Palestine Polytechnic University
Deanship of Graduate Studies and Scientific Research
Master of informatics

Framework For Securing Automatic Meter Reading Using Blockchain Technology

Submitted by:

Esraa Dbabseh

Thesis submitted in partial fulfillment of requirements of the degree Master of Science in Informatics
January, 2021

The undersigned hereby certify that they have read, examined and recommended to the Deanship of Graduate Studies and Scientific Research at Palestine Polytechnic University the approval of a thesis entitled: **Framework For Securing Automatic Meter Reading Using Blockchain Technology**, submitted by **Esraa Dbabseh** in partial fulfillment of the requirements for the degree of Master in Informatics.

Graduate Advisory Committee:

Dr. Radwan Tahboub (Supervisor), Palestine Polytechnic University.

Signature:_____ Date:_____

Dr._____(Supervisor), Palestine Polytechnic University.

Signature:_____ Date:_____

Dr._____(Internal committee member), Palestine Polytechnic University.

Signature:_____ Date:_____

Dr._____(External committee member), ...University.

Signature:_____ Date:_____

Thesis Approved

Dr. Murad Abu Subaih
Dean of Graduate Studies and Scientific Research
Palestine Polytechnic University

Signature:_____ Date:_____

DECLARATION

I declare that the Master Thesis entitled **"Framework For Securing Automatic Meter Reading Using Blockchain Technology"** is my original work, and hereby certify that unless stated, all work contained within this thesis is my own independent research and has not been submitted for the award of any other degree at any institution, except where due acknowledgement is made in the text.

Esraa M. Dbabseh

Signature:_____ Date:_____

STATEMENT OF

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for the master degree in Informatics at Palestine Polytechnic University, I agree that the library shall make it available to borrowers under rules of the library.

Brief quotations from this thesis are allowable without special permission, provided that accurate acknowledgement of the source is made.

Permission for extensive quotation from, reproduction, or publication of this thesis may be granted by my main supervisor, or in his absence, by the Dean of Graduate Studies and Scientific Research when, in the opinion of either, the proposed use of the material is for scholarly purposes.

Any coping or use of the material in this thesis for financial gain shall not be allowed without my written permission.

Esraa M. Dbabseh

Signature:_____ Date:_____

الملخص

قراءة العدادات التلقائية AMR من اهم القضايا الموجودة في المدن الذكية و الحديثة. تعاني كثير من شركات الكهرباء من انعدام الامن و وجود الكثير من المشاكل في العدادات. اكثر الهجمات شيوعا هجوم denial of service الذي يهدد جميع المستخدمين، كما يهدد بشكل اساسي امن البيانات و كذلك تخزين البيانات و توافر البيانات و العدادات الذكية في الشبكة. من الهجمات الاخرى التي تؤثر على شبكة العدادات الذكية هجوم man in the middle الذي يؤثر صحة البيانات و سلامتها. يمكن استخدام انترنت الاشياء Internet of Things (IoT) لتحقيق AMR فعالة و موثوقة في الوقت الفعلي.

تعتبر مشكلة الامان حرجة و مهمة جدا في نظام AMR . Blockchain هي تكنولوجيا و تقنية متطورة للغاية يمكن استخدامها لتأمين الكثير من الانظمة مثل قراءة العدادات و التحكم فيها. يعنمد Blockchain على فكرة تسلسل البيانات بطريقة امنة و موزعة.كذلك يعتمد Blockchain الامان الذي تمثل البيانات في Blocks الموجودة في سلاسل (قراءة العدادات على سبيل المثال). يتم انشاء Blocks و التحقق منها بواسطة العديد من الاجهزة الموزعة في الشبكة. يمكن تنفيذ تطبيقات Blockchain بأستخدام العديد من اللغات مثل Ethereum .

في هذا البحث سوف نقدم قراءة جديدة للعدادات بأستخدام تقنية Blockchain لتلبية متطلبات الامان الكاملة لانظمة AMR . تظهر النتائج ان الحلول المقترحة

تحقق القدرة على منع هذه الهجمات عندما تم إطلاق هجوم DDoS ، لم تستجب هذه الخوادم لطلبات المهاجم ، لذلك لم تؤثر هذه الطلبات على البيانات نفسها ، لكن سرعة استجابة شبكة blockchain للمعاملات الواردة من الخوادم انخفضت بشكل طفيف للغاية. كذلك لم يؤثر هجوم MiM على العمل المقترح. نظرًا لأن المهاجم لم يتمكن من فهم طبيعة البيانات الواردة من العدادات ولم يتمكن أيضًا من تغيير البيانات المحفوظة داخل شبكة blockchain .بالاضافة الى ذلك، تظهر النتائج ان Blockchain يمكن ان توفر تقنية واعدة يمكنها من المشاركة في تأمين العدادات .

Abstract

The Automatic Meter Reading (AMR) for energy consumption is one of the most important issues in smart cities, as meters and electricity companies suffer from insecurity. One of the most common attacks is a denial of service attack that threatens all users as well as mainly threatens data security, storage and availability as well as the man in the middle attack affecting data validity and integrity. The Internet of Things (IoT) can be used to achieve effective and reliable AMR in real time. The security issues in such a system are critical and very important to implement in the AMR and IoT based system. Blockchain is a very advanced technology and technology that can be used to secure events and transactions such as meter readings and meter control. It is based on the idea of sequencing data blocks in a secure and distributed manner. The blockchain representing the data in each block (reading the meter for example). The block is created and verified by many devices distributed on a network. Blockchain can be implemented in various ways and environments such as the Ethereum platform. In this thesis, we will present a new automated meter reading platform using blockchain technology to meet the complete security requirements of AMR systems. When DoS attack was launched, these servers did not respond to the attacker's

requests, so these requests did not affect the data itself, but the response speed of the blockchain network to incoming transactions from the servers was reduced very slightly. And MiM attack did not affect the proposed work. As the attacker could not understand the nature of the data coming from the meters and also could not change the data saved within the blockchain network. The simulation results show that the proposed solutions achieve a reasonable detection rate for these attacks. In addition, the results show that Blockchain could provide a promising technology that can participate in securing network meters.

DEDICATION

To my family: I could never have done this without your faith, support, and constant encouragement.

ACKNOWLEDGEMENT

Many people have directly or indirectly contributed to the successful completion of this thesis. They will all be remembered in my heart. First, I would like to take this opportunity to highly appreciate my thesis supervisor Dr Radwan Tahboub, for his support and useful comments and immense knowledge.I appreciate my family encouragement especially my grate father and mother. Their support and encouragement was the reason for all the success I have made. I express my deep sense of reverence and gratitude to all of my respected teachers for their invaluable knowledge they imparted to me.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AMR	Automatic Meter Reading
IoT	Internet of Things
GSM	Global System for Mobile
SMS	Short Message Service
GPRS	General Packet Radio Service
P2C	Power to Communication
TCP	Transmission Control Protocol)
IP	Internet Protocol
SCADA	supervisory control and data acquisition
RF	Radio Frequency
SoC	System on Chip
LED	Light-Emitting Diode
NB-IoT	Narrow Band Internet of Things
DoS	Denial of Service
MiM	Man-in-the-Middle
ARP	Address Resolution Protocol

MedRec	Medical Record
RPC	Remote Procedure Call
EVM	Ethereum Virtual Machine
IDE	Integrated Development Environment
LOIC	Low Orbit Ion Cnnon
IRC	Internet Relay Chat
ICMP	Internet Control Message Protocol
SYN	synchronize
FDI	False Data Injection Attack
EVD	Eavesdropping Attack
DDoS	Distributed Denial of Service

Chapter 1

Introduction

The development of technology and the existence of the Internet play a vital role in all areas of life. One of the most important of these applications and technologies is the Automatic Meter Reading Technology (AMR). The automatic meter reading is intended for remote monitoring and controlling of the local energy meters. This technology enables regular meter reading without anyone visiting every home. The reading can be achieved with a micro-controller that continuously monitors and records the meter reading in the databases [19]. The data is transmitted by using the internet to achieve efficient and reliable AMR in real time. The safety of smart meters is one of the tasks in the world. The automatic meter reading will be the consumer friend, because it care of the problems. Automated metering uses online applications, and in recent times, online applications have a significant growth which is being developed for many purposes. These apps mostly deal with databases that must be protected because they often contain sensitive data [20]. In addition to the fact that databases store private data, they serve a large number of users. Attention needs to be focused on many attacks, single or group. Therefore, the applications should provide security and don't

allow unauthorized persons to access and read this data without knowing its details; Otherwise, the data loses its meaning and value [28] [36]. Electricity meters reading are one of the most common applications to focus on, due to the increased electricity consumption. Many companies, especially electricity companies, are looking to find solutions and methods to prevent and reduce electricity theft. There has been a lot of results aimed at sending data over the Internet of Things and storing it in the cloud and other solutions. But these solutions are still central and there is a third party controlling them[9]. One of the technologies that has appeared recently is blockchain technology that has changed a lot of applications, because it has a lot of features that makes it stand out from the rest. The most important of these features is that it is distributed and decentralized. The idea of the blockchain is a network that contains a large number of users who send transactions to each other. These transactions must be validated and all values verified before entering the blockchain. Data and transactions are accepted and added if it's validity is proved by so-called miners. Validate these transactions by solving mathematical equations that are present within each transaction. Thus, makes this technology powerful and distinct from others [53].

1.1 Problem Statement

The latest technology used in electricity meters has focused on Internet of Things technology. It depended on the Internet and each meter sends data from the meter to the server. The server stores the data in the database inside the cloud [33]. The deployment of smart meters comes as one of the main concerns for the security of information related to consumer privacy, data integrity, authentication and availability of the system for all users at anytime

who are authorized to access this network and its applications. Smart meters are the weakest when mentioning security attacks[24]. Smart meters are easy to attack, especially when these networks rely on wireless technologies. The attack launched on smart meters can cause data corruption, unavailability of service or failure to send data to the server and then to the database for storage. First of all, a denial of service attack against smart meters within the network, it has a lot of negative impacts on the network. The effect of this attack is on data validity and availability [1]. It showed that the smart meters are in response to a denial of service attack. The number of lost packets was apparent and the smart meter had become overwhelmed in response to traffic resulting from requests from the denial of service attack. When traffic increases, the smart meters may disconnect from the network. Another attack that affects the smart meters is the man in the middle attack. The results indicated that the smart meters have an impact on the network. This attack threatens data privacy as well as data validity. The attackers managed to succeed in their attacks against network meters.

1.2 Motivation

The increased security of networks has made it more difficult to penetrate server operating systems. On the other hand, methods of attacking these networks were developed. Attackers can exploit network vulnerabilities, gain access to and alter data. There is a great need to find an effective and resistant solution to these attacks, and it does not contain security flaws that make it strong and reliable. In our work, blockchain technology has been used. The emergence of blockchain technology has solved many security problems because it has many features. Blockchain is an advanced technology

and it is often used by smart technology because it combines many other advanced technologies. The combined scheme uses the blockchain to replace a centralized system with a decentralized system thus it makes the system reliable [12]. The installation of smart meters with IoT will greatly improve the smart meter network. The meters will automatically send the data to the blockchain to share with all stakeholders involved in the process and so the process becomes transparent. Blockchain uses node agreement to ensure that transactions are not tamper and cannot be altered. Consumers will have better confidence not to have their bills tampered . The blockchain will be used for automatic meter reading to make it more secure and transparent. Meter reading is transaction and verification based on pre-existing database. This provides confidence that previous readings are correct and have not been modified.

1.3 Research Objectives

This research aims to find solutions for smart energy meters, and data protections that meters have. Protecting meters from any possible attacks is one of the basic tasks that represent a problem for all users. Among the most important goals of this research were the following:

1. Understand the different issues and challenges related to securing energy and automatic meter reading systems including securing the meter readings and storage.

2. Developing an energy meter reading framework that incorporates node server in different locations in the AMR system.

3. Creating a blockchain-based model to secure smart meter networks (node servers) from many attacks.

1.4 Contributions

In this thesis , a new way to save the smart meter reading network is presented using blockchain technology, which contributes to solve many problems facing smart meters network. A summary of the contributions can be summarized as follows:

1. Identification of challenges related to securing energy automatic meter reading networks and node servers.
2. Adoption of the blockchain in the smart meter network node servers.
3. Utilizing the power of blockchain to make the energy meter reading network and transactions (readings) relevant, safe and reliable.
4. Utilizing the power of Blockchain to prevent security attacks on the smart meter network.

1.5 Research Methodology

In this thesis the methodology will be applied as follows:

1. Read the basic concepts related to blockchain technology, its characteristics, strength, and method of implementation.
2. Understand the existing smart meters and their implementation methods and their distictive features.
3. Analyze the security issues of smart meters.
4. Design a blockchain-based smart meter network between the server nodes.
5. Implement the proposed work and discuss its results.

6. Test the framework against a denial of service attack and a man in the middle attack.

1.6 Expected Publications

The following paper has been submitted and accepted for publication at ITNG2021 conference:

1. Israa Dababsa, Radwan Tahboub, "Framework For Securing Automatic Meter Reading Using Blockchain Technology". 18th International Conference on Information Technology: New Generation, April 11-14, 2021, Virtual Mode.

1.7 Thesis Organization

Chapter 2 provides an overview, introduction and background on smart energy meters, their importance, types, and consequences. It also provides a background on blockchain technology, some of its platforms, and an overview of ethereum smart contracts. Chapter 3 shows a review of many current and reference works in the field of smart meters, and describes the proposed work and research in the field of smart meter security and meter attacks and their discovery. Moreover, it shows several blockchain based approaches to security and privacy. The research methodologies selected for this thesis, how we design the research, the experimental tools used, and the expected results are presented in Chapter 4 . In Chapter Five, we proposed our framework approach for detecting and preventing denial-of-service and man-in-the-middle attacks at run time, including framework architecture and design concept, smart contract architecture, and participant node structure.

Moving to Chapter 6 that illustrates denial-of-service attacks and the man in the middle to assess our approach. The proposal along with the implementation details are revealed, then we discussed the results to show the effectiveness of our proposed work. Not to forget Chapter Seven concludes the thesis with future work, followed by references.

Chapter 2

Background

This chapter provides a background and an introduction to the automatic meter reading and its importance, after which an overview of the blockchain and its implementation methods will be presented, and then an overview of the ethereum smart contracts.

2.1 Automatic Meter Reading.

AMR technology allows the automatic collection of consumption and diagnostic data from meter. This can lead to decrease labor costs and more accurate billing. The specific way in which AMR works varies from brand to brand and system to system. Basically, the meters are equipped with sensors that register the meter automatically. These sensors then transfer the data electronically. The data is then transferred to a central database for billing and analysis, which reduces the chance of input errors. These meters help in accessing accurate and up-to-date data from meters and closely monitor and control energy costs. These meters also help solve many problems, especially in reaching remote areas that are difficult to reach periodically [29]. Electronic measurement technology (electronic measurement) has gone through

rapid technological developments and there is an increasing demand for a reliable and effective AMR system.

