.

5.4.2 Advantages

An off-Chain storage blockchain has proven to be advantageous over an on-chain storage blockchain within the Saudi Arabian health sector. Specifically with respect to processing time, response time and capacity. While it was disadvantageous from a security point of view. In our case this was not a major issue as we have improved the connectivity security of our platform by implementing additional cryptographic techniques as previously discussed in Chapter 4. these advantages are presented in the following Table 5.1:

Table 5.1: On-Chain Storage Blockchain Vs. Off-Chain Storage Blockchain

	On-chain Storage Blockchain	Off-chain Storage Blockchain
Processing Time	Due to the data being constantly stored in the block itself, it makes the processing time of a transaction much higher.	Due to the data being stored in a database away from the blockchain, it makes the processing time of a transaction much faster.
Response Time	When the block is filled with data stored in it, the response time of a block becomes much slower.	When data is being stored in a database away from the blockchain, the response time of the blockchain remains unaffected.
Capacity	A blockchain can store a limited amount of data in a single block.	An external database can store much more data.
Security	Blockchain uses secure hashing algorithm (SHA) which is a 256-bit cryptographic hash function used for digital signatures.	Additional Cryptographic Techniques and implementations are required to further secure the connection between the blockchain and the external database.

5.4.3 Drawbacks

Normally with any project there are some limitations that may drawback the progress or obstruct the outcome of that project. For our front end implementation, constant framework updates were required during and after we finished our work which introduced multiple conflicts in our code. With that we had to work around it and constantly updating our framework multiple times which effected our time frame.

Due to simulation purposes, we have used a random generator to generate all agents including patients. We later distributed them randomly within the list of hospitals we have obtained earlier which caused our front end to read 0 patients accounts created. New patients accounts can only be counted towards our front end's patients section if these accounts are created individually and directly from the blockchain.

5.5 Chapter Summary

The Saudi Arabian Health Sector has recently began a 10 year transformation program which focuses on extended and regular development. Aiming to improve the health sector structure and integrating new technologies along the way to help cope with the development that the whole country is undergoing.

With our proposed case study example in the Saudi Arabian Health Sector and based on our simulation results previously presented in chapter 3, and our security testing presented in chapter 4, we can confirm that our platform can make a difference within the health system by establishing much faster transactions, retrieving old data and writing new ones, providing more efficiency as the health sector is considered to be a sensitive sector containing many critical cases, and more security regarding patient data and privacy policies as well as medical error avoidance.

Chapter 6

Conclusion and Future Research

With the rapid advancement in technology, blockchain is proving to be one of the greatest technological innovations both in the public sectors and the private sectors. The rising cases of cybersecurity issues have seen the wide adoption of the blockchain technology in many fields such as finance, security, and Internet of Things (IoT) [9]. However, many people are yet to understand how blockchain technology can be applied to IoT, and this can be seen to be a reason why many researchers focus on exploring this subject, hence the motivation for this thesis.

Blockchain technology introduced a huge change in the world of information technology and cyber security. It makes day to day operations safer and simpler, developing the way personal information is reserved and stored, and how services and transactions are processed. This technology establishes an immutable, permanent and tamper-proof record of each and every transaction. With its impenetrable digital ledger, it makes data theft, hacking, fraud, and information loss unachievable and impossible. The technology will influence and affect each and every industry world wide counting healthcare, manufacturing, transportation, retail, and real estate. Companies such as Google, Microsoft, Intel, IBM, American Express, and Walmart are all becoming blockchain early adaptors. Around 400 trillion American dollars across numerous industries are set to be transformed by blockchain.

In this thesis, we have attempted to solve the blockchain storage issue by developing an off-chain storage blockchain for managing IoT Devices. The main research question of this thesis was: **Does the capacity constraint in IoT devices negatively effect the speed of the trans-**

actions when connected and managed within a blockchain? And can we solve this issue by efficiently moving the data storage off-chain instead of saving all the storage within the blockchain blocks? We addressed this question through the main contribution chapters (Chapters 3,4 and 5) in this thesis by developing our own off-chain storage blockchain platform.

First, we started by building our own private blockchain platform. The proposed methodology applied was creating a smart contract and managing the blockchain. Then connecting some nodes (IoT devices) to it using Amazon Web Services (AWS) and connecting it to an external database (Cloud) to remove the history load of the blockchain. For the nodes (IoT Devices), Amazon Web Services was used. AWS represents through virtualization, a large set of computing resources, such as storing and processing capacities can be split, assigned, and dynamically sized to satisfy customers' demand. The performance of the proposed methodology is tested and benchmarked using Bitcoin's average and peak readings. Bitcoin is a cryptocurrency which is just a Blockchain use case yet it still remains the most common Blockchain application used up to date. The results show the edge our platform have over the bitcoin model while outperforming the benchmarked use case in features like read and write speed as well as transaction rates.

Next, we proceeded to securing the connection between the blockchain and the off-chain stored data. The proposed methodology applied a couple of cryptographic techniques into our platform. A data encryption algorithm was developed to encrypt data and produce a cipher text file. Then a public key cryptography is used to encrypt the symmetric key which results in a double encryption technique. Data Validation was another algorithm developed where the validator uses the same function for generating a hash value of the received cipher text data. As well as, the validator supplies the validation algorithm with the validation key and the digital signature and extract the original plain data's hash value. After that, an authentication process was implemented for testing purposes. The results show the system proceeding with the called function if the caller of the function has the authority as well as the right access rights. In another scenario, the system declines the called function if the caller of the function does not have the authority as well as the right access rights. After that we tested our platform by simulating a

DDos attack against it and presented the simulation parameters as well as the results.

