QATAR UNIVERSITY

COLLEGE OF ENGINEERING

# BLOCKCHAIN TECHNOLOGY AND REPUTATION SYSTEM FOR SMART GRIDS TO ADDRESS CYBER-ATTACKS

BY

MAHDI KHALAF ALKAEED

A Thesis Submitted to

the College of Engineering

in Partial Fulfillment of the Requirements for the Degree of

Masters of Science in Computing

January 2021

# COMMITTEE PAGE

The members of the Committee approve the Thesis of
Mahdi Khalaf Alkaeed defended on 29/11/2020.

Dr.Khaled MD. Khan
Thesis/Dissertation Supervisor

Prof. Amr Mohamed
Committee Member

Dr. MD Anwarul Hasan
College Representative

Approved:

Khalid Kamal Naji, Dean, College of Engineering

# ABSTRACT

ALKAEED, MAHDI, KHALAF., Masters : January : 2021, Masters of Science in Computing

Title: Blockchain Technology and Reputation System for Smart Grids to Address Cyber-Attacks

Supervisor of Thesis: Khaled, MD, Khan.

The smart grid model has made a big technological leap over the traditional electrical grid. This model contributes to protecting the physical environment as it provides many benefits such as improved quality of services, efficient use of the traditional electrical grid, and renewable power resources that depend on many resources such as the sun and wind energy. However, smart grids suffer from some security problems such as the communication protocols. These protocols do not include proper authentication and access control mechanisms. The consequences of security breaches in smart grids are devastating because this could lead to the complete layoff of the power grid and cause economic effects on the power systems.

To address the security issues (unsafe communication protocols - internal attackers) in smart grids, we propose in this research a new distributed framework to address internal attackers to protect smart grids against False Data Injection (FDI) attack based on Blockchain Technology and a reputation score system to enhance self-defense capability. Blockchain is a distributed data architecture in which all data elements are permanently registered after validation by most nodes in a P2P (Peer-to-Peer) network. We define reputation as the user's reliability, and more precisely and clearly, reputation is the opinion of a machine or user about devices and other users. This thesis presents actual results as a conceptual reference to assist smart grid

developers and researchers in proposing a secure architecture for smart grids and to provide a performance analysis of this approach based on implementing Blockchain technology and reputation score system in the smart grid domains and sub-domains.

# DEDICATION

*I dedicate this thesis to my father, family*

*Friends and supervisor*

*Dr. Khaled.M.Khan*

ACKNOWLEDGMENTS

Without the support of the surrounding people, this thesis was not possible. To my family and my friends and I extend my sincere thanks to my supervisor Dr. Khaled M. Khan for his significant support and motivation to me through this journey. His amazing experience in cybersecurity has been great for many years, work ethic, and unlimited patience, all this makes ideas into reality. His constant encouragement to me during the most frustrating periods to solve all the problems we faced enabled me to work and achieve what is required. He also has the greatest credit for my success in publishing many scientific papers, as we could publish 3 papers related to this thesis in scientific conferences in several countries. Many gratitude and thanks also to the Qatar National Research Fund (QNRF) for providing funding for my research's. Thank you all very much for everything.

Above all, I thank God Almighty for his preservation, care, and help for me to succeed in my studies, work, and life. Bless me.

# TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

# LIST OF ABBREVIATIONS

SGs Smart Grids

IioT Industrial Internet of Things

GUI Graphical User Interfaces

FDIA False Data Injection attack

DERs Distributed Energy Resources

P2P Peer-to-Peer

TA Trusted Authority

CR Credit Reference

SHA Secure Hashing Algorithms

ECDSA Elliptic Curve Digital Signature Algorithm

RIPEMD RIPE Message Digest

WSM Weighted Sum Method

CA Control Authority

AES Advanced Encryption Standard

IoT Internet of Things

AMI Advanced Metering Infrastructure

## JOURNAL PUBLICATION

Accepted: Date Submitted by the Author:19-Nov-2020. Article Title : Distributed Blockchain and Reputation System for Smart Grids to Address Cyber-Attacks. Author(s): Mahdi Alkaeed, Khaled M. Khan.

## CONFERENCE PUBLICATION

[1] M. Alkaeed, M. M. Soliman, K. M. Khan and T. M. Elfouly, "Distributed Framework via Block-chain Smart Contracts for Smart Grid Systems against Cyber-Attacks," *2020 11th IEEE Control and System Graduate Research Colloquium (ICSGRC)*, Shah Alam, Malaysia, 2020, pp. 100-105, doi: 10.1109/ICSGRC49013.2020.9232544.

# CHAPTER 1: THE INTRODUCTION

## 1.1 Background

Electricity is the major driver for all technologies, without it, the technologies lose their benefits and become limited or useless [1]. However, to meet the needs of the near future, we need a new secure and safe electrical grid. This new electrical network can handle many computers, equipment, and the latest technologies. This network can control and operate the complexity and growing electricity needs of this century [2]. Thus, to meet the demand for current and future requirements, we urgently need a smart and secure electrical grid, known as the Smart Grid (SG).

Integrating modern communication networks with power networks led to the emergence of many security issues that did not appear with traditional networks. These security issues (such as the integrity of the messages) could pose an actual threat to power grids, which could lead to their complete suspension. All of these have led to the need to develop protection technologies to protect networks and speed up recoveries and restore in the event of cyberattacks or natural disasters. The integration of smart grids with modern communication networks brings the reliability problems to SG systems such as the receiving attacker controlled messages. One of the most important features of modern communication systems used is the ability to deliver messages through different components of the SG with high efficiency and speed, which contributes to the speed of response of system operators to face critical situations. Despite this, there are many security issues, and among them, the most important issue is the reliable SG [4].

The reliability of the network when sending these messages is a real problem as the success of any SG hacker and then his ability to send wrong messages can have a dangerous impact and dire consequences on the power grids, such as complete power

outages in many areas for varying periods. Smart grids comprise many complex and heterogeneous technologies such as Advanced Metering Infrastructure (AMI) and Supervisory Control and Data Acquisition (SCADA) systems and a group of substations. These systems use insecure protocols where the protocols are the same as those used for traditional network communication. This allows for the possibility of many attacks such the Russian worm Stuxnet [3]. This cyberattack caused power outages for over 225,000 people [4]. Another example of attack happened during 2009 when attackers from China and Russia attempted to perform unauthorized access to American electrical grids [5].

In 2014, a range of energy system infrastructure came under attacks in countries such as Germany, Poland, Spain, and the USA. This is known as Dragonfly attack [6]. The history of cyberattacks against SCADA power systems goes back to 1982. Today, it is essential to protect SGs with Intrusion Detection Systems (IDS) to prevent intruders in a timely manner.

The deep integration of electronic and physical power grid resources gives hackers the ability to inject false data into the network to influence decision-making processes in control centers, which could lead to serious consequences such as power outages and large material losses [22]. Vulnerabilities related to smart grid data security (e.g., networks protocols that do not require authentication) should be taken into serious consideration as they have been exploited previously and led to cyberattacks (e.g., attacks on Ukrainian power grid stations) and can cause the credentials of power system operators to be stolen (2015 Ukraine blackout ) [4].

The basic operations of the administrator and supervisor of the modern SCADA system in smart grids involves data collection and analysis of data in remote terminal units, where data is sent as a plain text through communication channels from smart

meters to control centers [7]. This provides centralized management of file storage and management, but creates high risk and possibility of manipulating this sensitive data by attackers when this data is sent unencrypted. The presence of an IDS systems is necessary to provide adequate protection for all parts of the SG that meet the entire SG systems from cyberattacks such as command injection and FDI.

AMI provides bidirectional communication (two way) between power consumers and providers (companies) in Smart Grids that provides two-way data exchange between these components. However, this two-way communication relies on the information and communication technology and components that may have severe weakness. A good example is wrong data entry attacks on smart meters.

SCADA and AMI communications are based on Modbus [8, 10], and DNP3 [11] protocols. These protocols are not secure, as they do not provide integrated authentication and access control mechanisms. Thus, any proposed protection system must take into consideration of all potential weaknesses in the SG systems and their protocols which are used. Substations in smart grids are an important location in the grid as their tasks are to divide, combine, and convert electrical energy. At present, the operations of the substations are controlled automatically by control centers or automatic substation. The communication mechanism among these components are based on the International Electronic Commission Standard (IEC 61850) [12, 13]. This provides several goals such as the ability to simplify configuration, long-term stability, and interoperability.

The protocols which are in the IEC 61850 do not provide any of the protection features against various cyberattacks, as it is possible to exploit vulnerabilities of the protocols used. Although this standard uses basic security measures that include traditional authentication mechanisms. Hence, providing the IDS is a necessary tool for

protecting substation data and integrity during the information exchange process through the different SG components.

Modern smart grids are usually equipped with several systems running simultaneously to provide updated data in real-time. This information relates to several measurements such as voltage, frequency, and current. These systems integrate with conventional power systems (SCADA systems), this provides additional and wider monitoring mechanisms for the entire electrical network by distributing many sensors and smart meters. This gives the system operator greater ability to identify potential problems to make decisions that avoid revealing important information related to the mechanism of operation of these systems, the discovery of which may lead to devastating results.

More specifically, its synchro phases depend on IEEE C37.118 [14]. Since this protocol rarely provides a built-in authentication mechanism, this poses a major security hole and an opportunity for attackers to launch MITM and FDIA.

## 1.2 Why FDIA is Addressed in This Research?

This thesis highlights the False Data Injection Attack (FDIA) [15]. If an attacker gets the system user's credentials, then he/she can inject false information to tamper with smart grid systems. Smart meters are an integral part of smart grids to collect data and send to control centers, these meters and sensors are geographically distributed in modern energy systems. If an adversary gets administrator credentials, he can inject harmful data into smart meters of SGs. Here, this attack leads to false results to assess the situation and prevent taking the right decision.

SGs include many asynchronous connections between heterogeneous communication systems and protocols with various industrial components. The

multiple mixture of insecure systems and protocols and a mix of legacy hardware led to many vulnerabilities exist in protocols that are in SCADA such as Modbus [16], DNP3 [17], IEC 61850 [18, 19]. It exposes these networks to various attacks such as Denial of Service (DoS) attack that may impact the integrity of messages exchanged in SG systems [20], [21]. The most dangerous of which is the FDIA, which is still considered one problem that researchers seek to find solutions now a days. It is difficult to detect internal attackers performing FDIA. Enhancing capabilities in smart networks to defend themselves against various cyberattacks requires adopting the latest technologies to enhance system security [22], [23]. The effects of FDIA have been demonstrated in several previous studies that showed its effects on SG systems (more details in Chapter 2) [24].

## 1.3 The Smart Grid

The SG is based on a huge number of computers and other equipment with more capabilities. It provides two-way communication between customers and energy company utilities in order to provide better integration with the solar and wind renewable power generation [25-27]. The SG systems provides flexibility, reliability, and quality of power delivery of the industrial fields [28, 29]. The concept of the SG includes smart metering and smart devices, energy-saving resources, and deploying renewable energy resources [30, 31], as shown in Figure1.

Besides the previous technologies, smart grids comprise a complex and heterogeneous set of technologies that encompass a group of systems including AMI and SCADA systems. AMI system is considered as an integrated system comprising communication networks, smart meters, and better management for the system's data. SCADA system is a control system that includes computers, communication networks,

and Graphical User Interfaces (GUIs) for managing high-level process oversight [27].

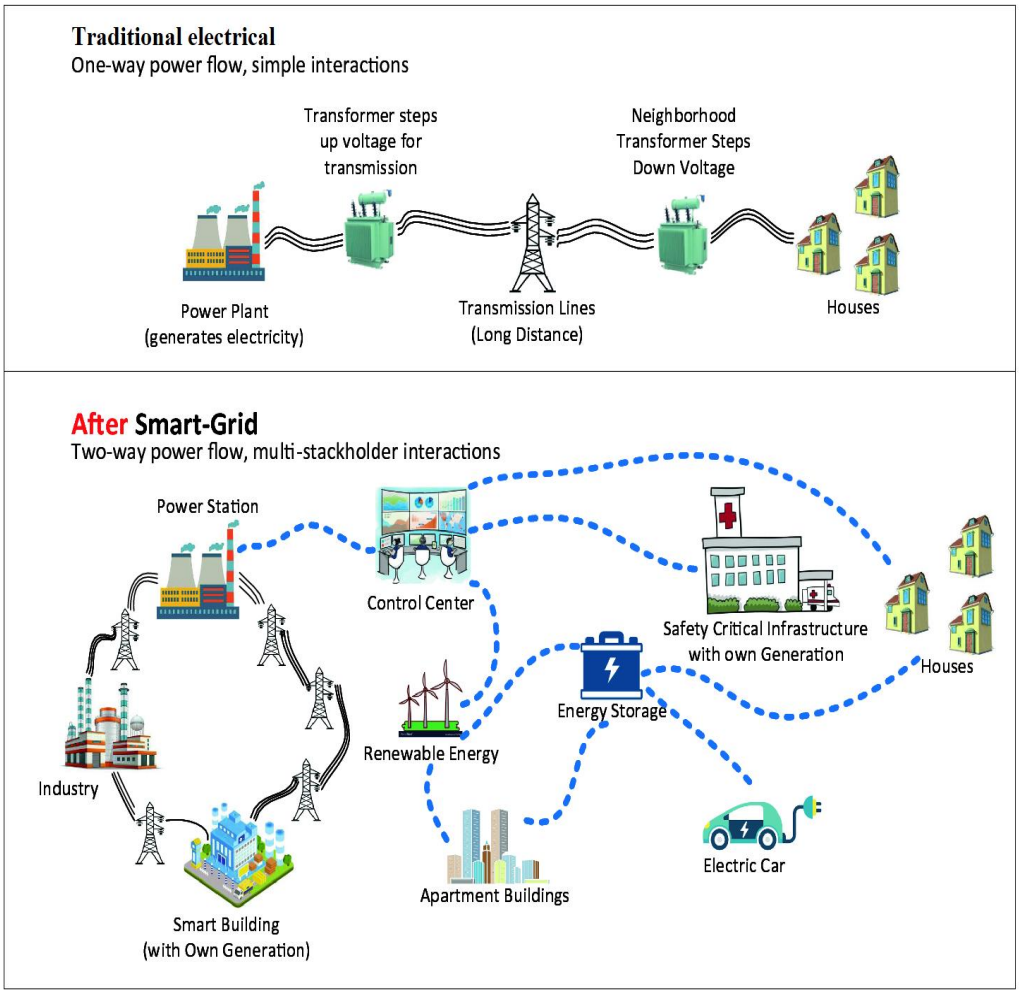


Figure 1. Smart grid characteristics vs. the traditional electrical grid.

All this has become important to the development process in the economic, health, and environmental fields. Besides, many improvements in SG technology have led to improvements that have made many services into realities [32].

SG allows a consumer to save more money by sharing daily consumption usage. Then, a consumer can manage energy consumption based on the information available. It also enables one to choose the best time to buy electricity. The continuous flow of

energy and the provision of mechanisms to protect these resources has become one of the national security priorities of countries. Also, relying more on renewable energy resources to ensure the continued flow of energy even during disasters, wars, or emergencies has become a necessity.

Table 1. Traditional power grid vs SG.

| Concepts | Traditional power network | Smart Grid |
|---|---|---|
| The possibility of interaction between energy network customers and service providers | There is no possibility to interact with the network. | Customers are involved in the mechanism of smart grid work. |
| The possibility of the integration with energy renewable sources | Confronting the problem of renewed penetration | Enhancement in the integration process with renewable resources |
| Options available to customers | Market monopoly, no choice | More options for clients with digital market trading |
| System processes | No efficiency in operations | More efficiency in operations |
| Protection mechanisms | Only relying on hardware(devices) protection methods | The smart grid can self-repair - less harmful when power is off |
| Reliability and security | Less reliable and more vulnerable to both of external and internal attacks | More reliable and less vulnerable to external attacks not internal attacks |

## 1.4 Problem Statement

Ukraine's smart energy grids are one of the basic infrastructures, as in other countries. This structure was exposed to cyberattacks in 2015, which led to the complete demobilization of this network for hours, and plunging the Ukrainian capital in darkness for hours as shown in Figure 2 [77]. This cyber-attack has shed light on the possibility of this attack to happen in other countries, such as the United States [55].

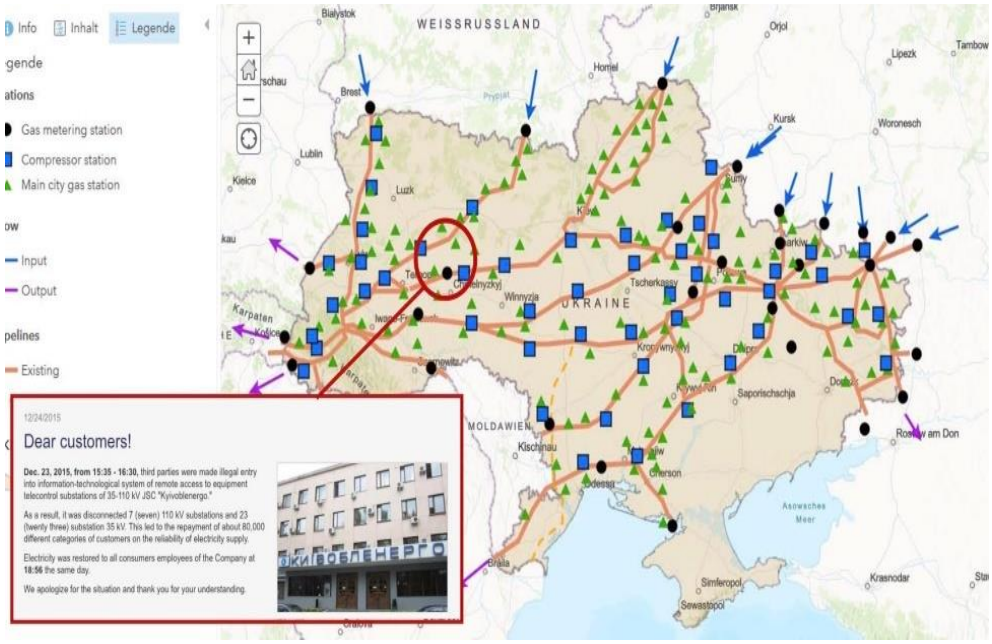


Figure 2. December 2015 Ukraine power grid cyberattack.