GSM Based AMR

The GSM network provides global coverage across countries and thus enables communication without the need to implement a new communication infrastructure for this purpose only. GSM technology also provides services such as SMS and GPRS to request and retrieve reading from homes to the power supply wirelessly. An application of this system has a GSM modem and a P2C interface card installed inside and connected externally through RS232 from which meter readings are obtained. The SMS system is used to request and retrieve energy meter readings from every home at any time and even to disconnect the electricity connection in case the bill is not paid. The user is also notified, given notes and is able to check the status of his meter from anywhere in the world using the SMS system[3].

Zigbee Based AMR

ZigBee is a set of communication protocols used to build small personal networks using low-power digital radios. The range of the mid-device based on ZigBee is limited to 10-100 meters and can be further extended using a mesh network of ZigBee devices. ZigBee digital power meter is installed in every consumer unit and electronic electricity billing system at the power supply side. The digital meter directly measures the electricity consumption. This meter's value will be sent via Zigbee transmitter. The Zigbee transmitter sends the received data from the digital meters to the central node using the Zigbee transmission protocol. Each set of wireless sensor nodes contains one central node. This central node is connected to the substation via TCP / IP. The central node collects data from all transmission terminals (readings of all meters) and converts this data into TCP / IP packets. For this purpose,

it will require converting Zigbee to TCP / IP. The data received from the end device nodes is sent to the computer using the RS 232 protocol [38].

IoT Based AMR

The Internet of Things enables object sensing and remote control over existing network infrastructure. IoT based power meter reading consists of the console and WIFI part, the control part plays a major role in the system where all information can be sent through this control unit to the other part of the system and also store information on it. WIFI part performs IoT operation according to controller. The control unit in the meters reads the data on the meter panel. After that, the data is sent to the central console, which is usually from a cloud. The data is sent via the internet and stored in the database.

2.2 Blockchain

Cryptographic technologies are based on the science of cryptography, which protects sensitive information that cryptographic techniques use to restrict behavior instead of using trusted third parties. Blockchain is a series of continuous data records called blocks that are linked together and secured with cryptography. Based on a peer-to-peer topology, the blockchain is a distributed ledger technology that allows data to be stored globally on thousands of servers while allowing anyone on the network to view anyone else's entries in nearly real time. This makes it difficult for a single user to control the network. Encryption technologies rely on cryptography, which protects sensitive information that cryptographic techniques use to restrict behavior rather than using trusted third parties. Blockchain technology ensures that the problem of double spending is eliminated, with the help of public key

cryptography. Each agent is assigned a private key that remains confidential as a password and a public key shared with all other agents. A blockchain begins when the user sends transaction to other user and transactions are enabled, although they can be tracked, but are anonymous. Public keys are cryptographically generated addresses stored in the blockchain. The amazing feature of blockchain is that public keys are never associated with a real-world identity.

Blockchain is a chain of blocks. When we say "block" and "chain" we are actually talking about digital information stored in the database. Existing blocks are precisely digital pieces of information. The blockchain is a decentralized network that contains a shared, unchanging authority ledger, which means that the information inside the authority ledger is open and available to all. The blockchain network is transparent and this feature makes its reliable [39]. This technology, is an easy way to pass information in a completely secure way. The block is created and verified by thousands of devices distributed on the network. It is added to the previous group of chains and stored across the network as shown in figure 2.1 If someone wants to forge a single transaction, they are forced to change the entire previous chain and this is almost impossible. So the data is not changeable and the database is managed using a peer-to-peer network.

The block is made in batches of encrypted and hashed transactions in the Merkle Tree as shown in Figure 2.2. Each block contains a timestamp and is connected to the chain by saving the hash of the previous block [31]. Merkle tree use the SAH 256 hash function. As shown in Figure 2.3 the cryptographic hash function takes a block of input data, creates smaller outputs and converts it to a fixed and unpredictable length. The hash function is designed so that there is no shortcut to obtain the desired output[47].And

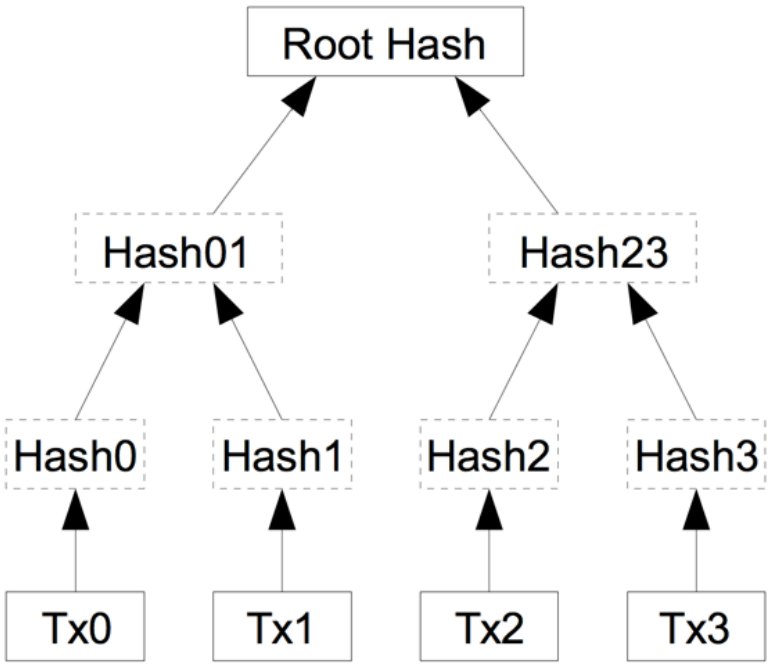

Figure 2.1: Transactions Hashed in a Merkle Tree. Image Source [35].

making it more secure, that each hash is associated with the previous hash as shown in the Merkle Tree.

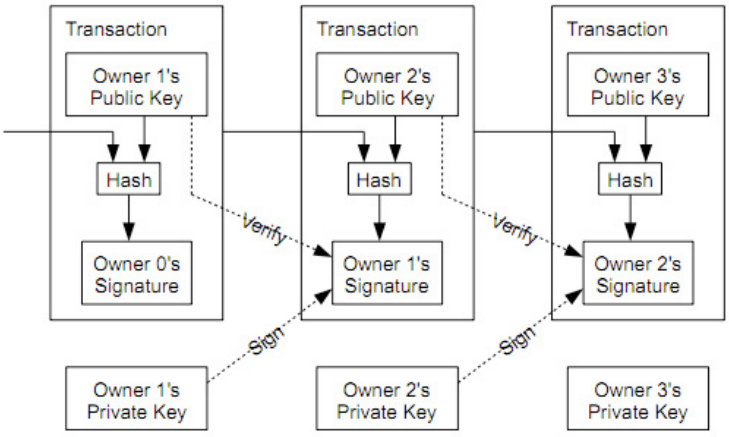

Figure 2.2: Transaction Chain in Blockchain. Image Source [35]

Blockchain is a decentralized application that cannot be tampered with

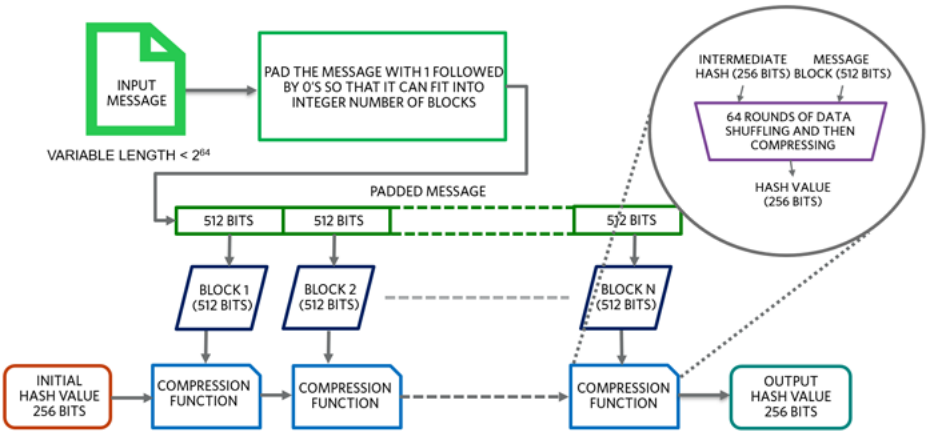

Figure 2.3: Block Diagram of a SHA-256

but like centralized applications that a malicious user can access a computer. If the attacker wants to control the network, he must have at least 0.51 network devices and chain copies that are distributed in all network devices. Adding blocks after verification by miners who verify the validity of the transactions issued by the participating devices through a consensus algorithm. The miner performs the computation associated with each transaction included in a block, resulting in an updated state. When a miner successfully miners a block, he broadcasts the block to the blockchain network. Then all nodes verify the validity of the transaction and accept the block as valid, add the new block to their copy of the blockchain, and move to another block. Miners receive a reward when they solve a complex math problem associated with each transaction[35].

2.3 Ethereum

Ethereum is a decentralized computing platform. It generates a cryptocurrency token known as Ether. Ethereum was released in 2015 and is open source software for major chains used in cryptocurrencies and ether. It enables the creation and operation of smart contracts and distributed ap-

plications (DApps) without any interruption, fraud, control or interference from a third party. Ethereum helps developers create and deploy distributed applications, not only because it is a platform but also a complete Turing programming language. Ether is used to pay transaction fees and the main internal encoding fuel for ethereum. There are two types of accounts: the first type is externally owned accounts that are controlled by private keys, and the second type is the contract account that is controlled by its contract code. Ethereum uses a mining method, which is an algorithm called Proof of Work algorithm[26]. Miners use this algorithm to verify the validity of a transaction before adding it to the chain of blockchain[45].

Smart Contract

Smart contracts are applications that run on the Ethereum Virtual Machine. The contracts are written in Turing-Complete bytecode, called the Ethereum Virtual Machine (EVM) bytecode [48]. A smart contract becomes like a self-running computer program, executing automatically when requirements are met. It aims to facilitate negotiation, digital execution, verification or enforcement of a contract. Smart contracts allow reliable transactions to be conducted without third parties. Since smart contracts run on the blockchain, they operate exactly as they were programmed without any possibility of censorship, downtime, fraud, or third-party interference. Every transaction can be handled by a large network of unknown individuals called miners, who verify the authenticity of every transaction issued by any user before adding that transaction to the blockchain. A user can send the contract to the blockchain as a transaction to create it, call its functions, make decisions, or even use that contract to send Ether or coins to other users. Smart contracts will continue to operate until the amount of gas runs out or there is a specific job in the contract that requires termination of the contract [10].

Chapter 3

Literature Review

Reading meters and bills are one of the complex tasks of electricity. The pre-approved method is manual meter reading; it is a person who visits every house to take the meter reading. This process takes a long time. It is also not safe and impractical to have many problems with this technology. Researchers have proposed many different technologies to make the meter reading process easier and available [17]. The various methods in this process differ from each other in terms of the nature of work. For example, some meters relied on GSM technology to transmit data[37]. Some authors suggested a second method based on SCADA, which is a system that works with encoded signals over communication channels to provide control over remote equipment [15]. The last and the most famous technology was that of relying on the Internet to transfer data. In our study, many research papers in the chapter of automatic meter reading were reviewed. In addition, papers blockchain technology were read to enhance security and privacy. Some papers that presented findings related to the security and privacy of smart meters were also discussed.

3.1 Automatic Meter Reading Techniques

In recent years, with the advancement of technology and the Internet, smart and electronic meters have been developed. Meter reader uses new technologies to read meter value on electronic screen meters. There are many different new technologies used to read meters, the most important one is that which uses Internet technology. AMR can be classified into wired and wireless systems, depending on the medium used to transmit the readings. Both systems have advantages and disadvantages. Measuring power over the wire is an expensive system because it requires a change in the infrastructure compared to wireless units. WIFI is more suitable for this type of application because WIFI has become one of the common facilities everywhere [41] [5].

Here we will talk about different techniques and methods described by the authors. Wessam et. al. [32] discuss a new way to secure meter reading against tampering or malfunction to discover and correct customer attacks that aimed to change smart meter readings. The idea of linear error-correcting block codes was used, which was used in a system of Communications to detect and correct errors in data transmission. It was suggested to use codes with some modifications in order to detect false readings in some meters that measure electrical energy. Nayan et. al. [21] proposed a new way to provide a way to recharge electricity meters remotely, so customers pay meter bills and recharge the meters by sending a message to the service provider. The automatic meter reading system that is designed consists of a simple, low-cost wireless GSM power meter and a web interface associated with it for automating billing and managing the collected data. This method transfers data and meter readings to the remote service provider using GSM. The readings are sent to the nearby central station using RF and from there to the web server using GSM as shown in figure 3.1. A GSM based wireless

communication module is incorporated with ARM to have remote access over the usage of electricity.

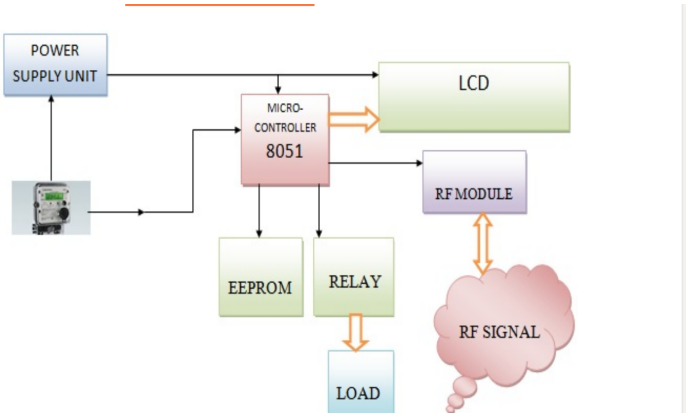

Figure 3.1: Home Communicable Unit. Image Source [21]

Karthikeyan et. al. [23] proposed a system is cost effective because it requires a simple upgrade to meters rather than a full replacement. Moreover, it is lightweight and compact with SoC's (System on chip) used to control and communicate. The figure 3.2 illustrate the system consists of a power meter, optical sensor, and NodeMCU. This part of the system is on the consumer's side. The optical sensor that is used to detect the LED flash is connected to the power meter. The wireless router is configured through an Internet connection after the authentication process is completed, the data is transferred to the cloud. The cloud is used to store data from different meters. Received data is stored in the specified variable. The main server handles data received for billing and creates alerts for clients. The server acts as a bridge of communication between clients and the main provider.

Xingyuan et. al. [16] proposed designing a new generation of meter-based meter reading system through Narrow Band Internet of Things (NB-IoT) technology. The direct connection between the power meter and the main station system was achieved. The intermediate equipment measurement station was deleted and the complexity of the platform structure was reduced.