Finally, we integrated our off-chain storage blockchain. We have used the Saudi Arabian Health Sector as our use case. And based on how the Saudi Arabian Health System is structured, we have used the Saudi Arabian Ministry of Health as our main contract deployer and we have also obtained a list of 50 Saudi Arabian hospitals and implemented them into our platform. For this implementation, we have developed a front end page that reads the data directly from our platform and presents it in a live feed manner. This front end display includes the main deployer of contract, followed by the list of hospitals with each hospital specification presented next to it, as well as the amount of transactions made in the last 50 blocks, and finally a speedometer that displays the transaction rate per second. The results show a smooth flow of transactions with no interruptions within the blockchain itself as well as a smooth flow in data collection and transfer between the front end and the platform.

6.1 Major Findings

In Chapter 3, we investigated if removing the data storage from the blockchain itself (blockchain stores the history ledger in each block) and moving it to an external off-chain storage (cloud) could speed transaction with IoT devices. In a Blockchain, each node must store the full history of the blockchain. This affects transaction times and limits lightweight nodes, such as IoT devices, from joining the network. As time passes, history becomes larger, and the problem will be aggravated. The proposed methodology uses Ethereum for building the blockchain and AWS for generating virtual IoT devices as well as the off-chain database. The Simulation of our platform was done by running the same simolation script on 11 different computers in parallel. Ten of the eleven computers were VPCs rented from the AWS cloud provider, which ran on Ubuntu 16.10. We installed all necessary software to be able to run the simulation on each machine, such as Python compiler, Web3.py library, Solidity compiler, Ethereum software and Geth. The 11^{th} computer was a Macbook Running on macOs Mojave, which had the same software installed. The results obtained from our simulations (for 150, 350 and 500 users) were benchmarked againt bitcoin's average and bitcoin's peak rates of all times and this benchmarking favoured our platform results in both transaction rates and read and write speed.

In Chapter 4, we investigated the cryptographic part of our project. Even though blockchain is known for its safety and tamper-proof specification that makes it an ideal technology from a security point of view, we still had to increase the security level of the system by implementing a few extra security mechanism and other cryptographic techniques because we are using an external database (off-chain storage) away from the blockchain itself. This was addressed after designing the system and creating all modules, and after connecting them to each other. Blockchain uses a secure hashing algorithm (SHA) which is a 256-bit cryptographic hash function used for digital signature. It will require 2^{256} guesses to get the private key of the agent right. For data encryption, a symmetric key S_k was used to encrypt the data and produce a cipher text file C_t. Then did a double encryption technique by using a public key cryptography to encrypt the symmetric key S_k. We encrypted the symmetric key S_k by using the receiver's public key $R_(pk)$ and send the cipher text file C_t and denote the encrypted symmetric key by using the cipher key C_k. For data validation, the validator uses the same hash function to generates the hash value $H_(vc)$ of the received cipher text data (C_t) while also supplying the validation algorithm with the validation key and the digital signature and extract the original plain text data's hash value $H_(vp)$. If both hash values are identical, that verifies that the data file has not been tampered with during the transfer process between both ends of this message (sender and receiver). For testing purposes, we have implemented our technique using a medical organization example. When a doctor intends to update any data related to patient's records, the function presented in the authentication algorithm combines the on-chain components with the off-chain components. The results we obtained shows the system proceeding with the called function if the caller of the function has the authority as well as the right access rights. It also shows the system declining the called function if the caller of the function does not have the authority as well as the right access rights. After that we tested our proposed platform by simulating a DDos attack against it with the parameters presented previously and obtained the results of that simulation. The results confirms that our platform along with its security mechanisms are capable of handling such types of attacks.

In Chapter 5, we acknowledged the transformation the Kingdom of Saudi Arabia is going through within its national transformation program "Vision 2030" in general. We then investigated by going deeper into the Saudi Arabian health sector transformation program in particular and showed how our platform can play a major role in this transformation and can aid this program in achieving its aims and goals. For this implementation, we have developed a front end page that reads the data directly from our platform and presents it in a live feed manner. Because 60% of the Saudi health services are provided through the Saudi Arabian Ministry of Health, we have presented the Ministry of Health on top of our front end page as the deployer of contract followed by the list of hospitals with each hospital specification presented next to it. We have also integrated a plot that displays the amount of transactions made in the last 50 blocks as well as a speedometer that displays the transaction rate per second. We then used a random generator for our agents (doctors, nurses, and patients) and integrated a random amount of each agent into each hospital. These doctors, nurses, and patients are all directly interacting with the blockchain and the front end system is only reading and displaying the results directly from our built platform. The results of this implementation shows and confirms that there were no inconsistencies between the database and the blockchain nor there are any interruptions within the blockchain itself. We then conducted a comparison between and on-chain and and off-chain storage blockchain which supports the integration of our platform. And finally, we displayed some challenges and drawback that we encountered during this research.

The major research contributions of this thesis lined with research questions could be summarized as follows:

- Developed a new blockchain architecture module for managing IoT devices, which shows that an off-chain storage solution is suitable for solving the capacity constraint of the history ledger and its ability to manage small portable IoT devices smoothly compared to a standard blockchain.

- developed novel cryptographic algorithms for the architecture of data storage and security. We then evaluated, and validated them. later we presented our results which complements our proposed platform and secure the management of the IoT devices and its connection

with the off-chain storage database (cloud). And presenting these mechanism's ability to withstand an attack (In this case, DDos Attack).

- Introduced an application problem (the Saudi Arabian health system) to evaluate the proposed architecture and evaluated this sector's application using the implementation of our module. We did this by evaluating the efficiency, effectiveness and robustness of our system. we later presented an implementation overview which shows all the data flow and transactions performed by the blockchain with the Saudi Arabian health care system aligned with the transformation and development program the sector is currently going through.