This attack was carried out by hackers by sending fake e-mail messages and then they could get the basic credentials that allowed them to gain access and control that electrical network.

If an adversary obtains the admin credentials and gets permissions that allow him/her to gain full access and control over the smart grids substations, then the attacker can manipulate or inject wrong information for smart meter measurements or in control

authority systems signals in order to change the dynamics of the electrical network. False Data Injection (FDI) can be a very dangerous cyber-attack to the SG operations as it is also very hard to detect it. This issue can have severe security and economic effects on power systems [33, 34]. This thesis investigates how do we (i) detect an attacker, (ii) prevent the adversary, and (iii) withdraw permissions from an attacker to limit potential threats.

Following the assumptions of multiple security weaknesses present in SG networks, such as the use of insecure protocols and the inability to prevent internal adversaries from launching the FDI attack, we plan to address the following specific issues in this thesis:

i) Secure the smart grids against FDI an enormous problem that can mislead the control center without the system being able to detect that false data alone.
ii) Define a classification process for smart meters and substations to benign, malicious or semi hones, this classification process is very important to develop an advanced protection system. Thus, it helps to know the reliability of the data received from the contract if it is false or correct based on the contract classification.
iii) Illustrate the rate of events by adversaries who are trying to send (FDI) attacks in two cases, in the normal case without using the proposed approach, and when applying the proposed approach, and to clarify the differences between them to show the effectiveness and feasibility of our proposed framework.

## 1.5 Significance of The Research Problem

We live in an interconnected world. We connect all vital infrastructure all over the world to electricity. The electrical network is a very critical and necessary asset.

This grid is a logical target for many cyber-attacks. Solving this specific security problem is very important because these infrastructures have to be very reliable as the economies of the countries depend on these vital networks.

Attackers are trying consistently to exploit vulnerabilities in electrical grids systems. Hence, electrical network security and defense methods are needed to protect their systems. Cyber-attacks against the Ukrainian energy sectors that may be the prelude to broader and larger attacks, threatening the economies of countries. Analyses of these types of attacks have become a big necessity in order to avoid a recurrence. Developing traditional networks to become smarter is the best solution using modern technologies to prevent hacking and cyber-attacks to gain access to SG assets.

## 1.6 Thesis Contributions

To address these specific security issues in smart grids, we propose a distributed framework based on two lines of defensive technologies:

a) The first one is the utilization of a reputation score system to enhance self-defense capability to address cyber-attacks on smart grids. The reputation score system gives each smart meter in the smart grid a credit or reputation score value that can be used for data verification against cyber-attacks.
b) The second line of protection is the use of the Blockchain technology that can protect the data sent to all agents or nodes (smart meters). Blockchain technology enhances the privacy, security, and durability of the smart grid. We consider smart meters and substations as nodes in the Peer-to-Peer (P2P) network. Besides, the smart meter transactions which contain the measurements of the meter encapsulate as blocks in the chain [35].

The major aim of the proposed framework is to provide an integrated system that could equip smart grids systems with a self-defense-capability to ensure the protection of data during its transfer between various nodes. We summarize the major contributions below.

1) We propose a secured architecture for smart grids based on a reputation score to protect smart grids against false data injection (FDI) attack.
2) We Develop a private blockchain framework to verify the reliability and integrity of transactions among smart meters because regular blockchain-based on proof of work requires more time to generate a new block and this is not useful for SG transactions which is very critical and requires a few seconds for its transactions.. This mechanism provides confidentiality and integrity for data in three layers (sensing, communication, and control layer).
3) We provide a performance analysis of our above approaches applied to smart grids in three different scenarios:
    - Scenario-1: This is a traditional scenario where the smart grid uses only the authentication process as the main protection method.
    - Scenario-2: This scenario is the implementation of Blockchain Technology on smart grids.
    - Scenario-3: This scenario is a combination of Blockchain and a reputation score system on smart grids.
4) We offer a set of practical recommendations based on a mathematical foundation on when the people should apply our proposed approaches to the above scenarios of smart grids in order to deal with various security attacks.

## 1.7 Outline of the Thesis

We organize this thesis as follows. Chapter II introduces the SGs security and privacy concerns and the literature review. We introduce the methodology and our suggested scheme in Chapter III. Chapter IV introduces the performance analysis and evaluation. Then, results, analyses, and discussions are provided in Chapter V. Ultimately, we conclude the work in Chapter VI.

# CHAPTER 2: LITERATURE REVIEW

We structure this chapter as follow: Section I highlights the security and privacy concerns in smart grids. We divide this section into subsections. The first subsection describes the most important challenges that the smart grid facing, while the second subsection illustrates different cyberattacks against SG systems. Subsection 3 covers the impact of FDIA on smart grids.

In Section II, we have described the related work. This section contains subsections. Subsection 1 covers the reputation score methods in previous IoT studies. Subsection 2 covers the use of the Blockchain technology in smart grids and their benefits and weakness in the previous studies. The last subsection illustrates the Weighted Sum Methods strategies. Finally, Section III concludes this chapter.

## 2.1 Security and Privacy Concerns in Smart Grids

Cyber-attacks may affect the security of smart grids and economies of countries. These attacks may destroy the smart grid's control system. In December 2015, "BlackEnergy" malware infected several Ukrainian substations which resulted in loss of power more than half of the houses in some regions of Ukraine for a few hours [55].

An adversary can cause negative impact or harm after he/she has a full awareness of the smart grid mechanism to control various components of physical interaction with the target network components to cause malfunctions and damages. If the attacker knows how to control the network and its components, then he/she can exploit various resources to control different applications that control the power which can cause potential damages such as network instability, power losses and outages.

In the SG, an attacker can exploit one or more vulnerabilities in three layers of smart grids (sensing, communication, and control layer). Some of these vulnerabilities

include replacing packets in communication channels (v1) in the communication layer, interrupting the operation mode computation (v2) in the control layer, compromising meter/sensors readings (v3) in the sensing layers [56]. Figure. 3 illustrates the tree diagram representing potential attack paths against smart grid layers. The green track in Figure. 3 shows a successful attack against the three layers.

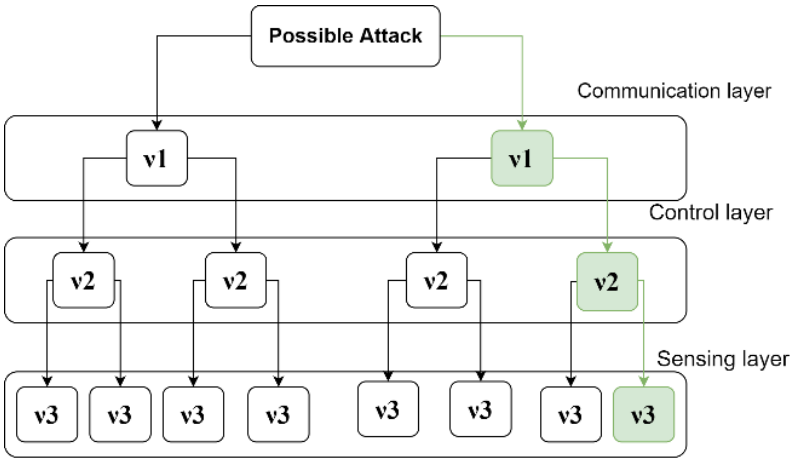


Figure 3. Tree diagram represents potential attacking paths against SG layers.

### *2.1.1 Challenges*

The most important challenges that the smart grid are:

1) Safety and Security: integrating the power grid with the communication networks creates new threats that do not occur in traditional networks, and these various threats may prevent the power grid from performing its tasks.
2) Reliability: The integration process also brings many reliability problems for the SG assets. For example, the fake messages issued by adversaries sent to the smart grid can have dire consequences, and ultimately it leads to power failure.
3) Power Quality: One of the important challenges is the ability of power stations

to provide a high-quality-energy to consumers continuously.

4) Interaction between network and customers: Improving energy reliability requires customer involvement in network activities like demand response, power quality selection as they wish.

### *2.1.2 Different Attacks Against Smart Grids*

In [57, 59], the authors show that there are many gaps in smart grids such as using insecure protocols. These protocols do not provide integrated authentication mechanisms and access control mechanisms.

However, when using authentication mechanisms in SG systems, the problem of internal attackers remains, that considered one of the major problems difficult to correct and is still under study and raises the interest of researchers [57]. An adversary can carry out a cyberattack where it is very hard to detect an internal adversary of the system in a reasonable time. Besides, SGs like other networks, are vulnerable to Denial of Service (DoS) attacks by sending large numbers of packets to the network by an attacker [57, 58].

SG systems and components (devices) also use weak or default passwords without encryption mechanisms for authentication mechanism to users [60]. The absence of mechanisms to authenticate these systems considered a security vulnerability because unauthorized persons can exploit SG systems and components to access, manipulate, and sabotage.

Malware is one method that attackers used to gain control of SGs and extract data is malware, which caused heavy damage to the smart grid system. In [62], researcher points out that malware, via the malicious control communication injection

process, can affect SCADA systems [61-64].

Table 2 summarizes some of the most important cyberattacks against smart grids. It shows each cyberattack, the target domain, the target network level, the different applications, and different protocols used. SG domains includes Advanced Metering Infrastructure (AMI), distributions, transmission, and generation. We notice that the Distribution domain (SCADA/Subsections) uses Modbus protocol, which doesn't use authentication mechanisms leading to unauthorized remote control.

Table 2. Summarize the most important cyberattacks against smart grids.

| The Domain | Network Type | Applications | Attacks |
|---|---|---|---|
| AMI | (HAN) home areas network | Eergy consumption / monitoring.<br>Pricing information. | Spoofing<br>DoS attacks<br>Denial Of Services attacks |
| Distributions | Distribution SKADA | Distributed data .<br>Fault/Error detection.<br>Various energy resources. | Spoofing – DoS<br>Unauthorized remote control(BackdoorDorshel (KillDisk software) |
| | Distribution Substation | Preventive relay. | packet injection attacks.. |
| Transmission Generation | SKADA Transmission Substation | Measurement and control data.<br>EMS functions. | Spoofing (MitM)<br>Spoofing |

### *2.1.3 False Data Injection (FDI) Attack*

The FDI attack injects malicious data into smart meters that can mislead control centers. Hence, this attack leads to false results to assess the situation and avoid making the right decision. An FDIA would fool a system operator into believing that the smart grid system is operating in a safe state when in reality it is not. This attack deceives the system operators into taking corrective action that includes rescheduling the generator load shedding. Besides, these procedures are unnecessary and very expensive.

Liu et al. [65-66] explained that FDI attack could have severe economic effects on smart grids. Here, an adversary must have prior knowledge of smart grid systems and the ability to perform a thorough analysis of the target network's topology. Besides, he/she should fulfill another requirement to carry out this attack, which is the full knowledge of a system-user-credentials to have physical access to tamper smart grids systems. An adversary can use the compromised nodes to inject false data. Hence, (s)he can tamper with smart grids equipment. As a result, they enter this wrong data into the smart grid systems, which leads the systems to generate false reports or energy outages.

The impact of an FDIA attack on the integrity and privacy of smart grid data was first studied by Liang GQ et al. [67]. The FDI attack is very difficult to detect by the normal detection mechanism in smart grids systems. FDA attacks not only inject wrong data into the system, but it degrades system service. FDIA destroys data integrity and data privacy. Data integrity in all IoT applications is a very important requirement which is why this attack poses a much bigger threat. It takes a lot of care to detect and prevent this attack. We need to ensure that smart grids systems and smart grids protocols are secure. Even smart grid applications have to be well designed to prevent any false value from being injected.

To protect data from an attacker, we must restrict access control. Data encryption

technologies can protect data integrity and prevent wrong data entry. Although encryption techniques prevent external attacks, they cannot prevent an insider attacker (an allowed user) from within.

In [68], the authors present how an adversary can launch a stealth attack without being discovered by intrusion detection systems. The authors consider that if a system comprises ( $n + 1$) substations, smart meters number ($n$) and the nose (n) then the case estimation model in the linear power flow model:

$$m = Hx + e$$

*Jacobian matrix denoted by H, and e Gaussian distribution*

If the vector of malicious data denoted by ($b$), that they could inject into meters measurements data ($m$) through the attackers, hence the measurement vector after attack as:

$$M_{bad} = z + b$$

The adversary's goal is to find a malicious data vector that keeps the metric unchanged before and after the attack. Through this method, a hacker can carry out a stealth attack without being detected. The basic idea in previous model is that an FDIA attack relies on searching for a malicious data bus and using it to make the target function before and after the attack below the threshold ($t$), defined as:

$$J ( \hat{x}_{\text{bad}}) < t$$

In this article, the authors show that it is very difficult to find an analytical method capable of knowing the relationship between the system parameters and the malicious data.

Finally, as a summary of the FDIA, this cyber-attack is a very dangerous and harmful that threatens the safety of SGs operations and the economies and security of countries. It can completely change the state variables that are used in the upper layers

associated with deciding based on those parameters. Hence, control centers will be deceived, and then costly or unnecessary operations will be executed within the smart grid based on this false data [69].

## 2.2 Related Work

Here, we compare and show the novelty of this research work considering this review. The first subsection of this chapter introduces the reputation system methods to address cyber-attacks in various IoT applications and discusses the advantages, disadvantages, and weaknesses of the various studies. The next subsection introduces Blockchain-based research initiatives. This subsection explains the importance of this emerging technology in providing protection and integrity of transaction data between the various components of smart grids. The final subsection presents the Weighted Sum Methods (WSM) in various IoT applications.

### *2.2.1 Reputation Score Methods*

A reputation score specified as the faith of a device or user about other devices and users, and more clearly a reputation score defined as the user's credibility [36]. Reputation score values are updated frequently, but old values are not erased or reset [37].

In [37], the authors conclude that traditional authentication systems based on the public key infrastructure providing vehicle networks and the Internet of Things (such as smart grids) do not assess message integrity and confidentiality. To solve these security issues, this approach uses the reputation score method to reduce the malicious and untrusted transactions from the source in IoT networks.

In this approach, the Trusted Authority (*TA*) is considered a trusted zone for

reliably managing the reputation system. The *TA* prohibits the use of the system by nodes (vehicles or smart meters) whose reputation values fall below a certain threshold. This strategy reduces the untrusted transactions in smart grids. The Credit Reference (*CR*) update process is continuous and synchronous. Besides, when the *CR's* period will end, the node (vehicle in this case) sends a message request *Mku* to *TA* asking for updating the *CR's* by the *TA*. Initially, *TA* checks the vehicle reputation score (*RSv*). If *RSv* is more than the minimum threshold, the *TA* requests a new (*CR's* encrypted transaction to the vehicle. Initially, *TA* is verifying the *RSv*. If this value is more than the threshold $N_{threshold}$, *TA* requests a new vehicle to prevent it from being known by the hackers. The weaknesses this approach brings is that we cannot guarantee the accuracy and reliability of a vehicle reputation score when vehicles calculate their reputation scores. Thus, if an adversary breaks into the Board on the Unit (BOU) inside the vehicle, then it can calculate the reputation score that it likes.

In another approach, Dötzer *et al*. [38] introduce a new reputation method technique to address piggybacking attack. This attack is a wiretapping attack that is the stealthy electronic surveillance of telephone, cellular, fax, telegraph, or Internet-based communications. Piggybacking also refers to a person allowing another person to follow them directly in a restricted area. For example, an adversary X calls an employee E to open the door for him because he has forgotten his ID. Another way involves X to ask E to borrow his laptop for a few minutes, during which the adversary can quickly install malware. Here, an adversary can access the system during periods of inactivity in the legitimate communication of a user who may use the system [39]. In this approach, the reputation score system is used to solve piggybacking attacks.

Here, a vehicle (vi) generates a transaction (Msg), then sends it to other vehicles. The receiving node will attach its own opinion on the reliability of the message (Benign/

malicious). This depends on the previously collected opinions that attached to the message, and on the content of the message (Msg content). Each node, upon receiving a message, performs a calculation and gathers previous opinions before deciding and giving its own opinion. The weakness of this approach is that the mathematical operations can create a significant burden. Besides, they did not discuss implementation details such as setting up the reputation system and updating the vehicles' reputation scores.

In the research work reported in [40], the authors developed a reputation score system for vehicular networks to provide practical, and robust message reliability to address cyber-attacks. Their scheme requires the reputation aggregation (*Aggr*) algorithm. This algorithm calculates a reputation score for each node (vehicle, *vi*) based on all the nodes feedback. Besides, this algorithm uses a specified time (*T*) as a threshold to collect all the nodes feedback and ignored all ones whose corresponding transaction was sent before (*T*) in the past if required, for efficient data storage. We define the feedback subset selected by the Aggr algorithm:

$$F = \{F : (id_{Vb} = id_V) \wedge (t_b \geq t_a - T)\}$$

Where $id_{Vb}$ denotes a vehicle ($V_b$) identity, $id_V$ denotes a new vehicle unique identifier, *tb* denotes the aggregation time, ta denotes the current time.
The parameter *T* represents a sufficient period during which many nodes report node-related feedback.

The weaknesses of this approach is that the (*Aggr*) algorithm depends on its work on the feedback of other nodes within a specific period. However, there is no mechanism to guarantee the integrity of this feedback (fake or real).

### *2.2.2 Blockchain Methods*

This section summarizes the current use of Blockchain in smart grids. A Blockchain protocol represents an encrypted secure distribution digital ledger across the (Peer-to-Peer) P2P network of devices and systems. This distributed database contains an ever-growing transaction history and arranged chronologically. The ledger is the major data structure that contains both execution files and digital transaction records. These transactions are collected in the form of encrypted, time-signed blocks, and each block is linked with the previous block in an encrypted form, all those blocks form a series of records that represent the order of events within the network (all digital transactions) [41].