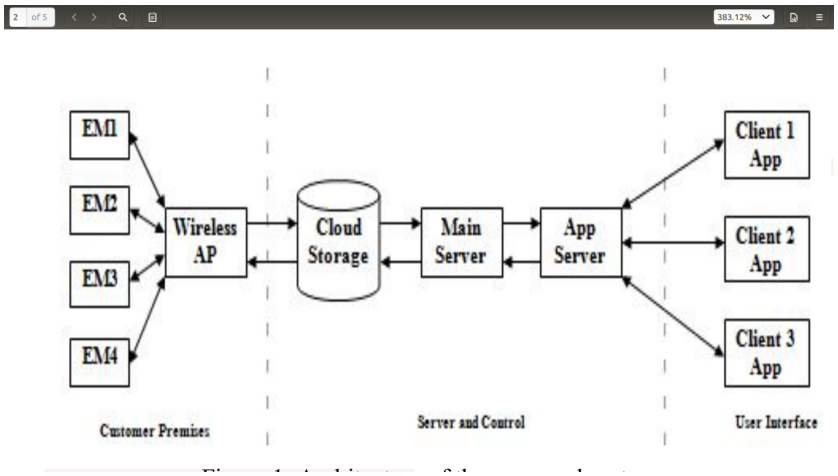

Figure 3.2: Architecture of The Proposed System. Image Source [23]

The central management and real-time monitoring capacity of the power meter was improved, and the group coverage rate was improved effectively. Also the number of connections to one base station can be increased easily. The smart meter connects directly to the NB-IoT network via a remote connection unit that supports the standard NB-IoT connection, which eliminates the link between the collector and the concentrator in the system structure as shown in the figure 3.3.

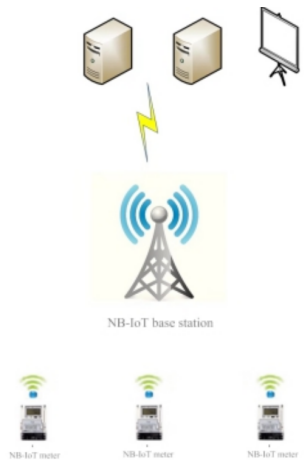

Figure 3.3: Remote meter reading application architecture based on NB-IoT. Image source [16]

Pranav et. al. [41] proposed the smart power meter is improvement

over the traditional prepaid power meter that is used today. It uses IoT technology to monitor and manage energy. Unlike traditional prepaid meters, this system provides an interactive interface for both consumers and utility companies. The system was designed to resort in a local server and database when the internet connection was resumed. In this research, as the figure 3.4 illustrate, a digital power meter consisting of blinking LED signal was used. It is coupled with a controller using Optocoupler. This microcontroller reads data and sends it to the IoT platform using the WiFi unit. Sequentially transmits data to the IoT platform for display where power meter readings can be accessed globally. The reading of energy consumed in both digital and analog format is displayed on the platform website. Energy consumption reports are generated daily and can be monitored around the clock at any time.

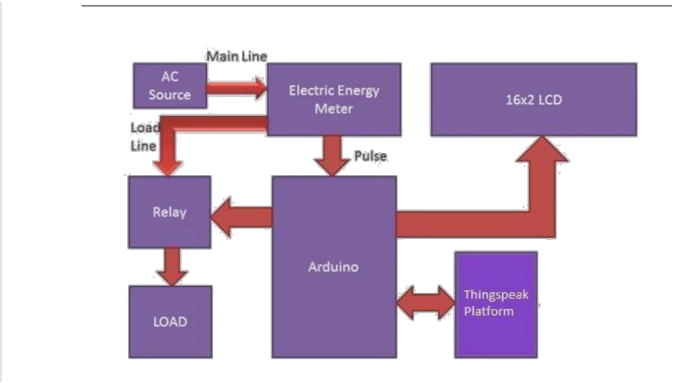

Figure 3.4: Block Diagram of IOT Based Smart Energy Meter. Image source [41]

As we can see from the studies reviewed in this section, all previous solutions and methods provided additional advantages for using smart meter tracking data to identify patterns, behaviors, and the ability to disconnect the customer from the electricity grid. However, with the deployment of smart meters, one of the major concerns comes to the security of the information regarding consumer privacy, data integrity, authentication, access control, and

system availability. This is because smart meters are the weakest link when it comes to potential security breaches. Smart meters are easily attacked from home and neighborhood networks, especially when these networks rely on wireless technologies. Since all of these solutions are centralized, there is a third party that disables them. To solve these problems, a decentralized system has been proposed which has several advantages that make it reliable. It is the use of an automatic meter reading system using the previously discussed blockchain technology.

3.2 Common Security Attacks for AMR

The Internet of Things (IoT) era has brought new challenges specifically in the areas of security and privacy. The development of smart grid energy systems and the attempt to keep pace with security and the acquisition of many advantages in many countries has led to the widespread deployment of smart meters to achieve the desired benefits. However, there are many concerns among consumers and service communities regarding information security when it comes to smart meters. All systems try to reach a high level of protection and safety. In general, the core underpinning of information security is based on Confidentiality, Integrity and Availability. These three attributes are known as the "CIA triad" as illustrated in the figure 3.5. For a security program to be considered comprehensive and complete, it must adequately address the entire CIA triad. Confidentiality is the protection of system data, resources and objects with complete confidence from unauthorized viewing and any other access. Integrity means that the data is correct and protected from unauthorized modifications to ensure its reliability and correctness. Availability means that authorized users have access to

the systems and the resources they need at any time [44].

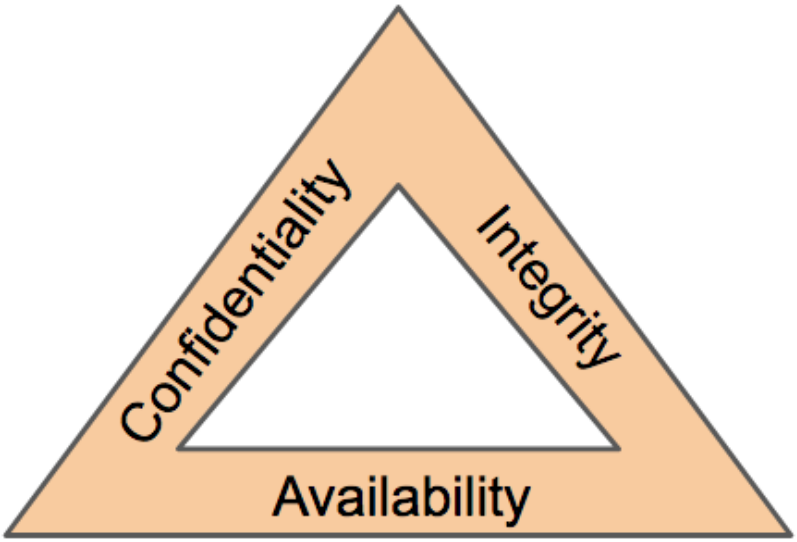

Figure 3.5: CIA Triad. Image Source [44]

Because the development of security systems, attackers try to find security holes in the new systems, where we will display some of the expected attacks on smart meters and display the results of these attacks on smart meters [25].

3.2.1 Denial of Service (DoS) Attack

Attackers may be tempted to execute a denial of service attack on a smart meter or smart grid. In any way, power outages will take a heavy toll. In this attack, the attackers send a large number of requests to the smart meter causes a malfunction. A typical DDoS attack is designed externally to shoot down a large portion or the entire target network. Competition for resources is a core issue in DoS offense and defense. If the defender has sufficient resources to measure a DoS attack, the attack will not succeed, and vice versa [30]. This demolition is usually carried out by attacking the system beyond its capabilities, and most of it relies on exploiting the security

vulnerabilities in the communication protocols used, such as TCP / IP. Ye et al.[22] explaining how a conventional DoS attack by flooding the smart meater with requests could result in the packet delivery rate dropping to 0.34. Moreover, they are introducing a new type of attack called a puppet attack which can bring the packet delivery rate up to 0.11.

3.2.2 Man in the Middle (MiM) Attack

The resilience of smart energy meters to common security attacks is one of the most common attacks that can be used as an active or passive attack[4]. In its most obvious form, the MiM attacker uses a tool to intercept network traffic between two connected parties like a smart meter and the linked server. The attacker can then perform a host of malicious actions. It's a notorious example of a smart grid topology attack. This attack occurs when an opponent intercepts network meter data from remote stations, and forms part of them, then forwards the modified version to the control center. In the absence of data alerts in modern power systems, the enemy can manage both the grid data and the meter data accurately. Khaled Shuaib's et al.[43] results showed that the attacker's host successfully redirected traffic between the smart meter and the server using ARP. In general, all experiments clearly show that the tested smart meters and related servers running the smart grid application software associated with this, it is vulnerable to common DoS attacks as well as ARP cache poisoning attack. Thus, tested smart meters and their associated servers can be easy targets of common network attacks that may provide a secure connection to exchange smart grid data.

3.2.3 Other Security Attacks

Smart home and smart meter entities could become targets for a physical attack by an adversary or even by a mischievous customer. We introduce some of the most basic scenarios of interaction between entities within the smart home or meter and discuss potential threats and their possible consequences.

Attacks threaten successful device energy consumption reporting; the smart meters within the network send the data to its central point and are able to provide detailed consumption information about the house that is connected to it. The collection and transmission of consumed data from smart home devices or meters creates a great risk to customer privacy. While transmit this data, it may happen a wiretapping attack [18], by an adversary for example, could result in valuable consumption data leaking to the adversary who can then process them to infer a lot about a customer's lifestyle. Presence information can also be inferred through traffic analysis attacks.

Meter tampering attack [2], this is a physical attack, in which the attacker successfully captures the device hardware and manually tampers with its electronic circuit. The primary motive of the attack was to change the device ID of the smart meter. By analyzing the EEPROM memory dump, the device ID was found to be stored in EEPROM itself. They replicated the ID of a different smart meter on its EEPROM, enabling the hacked smart meter to impersonate another one at the attacker's will.

3.3 Blockchain Security and Privacy

Recently, many works have been done based on blockchain concept. In this section we made a review for some of those researches that aimed to use this technology in order to enhance security and privacy. Jidian Yang et. Al [49],

proposed a trusted routing scheme using blockchain and reinforcement learning to improve the routing security and efficiency for WSNs. A practical routing scheme is introduced in order to obtain routing information for the routing nodes on the blockchain, making the routing information trackable and impossible to tamper with and alter. Blockchain based network architecture to enhance the reliability and trust of information. Blockchain is a distributed ledger with antitampering and decentralization properties, tracking information and using blockchain transactions to record information associated with each node. The information about the routing network is transferred to the blockchain network, to efficiently operate the blockchain-based routing network architecture. The routing information associated with the nodes is recorded in the smart contracts including registry nodes, token nodes, and blockchain transactions. All this content is verified by server nodes and then sent to the blockchain. Smart contracts are manipulated by authenticated server nodes and execution results are returned to the blockchain network.

Ariel Ekblaw et. al. [14] proposed in this paper , MedRec it is new decentralization management system for handling electronic records, using blockchain technology. The system provides patients with a comprehensive and stable record and easy access to their medical information across service providers and treatment sites. MedRec manages authentication, confidentiality, accountability and data sharing - critical considerations when dealing with sensitive information. The modular design integrates with suppliers' existing local data storage solutions, facilitating interoperability and making proposed system comfortable and adaptive. This system encourages medical stakeholders to participate in the network as a miners. This provides them with access to anonymous data collection as mining rewards in exchange for maintaining and securing the network via proof of work. Thus, MedRec pro-

vides large data to enable researchers while engaging patients and service providers in choosing to produce metadata. Blockchain technology supports the use of "smart contracts", which allows us to automate and track certain state transitions. Through smart contracts on the ethereum blockchain record patient-service relationships that link the medical record with display of permissions and data recovery instructions for implementation on external databases. It include log encryption hash blockchain to ensure no tampering, for ensuring data integrity. Service providers can add a new record associated with a specific patient, and patients can allow sharing records between service providers. In any case, the party receiving the new information receives an automatic notification and can verify the proposed record before accepting or rejecting the data. This makes participants aware and participate in the development of their records.

Ali Kaan Koç et. al [50] proposed an electronic voting system. They proposed electronic voting as an important topic that is related to online services. Blockchain with smart contracts appears as a good candidate for use in developing safer, cheaper, transparent and easier to evacuate systems. Ethereum and its network are one of the most suitable networks, due to their consistency, wide spread and providing smart contract logic. The electronic voting system should be safe. Also, it should not allow repeated voting and be completely transparent, while protecting the privacy of attendees. In this work, a sample of the voting application was implemented and tested as a smart contract for ethereum network using ethereum wallets and Solidity language. The Android platform also allows voting for people without Ethereum wallet. After the elections are held, the ethereum blockchain will finally keep the ballot and ballot records. Users can post their votes on an Android device or directly from their ethereum wallets, and these transaction requests

are handled unanimously from every single ethereum node. This consensus creates a transparent environment for electronic voting.

Chapter 4

Security Issues in AMR Networks

4.1 Overview of Security Issues in AMRs

The smart meter network faces many challenges in the field of information security. Many systems try to reach a high level of security. Information security is focused on the concepts of confidentiality, integrity and availability. Confidentiality is the prevent access to data or objects related to the system. Often information must be protected and preserved. The smart meter network is exposed to direct or indirect attacks to capture network traffic also to find out the data coming from the meters to the servers. This can be considered a MiM attack and Eavesdropping Attack (EVD) that breaks the confidentiality of the data in the smart meter network. MiM attack in which a malicious smart meter snatches the identity of other legitimate smart meters. By masquerading as an authorized meter to access the network, an attacker can receive and alter the content of received messages. as shown in Figure 4.1 and thus the data loses its confidentiality.

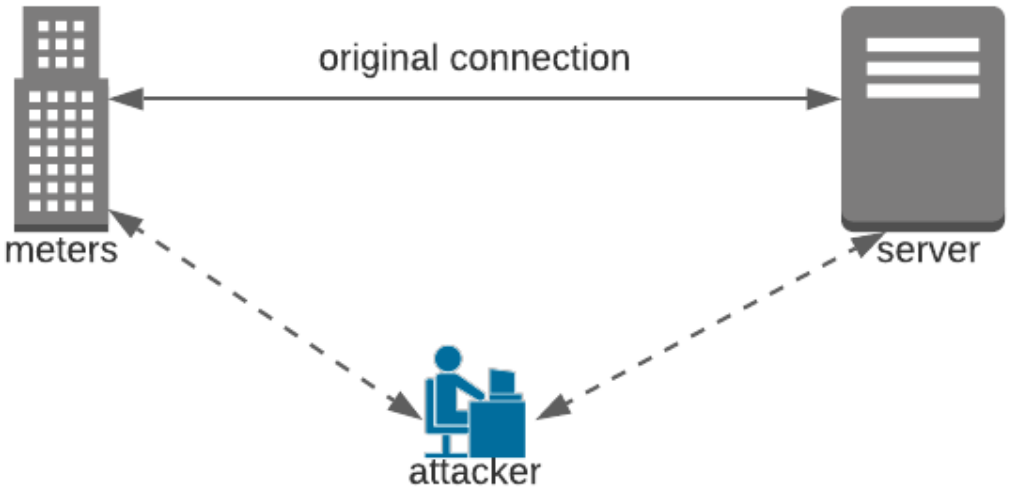

Figure 4.1: Confidentiality and MiM attack in smart meter

EVD can be defined as recording and listening for traffic between meters and servers. As shown in figure 4.2, the attack is dangerous and it depends on the motives of the attacker. This attack violates consumer privacy by analyzing the readings coming from the meters and identifying patterns of consumer behavior [7].