6.2 Limitations

We have encountered a couple of limitations with our current study presented as follows:

- The decision to build our off-chain storage blockchain platform using a public blockchain was made in this project's early stages. Soon after completing the platform and as soon as we entered the simulation phase, we obtained disrupted results affected by public interference on the network which resulted in our data and results obtained being inaccurate. Each simulation made gave us a different set of results than the other simulations. At one point the results were improving and at another the results were worsening depending on the public's interaction on the network at the time of the simulation. For that reason, we have decided to switch to a private blockchain and eventually we have obtained stable results as presented in this thesis.

- The presented results were affected by the limitations we had using AWS free tier specifically with bandwidth and connectivity speed. This implementation and simulation process could be well improved with many factors. With the necessary accessibility to many other features and exceeding the restrictions of connectivity, we can improve our transactions per second as well as read and write speed of our platform even further.

- Cost was a major issues we had encountered. even though we were using AWS free tier and Ethereum which is a free to use platform, we had to buy some Ether for simulation purposes and pay a small amount of fee each time we did a simulation. Over the past couple of years we have simulated more than 100 times for testing purposes which led to a respected amount being paid.

6.3 Future Work

Advantageous and beneficial developments and expansions to the work proposed in this research could take the following directions:

- Blockchain is a technology that is being developed and improved by the moment. Many studies and projects are addressing different gaps and issues while proposing various ways to close these gaps. The system implemented in this research is a preliminary prospective of a much bigger prospective. It can make a huge difference in the way blockchain is handled and eventually encourage multiple enterprises from different fields to introduce this technology to its transactions (Such as medical enterprises, teaching facilities and many other government and private sectors).

- A couple of cryptographic thechniques were presented in this thesis including data encryption, data validation and data authentication. A Merkle Tree can also be built and implemented to further increase security connection between the blockchain and the off-chain storage database. The features of the data obtained from the DDos attack simulation results could also be used for developing and evaluating an IDS.

- In our proposed solution we addressed the issue of storage constraint in blockchain technology and how this issue can affect the speed of transaction by time when the history ledger and the data saved becomes larger. An on-chain storage solution still needs to be addressed and investigated.

Appendix A

An off-chain storage blockchain for managing IoT Devices

Source Code

The Source Code of our proposed Off-Chain Storage Blockchain platform has been uploaded using Github and can be accessed using the following URL:

`https://github.com/falkurdii/PhD_Thesis.git`

Appendix B

Blockchain in Saudi Arabian Health Sector

List of Saudi Arabian Hospitals Datasets

The list of Saudi Arabian hospitals used for our off-chain storage platform use case scenario integration in chapter 5, section 5.4, has been uploaded using google drive and can be accessed using the following URL:

`http://tinyurl.com/LOH-KSA`

References

[1] V. Denis. (2019) Understanding blockchain technology. [Online]. Available: https://cia.news/en/understanding-blockchain-technology/

[2] M. T. Oliveira, G. R. Carrara, N. C. Fernandes, C. V. Albuquerque, R. C. Carrano, D. S. Medeiros, and D. M. Mattos, "Towards a performance evaluation of private blockchain frameworks using a realistic workload," in *2019 22nd conference on innovation in clouds, internet and networks and workshops (ICIN)*. IEEE, 2019, pp. 180–187.

[3] S. Prabhu. (2020) Blockchain. [Online]. Available: https://devopedia.org/blockchain

[4] A. Chopra. (2021) Blockchain — Understanding Its Uses and Implications. [Online]. Available: https://medium.com/nerd-for-tech/blockchain-understanding-its-uses-and-implications-162b6d1cffd5

[5] Csiro. (2020) Encrypting On-Chain Data. [Online]. Available: https://research.csiro.au/blockchainpatterns/general-patterns/data-management-patterns/encrypting-on-chain-data/

[6] S. Alzahrani and L. Hong, "Generation of ddos attack dataset for effective ids development and evaluation," *Journal of Information Security*, vol. 09, pp. 225–241, 01 2018.

[7] M. K. Khalil, S. Al-Eidi, M. Al-Qaed, and S. AlSanad, "The future of integrative health and medicine in Saudi Arabia," *Integrative medicine research*, vol. 7, no. 4, pp. 316–321, 2018.

[8] N. Dashkevich, S. Counsell, and G. Destefanis, "Blockchain application for central banks: A systematic mapping study," *IEEE Access*, vol. 8, pp. 139 918–139 952, 2020.

[9] F. Alkurdi, I. Elgendi, K. S. Munasinghe, D. Sharma, and A. Jamalipour, "Blockchain in IoT security: a survey," in *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*. IEEE, 2018, pp. 1–4.

[10] M. Swan, "Anticipating the economic benefits of blockchain," *Technology innovation management review*, vol. 7, no. 10, pp. 6–13, 2017.

[11] A. Ouaddah, A. Abou Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," in *Europe and MENA cooperation advances in information and communication technologies*. Springer, 2017, pp. 523–533.

[12] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)*. IEEE, 2016, pp. 1392–1393.

[13] Y. Yuan and F.-Y. Wang, "Blockchain: the state of the art and future trends," *Acta Automatica Sinica*, vol. 42, no. 4, pp. 481–494, 2016.

[14] M. Samaniego, U. Jamsrandorj, and R. Deters, "Blockchain as a service for IoT," in *2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. IEEE, 2016, pp. 433–436.

[15] P. Kasireddy, "Fundamental challenges with public blockchains," *Medium, blockchein [23.03. 2019]. URL: https://medium. com/@ preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428*, 2017.

[16] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review," *PloS one*, vol. 11, no. 10, p. e0163477, 2016.

[17] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. Leung, "Decentralized applications: The blockchain-empowered software system," *IEEE Access*, vol. 6, pp. 53 019–53 033, 2018.