Blockchain technology contributes to delivering significant benefits to energy system operations and consumer systems. It provides neutrality, tamper-proof transactions, and transparency. Researches, decision-makers, business players, and utility companies are pursuing blockchain innovation in smart grids [42, 43].

Blockchain technology aims to protect all transaction information and prevent it from being tampered with in the SG and this is the most important feature of its multiple features [44]. The distributed energy resource scheduling mechanism (DERs) builds a trustworthy platform based on blockchain technology. Here, all DERs transactions are reliable and guaranteed because of the voting mechanism adopted in the blockchain protocol. It involves verifying any transaction requires sending it to all nodes in a peer-to-peer network to verify its authenticity by all the nodes that vote if a transaction is true or false. Applying this in SGs makes the blockchain protocol a secure way to provide integrity and validity of all transaction data in smart grid systems (AMI, SCADA).

In [45], the authors proposed a protection framework that contains distributed

private Blockchain for the smart grid to address different cyber-attacks (such as FDI attack). In this approach, the SCADA grid purposes to collect, transmit, and store measurements (voltage, current and reactive power flow) in real-time. They consider that there is a communication path between each smart meter to achieve a P2P network where within each meter is a basic storage information contains the public keys for all nodes, and the node private key. A node private key is using for data encryption while node public keys are being used for data decryption. The receiver node compares between two message digests (*message digest1*, *message digest2*). The receiver decrypts the digital signature of the message using the sender's public key to get *message digest1*. While the hashing value for the sender's plaintext gives the *message digest2* (using hashing function such as SHA256 [46]). If *message digest1* equals *message digest2*, the received measurements are successfully verified, otherwise, there is data tampering.

In this approach, each node in the P2P network has one opportunity to check the reliability of the data which is received and votes on its verification results. The generation of a new block and adding it to the chain depends on the voting mechanism and a threshold (*t*), is defined as below:

$$if\ \frac{K}{N} > t\ ,\ the\ received\ data\ are\ successfully\ verified,\ and\ it\ can\ be\ added\ by\ a\ new\ block\ in\ the\ chain. \quad (1)$$

$$if\ \frac{K}{N} < t\ ,\ there\ is\ a\ data\ \ tampering,\ and\ it\ will\ be\ ignored$$

$$where,\ K\ denotes\ the\ most\ voted,\ t > 50\ \%.$$

The weaknesses of this approach is that if the credentials of employees, producers, or consumers of a smart grid system are stolen or abused by an adversary, it is very hard to detect him.

In [47], the authors proposed an approach that enables smart grid customers and

users to monitor their energy use. This approach argues that in an SG, the users can get the meter reading over the Internet, so it reduces data from an unauthorized user. They developed a model based on Blockchain protocol to tackle these issues. They planned a smart grid monitoring mechanism to secure data transmission between consumers and utility companies. The proposed system model in their researches comprises many layers. The user layer comprises all entities that get electricity from the utility company. The user layer interacts with the registration and authentication layer directly in SG to authorized registered users to be an entity in this system. Besides, it will process all the information which sent to SG with the data processing layer.

Besides, the proposed approach relies on an automatic reporting mechanism for any illegal actions implemented in the SG system and also launches a procedure to prevent access to the SG systems automatically at the same time. Besides the above, the illegal actions that have been flagged Reported using the corresponding user's unique identifier is stored securely in a database. The authentication layer comprises the authenticator and the register.

The weaknesses of this approach, although this approach prevents external adversaries from accessing data without permission, it cannot prevent internal adversaries.

In [48], Aitzhan and Svetinovic in this approach addressed the problem of relying on a third party to provide the reliability of transactions in SGs where their approach relies on providing reliability of SGs transactions without relying on a reliable third party. This approach combined multiple signatures with Blockchain and anonymous message flows for decentralized smart grids. They defined a transaction:

$$Tx = nVersion \,||\, viNum \,||\, vin \,||\, voutNum \,||\, vout \,||\, nLockTime$$

*where, vin the input and vout the output, vinum the number of transactions input,*

*voutNum the number of transaction output, nLockTime A timestamp for a transaction before we included it in a block before we can replace it.*

The validation process of a transaction involves using the Elliptic Curve Digital Signature Algorithm (ECDSA) to generate public, and private key to sign a transaction [49].

Whereas, the other peer-to-peer transaction signed allows verification that the sender is someone claiming to have the codes they wish to send. Besides, using the private portion of the ECDSA pair of keys (public and private key) as a digital signature. An encrypted wallet stores the decrypted transactions. Whereas the public key for key pairs is used to create an address that represents unique strings from 27 to 34 alphanumeric characters, e.g., 1G76f3EaJK43ALnMtgrfedceQypeLjRMKd. This approach defines the generation of an address process:

$$Hash = RIPEMD\text{-}160\ (SHA256(pubKey \oplus rScript))$$

A pubkeyHash is a result of hashing the public key using SHA256 and then RIPEMD160 (SHA256 is a one-way hash function)[50].

While, RIPEMD160 (RIPE Message Digest) is a hash function suitable for applications where the longer hash result is very necessary. Hence, double hashing process to check the reliability of the address by creating a title checksum and appending it to the summary.

$$checksum = Truncate(SHA256^2\ (hash \mid\mid 0x00))$$

In this case, the system forces all users to use a new address in every new transaction:

$$address = Base58(hash \mid\mid 0x00 \mid\mid checksum)$$

In this approach, the authors presented a practical and reliable method to provide protection for all transactions of the decentralized power grid components from SG as

this provided a high privacy and security mechanism.

Weakness in this approach, although this approach provides a higher level of privacy and security against external attackers, it is difficult to prevent or detect internal opponents.

### *2.2.3 Weighted Sum Method (WSM)*

Current decision strategies mostly have one major component such as execution time and traditional authentication mechanisms to give the impression that something is not normal, or a node is unreliable. This is not enough to prevent internal adversaries.

WSM is a multi-criterion decision-making method in which there are multiple criteria such as transaction duration and amount of energy consumption). Through this strategy, we can build a decision based on many more effective data related to the effectiveness of any node.

In [51], [52], the authors concluded that the Weighted Sum Model (WSM) [53], is a successful method to provide a solution for multi-purpose optimization problems. As in this approach, based on several goals, each node has a different weight, and this weight allows each node to distinguish from the rest of the others. In this approach, WSM gives each alternative $A_i$ a weight score ($WSM_{score}$). Selecting the best alternative is by selecting the alternative that has the most WSM points ($A* {}^{WSM^{-}score}$).

The higher score is the better alternative, according to the objectives assumption. In this approach, the authors assumed that the objectives are negative, the better alternative becomes the least valuable (least expensive in the case of calculating the cost of materials). They perform the alternate normalization of a user-defined biggest acceptance value of each criterion.

Besides, normalization of the user-specified maximum number of parameters

adapts to another strategy called user-based decision [54]. The advantage of setting the maximum acceptable for each target by the user is the possibility to consider alternatives that violate these regulations to maintain the specified conditions [51].

Florian Helff and Laurent d'Orazio [51] described that environmental weights are set by system users. These factors, for example, energy consumption, voltage, current battery status. The user weight is related to the user historical behavior. For example, the power consumption, number of inquiries, and execution time. An alternative $A_i$ a weight score ($WSM_{score}$) *is defined as follows:*

$$A_i^{\,WSM\_Score} = \sum_{j=1}^{n} wj \, \frac{aij}{mj} \quad (1)$$

*where, ($w_j$) denotes the weight of user and environment for objective j. $a_{ij}$ denotes a corresponding parameter. And, $mj$ denotes a maximum value for objective j which is defined by the system users.*

The best alternative is selecting the alternatives that has the most WSM points ($A*^{\,WSM^{-}sc}$) equation is defined as follows:

$$A*^{\,WSM\_Score} = min \sum_{j=1}^{n} wj \, \frac{aij}{mj} \quad (2)$$

## 2.3 Conclusion

The above discussion on the related works suggest that although many relevant research works such as reputations systems have been proposed on vehicular networks, no recent work has been done on smart grids. As we have seen, there are many problems in the previous studies and weaknesses, so we propose a new framework based on an integration between the reputation system and the blockchain protocol to provide integrity and security of messages in the SG to address different cyber-attacks. Our

proposed research attempts to provide a simple concept about how to address identified specific security concerns on smart grids using private blockchain and reputation systems.

Finally, Blockchain technology provides reliability and tamper-proof transactions between the different SGs components. Besides, the feature of using the WSM is to define a classification process for nodes to (benign, malicious or semi hones), and to provide a classification method for a transaction according to meters weighted sums to (low, medium, and high).

# Chapter 3: The Proposed Solution for Security And Privacy Problems In SG

Chapter 3 is structured as follows: In Section I, the proposed scheme and methodology has been shown. In Section II, we have displayed the reputation score system. Section III covered the Weighted Sum Method (WSM), and the algorithm which is used in this approach. In section IV, we have shown the private Blockchain Protocol. Section V describes the generation of blocks and submission to chain in the private Blockchain protocol. Section VI covers the generation of Blocks with reputation scores values and submission to the chain. Finally, the conclusion is illustrated in Section VII.

## 3.1 The Proposed Scheme

We divide this section into two subsections. The first subsection discusses an overview of the proposed framework. Then the methodology is explained in the second subsection.

### *3.1.1 Overview*

To address the security issues of the smart grid, we present a framework that uses the characteristics of reputation points and Blockchain technology. Reputation is the general knowledge and combined opinion of a particular node. A Blockchain protocol represents an encrypted secure distributed digital ledger across the (peer-to-peer) p2p network of devices and systems [70].

In the proposed framework, we consider that there is a communication path between smart meters to achieve a P2P network. Each meter has a basic storage information containing its cryptographic private key, public keys for all nodes, and reputation scores for all nodes. Besides, each smart meter in this network contains a copy of the distributed ledger [70].

This involves using more space from the smart meter memory, and in to solve

this issue we can use a floating genesis block to reduce the ledger size [75]. A distributed ledger contains a list that includes all transactions between the smart meters. These stored transactions are essential to return to that data when necessary. Each node (smart meter/substation) knows which other nodes made which transactions.

### *3.1.2 Methodology*

An abstract diagram of the proposed work is shown in Figure 4. Assume that an employee *E* wants to get a smart system *S* services. In this case, *E* must register his information with the Control Authority (*CA*) to obtain the credentials *C*. *E* can log into *S* easily by using *C*. If *E* has just been registered, the *CA* gives it a default value ($P_v$ ) which should be more than the reputation score threshold ($R_{threshold}$). After the authentication process, *S* sends a request *R* to the reputation score system to get a response/feedback containing a reputation score value $RS_i$ (more details are shown in this section part C). If the value $RS_i$ is greater than a threshold, *S* grants *E* permissions. Otherwise, when the $RS_i$ value is smaller than a threshold, *S* prevents *E* from damaging the smart grid by using the stolen credentials, as shown in Figure 4 (a). System *S* knows the credentials *C* have been stolen and it depends on *E's* behavior (multiple criteria-as it shown in Section III).

After obtaining the permissions, *E* can use the services of the smart grid system *S* and can make a transaction *Txn* (for example, a request for power supply). $RS_i$ must be added in each transaction to achieve more integrity of messages (*Msg*), see Figure 4.(b).

Then the Blockchain consensus algorithm in *CA* distributes *Txn* to all nodes to get feedback for voting. In each node, there is a pool of valid transactions (Ledger copy). Each node *N* in the Blockchain network verifies the integrity of the received

*Txn* and votes on its verification results using the sender's public key ($Sender_{public\_key}$). Each meter has basic storage information containing the node's private key, public keys for all nodes, reputation values for all nodes [71]. We can protect the basic storage information by storing this information in local Blockchain and in case of any new update, a new block, in this case, will be added to this chain. These stored values are necessary for double verification of each transaction. This dual process relies on checking the sender's signature with his public key and checking his reputation as depicted in Figure 4(c). We will discuss it in more detail in the latter subsections.

The *CA* verifies the transaction validity according to the feedback of all the nodes based on a voting threshold $\tau \in$ [50% -100%] [72]. When the voting condition is achieved, the transaction is added in a block to the chain. In this case, the sender node is classified as a penguin node, not as a malicious one, Figure 4(d).

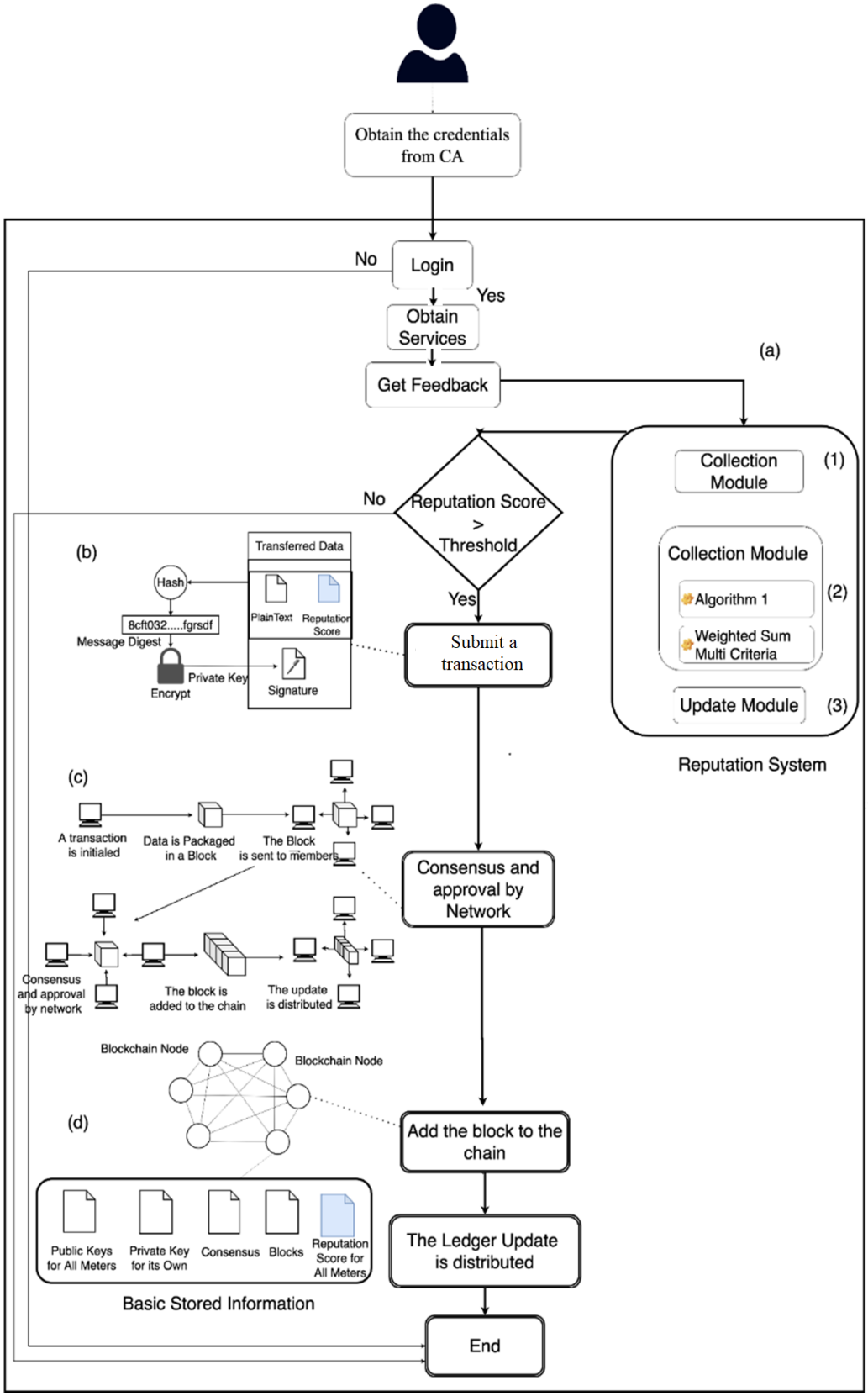


Figure 4. The proposed framework diagram.

## 3.2 Reputation Score System

This section is divided into five subsections. First, the collection module is discussed. The calculation module is explained in the next subsection. Then an update module is illustrated, as shown in Figure 5. Afterward, the weighted sum method is explained. Algorithm 1 is explained in the final subsection and its purpose is to calculate the reputation score of a smart meter. Reputation score is as the faith of a device or user about other devices and users, and more clearly a reputation score is defined as the user's credibility [73]. Besides, the reputation scores are frequently updated, but old values are not erased or reset [74].

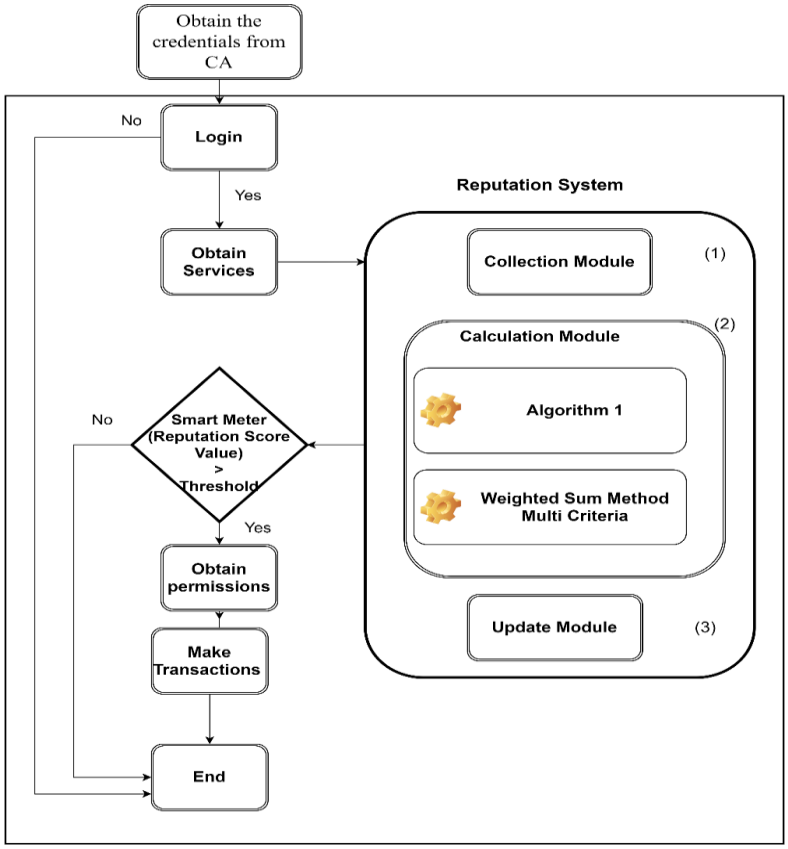


Figure 5. Reputation score model.