One of the concepts related to information security is integrity. It means protecting information from unauthorized change. These measures have an impact on the accuracy and completeness of the data. In the smart metering network, the safety of the data coming from the meters is one of the basic tasks in a network. Changing the data of the meters is one of the biggest problems facing the network, which leads to large losses in the electricity companies. False Data Injection (FDI) Attack; a type of attack that attempts to tamper with the integrity of the data by injecting wrong data into the network with the aim of misleading the control center into making a wrong decision about the billing process. This attack occurs when the attacker

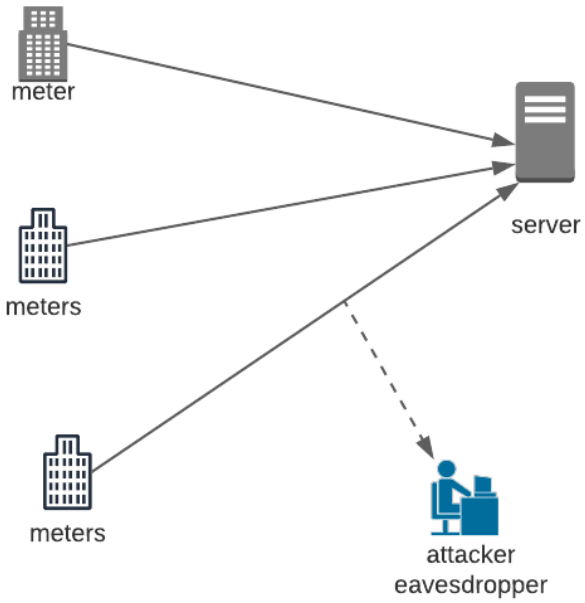

Figure 4.2: Eavesdropping Attack on Meter Network

captures data and changes it before it reaches the server. [43].

It is useful for the information system to be available to authorized users. Availability measures should protect the user's access to the system at any time he wants without interruption. The availability of the smart meter network between the meters and the servers and its response is a high priority for electricity companies. A denial of service attack is an attempt to render the system unavailable, such as denying access to a smart meters network. The attacker succeeds when consuming system or network resources. Disabling availability on servers for a short time can cause many readings to be lost. A DoS attack is that attackers frequently use to disrupt the smart meter network. As shown in Figure 4.3, the attacker, whether a meter or a malicious user, sends requests to the servers as to occupy the server with these requests and leave the requests that must be met. Thus, a number of readings coming from the meters are lost [22].

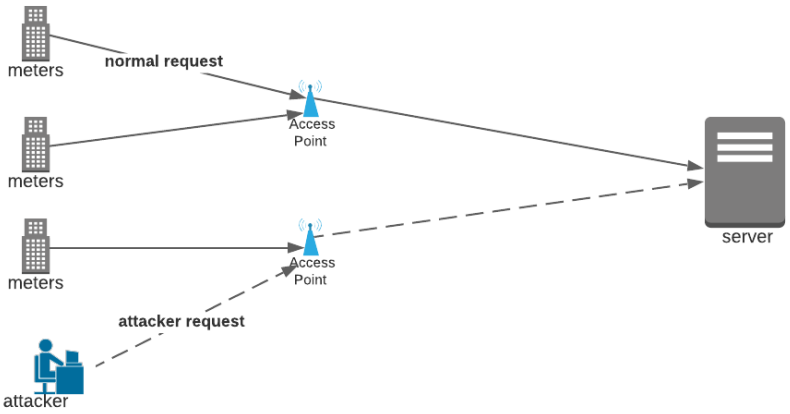

Figure 4.3: Availability and DoS Attack in AMR

SYN flood is a type of DDoS attack that occurs when an attacker sends a series of TCP sync requests to a target in an attempt to consume network resources. In a smart metered network, the attacker sends the SYN request to the server, The server then responds to each one of the connection requests and leaves an open port ready to receive the response. While the server waits for the final acknowledge packet, which never arrives, the attacker continues to send more SYN packets [40].

UDP flood, is an attack that floods the target with UDP requests similar to SYN attack, but this attack is faster. This attack does not attempt to exhaust network resources, but rather aims to consume server bandwidth and prevent access by legitimate users [51].

Replay attack resends a previously sent message. Valid data is maliciously and fraudulently duplicated. As shown in the figure 4.4 after the attacker obtained the meters data while sending it to the network, he sent it back to the server.

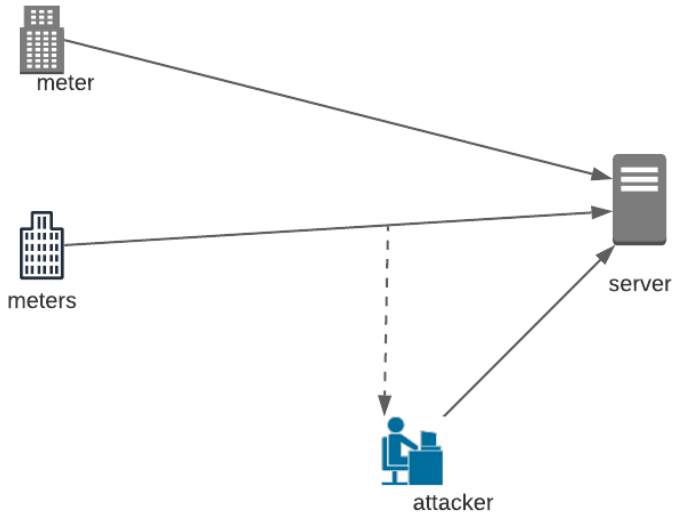

Figure 4.4: Replay Aattack on Meter Network.

4.2 Proposed Framework for Blockchain based AMR

Blockchain is the core technology that efficiently organizes and secures data to ensure its security and integrity. In our proposed work in blockchain technology, the server creates a digitally signed transaction that contains the readings coming from the meters. This transaction is sent to the miners who verify the correctness of the transaction. Miners broadcast the transaction as a block to all servers that make up the blockchain if the transaction proves to be valid. Then this data is stored in the network.

In our proposed work, meter reading was secured between server nodes in the blockchain network. Figure 4.5 shows that when an attacker attempts to write to a blockchain network, the address of the server that sent the data to the network will be verified from the addresses allowed to write to the blockchain network. Likewise, if the attacker was able to know a valid

address, he wouldn't also be able to write, because he does not have the private key of the server on which the transaction is signed. So this network will be resistant to this attack [46]. And the block header consists of a hash

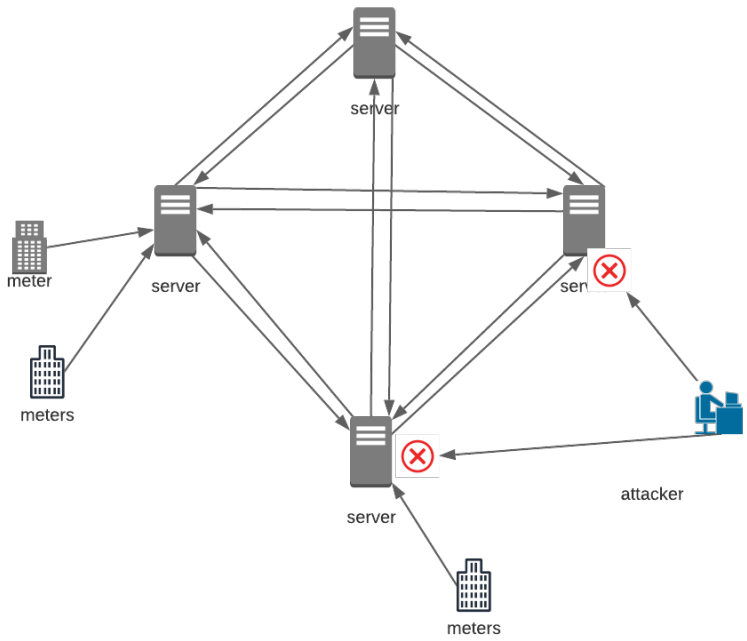

Figure 4.5: Integrity in Blockchain Meter Network.

of the last block header defined as previous hash, a timestamp, and a Merkle root of the transaction data. These blocks are form a chain. The hash of the last block header contains all of the information about the last block, which ensures the integrity of the block data. If transactions in the previous block are maliciously altered, the Merkle root of all transactions involved in that block is also changed and this is impossible [8].

The data that are sent from the servers to the blockchain network will achieve the concept of confidentiality because the data that are sent by the server to the blockchain will be in the form of a hash value by using the SHA256 algorithm its outputs are unpredictable as shown in Figure 4.6. As no one understands the nature of the data, the concept of confidentiality

won't be broken [46].

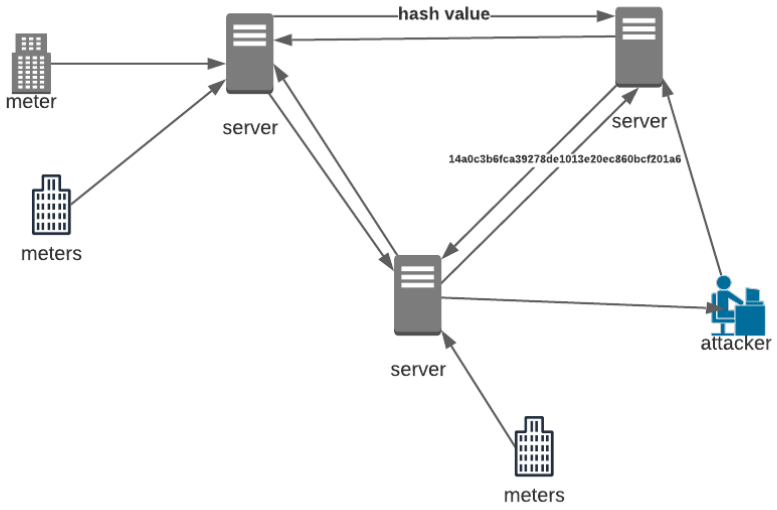

Figure 4.6: Confidentiality in Blockchain Meter Network

Since the blockchain systems are independent and do not depend on any technology, the availability in the meter network using blockchains will be ensured. For the denial of service attack to succeed, requests are sent to one node because the system is central. As the blockchain is a decentralized system linked to multiple nodes, a denial of service attack needs access to the different nodes at the same time to damage the network. This prevents denial of service attacks through the decentralization of the network[52].

Replay attack resends a previously sent message. And the data that are sent is correct, but duplicate. In a blockchain network when the attacker tries to send a previous reading saved in the blockchain network, this technology prevents this attack because every transaction (i.e. reading a meter) has an unrepeated timestamp is used. It is placed so that a distinction is made between the original (first) transaction and that no repeat transaction is accepted after it. [6].

In Table 4.1, an illustration of the various security attacks on the smart

meter network is provided. Also, how to prevent them and countermeasures have been clarified through the proposed framework using blockchain technology.

Table 4.1: Relationship Among Various Attacks on Blockchain.

attacks	Countermeasures
replay	timestamp in secure programming
MiM	digital signature and private key
EVD	encrypted data using sha256 algorithm
FDI	merkle tree and defined valid address to write in smart contract
DDoS	distributed and decentralized network

Chapter 5

Blockchain based AMR Framework Design

5.1 Introduction

In this chapter we provide an overview of the proposed framework. The proposed work focuses on the new AMR platform technology. It aims to increase confidence, security, prevent attacks and modify data in this technology. As it is evident from the studied work, many researches and technologies try to achieve these goals in discovering and preventing those actions , preserving smart meters and the safety of the readings issued by these meters, such as [32][21] [23][16][41] but as far as we know, none of them uses blockchain technology to save the data issued from the meters and store them properly and not to tamper with them by any malicious user. This thesis provides a framework that uses an established approach to maintain meter reading safety and prevent the numerous attacks. It uses an approach that combines smart meters and blockchain technology. Blockchain technology will be used to save meter readings and maintain their integrity and availability from any

alteration or tampering.

5.2 Framework Design

The proposed model aims to create a hybrid model consisting of a cluster of servers with a blockchain, in order to maintain electricity meters and read data, as well as many of the features available. This improves the safety of multiple attacks and also monitors and controls meters. In general, the Energy Authority is mainly responsible for smart meters. As Figure 5.1 shows, smart meters are distributed in cities and villages, and each group of meters belong to a specific server. In the end, all servers and companies return to the Energy Authority. The Energy Authority is solely responsible for smart meters and electricity.

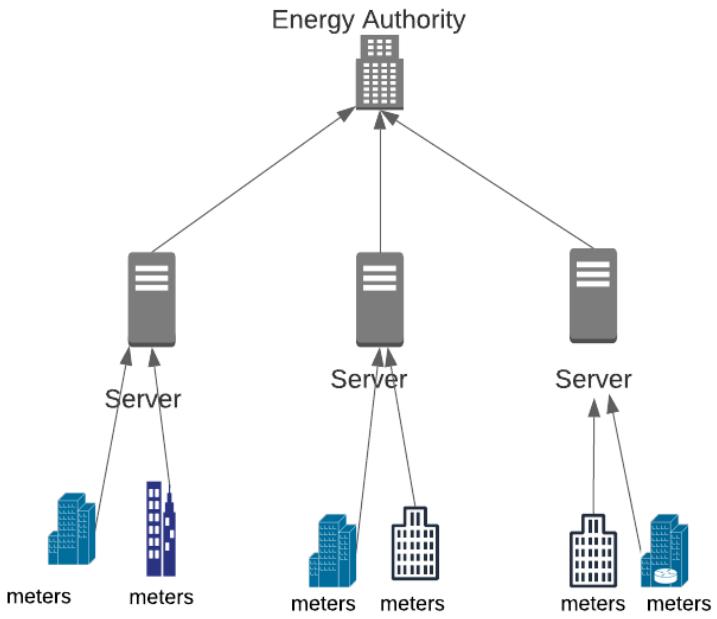

Figure 5.1: Framework For Securing Database in Electricity Company.

The proposed system, as shown in Figure 5.2, has two main components. The first is a network of smart meters distributed in the regions of customers. It consists of a control panel through which data is read and displayed on the LCD screen. The second component is the blockchain network, the data coming from the meters will be used as input to the blockchain network, whether for examination, control, or preservation. This app is used to store meter reading for all users. These components will be used to prevent multiple security attacks.

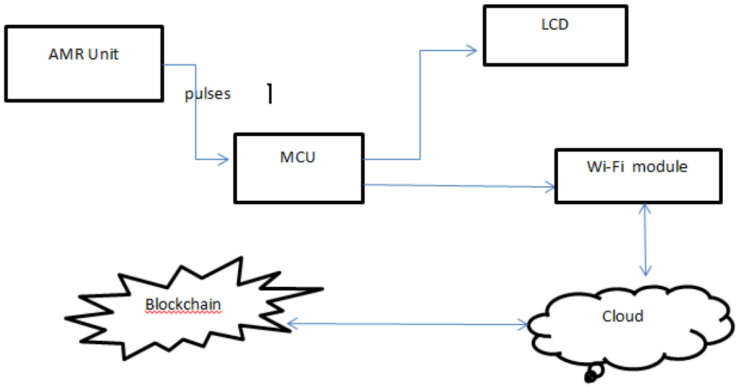

Figure 5.2: Frame Structure for Meters Networks.

5.2.1 Meters Network Layer

This layer consists of distributed smart meters. Consumption data is collected remotely from customer facilities using wireless technologies, communication lines, or satellites to process and bill the data. The meter mainly consists of an optical sensor, a controller and an LCD screen. When the optical sensor used is connected, you can detect the LED flash of the power meter. When electricity is consumed, the LED flash lights up to announce the change in the reading on the control panel, and the reading is changed

directly on the LCD screen in the meter. The data is sent to the blockchain network every specific period as server is determined. The data is sent to the blockchain network using internet technology.