[18] S. Demirkan, I. Demirkan, and A. McKee, "Blockchain technology in the future of business cyber security and accounting," *Journal of Management Analytics*, vol. 7, no. 2, pp. 189–208, 2020.

[19] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trustless medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14 757–14 767, 2017.

[20] C. Zhang and Y. Chen, "A review of research relevant to the emerging industry trends: Industry 4.0, IoT, blockchain, and business analytics," *Journal of Industrial Integration and Management*, vol. 5, no. 01, pp. 165–180, 2020.

[21] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing," *Information Sciences*, vol. 462, pp. 262–277, 2018.

[22] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6–14, 2018.

[23] B. Zhao, P. Fan, and M. Ni, "Mchain: A blockchain-based vm measurements secure storage approach in iaas cloud with enhanced integrity and controllability," *IEEE Access*, vol. 6, pp. 43 758–43 769, 2018.

[24] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in *Banking beyond banks and money*. Springer, 2016, pp. 239–278.

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

[26] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the thirteenth EuroSys conference*, 2018, pp. 1–15.

[27] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *Journal of economic Perspectives*, vol. 29, no. 2, pp. 213–38, 2015.

[28] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Fairaccess: a new blockchain-based access control framework for the internet of things," *Security and communication networks*, vol. 9, no. 18, pp. 5943–5964, 2016.

[29] P. Dunphy and F. A. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE security & privacy*, vol. 16, no. 4, pp. 20–29, 2018.

[30] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*. IEEE, 2017, pp. 557–564.

[31] P. S. R. BORES and A. Hlaciuc, "Digital currency in the current cyber security environment," *Contemporary Economy Journal*, vol. 1, no. 3, pp. 70–79, 2016.

[32] T. Swanson, "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems," *Report, available online*, 2015.

[33] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "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). IEEE, 2017, pp. 618–623.

[34] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *arXiv preprint arXiv:1906.11078*, 2019.

[35] S. J. Shackelford and S. Myers, "Block-by-block: leveraging the power of blockchain technology to build trust and promote cyber peace," *Yale JL & Tech.*, vol. 19, p. 334, 2017.

[36] P. B. Lowry, T. Dinev, and R. Willison, "Proposing a bold research agenda," european journal of information systems."

[37] M. Staples, S. Chen, S. Falamaki, A. Ponomarev, P. Rimba, A. Tran, I. Weber, X. Xu, and J. Zhu, "Risks and opportunities for systems using blockchain and smart contracts. data61," *CSIRO), Sydney*, 2017.

[38] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the internet of things (IoT)," *IEEE Internet Initiative*, vol. 1, no. 1, pp. 1–86, 2015.

[39] A. Bhawiyuga, M. Data, and A. Warda, "Architectural design of token based authentication of mqtt protocol in constrained IoT device," in *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*. IEEE, 2017, pp. 1–4.

[40] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for internet of things," *Future Generation Computer Systems*, vol. 89, pp. 110–125, 2018.

[41] M. El-Hajj, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Analysis of authentication techniques in internet of things (IoT)," in *2017 1st Cyber Security in Networking Conference (CSNet)*. IEEE, 2017, pp. 1–3.

[42] L. Atzori, A. Iera, and G. Morabito, "Understanding the internet of things: definition, potentials, and societal role of a fast evolving paradigm," *Ad Hoc Networks*, vol. 56, pp. 122–140, 2017.

[43] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. A. Kazmi, and C. S. Hong, "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges," *Future Generation Computer Systems*, vol. 92, pp. 265–275, 2019.

[44] C.-W. Tsai, C.-F. Lai, M.-C. Chiang, and L. T. Yang, "Data mining for internet of things: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 77–97, 2013.

[45] E. Casagras, "Casagras final report: Rfid and the inclusive model for the internet of things," *EU FP7 Project CASAGRAS*, 2009.

[46] B. Fekade, T. Maksymyuk, M. Kyryk, and M. Jo, "Probabilistic recovery of incomplete sensed data in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2282–2292, 2017.

[47] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet of things journal*, vol. 3, no. 6, pp. 854–864, 2016.

[48] H. Sato, A. Kanai, S. Tanimoto, and T. Kobayashi, "Establishing trust in the emerging era of IoT," in *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*. IEEE, 2016, pp. 398–406.

[49] A. Rayes and S. Salam, "Internet of things (IoT) overview," in *Internet of Things From Hype to Reality*. Springer, 2019, pp. 1–35.

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

[51] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[52] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE international conference on systems, man, and cybernetics (SMC)*. IEEE, 2017, pp. 2567–2572.

[53] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for ble-based devices in the internet of things," *ieee access*, vol. 6, pp. 24 639–24 649, 2018.

[54] L. Zhou, L. Wang, Y. Sun, and P. Lv, "Beekeeper: A blockchain-based IoT system with secure storage and homomorphic computation," *IEEE Access*, vol. 6, pp. 43 472–43 488, 2018.

[55] E. F. Jesus, V. R. Chicarino, C. V. De Albuquerque, and A. A. d. A. Rocha, "A survey of how to use blockchain to secure internet of things and the stalker attack," *Security and Communication Networks*, vol. 2018, 2018.

[56] Y. Zhang and J. Wen, "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, 2017.

[57] W. Pollard, "IoT semantic interoperability: Research challenges best practices recommendations and next steps," *IERC (European Research Cluster On The Internet Of Things)*, 2015.

[58] Z. Bao-Kun, Z. Lie-Huang, M. Shen, F. Gao, C. Zhang, L. Yan-Dong, and J. Yang, "Scalable and privacy-preserving data sharing based on blockchain," *Journal of Computer Science and Technology*, vol. 33, no. 3, pp. 557–567, 2018.