### *3.2.1 Collection Module*

This is the first module in the reputation system. It collects all messages received from smart meters. When an employee *E* wants to log into a smart system *S*, *S* sends a request *R* to a reputation score system to get a response/feedback. All received requests are stored in this module.

### *3.2.2 Calculation Module*

The next step is that the calculation module calculates a reputation score value for a smart meter using certain algorithm which we will discuss it in more detail in subsection 5. The reputation score (*RSi*) is a value that is not known to adversaries or users. This value is an anonymous value for adversaries and regular users because the process of calculating it depends on (Algorithm1). Besides, this algorithm uses many anonymous variables for adversaries and regular users, such as:

1. The smart meters number (*N*).
2. The previous reputation score of the smart meter - the historical value (*HRSi)*.
3. Transaction duration ($Txn_{duration}$). The duration value is used to know the time taken for a message to reach a control authority and this value is an important indicator of abnormal behavior.
4. Weighted sum $(W_i)$ of a smart meter (*ni*) where this value is calculated by the Weighted Sum Method (WSM) [75]. We will discuss it in more detail in subsection 4.

### *3.2.3 Updating Module*

This module updates the new value of reputation score ($RSi^{(t+1)}$) in the database (basic storage information), this value is the result of the calculation module.

### 3.3 Weighted Sum Method Multi Criteria Decision Making

This method will use multiple criteria (such as transaction duration, amount of energy consumption…etc) and we must determine the value of a node weighted sum based on multiple criteria effects [75].

We explain the Weighted Sum Method (WSM) with an example. Assume that we have 5 smart meters and we want to calculate the weighted sum of each one. Table 3 is a simple dataset consisting of 5 smart meters with criteria:

1. The number of failed attempts to enter the system ($Wrong_{login}$).
2. The amount of energy a node consumes every month (*Energy Consumption*).
3. Transaction duration ($T_{xn}$ Duration), when a message is late, this unusual delay causes a lot of suspicion.
4. And, the most important criterion is a message effect ($Msg_{effect}$). When a meter sends a request to supply power within the permissible limits, the effect of the transaction is considered normal. On the other hand, if a meter asking to supply a value greater than the permissible limits, it draws attention that something is wrong. The message effect equation is defined as follows:

$$Msg_{effect} = \frac{E\ required}{E\ Max} \qquad (2)$$

*Where $E_{required}$ is the energy required in a transaction. $E_{Max}$ is the maximum energy allowed.*

Assume that an employee E obtains the permissions and he wants to send a transaction asking to supply 750 gas (in the Ethereum gas is a measurement unit used for assigning energy assigned in each transaction), while the maximum allowable amount of gas is 1000 gas per a transaction, then:

$$Msg_{effect} = \frac{750}{1000} = 0.75$$

*Where, we consider the natural energy boundary between [0-500] gas.*

In this case all the expected values for $Msg_{effect} \ \epsilon [0 \dots 1]$), because the $E\ required \ \epsilon [0 \dots 1000]$).

Table 3. Sample.

| Meter | Wrong login | Energy-Consumption | $T_{xn}$-Duration | Msg $_{effect}$ |
|---|---|---|---|---|
| Meter1 | 1 | 2.7 KW | 10ms | 0.17 |
| Meter2 | 3 | 3.7 KW | 15ms | 0.34 |
| Meter3 | 4 | 5.7 KW | 13ms | 0.49 |
| Meter4 | 2 | 12.7 KW | 20ms | 0.91 |
| Meter5 | 1 | 5.7 KW | 18ms | 0.58 |

Consider the Criteria weights assumed by the control authority (CA) as follows: $W_{login}$ = 20%; *Consumption* = 10%; $T_{xn}$- Duration = 15%; $Msg_{effect}$ = 55%.

Assume that the ($w_j$) denotes the weight of a criterion ($C_j$) and ($a_{ij}$) is the performance value of the criterion. Then, the total weighted sum for a smart node ($Node_{weighted\_sum}$), is defined as follows [75]:

$$Node_{weighted\_sum} = \sum_{j=1}^{n} (w_j \times a_{ij}) \quad (3)$$

$$Msg_{effect} = \begin{cases} Positive, if\ Msg\ effect\ \epsilon [0 \dots 0.5]) \\ Negative, if\ Msg\ effect\ \epsilon\ ]0.5 \dots 1]) \end{cases} \quad (4)$$

Equation. 4 considers that if the value of the required energy in the meter falls within the abnormal limits [500-1000]gas, then this is an indication of abnormal behavior and this increases the value of a smart meter weighted sum.

Note that when the criteria of node values increase (transaction duration, power consumption, and $Msg_{effect}$), this gives signs of something abnormal, while small and medium values will not result in suspicion. Increasing criteria values lead to an increase

in the total weighted sum for a meter (Eq. 3). In this case, this leads to a decrease in the reputation value of the meter (Algorithm1). After applying Eq. 3 to Table. 3 we get weighted sums for each meter as shown in Table 4. For example, the weighted sum calculation process for the meters (1 and 5), is defined as follows:

$Node1_{weighted\_sum}$ = 0.2 ×1 + 0.1× 2.7 +0.15×10 +0.55 ×0.17=2.06.

$Node5_{weighted\_sum}$ = 0.2 ×1 + 0.1× 5.7 +0.15×18 +0.55 ×0.58=3.78.

Table 4. The weighted sum for each meter.

| Meter | Wlogin | Consumption | $T_{xn}$-Duration | Msg $_{effect}$ | Weighted sum |
|---|---|---|---|---|---|
| Meter1 | 1×0.2 | 2.7×0.1 | 10×0.15 | 0.17×0.55 | 2.06 % |
| Meter2 | 3×0.2 | 3.7×0.1 | 15×0.15 | 0.34×0.55 | 3.4 % |
| Meter3 | 4×0.2 | 5.7×0.1 | 13×0.15 | 0.49×0.55 | 3.58 % |
| Meter4 | 2×0.2 | 12.7×0.1 | 20×0.15 | 0.91×0.55 | 5.17 % |
| Meter5 | 1×0.2 | 5.7×0.1 | 18×0.15 | 0.58×0.55 | 3.78% |

### 3.4 Algorithm 1

The purpose of this algorithm is to calculate a new reputation score value for a smart meter. The algorithm executes inside CA in the reputation system/calculation module, see Figure 5.(2). The steps of this algorithm are defined as follows:

**Step 1:** Message Score *DC* represent the level of message points that increases or decreases depending on the weight of the node. Let (*DC*) be the message degree score, that it is defined as follows:

$$DC = w_i \times N \qquad (5)$$

*Where* ($w_i$ ) *the node weighted.*

*N represents the total number of nodes in smart grid.*

**Step 2:** We consider that the messages are classified according to meters weighted sums to low, medium, and high.

$$Msg_{classification} = \begin{cases} (w1)low\ ,\ if\ wi\ \epsilon\ [0 \dots 5[ \\ (w2)medium,\ if\ wi = 5 \\ (w3)high, if\ wi\ \epsilon\ ]5 \dots 10] \end{cases} \quad (6)$$

*Where, ($w_1 < w_2 < w_3 \epsilon\ [0 \dots 10]$).*

The evaluation score value (*ES*), is defined as follows :

$$ES = n_1 * u1 + n_2 * u2 + n_3 * u3 \quad (7)$$

$n_1$ is the number of smart meters by if their weighted sum wi $\epsilon$ low, $n_2$ is the number of smart meters if their weighted sum wi $\epsilon$ medium, and $n_3$ is the number of nodes that their weighted sum wi $\epsilon$ high. Besides, the smart meters number of nodes by *N*, *N=n1 + n2 +n3, u1 + u2 + u3 = 1 and u1, u2. u3* $\epsilon$ *[0...1])*.

**Step 3 and Step 4:** let the (*HRSi)* is a historical reputation score *(HRSi=RSi),* then the new reputation score value ($RSi^{(t+1)}$) is defined as follows:

$$RSi^{(t+1)} = \begin{cases} HRSi\ +\ (b * ES\ +\ y\ *\ DS), if\ wi\ \epsilon\ [0 \dots 5] \\ HRSi\ -\ (b * ES\ +\ y\ *\ DS), if\ wi\ \epsilon\ ]5 \dots 10] \end{cases} \quad (8)$$

*Where,* $b, y\ \epsilon\ [0 \dots 1]$ *We consider it as random numbers, b+y=1.*

If $RSi^{(t+1)}$ value is less than a specific threshold ($R_{threshold}$), then the powers are removing from a user as shown in Figure. 4.

Then the classification process for nodes to (benign, malicious or semi honest), is defined as follows:

$$Node_{classification} = \begin{cases} \text{Benign, if}\ RSi > R\ threshold \\ \text{Malicious, if}\ RSi < R\ threshold \\ Semi\ Honest, if\ RSi = R\ threshold \end{cases} \quad (9)$$

Assume that the reputation threshold ($R_{threshold} = 750$), then we consider a node ($n_i$) as malicious node if its reputation score ($RS_i < 750$), Eq. 9. Otherwise, it will be benign if ($RS_i > 750$) or semi honest if ($RS_i = 750$).

---

**Algorithm1**: Reputation Score Calculation Algorithm.

---

**The Input:**

The reputation scores of $n_i$ (the $i - th$ meter)

// $A=\{n_i \mid I = 1 \ldots\ldots N\}$ list of the meters

// $RSi=\{i=1 \ldots\ldots\ldots N\}$ list of meters reputation scores

**Output:**

//The new reputation scores $RSi^{(t+1)}$ of $n_i$

**While** (*current time(t) – time stamp(tt)*< $t_{threshold}$) **do**

1- Calculate the degree score
   $DC = N * wi$

2- Calculate the evaluation Score
   $ES = n1 * u1 + n2 * u2 + n3 * u3$

   $N = n1 + n2 + n3,\ u1 + u2 + u3 = 1$ and $u1, u2, u3 \in [0 \ldots 1]$.

   Get the historical reputation score (RS) : $HRSi = RSi$

3- Calculate the final reputation score $RSi^{(t+1)}$
   If ($wi \in [0 \ldots 0.5]$)

   $RSi^{(t+1)} = HRSi + (b * ES + y * DS)$.

   If ($wi \in ]0.5 \ldots 1]$)

   $RSi^{(t+1)} = HRSi - (b * ES + y * DS)$.

   //$b+y=1,\ 1 > b > 0\ ,\ 1 > y > 0$.

4- **End.**

---

## 3.5 Blockchain Protocol

In this section, we explain how the blockchain architecture controls the smart grid nodes. This architecture is a special case of distributed control architecture and is considered as a private blockchain [70].

In this framework, there is a communication channel between the nodes in order to realize a distributed p2p (peer-to-peer) network (See Figure. 3). In each node, its encryption private key is stored along with a list of all public keys corresponding to all other nodes and a list of reputation score values corresponding to all other nodes [70]. All transactions are first stored in the ledger that is located in the control authority (CA). Besides, in each node, there is a copy of the distributed ledger because the copies of this ledger are distributed to each corresponding smart meter memory (data broadcast) in the grid.

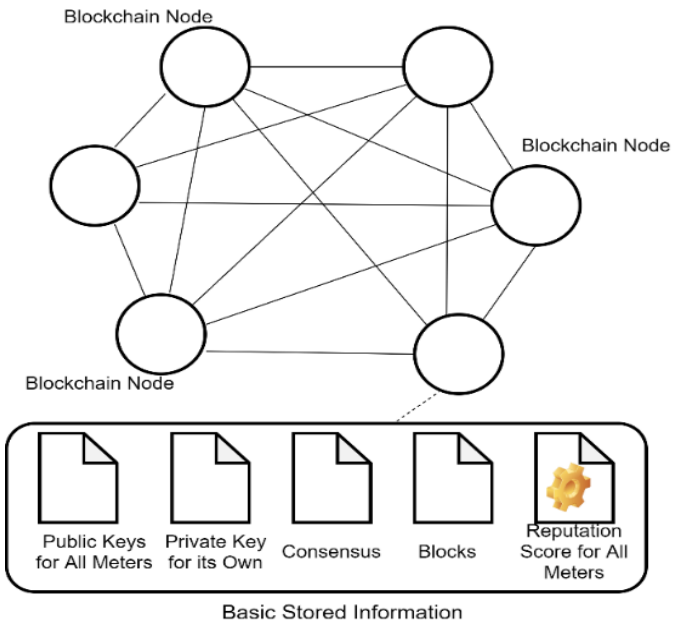


Figure 6. Distributed Blockchain database.

### 3.6 Generation of Blocks and Submission to The Chain

This section explains the steps of generating a new block step by step until the submission of it to the private Blockchain. At first, each smart meter in the smart grid has many sensors. These sensors are responsible for collecting many measurements (*Mi) such* as the current and voltage. These measurements (*Mi)* are submitted through a transaction (*Txn*) to the control authority to create new updates in the chain.

Each transaction ($Tx_n$), has the following parameters: (Transaction identifier ($Txn_{id}$), data content (measurements (*Mi*)), previous hash (*PH*), transaction duration ($T_d$) , current hash *(H),* and *nonce*. Each transaction is defined as follows:

$$Tx_n = Txn_{id} + M_i + PH + T_d + H + nonce \qquad (10)$$

Let *H(Txn)* be the transaction hashed to obtain the *message digest* (*Md1*), that is defined as follows:

$$Md_1 = H(Tx_n) \qquad (11)$$

*We denoted the one-way hash function by H(such as SHA256)* [34].

Let ($Ds_{msg}$) be the digital signature for the transmitted data. This digital signature is the process of hashing the original message ($Md_1$) encrypted with the private key of the node (*Node_private_key*) [39]. The digital signature is defined as follows:

$$DS_{msg} = E_{Node\_private\_key}(H(Tx_n)) \qquad (12)$$

*Where, E is an encryption method such the Advanced Encryption Standard(AES) or the TripleDES.*

In this case, the transmitted message (*Msg*) contains the transaction attributes (*Txn*) and its digital signature ($DS_{Msg}$). The transmitted (*Msg*) is defined as follows (See Figure.

7):

$$Msg = \{ Tx_n , DS_{Msg}) \} \qquad (13)$$

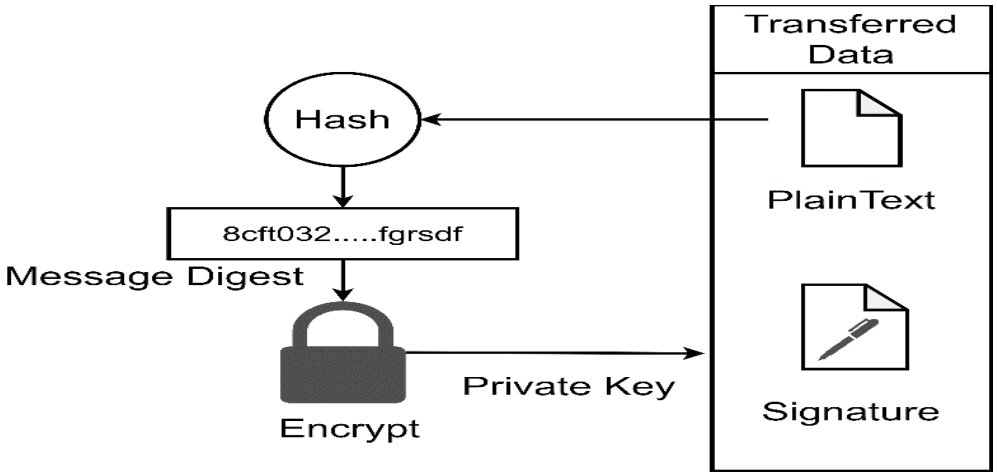


Figure 7.Transferred data (encryption process).

When a message (*Msg)* is received in the CA, it verifies the message validity according to the feedback of all nodes based on a threshold $\tau \in$[50%.. 100%] where the consensus algorithm in CA distributes the transaction to all nodes to get feedback for voting (see Figure. 8).

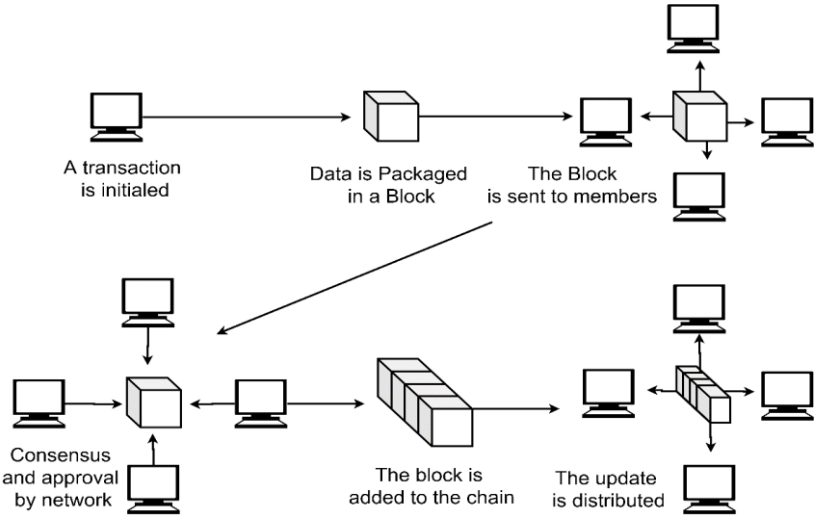


Figure 8. Broadcast and consensus algorithm.