5.2.2 Blockchain Layer

This layer consists of a group of servers, each server used in the blockchain network has a public and private key, as well as each user has an externally address through which data is sent and saved. By doing this, it preserves the integrity of the data and prevents the eavesdropping attack. These servers receive data from meters and store this data. Each group of meters goes back to one server to process the received data. Each reading of these meters is a transaction at the blockchain layer and it is only stored when that transaction is validated and then posted and stored if it is valid. This layer will act as a validator. This layer will first save the addresses of servers that are allowed to send data to the blockchain network, which means that any attempt to open a connection between the application server and the database server must first obtain permission from this layer. This prevented the MiM attack from being part of the network. Also, this layer will save the collected data that is coming from the servers. Which means any reading coming from the meters to the server will be entered and validated based on the previous value. We will use the ethereum blockchain platform as it is integrated into Turing's full blockchain instruction. The solidity language suites to allow smart contract programming and storage capacity to accommodate chain state. Smart contracts are codes that are maintained in ethereum blockchain accounts. These objects will be created when the smart nodes are deployed to the network. Ethereum blockchain contains code functionality and can interact with other contracts, make decisions, store data, or send Ether to

others. Smart contracts will be created to save user data. Every user need to send data to the server that must have a smart contract containing the hash value for pre-reading of all shared meters. Also, a smart contract is used as an index book that keeps all types of users side by side. These contracts may change the state of the smart contract, return a result, or transfer the value. To build this proposed model, the private blockchain must be configured for all servers and all participating nodes, such as the electricity company and the Electricity Authority in the private ethereum blockchain.

5.3 Experiment Procedures

The experimental research procedure is divided into three stages. Initially, the response time interacting with ethereum smart contracts will be measured to test the effectiveness of blockchain use in the proposed work. Second, we'll test the proposed work against a DDoS attack. Finally, we test the work against the MiM attack, EVD and FDI attack. In the proposed work, the response time interacting with smart contracts will be measured by sending a different number of transactions to the ethereum client. In our work, the first transaction was the establishment of a connection between the customer and the smart contract that was established. Another transaction is for the addresses (servers) to send data to the network to be basically saved. Also, another transaction is after creating a web application by searching for the meter data saved in the network.

In order to test a DoS attack, several methods can be used to achieve this goal. There are several DDoS attack tools that can create a distributed DoS attack against a target server, both open source (free) and commercial (paid) ones. In our experiments and simulations that we ran, an open source tool,

the LOIC tool, was used [34]. It is an easily available and free attack tool to attack the victim's website and it is one of the best tools to use in testing a denial of service attack. LOIC launched a DDoS attack using various flood methods, for example TCP, UDP, and ICMP to destroy resources like CPU time, storage, and bandwidth of the compromised host. LOIC is one of the free DDoS attack tools that helps to test network performance. It enables the creation of a DDoS attack online against any website control. Loic does not hide the IP address even if the proxy server is not working and helps you perform a stress test to verify the stability of the system. This DDoS program can be used to identify DDoS programs that hackers may use to attack the network.

To test the for MiM and EVD attacks, Wireshark was the first and most used network protocol analyzer tool in the world [42]. This program features a deep scan of hundreds of protocols, with more being added all the time, live capture, and offline analysis. It works on various operating systems such as Windows, Linux, and other platforms. This tool will be used to capture packets and know the data sent from the sender to the receiver. To test the FDI attack, Scapy will also be used as a packet processing tool for computer networks, originally written in Python[27]. We can forge or decrypt packets, wire them over the wire, capture them, and match requests and responses. It can also handle tasks such as scanning, tracking, investigation, unit tests, attacks, and network discovery. This tool will be used as an attempt to add false data to the network as well as change the network data.

5.4 Framework Architecture: Design Concept

Figure 5.3 shows an overview of the framework structure. As shown in the figure, any server must participate in the blockchain network in order to preserve the network and its data as well as obtain the benefits of using this framework. The use of blockchain within the proposed framework is to preserve data and prevent multiple attacks. The blockchain network can be public or private. A public blockchain is a network that anyone can download its protocol, read, write, and participate in the network. The public network contains data for anyone in the world to read and validate. In this network all nodes and transactions are equal, which means when transaction is validated, nothing can be changed in the public blockchain network. A private blockchain network offers the same degree of integration offered by a public blockchain network. But participants in a private blockchain network need read-write permission, dealing only with trusted nodes that participate in the private blockchain network. In addition, a private blockchain can easily create, initiate and publish transactions in the blockchain.

When a transaction is validated, it needs to be added to a block in the chain. The transaction is placed through a hash algorithm to convert it into unique numbers and letters, after which two transactions are segmented and placed through the hash algorithm to produce a new hash and so on. This is what makes segmentation unique and a major safety feature of blocks is that they work in one way. This is dealt with smart meters, whether transactions will be written or searched or otherwise. Figure 5.4 shows how the meters work with the servers in the network. We also learn that every smart meter contains a control unit and flash through which the value of the meter is changed. The data on the meter screen is read, the readings are

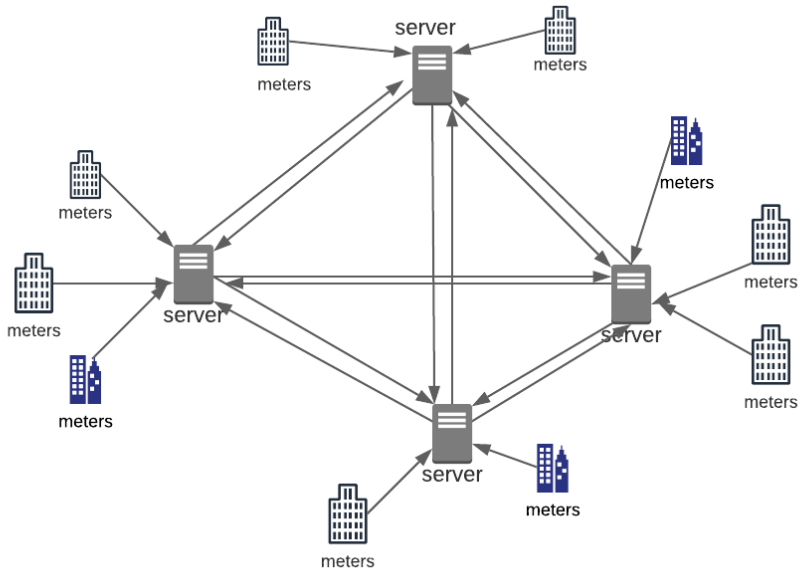

Figure 5.3: General Architecture of the Proposed Framework

sent to the server to which it belongs to every specific period of time that is determined by the server. Each server differs from another in the receiving data from the meters. The server is part of a blockchain network. One of the server's tasks is to send the received data from the meters and save it to the blockchain network. Each server stores the data in the blockchain network through transactions. In a smart contract, the addresses of servers that are allowed to read and write in the blockchain network are defined. Since the server is part of the blockchain network, each server has a unique address in the blockchain network. If the address is one of the allowed to write on the blockchain network so the data will be received from the server and stored. To increase safety of the received data from the meter to the server, it will write the data after making sure that the current reading value for this meter is greater than or equal to the previous value, in order to ensure the correctness of the upcoming data. We created a web application that enables electricity companies and responsible companies to search for

the previous values of meters at this moment.

5.5 Smart Contracts Architecture

A smart contract defines the rules between different organizations in executable code. Applications call a smart contract to create the transactions that are recorded in the ledger.

Using the blockchain network, we can turn these contracts into actionable software. Smart contracts are applications that are published in the authority book and executed independently as part of the validation of transactions. Until the smart contract is published in Ethereum, the transaction that sends the contract to the blockchain is executed and at this point, a unique address for the contract is determined by 161 bits. Once the contract is created, the address and balance are also created for it. Smart contract is written in several languages, but the language used to write nodes is solidity, which is the JavaScript language developed for writing smart contract. Solidity was chosen because it is a high-level programming language that is statically scripted, supports inheritance, multiformat, as well as having user defined libraries [11]. Figure 5.5 shows, the smart contract that was used in the proposed work. the Ethereum address has only one account that has the authority to use the contract, in order to preserve and recover the data. The use of a single account has a positive effect on securing the data contained in the contract. In this contract, addresses of users able to write into the blockchain network were identified. For example, in our reseach the server is part of the blockchain that receives data from the meters. The servers are the blockchain network users who can send the data to the smart contract and which has to save the data as a hashed chain in the blockchain. In the

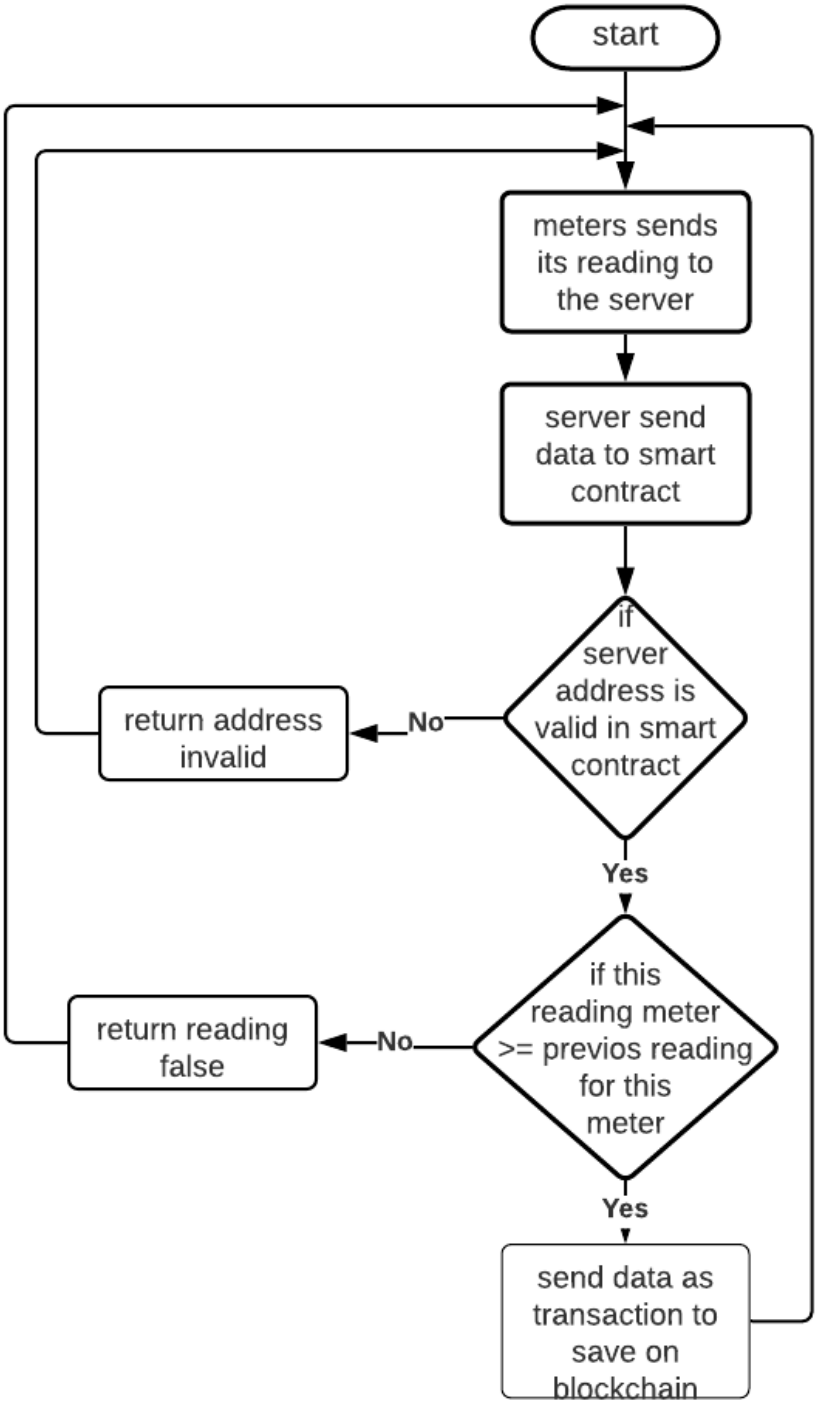

Figure 5.4: Flow Chart for Meter Network.

Ethereum blockchain, the SAH256 hash function is used. The cryptographic hash function takes a block of input data, creates smaller outputs and converts it to a fixed and unpredictable length. The hash function is designed so that there is no shortcut to obtain the desired output. This becomes critical when you are dealing with a massive amount of data and transactions. As shown in Figure 5.6, after confirming the validity of the transaction, the data is entered into the algorithm, to convert the data to the hash value. Each hash value is associated with the previous hash value, as shown in the figure.

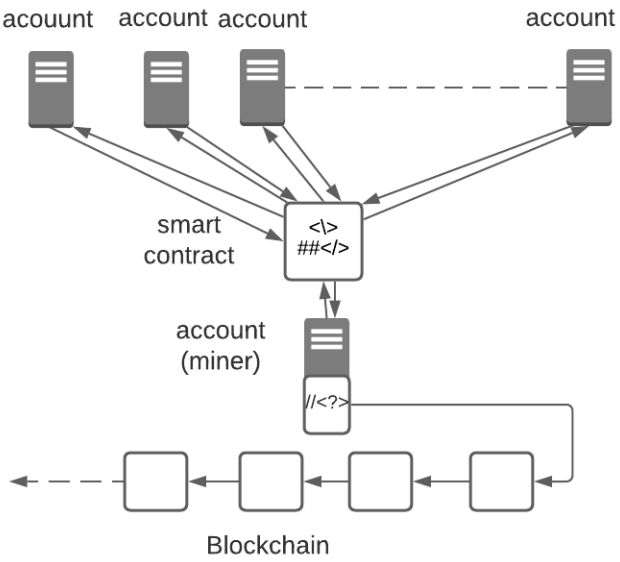

Figure 5.5: Smart Contracts Architecture

5.6 The Nodes Involved in The Proposed Framework

The proposed framework consists of many nodes connected to the blockchain network. These participating nodes may be a server, the electricity company, or smart meter. A prototype is made for the simulation purposes. This model

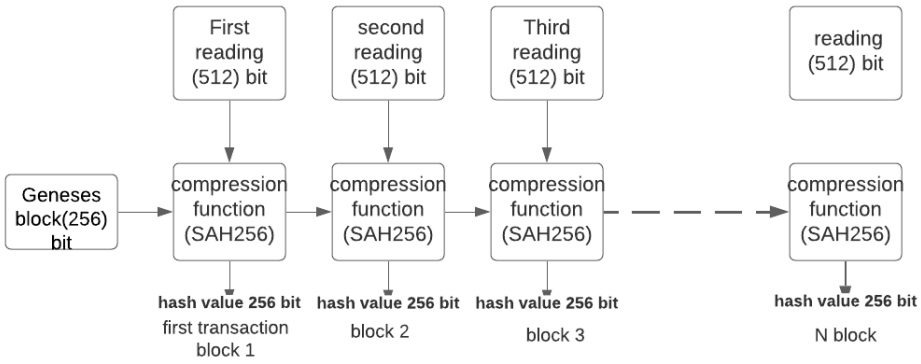

Figure 5.6: Use SHA256 to Store Readings in the Blockchain Network.

uses the special blockchain. In a blockchain, the nodes must begin with a custom block called Geneses block or block 0, which is the first one in the blockchain network. The participating servers are the primary nodes in the proposed work, they are the ones that receive data from meters and save it. This is the main reason and the first source for saving meter data in the blockchain network and preserves it from modification or change. As the data within the blockchain network can't be modified or added from an address that is not allowed to write on the network. Other nodes can be shared to work as miners in the blockchain. In addition to any other nodes that participate to maintain the network. Every node participating in the blockchain network has a copy of the blockchain data called Ledger. The blockchain works as a database that contains contracts, nodes, rules and permissions that restrict the use of the blockchain network. Servers are peers that are connected as peer-to-peer. The nodes have a variety of tasks such as saving a local copy of the blockchain, connecting to the Ethereum blockchain, sending and receiving transactions, in addition to encrypting transactions. To start the Ethereum Blockchain node, the node must contain Geth which acts as a client node for the Ethereum. The remote procedure

call (RPC) should be called via HTTP through a library web3.py. To execute the contract in Ethereum, a solidity compiler should be used as a compiler IDE based on Remix that can be combined with an Ethereum client.