[59] A. Assiri and H. Almagwashi, "IoT security and privacy issues," in *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*. IEEE, 2018, pp. 1–5.

[60] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of things journal*, vol. 5, no. 4, pp. 2483–2495, 2017.

[61] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[62] S. Tweneboah-Koduah, K. E. Skouby, and R. Tadayoni, "Cyber security threats to IoT applications and service domains," *Wireless Personal Communications*, vol. 95, no. 1, pp. 169–185, 2017.

[63] M. Ge, J. B. Hong, W. Guttmann, and D. S. Kim, "A framework for automating security analysis of the internet of things," *Journal of Network and Computer Applications*, vol. 83, pp. 12–27, 2017.

[64] O. Mavropoulos, H. Mouratidis, A. Fish, and E. Panaousis, "Apparatus: A framework for security analysis in internet of things systems," *Ad Hoc Networks*, vol. 92, p. 101743, 2019.

[65] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in internet of things," *Future Generation Computer Systems*, vol. 100, pp. 144–164, 2019.

[66] J. D. Lee, T. S. Yoon, S. H. Chung, and H. S. Cha, "Service-oriented security framework for remote medical services in the internet of things environment," *Healthcare informatics research*, vol. 21, no. 4, pp. 271–282, 2015.

[67] P. Hao, X. Wang, and W. Shen, "A collaborative phy-aided technique for end-to-end IoT device authentication," *IEEE Access*, vol. 6, pp. 42 279–42 293, 2018.

[68] T. Shah and S. Venkatesan, "Authentication of IoT device and IoT server using secure vaults," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018, pp. 819–824.

[69] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, and K.-Y. Yoo, "Secure signature-based authenticated key establishment scheme for future IoT applications," *Ieee Access*, vol. 5, pp. 3028–3043, 2017.

[70] Z. A. Alizai, N. F. Tareen, and I. Jadoon, "Improved IoT device authentication scheme using device capability and digital signatures," in *2018 International Conference on Applied and Engineering Mathematics (ICAEM)*. IEEE, 2018, pp. 1–5.

[71] A. A. Zaidan, B. B. Zaidan, M. Qahtan, O. S. Albahri, A. S. Albahri, M. Alaa, F. M. Jumaah, M. Talal, K. L. Tan, W. Shir *et al.*, "A survey on communication components for IoT-based technologies in smart homes," *Telecommunication Systems*, vol. 69, no. 1, pp. 1–25, 2018.

[72] R. Sahay, G. Geethakumari, B. Mitra, and I. Sahoo, "Efficient framework for detection of version number attack in internet of things," in *International Conference on Intelligent Systems Design and Applications*. Springer, 2018, pp. 480–492.

[73] P. L. R. Chze and K. S. Leong, "A secure multi-hop routing for IoT communication," in *2014 IEEE World forum on internet of things (WF-IoT)*. IEEE, 2014, pp. 428–432.

[74] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging sdn and nfv security mechanisms for IoT systems," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 812–837, 2018.

[75] E. Kim, K. Chung, and T. Jeong, "Self-certifying id based trustworthy networking system for IoT smart service domain," in *2017 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2017, pp. 1299–1301.

[76] D. Shin, V. Sharma, J. Kim, S. Kwon, and I. You, "Secure and efficient protocol for route optimization in pmipv6-based smart home IoT networks," *IEEE Access*, vol. 5, pp. 11 100–11 117, 2017.

[77] R. Giuliano, F. Mazzenga, A. Neri, and A. M. Vegni, "Security access protocols in IoT capillary networks," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 645–657, 2016.

[78] S. Kim and I. Lee, "IoT device security based on proxy re-encryption," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 4, pp. 1267–1273, 2018.

[79] J. Hou, L. Qu, and W. Shi, "A survey on internet of things security from data perspectives," *Computer Networks*, vol. 148, pp. 295–306, 2019.

[80] M. Singh, A. Singh, and S. Kim, "Blockchain: A game changer for securing IoT data," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*. IEEE, 2018, pp. 51–55.

[81] J. H. Jeon, K.-H. Kim, and J.-H. Kim, "Block chain based data security enhanced IoT server platform," in *2018 International Conference on Information Networking (ICOIN)*. IEEE, 2018, pp. 941–944.

[82] K. R. Sollins, "IoT big data security and privacy versus innovation," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1628–1635, 2019.

[83] R. Huuck, "IoT: The internet of threats and static program analysis defense," in *EmbeddedWorld 2015: Exibition & Conferences*, 2015, p. 493.

[84] A. K. Mandal, A. Cortesi, P. Ferrara, F. Panarotto, and F. Spoto, "Vulnerability analysis of android auto infotainment apps," in *Proceedings of the 15th ACM International Conference on Computing Frontiers*, 2018, pp. 183–190.

[85] F. Panarotto, A. Cortesi, P. Ferrara, A. K. Mandal, and F. Spoto, "Static analysis of android apps interaction with automotive can," in *International Conference on Smart Computing and Communication*. Springer, 2018, pp. 114–123.

[86] Z. B. Celik, E. Fernandes, E. Pauley, G. Tan, and P. McDaniel, "Program analysis of commodity IoT applications for security and privacy: Challenges and opportunities," *ACM Computing Surveys (CSUR)*, vol. 52, no. 4, pp. 1–30, 2019.

[87] G. Kambourakis, C. Kolias, and A. Stavrou, "The mirai botnet and the IoT zombie armies," in *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*. IEEE, 2017, pp. 267–272.

[88] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges," *IEEE access*, vol. 8, pp. 32 031–32 053, 2020.

[89] A. Ekramifard, H. Amintoosi, and A. H. Seno, "A systematic literature review on blockchain-based solutions for IoT security," in *The 7th International Conference on Contemporary Issues in Data Science*. Springer, 2019, pp. 311–321.