After broadcast the message (*Msg*) to all the nodes in the smart grid, each node verifies the integrity of the *Msg* using the sender public key ($Sender_{public\_key}$). Each node makes this verification process to ensure that the transaction is correct, and there is no tampering of the transmitted data. The steps are as follows according to Fig. 6:

$$Md_1 = H(Tx_n) \qquad (14)$$

$$Md_2 = D_{public\_key1}(Ds_{msg}) \qquad (15)$$

Finally, each node compares between two digits ($Md_1$, $Md_2$) if the two digits are equal, then the transmitted message is correct, and there is no tampering of the transmitted message. Otherwise, it is assumed that the transmitted data is tampered (FDIA), as shown in Figure 9.

$$Verfiy,\ Md_1 = Md_2 \qquad (16)$$

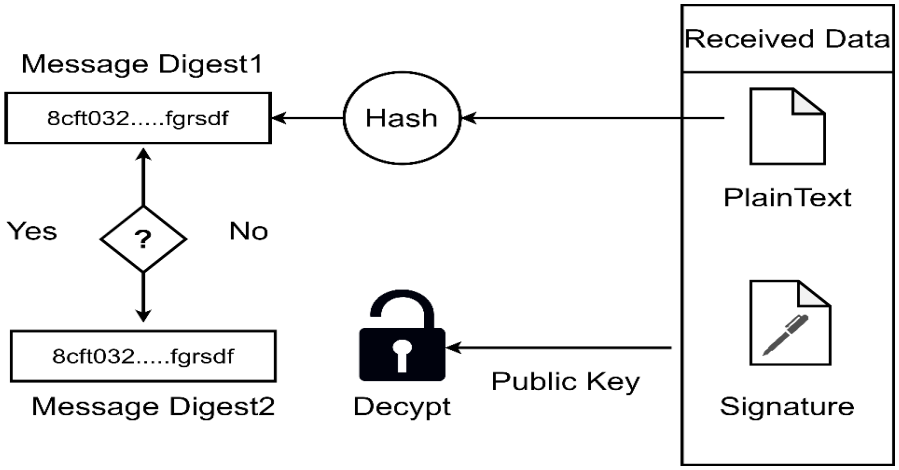


Figure 9. Transaction verification (decyption process).

When the voting condition ($50\% < \tau < 100\%$) is achieved the transaction is added in a block to the chain. The consensus algorithm gives each transaction approval, or rejection depending on a previous voting condition ($\tau$) [72]. Via the voting mechanism, the new block will be added to the chain and the distributed updates are done, otherwise the transaction is ignored and canceled then when ($\tau < 50\%$).

3.7 Generation of Blocks With Reputation Scores and Submission to The Chain

Here, we discuss the use of the reputation score system besides the previous blockchain framework. In this case, each transaction contains all the previous attributes according to Eq. 10, and the node reputation score value (*RSi*) is added as an extra attribute. All the steps in this scenario in the sender node is defined as follows, Figure. 10:

$$\boldsymbol{Txn}_{\text{ with reputation score}} = Txn_{id} + M_i + PH + T_d + nonce + \boldsymbol{RS_i} \quad (17)$$

$$Md_1 = H(\boldsymbol{Txn}_{\text{ with reputation score}}) \quad (18)$$

$$DS_{msg} = E_{Node\_private\_key}(H(\boldsymbol{Txn}_{\text{ with reputation score}})) \quad (19)$$

$$Msg = \{ \boldsymbol{Txn}_{\text{ with reputation score }}, DS_{Msg}) \} \quad (20)$$

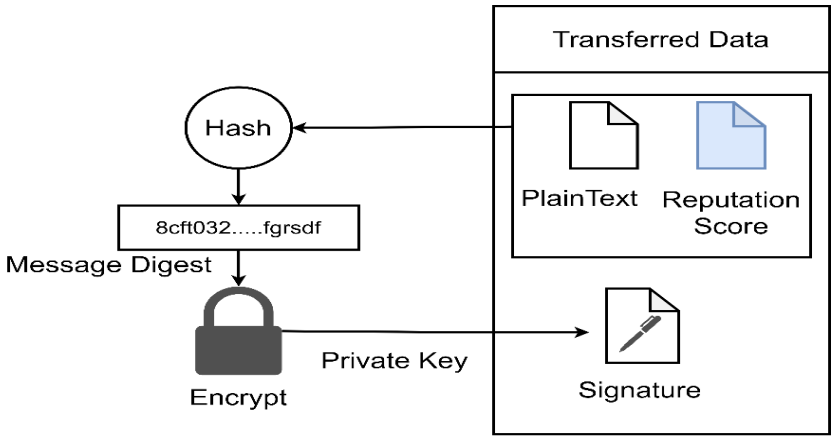


Figure 10. Transferred data (encryption process with reputation score).

After the message (*Msg*) is broadcast to all nodes in the smart grid, all the steps in this scenario in the received node are defined as follows according to Figure. 11:

$$Md_1 = H(\boldsymbol{Txn}_{\text{ with reputation score}}) \quad (21)$$

$$Md_2 = D_{public\_key1}(Ds_{msg}) \quad (22)$$

Finally, each node compares between two digits ($Md_1$, $Md_2$) if the two digits are equal or not. Besides, each node also compares between the received reputation score in the transaction (*RSi) and* the reputation score value that is stored in a meter's memory (*HRSi)*, where each node stores a list of reputation score values corresponding to all other nodes, as it is shown in Figure. 11:

$$Verfiy, \quad Md_1 = Md_2 \text{ and } RS_i = HRS_i \quad (23)$$

In the proposed scenario, when the Eq. 23 is computed, then the transmitted data is correct and there is no tampering of the transmitted data. Otherwise, there is a tampering of the transmitted data (FDIA).

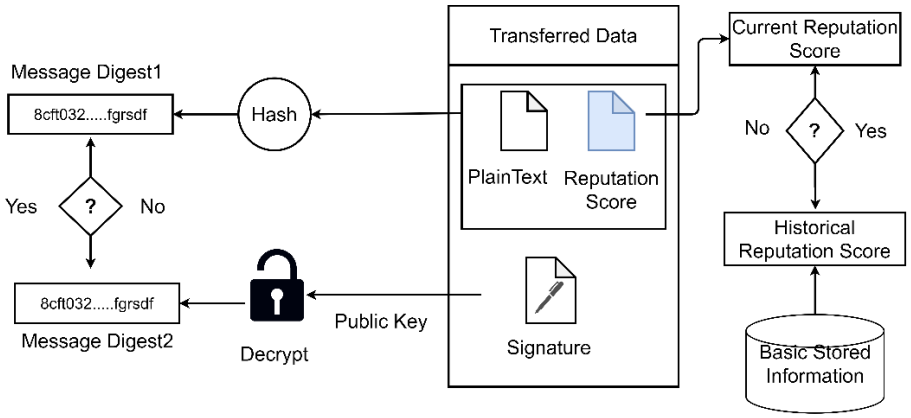


Figure 11. Transaction verification (decryption process with RSi).

The consensus algorithm in this scenario is the same as the previous scenario. It means that the reputation score value is added to each node and in each transaction between the nodes, Figure 12.

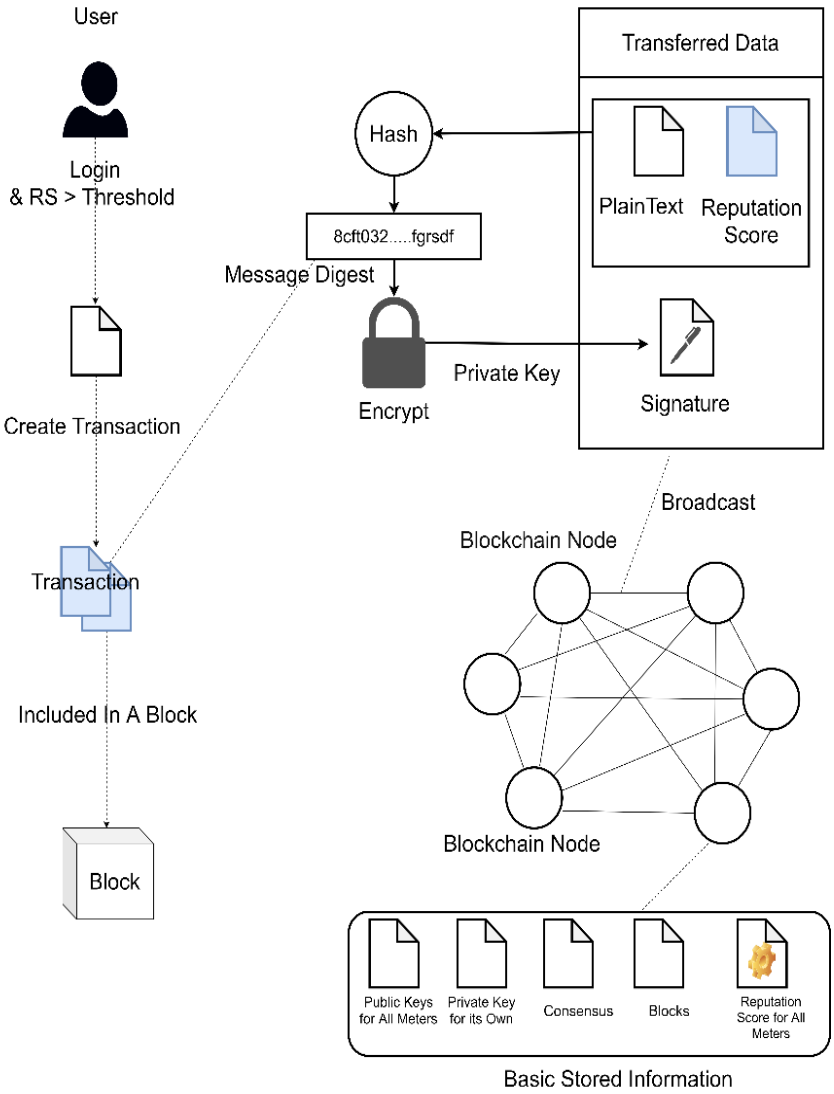


Figure 12. BlockChain and reputation score flow diagram.

## 3.8 Conclusion

The new proposed framework relies on integration between the reputation system, the Blockchain protocol, and the weighted sums methods to provide integrity and security of messages in the smart grid. However, this framework requires the provision of mathematical evidence to support this proposal to study the feasibility and know the improvements introduced by this proposed framework (Chapter 4 explains this more). It also requires a simulation of the smart grid system and applying this framework to it in order to draw conclusions and know the effectiveness of these results and their possibility of later application to real systems (Chapter 5).

# CHAPTER 4: THE PERFORMANCE ANALYSES AND EVALUATION

This chapter has been divided as follows: In Section I, the brief description and the general overview has been shown. In Section II, we have displayed the scenario 1, which is a traditional scenario where the smart grid uses only the authentication process as the main protection method. Section III covers the scenario 2 where the smart grid uses both of the authentication process as the main protection method and the Blockchain Technology to secure transactions in the P2P network). The section IV illustrates the scenario 3 where the smart grid uses both of the previous technologies (authentication process as the main protection method, the Blockchain technology, and the reputation score values) which is used in this approach. Finally, we have concluded Chapter 4 in Section V.

## 4.1 Overview

In this section, we offer a set of practical recommendations based on a mathematical foundation on when the people should apply the above scenarios to smart grids in order to deal with various attacks.

In each of the three scenarios (that was mentioned in the introduction), an adversary X can exploit one or more vulnerabilities V in three layers of a smart grid (sensing, communication, and control layer). Some of these vulnerabilities include replacing packets in communication channels (v1) in the communication layer, interrupting the operation mode computation (v2) in the control layer, compromise meter/sensor readings (v3) in the sensing layers.

Thus, the mathematical equation of the probability of a successful attack against a smart grid ($P_{successful\text{-}attack}$) is defined as follows, [70]:

$$P_{successful\text{-}attack} = 1 - [P(v1) \times P(v2) \times P(v3)]. \quad (24)$$

*Where, P(v1) indicates the probability of successful exploitation of vulnerabilities in the communication layer, P(v2) indicates the probability of successful exploitation of vulnerabilities in the control layer, and P(v3) indicates the probability of successful exploitation of vulnerabilities in the sensing layer.*

In this approach, we consider that we have a group of nodes (*N*) in the smart grid and we want to focus on the probability of success of any cyber-attack on (*n*) nodes in the smart grid where $n \leq N$.

## 4.2 First Scenario

This is a traditional scenario where the smart grid uses only the authentication process as the main protection method.

Table 5. Successful attacking capability and probability comparison.

| Item | | Scenario1 | Scenario2 |
|---|---|---|---|
| Data before sent in the sensing Layer | Capability | Hack into *n* smart meters | Hack into *n* smart meters: Gain n pairs of keys info |
| | Probability | $\frac{1}{3}\prod_{i=1}^{n}\lambda i$ | $\frac{1}{3}\prod_{i=1}^{n}\bar{\lambda} i \times \prod_{i=1}^{n}\bar{\xi} \iota$ |
| Data during transmission in the communication layer | Capability | Hack *n* channel | Hack into $\bar{K}$ channel: Gain n pairs of keys info |
| | Probability | $\frac{1}{3}\prod_{i=1}^{n}\eta i$ | $\frac{1}{3}\left(\prod_{i=1}^{\bar{k}}\bar{\eta} i \times \prod_{i=1}^{n}\bar{\xi} \iota\right)$ |
| Data after it is received in the control layer | Capability | Hack into control authority (CA) | Hack into *K* meters: Gain n pairs of keys info |
| | Probability | μ | $\frac{1}{3}\left(\prod_{i=1}^{K}\bar{\eta} i \times \prod_{i=1}^{n}\bar{\xi} \iota\right)$ |

Table. 5 represents the traditional case where there are no data protection mechanisms in this scenario just a traditional authentication mechanism [72].

Let (*Pa1)* be the possibility of attacking data on n smart meters in the sensing layer before transmitting, then it is defined as follows:

$Pa1=Pa_{senario1}(sensing\ layer) = 1/3(\lambda_1 * \lambda_2 * \lambda_3 \ldots\ldots \lambda_n) =$

$$\frac{1}{3}\prod_{i=1}^{n}\lambda i \qquad (24)$$

where we denote to the probability of attackers to hack n meters in the sensing layer as $(\lambda_1, \lambda_2, \lambda_3 \ldots\ldots \lambda_n \ldots\ldots \lambda_N)$, $0 \leq \lambda_i \leq 1$, $i=1,2\ldots.,n,\ldots..N$.

Let *Pa2* be the probability of attacking data on n channels in the communication layer, then it is defined as follows:

$Pa2=Pa_{senario1}(communication\ layer) = 1/3(\eta_1 * \eta_2 * \eta_3 \ldots\ldots \eta_n) =$

$$\frac{1}{3}\prod_{i=1}^{n}\eta i \qquad (25)$$

Where, we denote the probability of attackers to hack n channels as $(\eta 1, \eta 2, \ldots, \eta n \ldots. \eta_N)$, $0 \leq \eta i \leq 1$, $i=1,2\ldots.,n...N$.

Let *Pa3* be the probability of attacking data on the control authority in the control layer, then it is defined as follows:

$Pa3=Pa_{senario1}(control\ layer) = 1/3\ \mu \quad (26)$

Where, μ is the probability for attackers to hack data into control authority, $0 \leq \mu \leq 1$.

Finally, the total overall probability of successfully attack in the first scenario:

$P_{first\ scenario} = 1/3\ (Pa1 + Pa2 + Pa3) =$

$$\frac{1}{3}\left(\prod_{i=1}^{n}\lambda i + \prod_{i=1}^{n}\eta i + \mu\right) \quad (27)$$

## 4.3 Second Scenario

This scenario where the smart grid uses both of the authentication process as the main protection method and the Blockchain Technology. Table. 5 shows the second case where there is a data protection mechanisms using blockchain technology, and two pairs of keys that are using for encryption data before transmission of data. Let *Pb1* be the probability of attacking data on *n* smart meters in the sensing layer before transmitting, then it is defined as follows:

$Pb1 = Pb_{senario2}(sensing\ layer) = 1/3(\bar{\lambda}_1 * \bar{\lambda}_2 * \bar{\lambda}_3 ..... \bar{\lambda}_n).(\bar{\xi}_1 * \bar{\xi}_2 * \bar{\xi}_3 * ..... \bar{\xi}_n) =$

$$\frac{1}{3}\left(\prod_{i=1}^{n}\bar{\lambda} i \times \prod_{i=1}^{n}\bar{\xi} \iota\right) \quad (28)$$

Where, we denote the probability of attackers to hack n meters as $(\bar{\lambda}_1, \bar{\lambda}_2, \bar{\lambda}_3 ..... \bar{\lambda}_n ... \bar{\lambda}_N)$, $0 \leq \bar{\lambda}_i \leq 1$, $i=1,2..,n...N$.

While, the probability of attackers to steal a node's pair of keys as $(\bar{\xi}1, \bar{\xi}2, \bar{\xi}3, ... \bar{\xi}n ... \bar{\xi}N)$, $0 \leq \bar{\xi}n \leq 1$, $i=1,2..,n...N$.