Chapter 6

Proposed Framework Implementation and Results

6.1 Introduction

This chapter explains the practical approach to implement a smart meter network through a blockchain. To demonstrate the effectiveness of the proposed framework, it is adapted to prototype for testing. The results are discussed at the end of the chapter. The remainder of this chapter is organized as follows. Section 6.2 introduces the tools used in test models. Section 6.3 describes implementation of the proposed framework. Section 6.4 describes executing attacks on the proposed framework model and its results. Section 6.5 examines the implementation of the smart contract.

6.2 Experimental Tools

This section provides a simple introduction to the tools and models used to test the proposed action in both a DoS, MIM, EVD and FDI attacks. The following sections provide more details on the forms used. The server that is

used for this experiments is a desktop with 4GB DDR3 RAM and an Intel i3 processor.

6.2.1 Experimental DDoS Attack Tool

To test the proposed model in the event of a denial of service attack, the LOIC tool was used on the smart meter network. Blockchain network overload tested as well as denial of service attacks and distributed denial of service attacks. This tool floods the smart meter network (servers) with unwanted TCP, UDP, and HTTP requests in order to disable the service and make it unavailable. For the attack to succeed, the thousands of users must coordinate and direct simultaneous traffic on the network. One computer can't create enough TCP, UDP, and HTTP requests simultaneously. It takes a lot of computers all pointing to one location to have a real impact. Internet Relay Chat (IRC) enables LOIC and IRC to communicate. This feature allows anyone with a computer to participate in an anonymous attack and send a copy to an IRC server.

6.2.2 Experimental MiM, EVD and FDI Attack Tool

To test the proposed framework in the event of a MiM attack, a wireshark tool was used, which is a network packet sniffing tool. This tool enables to capture packets and data in real time using a variety of different interfaces. The tool analyzes, sorts, and exports data to other tools if it is needed. This tool is also used to troubleshoot network errors, which can be corrected by security professionals. Wireshark is a powerful and highly configurable tool for transmitting packet data. Scapy was used for FDI attack which is a Python program that can be used as part of sending packets to the network and forging them. It is also a powerful interactive packet processing program,

capable of forming and decoding packets of a large number of protocols and sending them. It provides us with the ability to modify network packets, allowing us to use an existing network protocol and define its parameters based on our needs.

6.3 Implementation of The Framework

This section explains the practical approach and the implementation of the blockchain network on the prototypes used. Also, it demonstrates the effectiveness of the proposed framework and present response time and Latency on Transaction. Latency is the time taken to transmit a packet over the network. The proposed framework present the response time in writing the meter data and validating this transaction by the server. Response time is the total amount of time it takes to respond to a request for data; meaning the number of transactions that are sent by the server to the blockchain network in a given unit of time.

The main concerns of this research are writing on the blockchain network and reading from that network when needed, and it is used to describe the readings that should be performed during the system's operating time. Whenever an attempt is made to implement writing or to make a connection to a blockchain network to read through specific addresses that are permitted to interact with this network, which are specified in the smart contract. Then these readings are sent after checking the addresses and comparing the current data with the previous one for this meter, the decision is to establish a connection to execute this transaction depends on the result returned from the ethereum blockchain. In this framework, the app connects directly to private ethereum. It connects by using Web3.py; It is a group of libraries

that allow an application to interact with a local or remote ethereum node.

Table 6.1: Response Time for Writing Data to The Proposed Smart Contract.

number of transaction	time(sec)
1	.27
100	19.5
200	41.07
300	61.98
400	82.72
500	90.5

At the start the ethereum blockchain Private Network was configured. Then the proposed contracts are also published in that blockchain. Using Web3.py, a new web application is created to interact with the ethereum blockchain to inquire about its meters and readings. The aim of this experiment was to measure throughput and response time of the system when deploying a contract, sending data as a transaction to the blockchain network, and storing this data. For this set of experiments, we published a special contract measuring response time and latency. Since this work is based on ethereum smart contracts, a new experiment is underway to evaluate the response time for reading the proposed smart contract. Table 6.1 shows the response time for writing smart contract data. The results showed that the response time was relatively acceptable in the experiment. On the other hand, in a true application server environment, the hardware specifications will be much more than the device used in our experience. This will positively enhance the response time.

Figure 6.1 and 6.2 illustrates measures of response time and latency for meter writing readings into a blockchain network. These results were for a simple sample of readings from the meters and written on the blockchain

network.

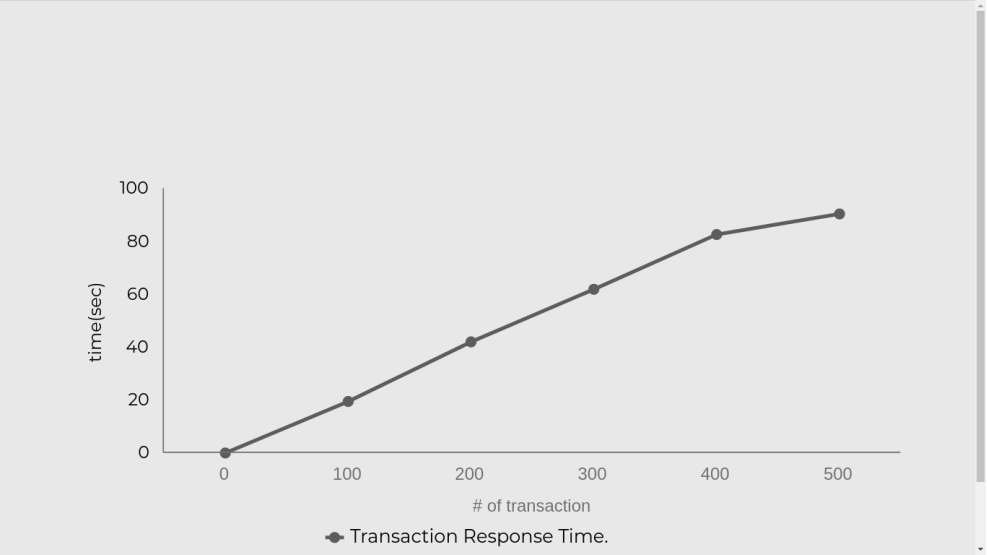

Figure 6.1: Transaction Response Time.

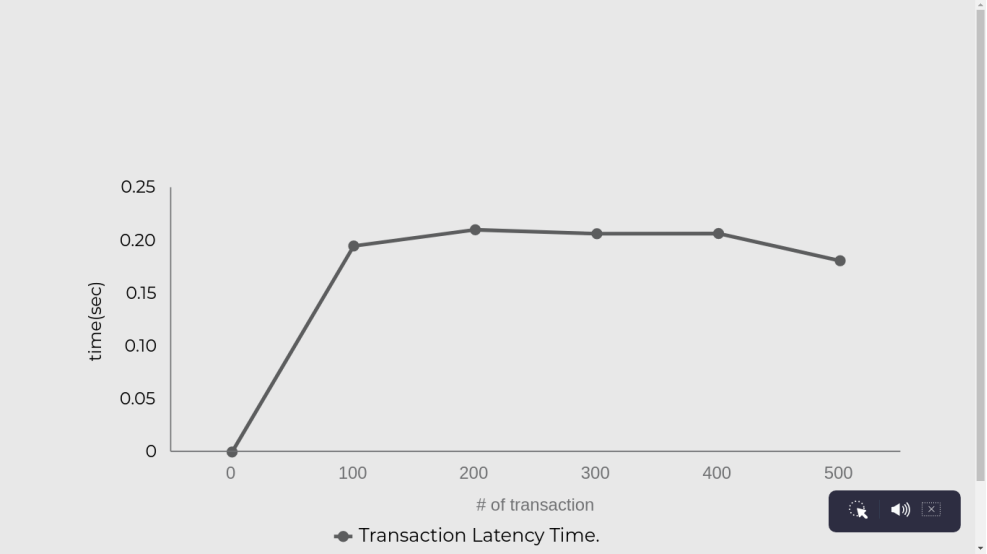

Figure 6.2: Transaction Latency

6.4 Experiment Results

To test the proposed framework, experiments were conducted with the types of attacks that were previously explained that are DDoS, MiM, EVD and FDI attacks. The following sections describe the results of the experiments

in more details.

6.4.1 DDoS Experiment Results.

Before adapting the proposed framework, the prototype of the smart meter system was tested against a denial of service attack. The test results are shown in Figure 6.3, which shows a screen shot showing the results of the attack for other previous working [22]. As shown in the figure, the system can be attacked with the Packet generator tool and make the meter grid completely insecure. Hence, readings can be delayed or lost. From the figure, you can see how many packets have been lost. As a result, this happened because the communication between the smart meters and the servers was established with vulnerabilities. These vulnerabilities are exploited to attack meters or the entire database. The Packet generator or LOIC tool sends a large number of requests to flood the network with these requests and the result of this, the network is unavailable and a number of data are lost.

In our experiment, we studied the effect of the aforementioned common DoS attacks on the performance of servers connected with smart meters. The experiment was conducted by launching DoS attacks on servers, and then studied their strength against such attacks by analyzing their response time and their ability to communicate with the smart server while under attack. Packet generation tools can be used to build traffic or attack packets. For example, LOIC was used here. This tool performs a DoS attack by sending too many random data in the form of UDP, TCP or HTTP to the blockchain network to be lost. The tool allows its users three types of the attack, and of course the attack varies according to the protocol used: HTTP, UDP, and TCP protocols. The large numbers of packets are created per second and sent to servers. These types of the attacks can be launched either singly or

simultaneously by the same attacking host causing more serious impact.

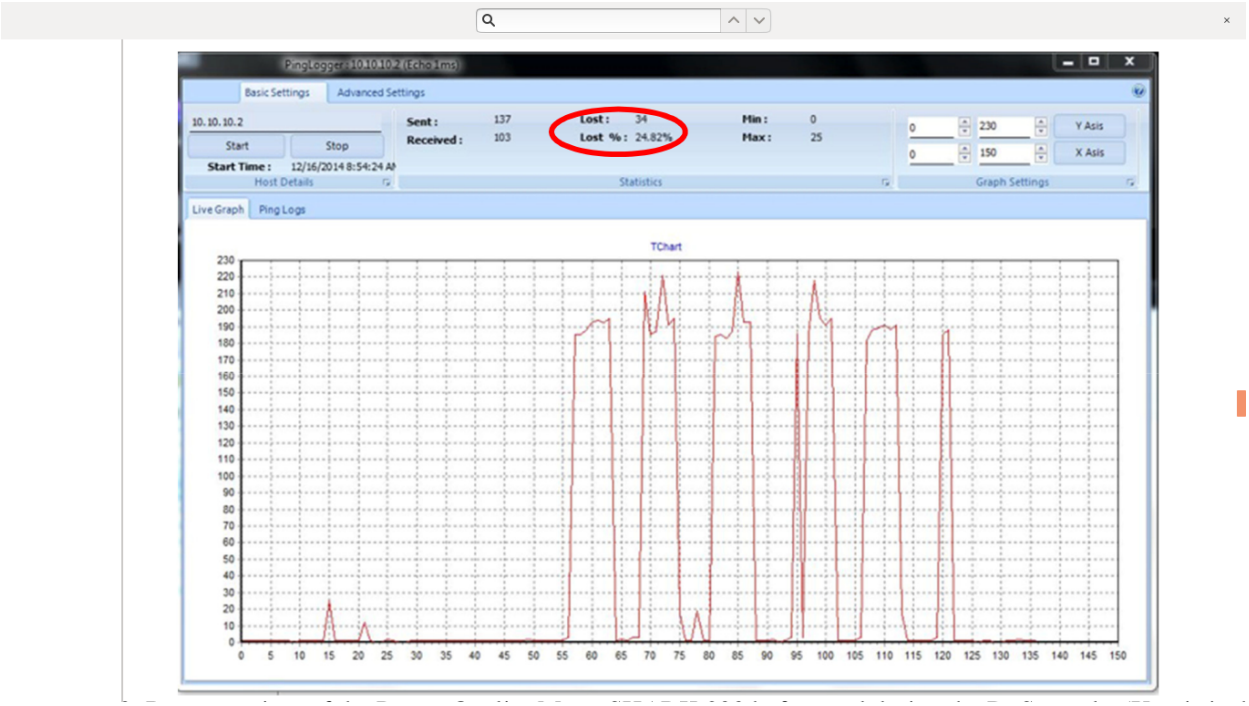

Figure 6.3: Data Traffic From The Server to The Blockchain Network. Image Resource [22].

Table 6.2: Response Time Writing Data to The Proposed Smart Contract With SYN Flood DDoS Attack.

of transaction	time(sec)
1	.4
100	29.04
200	54.1
300	79.8
400	104.5
500	131.5

Table 6.2 shows the response time for writing smart contract data with a SYN flood attack. When using the LOIC tool, TCP requests are sent to the smart meter network. The results also show that there is a slow de-

lay in writing data on the blockchain network. This is because this attack sends TCP requests, and the attacker is expected to send acknowledge to the connection, but there will not be acknowledge to drain network resources. Therefore, there is a delay for the data to arrive to the network.

Figure 6.4 and 6.5 illustrate the effect of SYN flood DDoS on transactions on a blockchain network, and the results of the experiments have also clearly shown that DDoS attacks had little effect on network performance. In short, after the DoS attack was launched, requests were sent in bulk to the blockchain network. However, the responses from these servers to requests were very slow as these requests did not affect the data itself as shown in the figure 6.6 but rather the speed of the blockchain network's response to the transactions received from the servers is decreased. It affects on the response time and latency of the network. Also, this delay in response time was not significant and had no effects the blockchain network as shown in previous research [13]. For example, figure 6.4 shows the effects of the DDoS attacks were launched. The response times were less than 0.4 ms before the DoS attacks. when testing SYN flood response times, they increased normally. This is because the network became overwhelmed trying to respond to the flood of attack traffic.