[90] A. Erdem, S. Ö. Yildirim, and P. Angin, "Blockchain for ensuring security, privacy, and trust in IoT environments: the state of the art," *Security, Privacy and Trust in the IoT Environment*, pp. 97–122, 2019.

[91] A. Sultan, M. A. Mushtaq, and M. Abubakar, "IoT security issues via blockchain: a review paper," in *Proceedings of the 2019 International Conference on Blockchain Technology*, 2019, pp. 60–65.

[92] P. Karthikeyyan, S. Velliangiri *et al.*, "Review of blockchain based IoT application and its security issues," in *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, vol. 1. IEEE, 2019, pp. 6–11.

[93] B. Alotaibi, "Utilizing blockchain to overcome cyber security concerns in the internet of things: A review," *IEEE Sensors Journal*, vol. 19, no. 23, pp. 10 953–10 971, 2019.

[94] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future generation computer systems*, vol. 82, pp. 395–411, 2018.

[95] H. Rajab and T. Cinkelr, "IoT based smart cities," in *2018 international symposium on networks, computers and communications (ISNCC)*. IEEE, 2018, pp. 1–4.

[96] S. Rathore, B. W. Kwon, and J. H. Park, "Blockseciotnet: Blockchain-based decentralized security architecture for IoT network," *Journal of Network and Computer Applications*, vol. 143, pp. 167–177, 2019.

[97] M. A. Rashid and H. H. Pajooh, "A security framework for IoT authentication and authorization based on blockchain technology," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2019, pp. 264–271.

[98] A. Haroon, M. A. Shah, Y. Asim, W. Naeem, M. Kamran, and Q. Javaid, "Constraints in the IoT: the world in 2020 and beyond," *Constraints*, vol. 7, no. 11, pp. 252–271, 2016.

[99] M. Singh and G. Baranwal, "Quality of service (qos) in internet of things," in *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*. IEEE, 2018, pp. 1–6.

[100] G. White, V. Nallur, and S. Clarke, "Quality of service approaches in IoT: A systematic mapping," *Journal of Systems and Software*, vol. 132, pp. 186–203, 2017.

[101] R. Kelly, "Internet of things data to top 1.6 zettabytes by 2020," *Campus Technology*, vol. 9, pp. 1536–1233, 2016.

[102] L. Mearian, "Self-driving cars could create 1gb of data a second," *Computerworld*, vol. 23, 2013.

[103] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[104] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 141, pp. 199–221, 2018.

[105] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE internet of things journal*, vol. 3, no. 5, pp. 637–646, 2016.

[106] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[107] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, and M. Guizani, "Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges," *IEEE wireless communications*, vol. 24, no. 3, pp. 10–16, 2017.

[108] F. Allhoff and A. Henschke, "The internet of things: Foundational ethical issues," *Internet of Things*, vol. 1, pp. 55–66, 2018.

[109] A. Rayes and S. Salam, "Internet of things from hype to reality," *Springer*, 2017.

[110] T. T. Zin, P. Tin, and H. Hama, "Reliability and availability measures for internet of things consumer world perspectives," in *2016 IEEE 5th Global Conference on Consumer Electronics*. IEEE, 2016, pp. 1–2.

[111] A. Mavrogiorgou, A. Kiourtis, C. Symvoulidis, and D. Kyriazis, "Capturing the reliability of unknown devices in the IoT world," in *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*. IEEE, 2018, pp. 62–69.

[112] M. Kim, "A quality model for evaluating IoT applications," *International Journal of Computer and Electrical Engineering*, vol. 8, no. 1, p. 66, 2016.

[113] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello, and A. Coen-Porisini, "A secure and quality-aware prototypical architecture for the internet of things," *Information Systems*, vol. 58, pp. 43–55, 2016.

[114] A. Rizzardi, D. Miorandi, S. Sicari, C. Cappiello, and A. Coen-Porisini, "Networked smart objects: Moving data processing closer to the source," in *International Internet of Things Summit*. Springer, 2015, pp. 28–35.

[115] 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, 2018.

[116] M. Dai, S. Zhang, H. Wang, and S. Jin, "A low storage room requirement framework for distributed ledger in blockchain," *IEEE Access*, vol. 6, pp. 22 970–22 975, 2018.

[117] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *Ieee Access*, vol. 6, pp. 38 437–38 450, 2018.

[118] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *2017 19th international conference on advanced communication technology (ICACT)*. IEEE, 2017, pp. 464–467.

[119] Y. Chao, X. Mi-xue, and S. Xue-ming, "Research on a new signature scheme on blockchain," *Security and Communication Networks*, vol. 2017, 2017.

[120] I. Eyal, "Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities," *Computer*, vol. 50, no. 9, pp. 38–49, 2017.

[121] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol," in *13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16)*, 2016, pp. 45–59.

[122] Y. Sompolinsky and A. Zohar, "Accelerating bitcoin's transaction processing fast money grows on trees," *Not Chains*, 2013.

[123] C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels," in *Symposium on Self-Stabilizing Systems*. Springer, 2015, pp. 3–18.

[124] C. Stathakopoulou, C. Decker, and R. Wattenhofer, "A faster bitcoin network," *Tech. rep., ETH, Zurich,. Semester Thesis*, 2015.

[125] K. D. Kumar, M. Sudhakara, R. K. Poluru *et al.*, "Towards the integration of blockchain and IoT for security challenges in IoT: A review," *Transforming Businesses with Bitcoin Mining and Blockchain Applications*, pp. 45–67, 2020.

[126] M. Urmila, B. Hariharan, and R. Prabha, "A comparitive study of blockchain applications for enhancing internet of things security," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2019, pp. 1–7.