Let *Pb2* be the probability of attacking data on $\bar{k}$ channels in the communication layer (scenario2), then it is defined as follows:

*Pb2=Pb$_{senario2}$(communication layer) =*

$$\frac{1}{3}\left(\prod_{i=1}^{\bar{k}} \bar{\eta} i \times \prod_{i=1}^{n} \bar{\xi} \iota\right) \qquad (29)$$

Where, we denoted the probability of attackers to hack $\bar{K}$ channel as *($\bar{\eta}_1$, $\bar{\eta}_2$,..... $\bar{\eta}_{\bar{K}}$), $0 \leq \bar{\eta}\, \bar{k} \leq 1$, i=1,2,.. $\bar{K}$ , where $\bar{K}$ is the number of communication channels:*

*$\bar{K}$ = ceil[$\tau \cdot N(N-1)/2$], $\tau$ voting threshold (50% < $\tau$ < 100%).*

While, the probability of attackers to steal a node's pair of keys as *( $\bar{\xi}_1$, $\bar{\xi}_2$ , $\bar{\xi}_3$ ,... $\bar{\xi}_n$...$\bar{\xi}_N$), $0 \leq \bar{\xi}_n \leq 1$, i=1,2..,n...N.*

Let *Pb3* be the probability of attacking data on K node on the control authority in the control layer (scenario2), then it is defined as follows:

*Pb3=Pb$_{senario2}$(control layer) =*

$$\frac{1}{3}\left(\prod_{i=1}^{K} \bar{\eta} i \times \prod_{i=1}^{n} \bar{\xi} \iota\right) \qquad (30)$$

Where, we denoted the probability of attackers to hack K node before verification as *($\bar{\eta}_1$, $\bar{\eta}_2$,..... $\bar{\eta}_K$), $0 \leq \bar{\eta}_K \leq 1$, i=1,2,..K* ,where the number of nodes is*: K = ceil($\tau \cdot N$),* $\tau$ is the voting threshold *(50% < $\tau$ < 100%).*

where, the probability of attackers to steal a node's pair of keys as *( $\bar{\xi}_1$, $\bar{\xi}_2$ , $\bar{\xi}_3$ ,... $\bar{\xi}_n$...$\bar{\xi}_N$), $0 \leq \bar{\xi}_n \leq 1$, i=1,2..,n...N.*

Finally, the total overall probability of successfully attack in the second scenario is defined as follows:

$P_{second\ scenario} = 1/3\ (Pb1 + Pb2 + Pb3) =$

$$\frac{1}{3}\left[\prod_{i=1}^{n}\bar{\lambda} \times \prod_{i=1}^{n}\bar{\xi} + \prod_{i=1}^{\bar{k}}\bar{\eta} \times \prod_{i=1}^{n}\bar{\xi} + \prod_{i=1}^{K}\bar{\eta} \times \prod_{i=1}^{n}\bar{\xi}\right] \quad (31)$$

## 4.4 Third Scenario

This scenario is the proposed framework where the smart grid uses both of the previous technologies (authentication process as the main protection method and the Blockchain Technology) and the reputation score values.

Table 6. Successful attacking probability in the proposed framework.

| Item | | Scenario3 |
|---|---|---|
| Data before sent in the sensing Layer | Capability | Hack into n smart meters :Gain n pairs of keys info **and reputation score value RS**. |
| | Probability | $\frac{1}{3}\prod_{i=1}^{n}\bar{\lambda}i \times \prod_{i=1}^{n}\bar{\xi}\imath \times \prod_{i=1}^{n}\bar{\S}\imath$ |
| Data during transmission in the communication layer | Capability | Hack into $\bar{K}$ channel :Gain n pairs of keys info **and n reputation score info RS**. |
| | Probability | $\frac{1}{3}\left(\prod_{i=1}^{\bar{k}}\bar{\eta}i \times \prod_{i=1}^{n}\bar{\xi}\imath \times \prod_{i=1}^{n}\bar{\S}\imath\right)$ |
| Data after it is received in the control layer | Capability | Hack into K meters :Gain n pairs of keys info **and n reputation score info RS.** |
| | Probability | $\frac{1}{3}\left(\prod_{i=1}^{K}\bar{\eta}i \times \prod_{i=1}^{n}\bar{\xi}\imath \times \prod_{i=1}^{n}\bar{\S}\imath\right)$ |

Table. 6 shows the proposed framework. Our contribution to this new framework is that we use the reputation score value in addition to all the previous protection techniques to increase reliability and security mechanisms. In this case, let (*Pc1*) be the probability of attacking data on *n* meters in the sensing layer before transmitting (Scenario 3), then (*Pc1*) is defined as follows:

*Pc1=Pc$_{senario3}$(sensing layer) =*

$$\frac{1}{3}\prod_{i=1}^{n}\bar{\lambda}i \times \prod_{i=1}^{n}\bar{\xi}\iota \times \prod_{i=1}^{n}\bar{\S}\iota \qquad (32)$$

Where, we denote the probability of attackers to steal each node's reputation score value as *( $\bar{\S}_1$, $\bar{\S}_2$ , $\bar{\S}_3$ ,… $\bar{\S}_n$…$\bar{\S}_N$), 0 ≤ $\bar{\S}n$ ≤1, i=1,2..,n…N.*

Let *Pc2* be the probability of attacking data on $\bar{K}$ channels in the communication layer (Scenario3), then it is defined as: *Pc2=Pc$_{senario3}$(communication layer) =*

$$\frac{1}{3}\left(\prod_{i=1}^{\bar{k}}\bar{\eta}i \times \prod_{i=1}^{n}\bar{\xi}\iota \times \prod_{i=1}^{n}\bar{\S}\iota\right) \qquad (33)$$

*Where in each transaction we will use a node's reputation value.*

Let *Pc3* be the probability of attackers to hack K nodes on the control authority in the control layer (Scenario3), then *PC3* is defined as follows:

*Pc3=Pc$_{senario3}$(control layer) =*

$$\frac{1}{3}\left(\prod_{i=1}^{K}\bar{\eta}i \times \prod_{i=1}^{n}\bar{\xi}\iota \times \prod_{i=1}^{n}\bar{\S}\iota\right) \qquad (34)$$

Finally, The total overall probability of successfully attack in the Scenario3 (proposed framework):

$P_{Third\ scenario} = 1/3\ (Pc1 + Pc2 + Pc3) =$

$$\frac{1}{3}\prod_{i=1}^{n}\bar{\lambda}i \times \prod_{i=1}^{n}\bar{\xi}\imath \times \prod_{i=1}^{n}\bar{\S}\imath \; + \frac{1}{3}\left(\prod_{i=1}^{\bar{k}}\bar{\eta}i \times \prod_{i=1}^{n}\bar{\xi}\imath \times \prod_{i=1}^{n}\bar{\S}\imath\right)$$

$$+ \; \frac{1}{3}\left(\prod_{i=1}^{K}\bar{\eta}i \times \prod_{i=1}^{n}\bar{\xi}\imath \times \prod_{i=1}^{n}\bar{\S}\imath\right) \quad (35)$$

## Conclusion

Here, we introduce mathematical analyzes of three different scenarios to obtain useful equations that can be used in simulations for smart grids. These mathematical equations represent a useful way to produce 3 units. In the next chapter, we use these equations in the  IEEE 118 benchmark to extract knowledge from the results.

# CHAPTER 5: CASE STUDY AND RESULTS

At first before going into details of the results, here a brief description of the summary of the findings, to show how all these protect SG from FDI attacks. Mathematical proof in the proposed approach proves based on probabilities that this approach using blockchain technology and reputation system will reduce the probability of any cyberattack, whether that attack is external or internal.

The external attacker must get the system user's credentials to get the permissions. Hence, when he gets these credentials, he becomes an insider attacker who can use a user's private encryption keys (private key and public key). Here, reputation score value is a hindrance to him, as this value must be known to him to be able to carry out the FDI attack, and impossible because the reputation score value depends on many parameters that change every period. All this increases the complexity of carrying out any external or internal attack and thus reduces the likelihood of the attack succeeding as has been demonstrated mathematically and it will be provided in practice by simulation software.

The rest of this section consists of the following parts: The first section describes the reference system used to study the various scenarios of any cyberattack, and this reference is the IEEE-118 standard. The second section presents the results of the mathematical foundation and the results of the practical simulations.

## 5.1 Case Study – IEEE 118 Benchmark

The IEEE-118 benchmark is considered as a reference system used to study various scenarios of any cyberattack, in which case, we use this framework to study and compare the results of using 3 different scenarios. This benchmark consists of 54

generators, 118 nodes (each node collects many measurements as current, power flow, and voltage). 186 branches (collects line status as a digital information OPEN/CLOSED), at the end of the line in each branch there are two meters.

We now have three mathematical equations (27, 31 and 35); each equation representing the probability of a cyberattack in three layers (sensing, communication, and control layer) of different scenarios (1, 2, 3). We denote these probabilities as follows: *Pa, Pb, Pc*. Using Matlab on the personal device, those default values (in IEEE-188 benchmark) were adopted in previous mathematical equations to extract the results, as we applied several nodes (representing smart nodes in the large network) ranging from 1 to 676.

## 5.2 The Results

Analysis and discussions of the results are provided in this subsection. Initially, results for mathematical foundation are presented with Matlab. Second, the practical application results of our simulation with Node.js are presented step-by-step.

### *5.2.1 Mathematical Foundation Results*

**Scenario 1**, in this scenario, the total numbers of the sensors that are responsible for gathering the information are defined as follows:

$Total\_Sensors_{scenario1}$ = *the sensors number in the nodes + the sensors number in the branches + the sensors number in end of each line = 118 + 186 + 186 *2=676.*

The total number of communication channels between the nodes and control authority is equal 676:

$Total\_Channels_{scenario1} = 676$

Where we assume that the probability of a successful attack on a control center database

in scenario 1 is 0.001, and the range of *n* is between these boundaries [1…676]. Hence, we can write Eq.(27) as :

$$Pa = \frac{1}{3}\left(x^n + x^n + 0.001\right) = \frac{1}{3}\left(2x^n + 0.001\right) \quad (36)$$

**Scenario 2**, in this scenario, the total number of the sensors (the same as in scenario1) is:

$Total\_Sensors_{scenario2} = 118 + 186 + 186 * 2 = 676.$

The number of communication channels between the nodes and control authority, in this case, is defined as follows:

$Total\_Channels_{scenario2} = N(N-1)/2 = 676(676-1)/2 = 228{,}150.$

If the voting threshold $\tau$ is set to a random value more than 50% (we assume that $\tau$ = 51%. Then:

$K = ceil[51\% \times 676] = 345$

and $\overline{K} = ceil[51\% \times 676 \times (676 - 1)/2] = 116,357$

Hence, we can write Eq.(31) as follows :

$$Pb = \frac{1}{3}\left(x^n.x^n + x^n.x^{116357} + x^n.x^{345}\right) = \frac{x^n}{3}\left(x^n + x^{116357} + x^{345}\right) \quad (37)$$

**Scenario 3** (the new proposed framework ): In this scenario, as we mentioned before that we added a reputation score value that an adversary may guess. It is in three layers (sensing, communication, and control layer) to obtain a successful attack. Hence, we can write Eq.(35) as :

$$Pc = \frac{1}{3}\left(x^n.x^n.x^n + x^n.x^n.x^{116357} + x^n.x^n.x^{345}\right) = \frac{x^{2n}}{3}\left(x^n + x^{116357} + x^{345}\right) \quad (38)$$

In the previous three mathematical equations (36,37,38), we consider that:

$x = \lambda i = \bar{\lambda} i = \eta i = \bar{\eta} i = \bar{\xi} i = \bar{\S}$i in [0.9, 0.999], and n in [1,11,21,31…..676]. Then we get the following results:

Figure. 13 shows the successful attacking probability and overall probability in the first scenario(1).

Where we note (for example) that when the number of smart meters equals n = 11 and the successful attack probability is (x = 0.9), the result of the total probability is (Pa = 0.2)

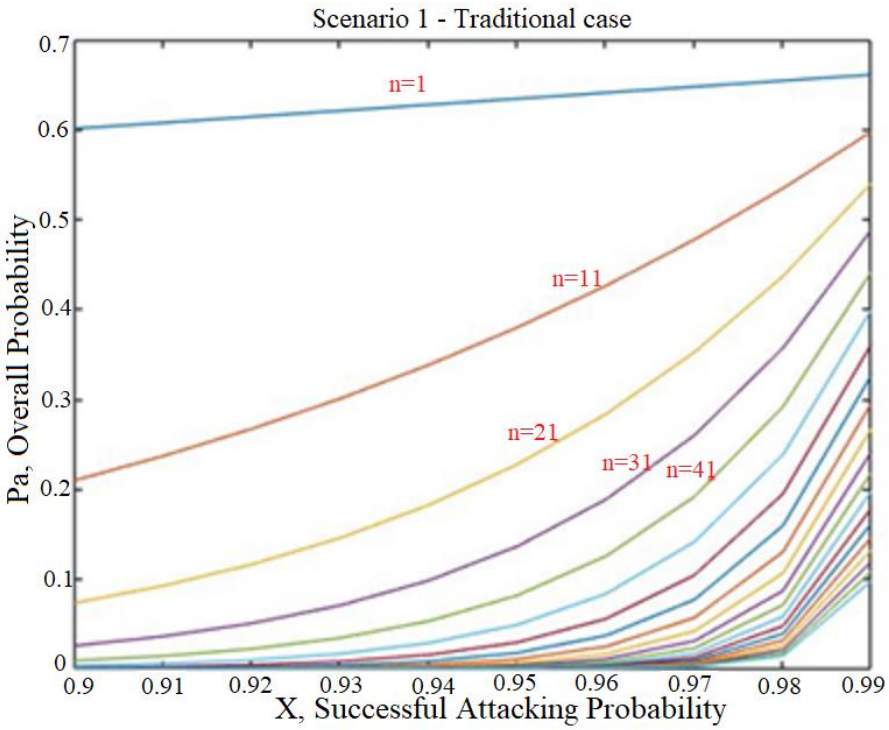


Figure.13. This is a traditional scenario where smart grids use only authentication as the main protection methods.

Figure.14 shows the successful attacking probability and overall probability in the second scenario (2), this scenario is the implementation of Blockchain technology to smart grids. Where we note (for example) that when the number of smart meters equals n = 11 and the successful attack probability is (x = 0.9), the result of the total probability is (*Pb* = 0.78). This is an indication that the results of the second scenario are much better than the first scenario.

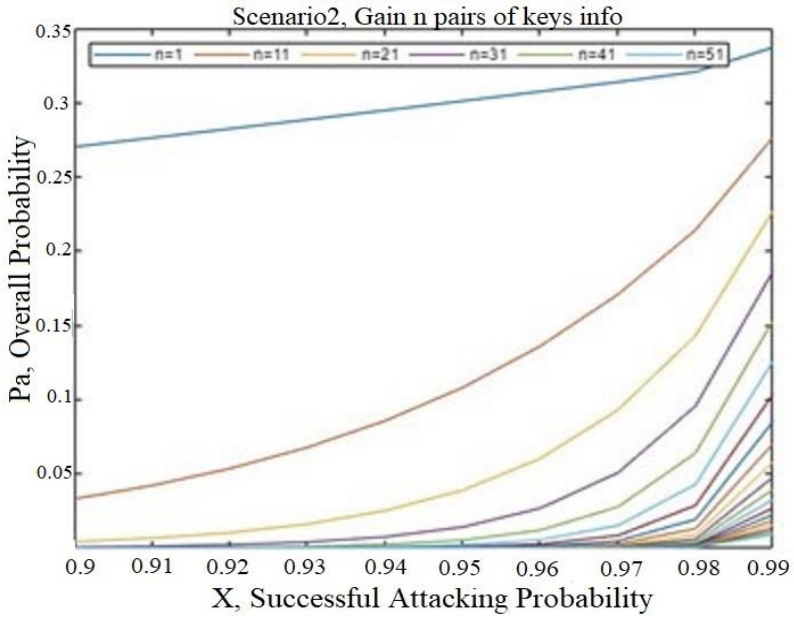


Figure. 14. Scenario 2, the implementation of Blockchain technology to SGs.

Figure.15 shows the successful attacking probability and overall probability in the proposed framework.

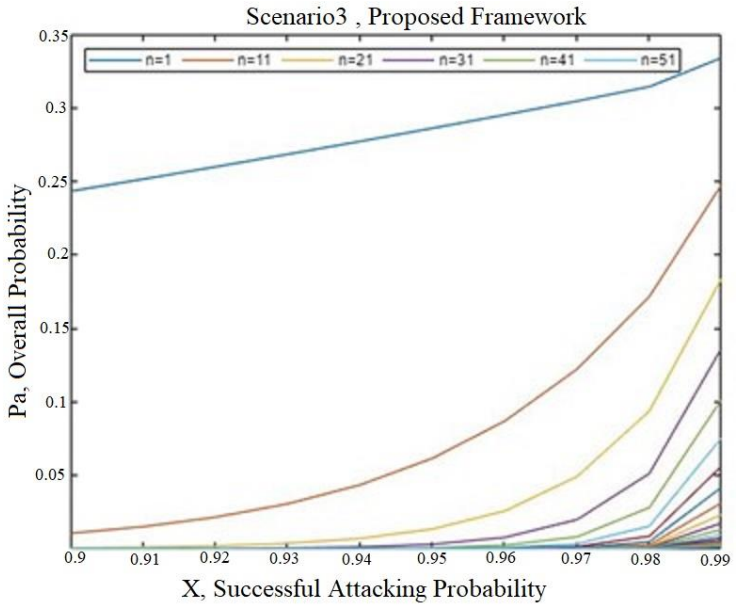


Figure.15. Scenario 3, this scenario is a combined implementation of both, Blockchain and the reputation score to smart grids.

Figure.16 shows the comparison of a successful attacking probability and overall probability in three scenarios when the number of smart meters equals n = 11. This is an indication that the results of the proposed scheme are much better than the first and the second scenarios.