Table 6.3 shows the response time for writing smart contract data with a UDP flood attack. Whereas, using the LOIC tool, UDP requests are sent to the smart meter network. The results also show that there is a slight delay in writing data on the blockchain network. However, this delay is less than the delay resulting from the SYN flood attack because this attack aims to consume network bandwidth and does not wait for any acknowledge from

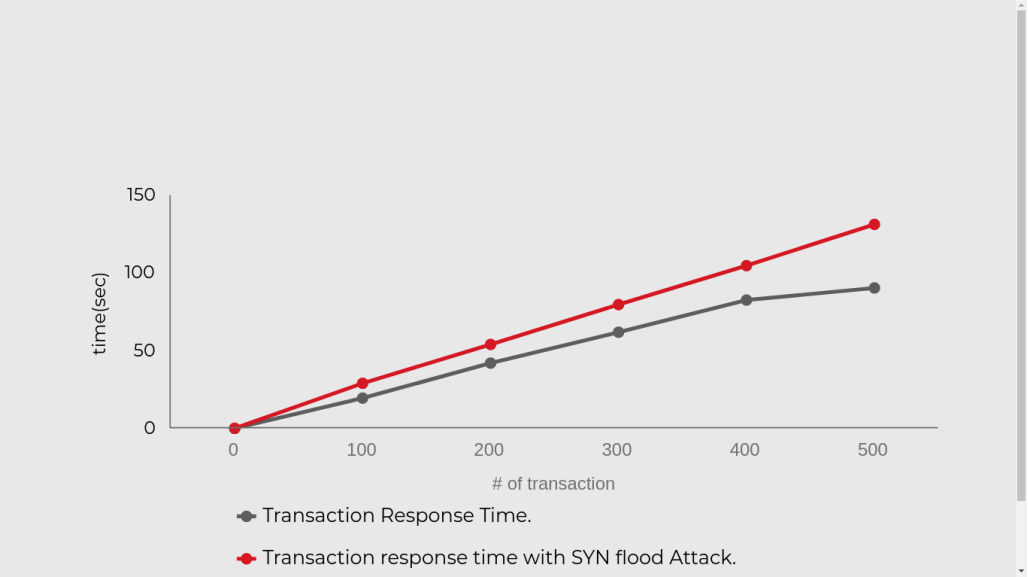

Figure 6.4: Transaction response time with SYN flood Attack

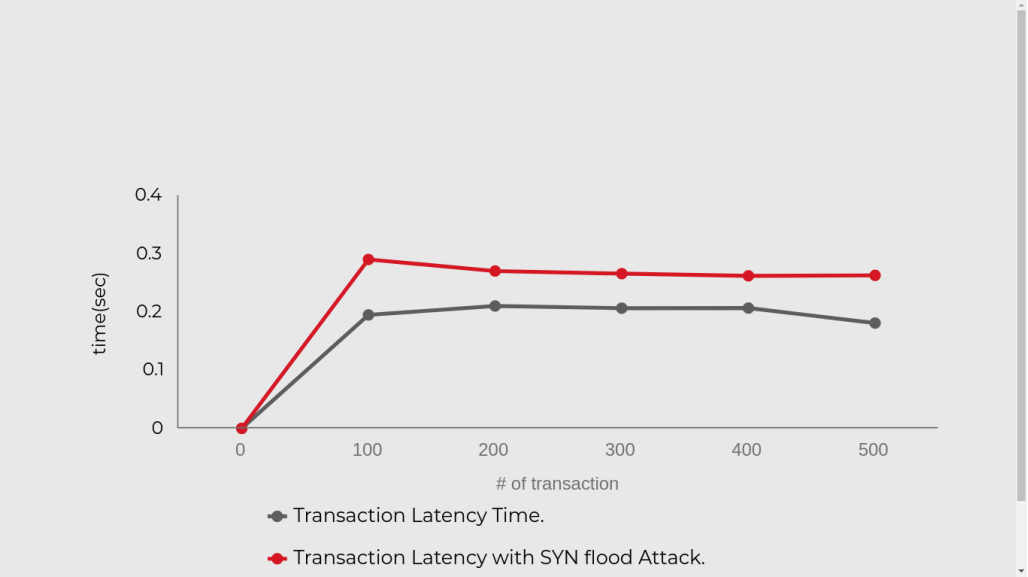

Figure 6.5: Transaction Latency with SYN flood Attack.

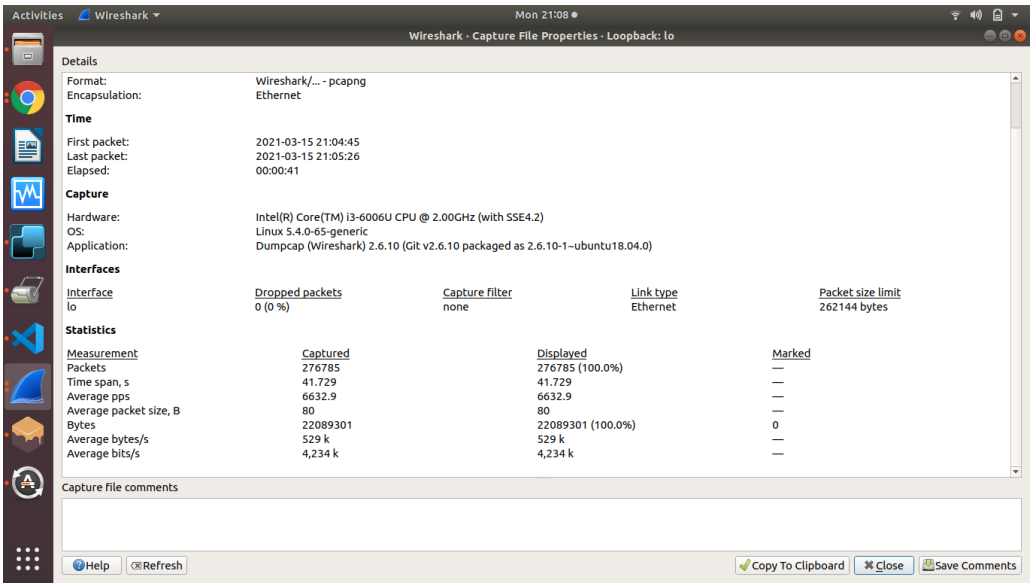

Figure 6.6: Data Traffic From The Server to The Blockchain Network with SYN Flood

Table 6.3: Response Time Writing Data to The Proposed Smart Contract With UDP Flood Attack.

number of transaction	time(sec)
1	.35
100	23.3
200	47.5
300	73.77
400	100.06
500	123.72

the attacker to connect.

Figures 6.7 and 6.8 illustrate the effect of UDP flood on transactions on the blockchain network in response time and Latency. The results of the experiments also clearly showed that these attacks had little effect on network performance. In short, after the DoS attack started, the responses from these servers to the requests were very slow because these requests did not affect the data itself, meaning that no reading was lost as shown in Figure 6.9.

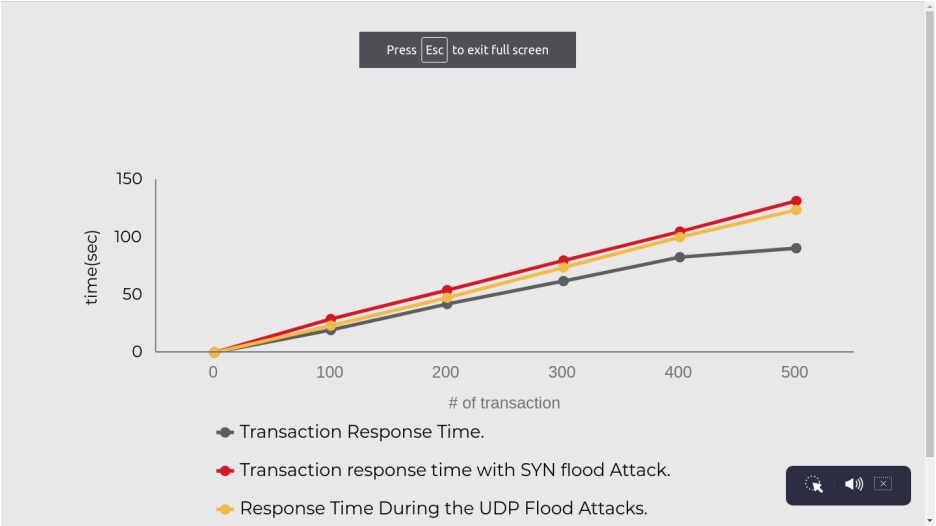

Figure 6.7: Response Time During the UDP Flood Attacks.

Figure 6.8: Transaction latency During the UDP Flood Attacks.

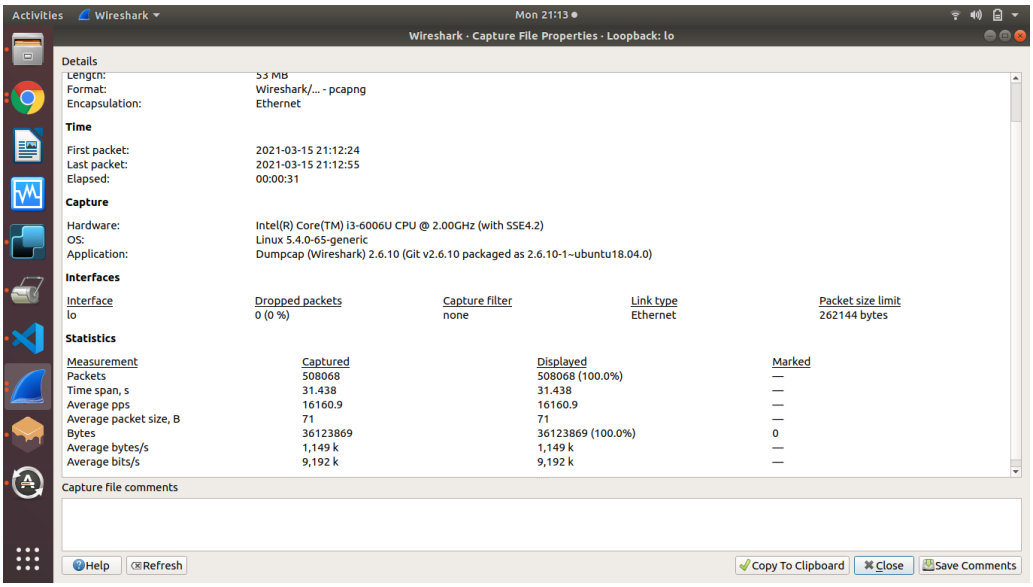

Figure 6.9: Data Traffic From The Server to The Blockchain Network with UDP Flood

6.4.2 MiM, EVD and FDI Experiment Results.

The results in previous researches [43] showed that the MiM attack on smart meters was successful, which makes the smart meter network insecure, so the data that is sent is readable by the attacker who can modify and add new data to the network. In our experience, we studied the effect of MIM, EVD and FDI attacks between servers and the blockchain network. The wireshark tool was used to capture packets sent from servers to the blockchain network. The results showed that data can be seen, but as it appears in figure 6.10, the attacker cannot be part of the smart meter network, it cannot know who is the sender or the receiver. Likewise, it is impossible to know the private key of each of the sender or receiver and this action will be successful in preventing a MiM attack. Also, as shown in the figure, the attacker cannot eavesdrop on the captured data because the data is encrypted using the SHA256 algorithm. The output of this algorithm cannot be predicted as this algorithm is nonrecoverable. However, the data cannot be eavesdropped, so

our work maintained the confidentiality of the data.

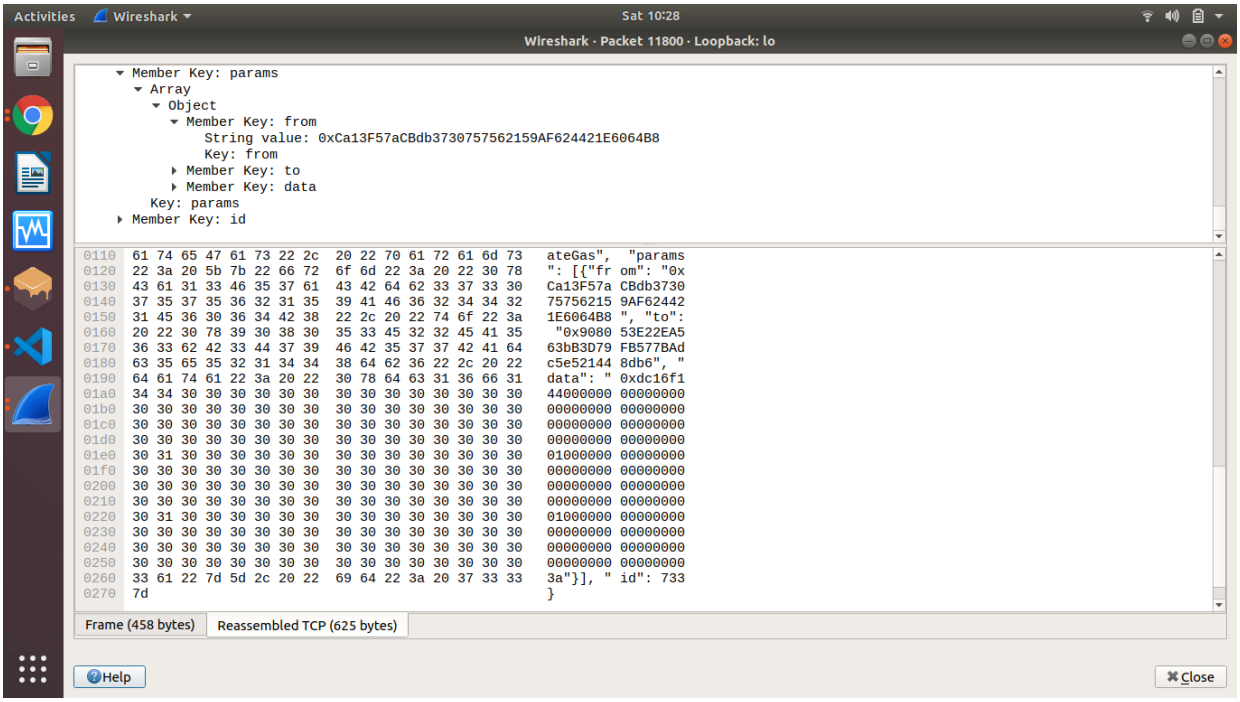

Figure 6.10: Data Captured by The Attacker.

A new experiment was conducted in an attempt to write on the blockchain network by FDI attack, it impersonates the sender's address and sends data to the receiver in order to change the integrity of the data and add new data. But as figure 6.11 shows, the results of FDI attack has failed. The attacker could not write on the blockchain network or change data.