[127] M. Dabbaghjamanesh, B. Wang, S. Mehraeen, J. Zhang, and A. Kavousi-Fard, "Networked microgrid security and privacy enhancement by the blockchain-enabled internet of things approach," in *2019 IEEE Green Technologies Conference (GreenTech)*. IEEE, 2019, pp. 1–5.

[128] S. Sinha and D. Deepika, "Stack based location identification of malicious node in rpl attack using average power consumption," in *2021 2nd International Conference for Emerging Technology (INCET)*. IEEE, 2021, pp. 1–5.

[129] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in *Proceedings of the second international conference on Internet-of-Things design and implementation*, 2017, pp. 173–178.

[130] K. Tiba, R. M. Parizi, Q. Zhang, A. Dehghantanha, H. Karimipour, and K.-K. R. Choo, "Secure blockchain-based traffic load balancing using edge computing and reinforcement learning." *Blockchain Cybersecurity, Trust and Privacy*, vol. 79, pp. 99–128, 2020.

[131] M. Simić, G. Sladić, and B. Milosavljević, "A case study IoT and blockchain powered healthcare," in *Proc. ICET*, 2017.

[132] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium blockchain-based malware detection in mobile devices," *IEEE Access*, vol. 6, pp. 12 118–12 128, 2018.

[133] N. Zhang, S. Zhong, and L. Tian, "Using blockchain to protect personal privacy in the scenario of online taxi-hailing," *International journal of computers communications & control*, vol. 12, no. 6, pp. 886–902, 2017.

[134] S. H. Lee and C. S. Yang, "Fingernail analysis management system using microscopy sensor and blockchain technology," *International Journal of Distributed Sensor Networks*, vol. 14, no. 3, p. 1550147718767044, 2018.

[135] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *International Journal of Production Research*, vol. 57, no. 7, pp. 2117–2135, 2019.

[136] M. Yoo and Y. Won, "A study on the transparent price tracing system in supply chain management based on blockchain," *Sustainability*, vol. 10, no. 11, p. 4037, 2018.

[137] T. Qu, S. Lei, Z. Wang, D. Nie, X. Chen, and G. Q. Huang, "IoT-based real-time production logistics synchronization system under smart cloud manufacturing," *The International Journal of Advanced Manufacturing Technology*, vol. 84, no. 1-4, pp. 147–164, 2016.

[138] R. Alcarria, B. Bordel, T. Robles, D. Martín, and M.-Á. Manso-Callejo, "A blockchain-based authorization system for trustworthy resource monitoring and trading in smart communities," *Sensors*, vol. 18, no. 10, p. 3561, 2018.

[139] K. Azbeg, O. Ouchetto, S. J. Andaloussi, L. Fetjah, and A. Sekkaki, "Blockchain and IoT for security and privacy: A platform for diabetes self-management," in *2018 4th international conference on cloud computing technologies and applications (Cloudtech)*. IEEE, 2018, pp. 1–5.

[140] 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, pp. 1–7, 2018.

[141] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, 2019.

[142] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Lsb: A lightweight scalable blockchain for IoT security and anonymity," *Journal of Parallel and Distributed Computing*, vol. 134, pp. 180–197, 2019.

[143] B. Zhang, J. Li, X. Zheng, J. Ge, and J. Sun, "A blockchain-based mobile IoT network interconnection security trusted protocol model," in *International Symposium on Cyberspace Safety and Security*. Springer, 2019, pp. 372–381.

[144] M. S. Hossain, S. Waheed, Z. Rahman, S. Shezan, and M. M. Hossain, "Blockchain for the security of internet of things: a smart home use case using ethereum," *International Journal of Recent Technology and Engineering*, vol. 8, no. 5, pp. 4601–4608, 2020.

[145] M. N. Islam and S. Kundu, "IoT security, privacy and trust in home-sharing economy via blockchain." 2020.

[146] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Computers & Security*, vol. 78, pp. 126–142, 2018.

[147] S. N. Mohanty, K. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. Lakshmanaprabu, and A. Khanna, "An efficient lightweight integrated blockchain (elib) model for IoT security and privacy," *Future Generation Computer Systems*, vol. 102, pp. 1027–1037, 2020.

[148] Y. Cheng, M. Lei, S. Chen, Z. Fang, and S. Yang, "IoT security access authentication method based on blockchain," in *International Conference on Advanced Hybrid Information Processing*. Springer, 2019, pp. 229–238.

[149] J. Choi, Y. In, C. Park, S. Seok, H. Seo, and H. Kim, "Secure IoT framework and 2d architecture for end-to-end security," *The Journal of Supercomputing*, vol. 74, no. 8, pp. 3521–3535, 2018.

[150] R. Krishnamurthy, G. Rathee, and N. Jaglan, "An enhanced security mechanism through blockchain for e-polling/counting process using IoT devices," *Wireless Networks*, vol. 26, no. 4, pp. 2391–2402, 2020.

[151] P. Angin, M. B. Mert, O. Mete, A. Ramazanli, K. Sarica, and B. Gungoren, "A blockchain-based decentralized security architecture for IoT," in *International Conference on Internet of Things*. Springer, 2018, pp. 3–18.

[152] Z. Bao, W. Shi, D. He, and K.-K. R. Chood, "IoTchain: A three-tier blockchain-based IoT security architecture," *arXiv preprint arXiv:1806.02008*, 2018.

[153] R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S. A. Kondaveeti, and S. Shekhar, "Continuous security in IoT using blockchain," in *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2018, pp. 6423–6427.

[154] W. Yang, H. Wang, Y. Wan, Y. Cao, Z. Zhang, and S. Chen, "A security architecture for internet of things based on blockchain," in *International Conference on Blockchain and Trustworthy Systems*. Springer, 2019, pp. 363–368.