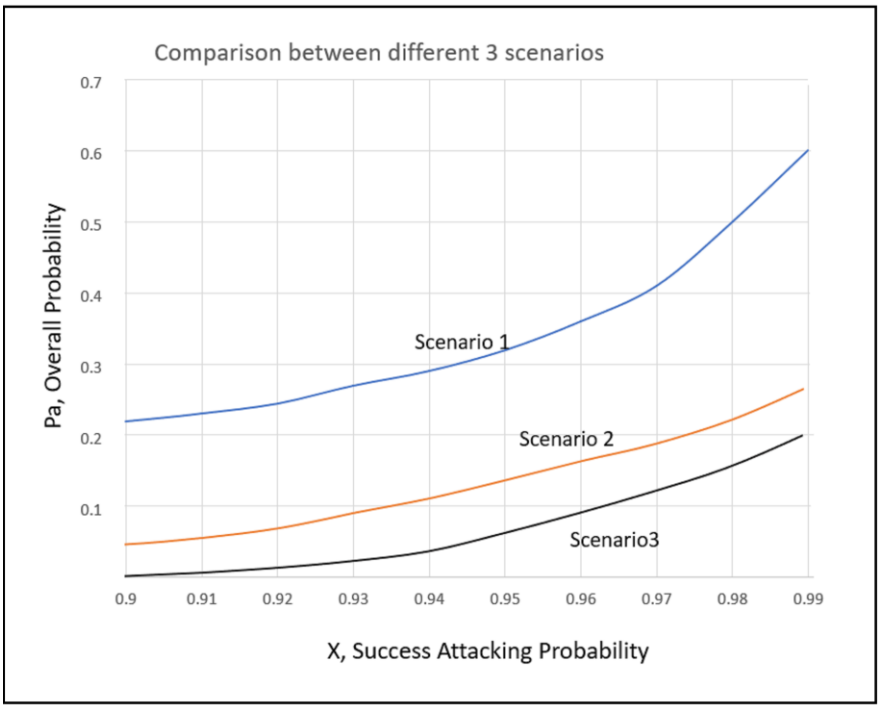


Figure.16 The comparison of a successful attacking probability and overall probability in three scenarios (n=11).

### *5.2.2Simulation Results*

In this framework we use Node.js for the implementation by generation virtual smart meters in [0…40]. We consider that the *CA* is the server that can response events (index.js) and analyze them (performance evaluation) to make the right classification for smart meters. We are running a simulation of the Qatari electricity transmission network as shown in Figure. 17, and Figure. 18 (Figure. 17 represents the nationality

electricity transmission grid in Qatar).


Figure. 17. Power Grid in Qatar.

The following picture (Figure. 18) illustrates a simulated map of Qatar's electricity grid structure. We used a simulation library (simulator.js) which uses geo-values for data based on the default geolocation for each power subsection, where it is an expressive simulation of the reality.

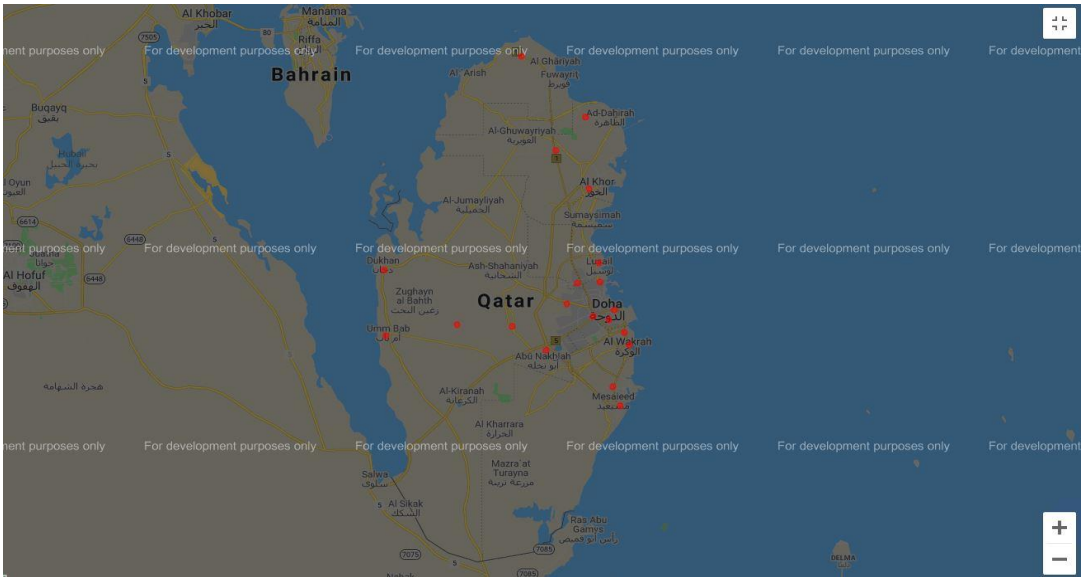


Figure 18. Simulation map of Qatar's power grid**.**

In this framework, Gas is a measurement which is using in Solidity). Besides, we depend on using the Ganache tool which quickly provides a private.

Since the major programming language used is JavaScript, the Node.js platform is used for the execution. The simulation process for a smart grid gives us excellent results that support mathematical proof (see Figure. 24).

Figure. 19 shows the results of the Weighted Sum Method (WSM) when applying this method to a simple database presented earlier in Table 3. This method is a suitable option that depends on many factors related to the node behavior, as explained earlier. We can see the result of applying this to five different nodes to get the weight of each node.

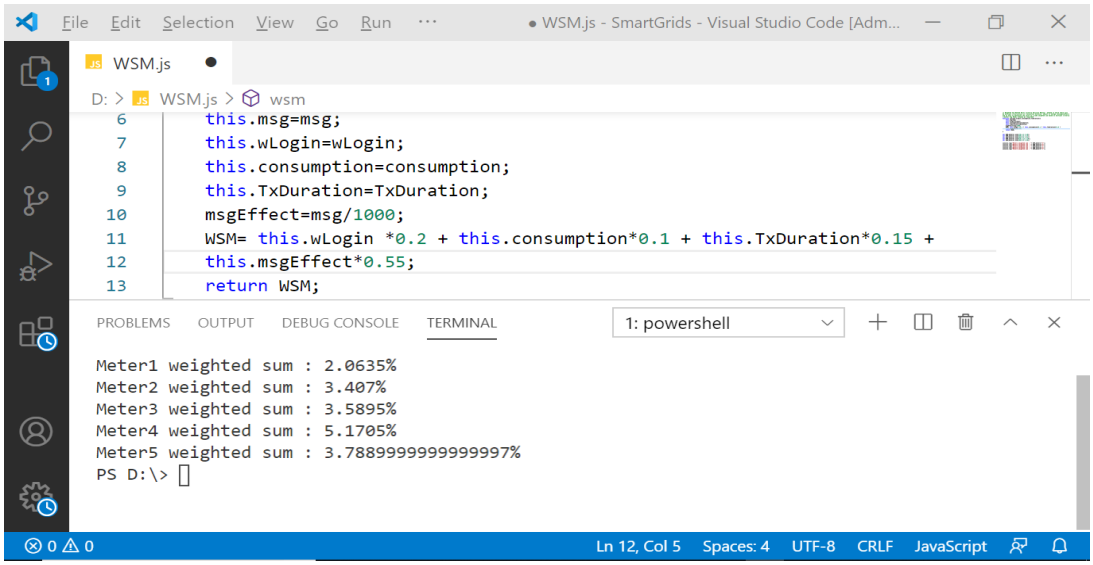


Figure 19. Weighted Sum Method simulation results.

The results of the simulation are shown in Figure 20, it introduce the classification process for smart meters to (benign, malicious, or semi hones). This is done by applying the previous simulation (Node.js) on 40 virtual nodes.

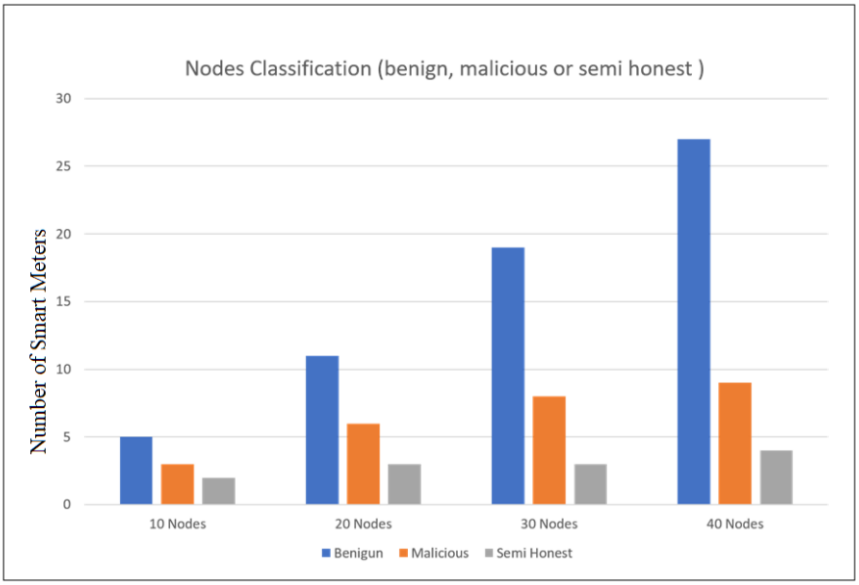


Figure.20 Nodes classifications (benign, malicious and semi hones nodes).

This facilitates the detection process of malicious nodes and make an appropriate classification for these nodes. Assume that an adversary *X* could log into the smart grid system *S*, then he is trying to send FDIA (wrong measurement) such as asking to obtain unnormal gas value (for example *X* send a transaction asking for supplying 880 gas), as shown in the Figure. 21.

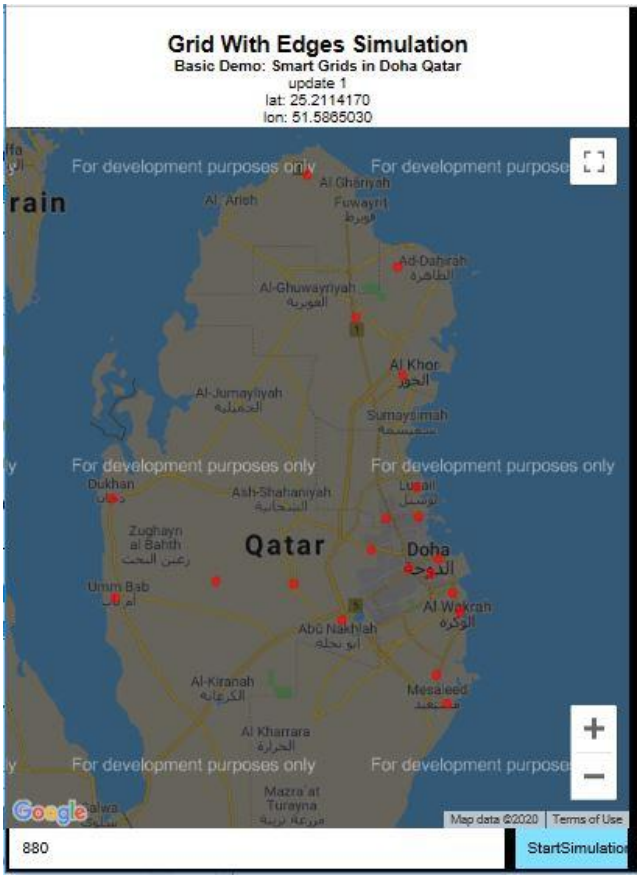


Figure 21. An adversary FDIA request.

On the server-side, the control authority (CA) analyzes the sender transaction. The reputation score system calculates the reputation value for this node(smart meter) using

Algorithm1 (in the calculation module). We consider that the default reputation score = 755, the reputation score threshold = 750 when the transaction value is 880 gas then we can see the results in Figure. 21. After the implementation as shown in Figure. 22, the new reputation score value equals 747.54, so we consider this node (smart meter) as a malicious node because the smart meter reputation score value less than the threshold (747.54<750).

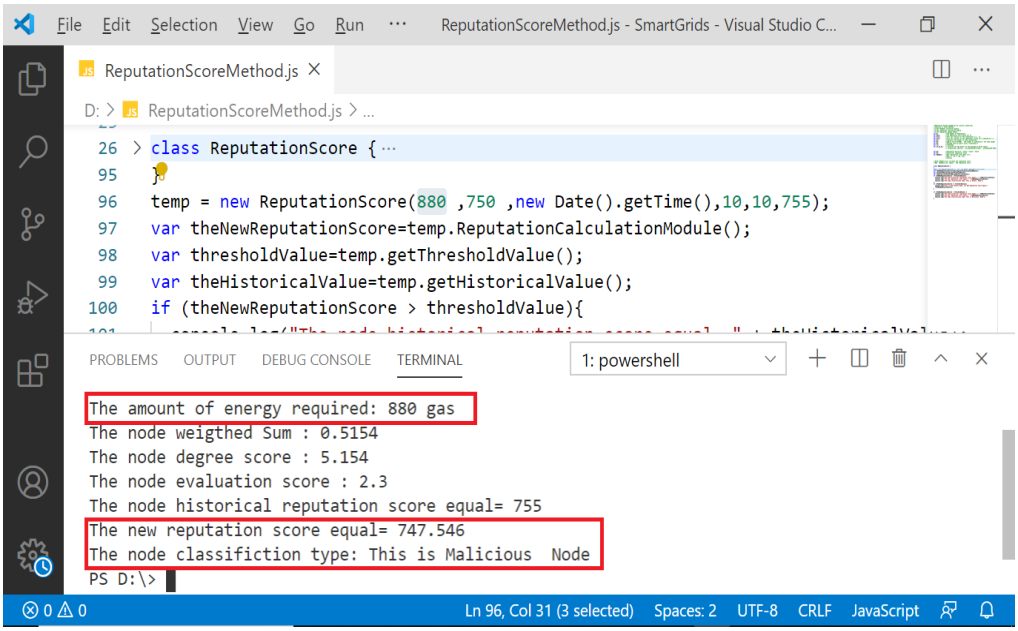


Figure 22. The Implementation results (malicious node).

Figure. 23 shows the results when the node transaction value equals to 150 gas (normal value). The implementation shows that the new reputation score value equals to 762.05, so we consider this node(smart meter) as a benign node because the smart meter reputation score value more than the threshold (762.05 > 750).

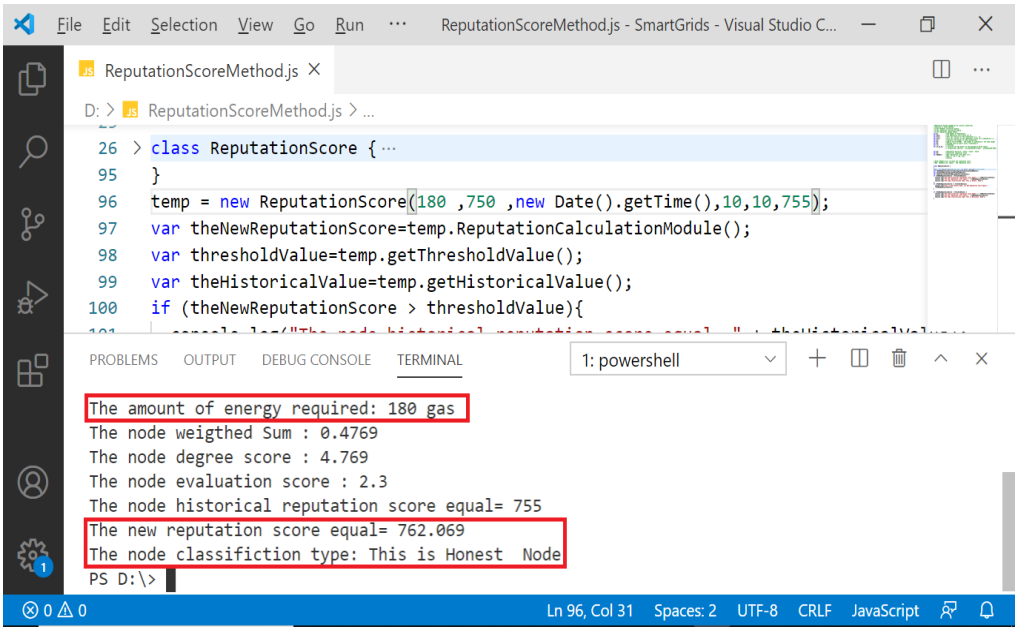


Figure 23. The implementation results(benign node).

Figure. 24 shows the new block generation process when a smart meter reputation score more than a threshold ($RS_{Threshold}$ = 750 as a default value).


Figure 24. New block generation.

Figure. 25 illustrates the number of adversaries and success rate in two scenarios. The first case, without using both Blockchain and the Reputation score, and the second case using our proposed approach.

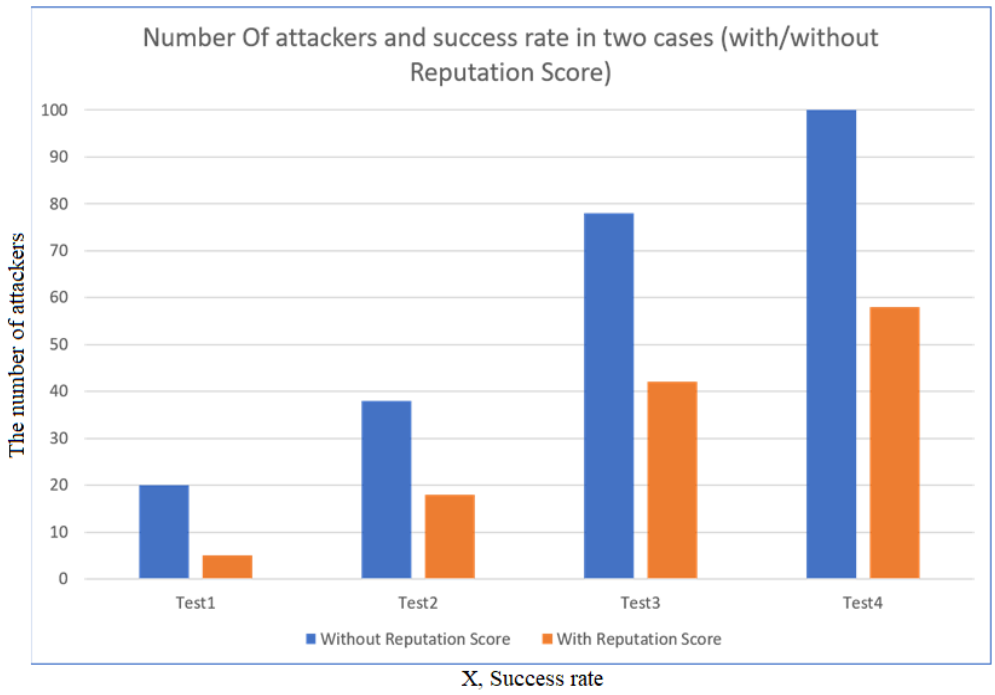


Figure 25. The number of attackers and success rates in two scenarios.