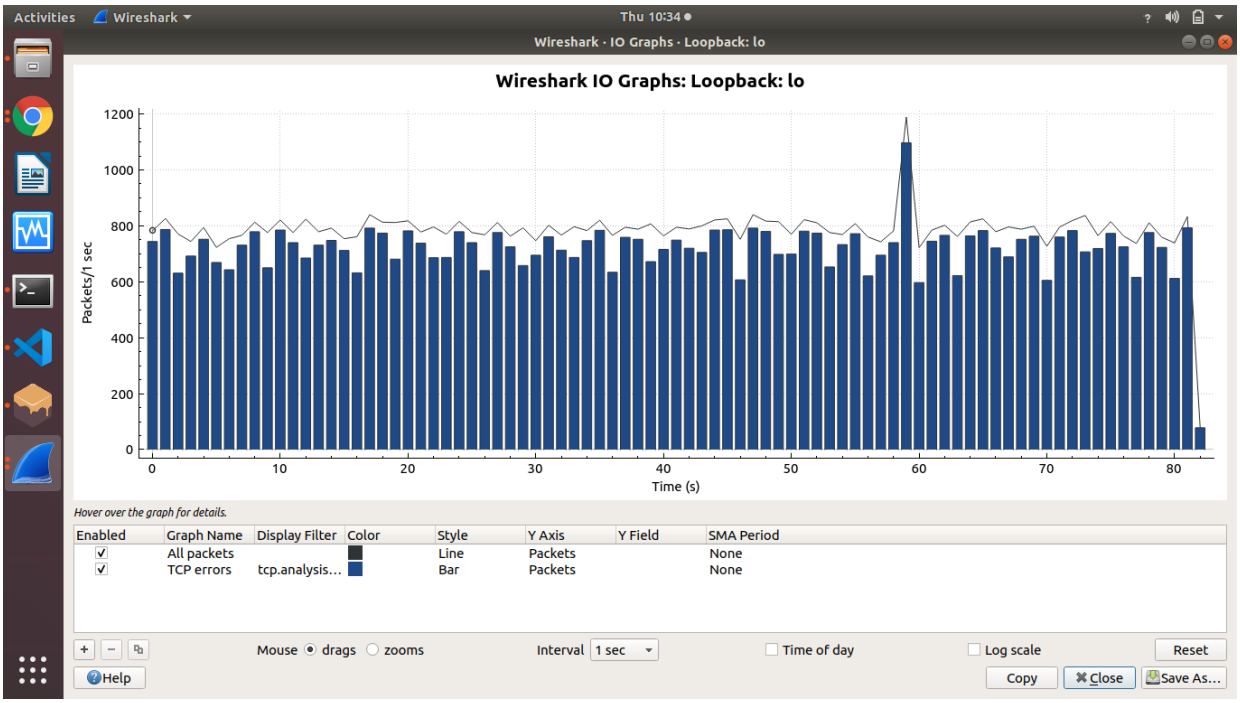

Figure 6.11: FDI Attack by Try to Add New Data Using Scapy.

6.5 Summary

After the framework was adapted in both attacks, the results showed that the attacks used were unsuccessful. This framework demonstrates that it is reliable, effective, and can be used to prevent denial of service and man-in-the-middle attacks. This improves the use of the smart meter network, whether for the user or for the electricity companies. In addition, the use of blockchain will add more security in the face of such attacks, and it will not affect the overall server response time because based on the results, blockchain has a good response time.

Chapter 7

Conclusion and Future Work

Smart meters are an essential part of smart cities. With continuous technical improvements, consumers will be able to choose flexible systems, actively participate in the electricity system, and save energy. If decentralized ledger techniques are applied, there may be multiple paths to enable consumers and energy companies to regulate financial transactions. Blockchain technology enables a transparent system of how to access critical data without threatening privacy issues and craft incentives for everyone to accelerate technology deployment. In this research we create a blockchain network that receives data from meters and sends it to servers, and then send the data to the blockchain network. Besides, we implement every server with an address in the ethereum network. It is through these addresses that data is sent and saved in the blockchain network. Blockchains are chains open to everyone who can read them. Transactions live in mempool before miner puts them in blocks. Generally, no one controls the blockchain so no one can go back to and change the data. As we saw in the results we cannot influence this network through the attacks, mainly because the networks are being paired and there is no need to trust the devices with each other, without a central

point of failure. When miners are found, there is no need for central authority to tie one node with another or associate a user with access to another machine.

The proposed work relies on the ethereum blockchain smart contract that is used to save data from the addresses that are allowed to be used for saving that were previously defined in the smart contract. The results also showed that this is done by checking the list of addresses allowed to write on the network. This step is done within the proposed smart contracts that sending the data by addresses for writing to the network. It is verified whether this address is authorized to write or not and positively affects the elimination of many attacks. The data is saved in the blockchain network using SHA256 algorithm, which makes the network and data strong and hard to break. The results also showed when testing the proposed work for a denial of service attack, no data was lost. This is because the network is decentralized and the blockchain network is linked to multiple servers and these servers must be accessed by the attacker at the same time. In addition, the man in the middle attack did not succeed either in understanding the data or changing or adding new data. This is because the attacker's address is not one of the addresses authorized to write to the network, and the server data is written in the form of a hash value and cannot be predicted or retrieved. Moreover, it showed that the use of Blockchain provides a new secure technology to save this sensitive information among other methods used to improve security in the smart meter network, and the response time to read data from the proposed contracts providing acceptable results. On the other hand, the time consumed must be investigated when testing against denial of service attack. Further papers might study this parameter and the effects that led to an increase in the response time writing data when the number of requests

increased. In addition to studying the implementation of the blockchain network in smart meters and studying the effects of this proposal in terms of safety and security.

Bibliography

[1] Yousef MAH Akbar. *Intrusion Detection of Flooding DoS Attacks on Emulated Smart Meters*. PhD thesis, Virginia Tech, 2020.

[2] Orlando Arias, Kelvin Ly, and Yier Jin. Security and privacy in iot era. In *Smart Sensors at the IoT Frontier*, pages 351–378. Springer, 2017.

[3] K Ashna and Sudhish N George. Gsm based automatic energy meter reading system with instant billing. In *2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s)*, pages 65–72. IEEE, 2013.

[4] Bharat Bhushan, G Sahoo, and Amit Kumar Rai. Man-in-the-middle attack in wireless and computer networking—a review. In *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)*, pages 1–6. IEEE, 2017.

[5] Prachi Bramhe, Akshay Sarode, Vicky Bonde, Rachana Mankar, Ayushi Kesharwani, and Samiksha Dhengale. Automatic electric meter reading using wifi. 2019.

[6] Nutthakorn Chalaemwongwan and Werasak Kurutach. A practical national digital id framework on blockchain (nidbc). In *2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, pages 497–500. IEEE, 2018.

[7] Dong Chen, Sean Barker, Adarsh Subbaswamy, David Irwin, and Prashant Shenoy. Non-intrusive occupancy monitoring using smart meters. In *Proceedings of the 5th ACM Workshop on Embedded Systems For Energy-Efficient Buildings*, pages 1–8, 2013.

[8] Moon Kyoung Choi, Chan Yeob Yeun, and Poong Hyun Seong. A novel monitoring system for the data integrity of reactor protection system using blockchain technology. *IEEE Access*, 8:118732–118740, 2020.

[9] Amruta Chore, Prasad Mali, Dinesh Vyanjane, and Vijay Karewar. Iot based smart electricity meter and billing system. *Int Res J Eng Technol (IRJET)*, 5, 2018.

[10] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and smart contracts for the internet of things. *Ieee Access*, 4:2292–2303, 2016.

[11] Chris Dannen. *Introducing Ethereum and solidity*, volume 1. Springer, 2017.

[12] Maria Luisa Di Silvestre, Pierluigi Gallo, Josep M Guerrero, Rossano Musca, Eleonora Riva Sanseverino, Giuseppe Sciumè, Juan C Vásquez, and Gaetano Zizzo. Blockchain for power systems: Current trends and future applications. *Renewable and Sustainable Energy Reviews*, 119:109585, 2020.

[13] Napolitano S Dusi , S Longo, and S Niccolini. A closer look at thin-client connections: Statistical application identification for qoe detection. *Communications Magazine IEEE*, 50.

[14] Ariel Ekblaw, Asaph Azaria, John D Halamka, and Andrew Lippman. A case study for blockchain in healthcare: "medrec" prototype for electronic health records and medical research data. In *Proceedings of IEEE open & big data conference*, volume 13, page 13, 2016.

[15] Florentina Magda Enescu and Nicu Bizon. Scada applications for electric power system. In *Reactive Power Control in AC Power Systems*, pages 561–609. Springer, 2017.

[16] Xingyuan Fan, Chun Zhou, Ying Sun, Jinyang Du, and Ying Zhao. Research on remote meter reading scheme and iot smart energy meter based on nb-iot technology. In *Journal of Physics: Conference Series*, volume 1187, page 022064. IOP Publishing, 2019.

[17] Elias Farah and Isam Shahrour. Smart water for leakage detection: Feedback about the use of automated meter reading technology. In *2017 Sensors Networks Smart and Emerging Technologies (SENSET)*, pages 1–4. IEEE, 2017.

[18] Isaac Ghansah. *Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks: Interim Project Report*. California Energy Commission, 2012.

[19] R Govindarajan, S Meikandasivam, and D Vijayakumar. Cloud computing based smart energy monitoring system. *International Journal of Scientific and Technology Research*, 8(10):886–890, 2019.

[20] Jay Greenspan and Brad Bulger. *MySQL/PHP database applications*. John Wiley & Sons, Inc., 2001.

[21] Nayan Gupta and Deepali Shukla. Design of embedded based automated meter reading system for real time processing. In *2016 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, pages 1–6. IEEE, 2016.

[22] Musaab Hasan, Farkhund Iqbal, Patrick CK Hung, Benjamin CM Fung, and Laura Rafferty. A security study for smart metering systems. *World Academy of Science, Engineering and Technology, International Journal of Urban and Civil Engineering*, 5(1):1–11, 2018.

[23] S Karthikeyan and PTV Bhuvaneswari. Iot based real-time residential energy meter monitoring system. In *2017 Trends in Industrial Measurement and Automation (TIMA)*, pages 1–5. IEEE, 2017.

[24] Tarek Khalifa, Kshirasagar Naik, and Amiya Nayak. A survey of communication protocols for automatic meter reading applications. *IEEE communications surveys & tutorials*, 13(2):168–182, 2010.

[25] Asad Masood Khattak, Salam Ismail Khanji, and Wajahat Ali Khan. Smart meter security: Vulnerabilities, threat impacts, and countermeasures. In *International Conference on Ubiquitous Information Management and Communication*, pages 554–562. Springer, 2019.

[26] Aggelos Kiayias and Dionysis Zindros. Proof-of-work sidechains. In *International Conference on Financial Cryptography and Data Security*, pages 21–34. Springer, 2019.

[27] Tiago H Kobayashi, Aguinaldo B Batista, Agostinho M Brito, and Paulo S Motta Pires. Using a packet manipulation tool for security analysis of industrial network protocols. In *2007 IEEE Conference on Emerging Technologies and Factory Automation (EFTA 2007)*, pages 744–747. IEEE, 2007.

[28] George Cristian Lazaroiu and Mariacristina Roscia. Blockchain and smart metering towards sustainable prosumers. In *2018 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM)*, pages 550–555. IEEE, 2018.

[29] Wen-xin LEI, Yi-xin JIANG, WEN Hong, Ai-dong XU, MING Zhe, Wen-jing HOU, and Yu-jun YIN. New features of automatic meter reading system: Based on edge computing. *DEStech Transactions on Environment, Energy and Earth Sciences*, (icepe), 2019.

[30] Tasnuva Mahjabin, Yang Xiao, Guang Sun, and Wangdong Jiang. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, 13(12):1550147717741463, 2017.

[31] Ralph C Merkle. A digital signature based on a conventional encryption function. In *Conference on the theory and application of cryptographic techniques*, pages 369–378. Springer, 1987.

[32] Wessam Mesbah. Securing smart electricity meters against customer attacks. *IEEE Transactions on Smart Grid*, 9(1):101–110, 2016.

[33] Shishir Muralidhara, Niharika Hegde, and PM Rekha. An internet of things-based smart energy meter for monitoring device-level consumption of energy. *Computers & Electrical Engineering*, 87:106772, 2020.

[34] Bharti Nagpal, Pratima Sharma, Naresh Chauhan, and Angel Panesar. Ddos tools: Classification, analysis and comparison. In *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 342–346. IEEE, 2015.

[35] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot, 2019.

[36] Oscar Novo. Blockchain meets iot: An architecture for scalable access management in iot. *IEEE Internet of Things Journal*, 5(2):1184–1195, 2018.

[37] Kennedy O Okokpujie, A Abayomi-Alli, O Abayomi-Alli, M Odusami, Imhade P Okokpujie, and OA Akinola. An automated energy meter reading system using gsm technology. 2017.

[38] Sarang D Patil, SN Pawar, and ME EC JNEC Aurangbad. Wireless amr system using zigbee technology. *International of Engineering Research & Technology*, 2(3):107–115, 2012.

[39] Marc Pilkington. Blockchain technology: principles and applications. In *Research handbook on digital transformations*. Edward Elgar Publishing, 2016.

[40] Gilang Ramadhan, Yusuf Kurniawan, and Chang-Soo Kim. Design of tcp syn flood ddos attack detection using artificial immune systems. In *2016 6th International Conference on System Engineering and Technology (ICSET)*, pages 72–76. IEEE, 2016.

[41] Birendrakumar Sahani, Tejashree Ravi, Akibjaved Tamboli, and Ranjeet Pisal. Iot based smart energy meter. *International Research Journal of Engineering and Technology (IRJET)*, 4(04):96–102, 2017.

[42] Praful Saxena and Sandeep Kumar Sharma. Analysis of network traffic by using packet sniffing tool: Wireshark. *International Journal of Advance Research, Ideas and Innovations in Technology*, 3(6):804–808, 2017.

[43] Khaled Shuaib, Zouheir Trabelsi, Mohammed Abed-Hafez, Ahmed M Gaouda, and Mahmoud Alahmad. Resiliency of smart power meters to common security attacks. In *ANT/SEIT*, pages 145–152, 2015.

[44] Michael G Solomon and Mike Chapple. *Information security illuminated*. Jones & Bartlett Publishers, 2004.

[45] Dejan Vujičić, Dijana Jagodić, and Siniša Ranić. Blockchain technology, bitcoin, and ethereum: A brief overview. In *2018 17th international symposium infoteh-jahorina (infoteh)*, pages 1–6. IEEE, 2018.

[46] Merrill Warkentin and Craig Orgeron. Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management*, page 102090, 2020.

[47] Gilbert M Wolrich, Kirk S Yap, James D Guilford, Vinodh Gopal, and Sean M Gulley. Instruction set for message scheduling of sha256 algorithm, September 16 2014. US Patent 8,838,997.

[48] Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.

[49] Jidian Yang, Shiwen He, Yang Xu, Linweiya Chen, and Ju Ren. A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks. *Sensors*, 19(4):970, 2019.

[50] Emre Yavuz, Ali Kaan Koç, Umut Can Çabuk, and Gökhan Dalkılıç. Towards secure e-voting using ethereum blockchain. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pages 1–7. IEEE, 2018.

[51] Mohd Azahari Mohd Yusof, Fakariah Hani Mohd Ali, and Mohamad Yusof Darus. Detection and defense algorithms of different types of ddos attacks. *International Journal of Engineering and Technology*, 9(5):410, 2017.

[52] Rui Zhang, Rui Xue, and Ling Liu. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, 52(3):1–34, 2019.

[53] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. IEEE, 2017.

Chapter 8

appendix

Framework For Securing AutomaticMeter Reading Using BlockchainTechnology.