[155] M. A. El-Dosuky and G. H. Eladl, "Spainchain: security, privacy, and ambient intelligence in negotiation between IoT and blockchain," in *World Conference on Information Systems and Technologies*. Springer, 2019, pp. 415–425.

[156] G. Spathoulas and A. Karageorgopoulou, "Security and privacy in the internet of things using blockchain technology," in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, 2019, pp. 284–290.

[157] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng, and J. Yu, "Direct acyclic graph-based ledger for internet of things: performance and security analysis," *IEEE/ACM Transactions on Networking*, vol. 28, no. 4, pp. 1643–1656, 2020.

[158] E. Bertino, "Data privacy for IoT systems: Concepts, approaches, and research directions," in *2016 IEEE International Conference on Big Data (Big Data)*. IEEE, 2016, pp. 3645–3647.

[159] Z. Wang, X. Dong, Y. Li, L. Fang, and P. Chen, "IoT security model and performance evaluation: a blockchain approach," in *2018 International Conference on Network Infrastructure and Digital Content (IC-NIDC)*. IEEE, 2018, pp. 260–264.

[160] M. Yu, J. Zhang, J. Wang, J. Gao, T. Xu, R. Deng, Y. Zhang, and R. Yu, "Internet of things security and privacy-preserving method through nodes differentiation, concrete cluster centers, multi-signature, and blockchain," *International Journal of Distributed Sensor Networks*, vol. 14, no. 12, p. 1550147718815842, 2018.

[161] J. Li, S. Hu, Y. Shi, and C. Zhang, "A blockchain-based trustable framework for IoT data storage and access," in *International Conference on Blockchain and Trustworthy Systems*. Springer, 2019, pp. 336–349.

[162] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "IoT information sharing security mechanism based on blockchain technology," *Future Generation Computer Systems*, vol. 101, pp. 1028–1040, 2019.

[163] M. Barati and O. Rana, "Enhancing user privacy in IoT: integration of gdpr and blockchain," in *International Conference on Blockchain and Trustworthy Systems*. Springer, 2019, pp. 322–335.

[164] H.-A. Pham, T.-K. Le, T.-V. Le *et al.*, "Enhanced security of IoT data sharing management by smart contracts and blockchain," in *2019 19th International Symposium on Communications and Information Technologies (ISCIT)*. IEEE, 2019, pp. 398–403.

[165] R. K. Behera, K. H. K. Reddy, and D. S. Roy, "Reliability modelling of service oriented internet of things," in *2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions)*. IEEE, 2015, pp. 1–6.

[166] J. Lin, Z. Shen, and C. Miao, "Using blockchain technology to build trust in sharing lorawan IoT," in *Proceedings of the 2nd International Conference on Crowd Science and Engineering*, 2017, pp. 38–43.

[167] F. Casino, L. Azpilicueta, P. Lopez-Iturri, E. Aguirre, F. Falcone, and A. Solanas, "Optimized wireless channel characterization in large complex environments by hybrid ray launching-collaborative filtering approach," *IEEE Antennas and Wireless Propagation Letters*, vol. 16, pp. 780–783, 2016.

[168] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *Ieee Access*, vol. 6, pp. 115–124, 2017.

[169] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of IoT data," in *Proceedings of the 2017 on cloud computing security workshop*, 2017, pp. 45–50.

[170] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: a survey," *Future generation computer systems*, vol. 56, pp. 684–700, 2016.

[171] V. Daza, R. Di Pietro, I. Klimek, and M. Signorini, "Connect: Contextual name discovery for blockchain-based services in the IoT," in *2017 IEEE International conference on communications (ICC)*. IEEE, 2017, pp. 1–6.

[172] F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera, "Overcoming limits of blockchain for IoT applications," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, pp. 1–6.

[173] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. bft replication," in *International workshop on open problems in network security*. Springer, 2015, pp. 112–125.

[174] L. Macedo, "Blockchain for trade facilitation: Ethereum, ewtp, cos and regulatory issues," *World Customs Journal*, vol. 12, no. 2, pp. 87–94, 2018.

[175] I. Bermudez, S. Traverso, M. Mellia, and M. Munafo, "Exploring the cloud from passive measurements: The amazon aws case," in *2013 Proceedings IEEE INFOCOM*. IEEE, 2013, pp. 230–234.

[176] O. Avan-Nomayo. (2018) Bitcoin Transactions Per Second Approaching All-Time High. [Online]. Available: https://bitcoinist.com/bitcoin-transactions-per-second-approaching-all-time-high/

[177] C. M. Cap. (2021) Coin Market Cap. [Online]. Available: https://coinmarketcap.com

[178] E. M. Tenorio. (2021) Advantages and disadvantages of Blockchain. [Online]. Available: https://www.bbva.ch/en/news/advantages-and-disadvantages-of-blockchain/

[179] A. Network, "Worldwide infrastructure security report," 2015.

[180] S. Walston, Y. Al-Harbi, and B. Al-Omar, "The changing face of healthcare in saudi arabia," *Annals of Saudi medicine*, vol. 28, no. 4, pp. 243–250, 2008.

[181] B. Jannadi, H. Alshammari, A. Khan, and R. Hussain, "Current structure and future challenges for the healthcare system in saudi arabia," *Asia Pacific Journal of Health Management*, vol. 3, no. 1, pp. 43–50, 2008.

[182] F. M. Albejaidi, "Healthcare system in saudi arabia: an analysis of structure, total quality management and future challenges," *Journal of Alternative Perspectives in the Social Sciences*, vol. 2, no. 2, pp. 794–818, 2010.

[183] Vision2030. (2020) Health Sector Transformation Program. [Online]. Available: https://www.vision2030.gov.sa/v2030/vrps/hstp/