# Chapter 6: Conclusion

In this thesis, we have presented three scenarios of security issues. The first scenario represents the smart grid in the traditional case where smart grids use only authentication as the main protection methods. Scenario 2 is the implementation of Blockchain technology to smart grids. Scenario 3 is a combined implementation of both, Blockchain and the Reputation score to smart grids. Besides, we have provided a practical simulation with some useful results as we are offering a set of practical recommendations based on the mathematical foundation on when the people should apply the above scenarios to smart grids to deal with various attacks.

We have solved the research problems with the proposed framework as reputation results have proven to be beneficial in spotting internal attackers. Its great potential can be taken advantage of and can be improved to adapt to different requirements. This value acts as a balance, and by increasing or decreasing this value, the reputation value increases or decreases, hence the reliability of the node. Thus when it falls below a certain threshold, the permissions are removed from the user.

We used a simple dataset in this work, but this method can rely on real and huge datasets. We can also apply the proposed framework to any IoT application and not only to smart grids, taking into consideration the fundamental differences between those applications to make the simple and necessary adjustments to be compatible with every application that wishes to apply this framework. This approach gives smart grid systems a significant advantage to address cyber-attacks as the Algorithm1 can calculate the scores, which are kept secret and never shared under any circumstances.

In the future work, we can use the same method on any IoT application but we might face some problems. For example, the data that are stored in a smart meter memory in the blockchain's form. Besides, the size of the smart node memory is limited

and because of the increase in the ledger size, this may cause this data to be lost over time. This is when the node memory capacity is less than the increased data volume.

However, we can reduce the blockchain size and solve the ever-growing Blockchain problem by using the floating genesis block which will improve the cost of distributing this ledger copy to each meter memory. In the future work, we especially recommend implementing the floating genesis block and its advantages on the smart grid. This method can decrease the size of the blockchain and that will improve the cost of distributing the copy of this ledger to each smart meter's memory.

REFERENCES

[1] A. S. G. Andrae and T. Edler, ‘‘On global electricity usage of communication technology: Trends to 2030,’’ Challenges, vol. 6, no. 1, pp. 117–157, 2015.

[2] E. Brynjolfsson, P. Hofmann, and J. Jordan, ‘‘Cloud computing and electricity: Beyond the utility model,’’ Commun. ACM, vol. 53, no. 5, pp. 32–34, 2010.

[3] C. Baylon, ``Lessons from Stuxnet and the realm of cyber and nuclear security: Implications for ethics in cyber warfare," in Ethics and Policies for Cyber Operations. Cham, Switzerland: Springer, 2017, pp. 213_229. [Online]. Available: https://doi.org/10.1007/978-3-319-45300-2_12.

[4] A. Hansen, J. Staggs, and S. Shenoi, ``Security analysis of an advanced metering infrastructure," Int. J. Crit. Infrastruct. Protection, vol. 18, pp. 3_19, Sep. 2017. [Online].Available:http://www.sciencedirect.com/science/article/pii/S1874548217300495.

[5] S. Gorman, ``Electricity grid in US penetrated by spies," Wall Street J., vol. 8, pp. 1_3, Apr. 2009.

[6] D. Starkey. Hacker Group Dragon_y Takes Aim at us Power Grid. [Online]. Available:https://www.geek.com/tech/hacker-groupdragon_ytakes-aim-at-us power-grid-1715157

[7] Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, and S. Sezer, ``Multidimensional intrusion detection system for IEC 61850- BASED SCADA networks," IEEE Trans. Power Del., vol. 32, no. 2, pp. 1068_1078, Apr. 2017.

[8] I. Modbus. (2004). MODBUS Application Protocol Speci_cation v1.1a. [Online]. Available:http://www.modbus.org/docs/ModbusApplication_Protocol_V1_1a.pdf

[9] I. Modbus. (2004). Modbus messaging on TCP. [Online]. Available: http://www.modbus.org/docs/Modbus_Messaging_Implementation _Guide_V1_0b.pdf.

[10] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, ``Attack taxonomies for the modbus protocols," Int. J. Crit. Infrastruct. Protection, vol. 1, pp. 37_44, Dec. 2008.[Online].Available:http://www.sciencedirect.com/science/article/pii/S18745 4820800005X.

[11] S. East, J. Butts, M. Papa, and S. Shenoi, ``A taxonomy of attacks on the DNP3 protocol," in Critical Infrastructure Protection III, C. Palmer and S. Shenoi, Eds. Berlin, Germany: Springer, 2009, pp. 67_81.

[12] P. Matou²ek. (2018). Description of IEC 61850 communication. Faculty for Information,Technology.[Online].Available:http://www._t.vutbr.cz/research/view _pub.php.en?id=11832

[13] R. E. Mackiewicz, ``Overview of IEC 61850 and bene_ts," in *Proc. IEEE PES* Transmiss. Distrib. Conf. Exhibit., May 2006, pp. 376_383.

[14] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, ``Analysis of IEEE C37.118 and IEC 61850-90-5 synchrophasor communication frameworks," in Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM), Jul. 2016, pp. 1_5.

[15] R. Deng, G. Xiao, and R. Lu, “Defending against false data injection attacks on power system state estimation,” IEEE Trans. Ind. Informat., vol. PP, no. 99, pp. 1–10, to be published, doi: 10.1109/TII.2015.2470218.

[16] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, ``Attack taxonomies for the modbus protocols," Int. J. Crit. Infrastruct. Protection, vol. 1, pp. 37_44, Dec. 2008.[Online].Available:http://www.sciencedirect.com/science/article/pii/S18745 4820800005X.

[17] S. East, J. Butts, M. Papa, and S. Shenoi, ``A taxonomy of attacks on the DNP3 protocol," in Critical Infrastructure Protection III, C. Palmer and S. Shenoi, Eds. Berlin, Germany: Springer, 2009, pp. 67_81.

[18] P. Matou²ek. (2018). Description of IEC 61850 communication. Faculty for Information,Technology.[Online].Available:http://www._t.vutbr.cz/research/view _pub.php.en?id=11832

[19] R. E. Mackiewicz, ``Overview of IEC 61850 and bene_ts," in Proc. IEEE PES Transmiss. Distrib. Conf. Exhibit., May 2006, pp. 376_383.

[20] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, “Cyber-security in smart grid: Survey and challenges," Comput. Elect. Eng., vol. 67, pp. 469_482,

Apr.2018.[Online].Available:http://www.sciencedirect.com/science/article/pii/S00
45790617313423.

[21] F.Wang, Z. Lei, X.Yin, Z. Li, Z. Cao, andY.Wang, ``Information security in the smart grid: Survey and challenges," in Geo-Spatial Knowledge and Intelligence, H. Yuan, J. Geng, C. Liu, F. Bian, and T. Surapunt, Eds. Singapore: Springer, 2018, pp. 55_66.

[22] W.-L. Chin, C.-H. Lee, and T. Jiang, ``Blind false data attacks against AC state estimation based on geometric approach in smart grid communications," IEEE Trans. Smart Grid, vol. 9, no. 6, pp. 6298_6306, Nov. 2018.

[23] Y. He, G. J. Mendis, and J. Wei, ``Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," IEEE Trans. Smart Grid., vol. 8, no. 5, pp. 2505_2516, Sep. 2017.

[24] Y. E. Song, Y. Liu, S. Fang, and S. Zhang, ``Research on applications of the Internet of Things in the smart grid," in Proc. 7th Int. Conf. Intell. Hum.-Mach. Syst. Cybern., vol. 2, Aug. 2015, pp. 178_181.

[25] Mohsen Fadaee Nejad; AminMohammad Saberian; Hashim Hizam; et al. (2013). “Application of smart power grid in developing countries”. 2013 IEEE 7th International Power Engineering and Optimization Conference (PEOCO) (PDF).IEEE.Pp. 427431. doi:10.1109/PEOCO.2013.6564586. ISBN 97 8-1-4673-5074-7.

[26] X. Fang, S. Misra, G. Xue, and D. Yang, ‘‘Smart grid—The new and improved power grid: A survey,’’ IEEE Commun. Surveys Tuts., vol. 14, no. 4, pp. 944–980, 4th Quart., 2011.

[27] W. Wang, Y. Xu, and M. Khanna, ‘‘A survey on the communication architectures in smart grid,’’ Comput. Netw., vol. 55, no. 15, pp. 3604–3629, 2011.

[28] L. Lyu, K. Nandakumar, B. I. P. Rubinstein, J. Jin, J. Bedo, and M. Palaniswami, “PPFA: Privacy preserving fog-enabled aggregation in smart grid,” IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3733–3744,Aug. 2018.

[29] W. Wang, Y. Xu, and M. Khanna, ‘‘A survey on the communication architectures in smart grid,’’ Comput. Netw., vol. 55, no. 15, pp. 3604–3629, 2011.

[30] N. GENSOLLEN, V. GAUTHIER, M. BECKER, AND M. MAROT, STABILITY AND PERFORMANCE of coalitions of prosumers through diversification in the smart grid, IEEE Trans. Smart Grid, vol. 9, no. 2, pp. 963970, Mar. 2018.

[31] X. Fang, S. Misra, G. Xue, and D. Yang, “Smart grid - the new and improved power grid: A survey,” IEEE Communications Surveys Tutorials, vol. 14, no. 4, pp. 944–980, Fourth 2012.

[32] https://www.smartgrid.gov/the_smart_grid/smart_grid.html.

[33] Peter Behr and Blake Sobczak, “Utilities Look Back to the Future for Hands-on Cyberdefense,” E&E News, last modified July 21, 2016, https://www.eenews.net/stories/1060040590.

[34] Pavel Polityuk, Oleg Vukmanovic, and Stephen Jewkes, “Ukraine’s Power Outage Was a Cyberattack: Ukrenergo,” Reuters, last modified January 18, 2017, https://www.reuters.com/article/us-ukrainecyber-attack-energy/kiev-poweroutage-in-december-was-cyber-attacukrenergo-idUSKBN1521BA.

[35] Li, Qin, et al. "A reputation-based announcement scheme for VANETs." IEEE Transactions on Vehicular Technology 61.9 (2012): 4095-4108.

[36] M. Usman, M. R. Asghar, I. S. Ansari, and F. Granelli, “Towards bootstrapping trust in d2d using pgp and reputation mechanism,” in Communications (ICC), 2017 IEEE International Conference on. IEEE, 2017, pp. 1–6.

[37] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, “RSMA: Reputation System-Based Lightweight Message Authentication Framework and Protocol for 5G-Enabled Vehicular Networks,” IEEE Internet Things J., vol. 6, no. 4, pp. 6417–6428, 2019, doi: 10.1109/JIOT.2019.2895136.

[38] F. Dötzer, L. Fischer, and P. Magiera, “VARS: A vehicle ad hoc network reputation system,” in Proc. 6th IEEE Int. Symp. World Wireless Mobile Multimedia Netw., 2005, vol. 1, pp. 454–456.

[39] David Kim, Michael G. Solomon (2010). Fundamentals of Information Systems Security. Jones , Bartlett Publishers. ISBN 978-1449671648.

[40] Li, Qin, et al. "A reputation-based announcement scheme for VANETs." IEEE Transactions on Vehicular Technology 61.9 (2012): 4095-4108.

[41] Condos J, Sorrell WH, Donegan SL. Blockchain technology: opportunities and risks. Technical report, State of Vermont, USA; 2016

[42] Burger C, Kuhlmann A, Richard P, Weinmann J. Blockchain in the energy transition a survey among decision-makers in the German energy industry.⟨https://shop.dena.de/fileadmin/denashop/media/Downloads_Dateien/esd/9165_Blockchain_in_der_Energiewende_englisch.pdf⟩,[accessed 15 May 2017] (2016).

[43] Utility Week. Electron reveals blockchain energy platform, ⟨http://utilityweek.co. uk/news/Electron-reveals-blockchain-energy-platform/⟩, [accessed 13 Jun 2017] (2017).

[44] P. Danzi, M. Angjelichinoski, Č. Stefanović, and P. Popovski, ‘‘Distributed proportional-fairness control in microgrids via blockchain smart contracts,’’ in Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), Oct. 2017, pp. 45–51.

[45] G. Liang, S. R.Weller, F. Luo, J. Zhao, and Z. Y. Dong, Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber

Attacks, IEEE Trans. Smart Grid, vol. 10, no. 3, pp. 31623173, 2019, doi: 10.1109/TSG.2018.2819663.

[46] Q.H. Dang, Secure Hash Standard, Technical Report NIST FIPS 180-4, National Institute of Standards and Technology, 2015.

[47] Gao, Jianbin, Kwame Omono Asamoah, Emmanuel Boateng Sifah, Abla Smahi, Qi Xia, Hu Xia, Xiaosong Zhang, and Guishan Dong. “Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid." IEEE Access 6 (2018): 9917-9925.

[48] N. Z. Aitzhan and D. Svetinovic, “Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams,” IEEE Trans. Dependable Secure Comput., vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.

[49] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://goo.gl/MqyCW7, Accessed on: Oct. 10, 2016.

[50] Q.H. Dang, Secure Hash Standard, Technical Report NIST FIPS 180-4, National Institute of Standards and Technology, 2015.

[51] Helff, Florian, Le Gruenwald, and Laurent d'Orazio. "Weighted Sum Model for Multi-Objective Query Optimization for Mobile-Cloud Database Environments." EDBT/ICDT Workshops. 2016.

[52] E. Triantaphyllou, Multi-criteria decision making methods: a comparative study, 44 ed., Springer Science & Business Media, 2013.

[53] I. Kim and O. de Weck, "Adaptive weighted-sum method for bi-objective optimization: Pareto front generation," in Structural and multidisciplinary optimization 29.2 , 2005, pp. 149-158.

[54] C.-H. Goh, Y.-C. A. Tung and C.-H. Cheng, " A revised weighted sum decision model for robot selection," in Computers & Industrial Engineering Vol.30(2), 1996.

[55] Cyber-attack against Ukrainian critical infrastructure, Alert (IRALERT-H-16-056-01) (2016) The Industrial Control Systems— Cyber Emergency Response Team (ICS-CERT), Department of Homeland Security, Washington, DC.

[56] N. Mhaisen, N. Fetais, and A. Massoud, Secure smart contractenabled control of battery energy storage systems against cyberattacks, Alexandria Eng. J., vol. 58, no. 4, pp. 12911300, 2019, doi: 10.1016/j.aej.2019.11.001.

[57] Idaho National Laboratory (INL). Vulnerability Analysis of Energy Delivery Control Systems, September 2011.

[58] National Institute of Standards and Technology (NIST). NISTIR 7628: Guidelines for Smart Grid Cyber Security, August 2010.

[59] M. Davis. Smart grid device security adventures in a new medium. IOA active,2009.http://www.blackhat.com/presentations/usa09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf (Accessed: 04- 22-2013).

[60] R. Wightman. Project Basecamp: Hacking and Exploiting PLC's. S4 Conference, January 2012.

[61] N. Falliere, L. Murchu, and E. Chien. W32.Stuxnet Dossier, Version 1.3. Symantec, Nov. 2010.

[62] U.S. House of Representatives, 112th Congress. Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, A report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence, October 2012.

[63] I. N. Fovino, A. Carcano, M. Masera, and A. Trombetta. An experimental investigation of malware attacks on SCADA systems. International Journal of Critical Infrastructure Protection, 2(4):139 { 145, 2009.

[64] N. Falliere, L. Murchu, and E. Chien. W32.Stuxnet Dossier, Version 1.3. Symantec,Nov.2010,http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (Accessed: 04-22-2013).

[65] Liu Y, Ning P, Reiter MK (2009) False data injection attacks against state estimation in electric power grids. In: Proceedings of the 16th ACM conference on computer and communications security (CCS'09), Chicago, IL, 9–13 Nov 2009, 12 pp.

[66] Liu Y, Ning P, Reiter MK (2011) False data injection attacks against state estimation in electric power grids. ACM Trans Inf Syst Secur 14(1): Article 13/1-33.

[67] Liang GQ, Zhao JH, Luo FJ et al (2016) A review of false data injection attacks against modern power systems. IEEE Trans Smart Grid. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber= 7438.

[68] Understanding the Smart Grid: Features, Benefits and Costs", U.S. Department of Energy, National Energy Technology Laboratory, 2008.

[69] Yuan YL, Li ZY, Ren K (2012) Quantitative analysis of load redistribution attacks in power systems. IEEE Trans Parallel Distrib Syst 23(9):1731–1738.

[70] N. Mhaisen, N. Fetais, and A. Massoud, Secure smart contractenabled control of battery energy storage systems against cyberattacks, Alexandria Eng. J., vol. 58, no. 4, pp. 12911300, 2019, doi: 10.1016/j.aej.2019.11.001.

[71] G. Liang, S. R.Weller, F. Luo, J. Zhao, and Z. Y. Dong, Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks, IEEE Trans. Smart Grid, vol. 10, no. 3, pp. 31623173, 2019, doi: 10.1109/TSG.2018.2819663.

[72] G. Liang, S. R.Weller, F. Luo, J. Zhao, and Z. Y. Dong, Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber

Attacks, IEEE Trans. Smart Grid,vol. 10, no. 3, pp. 31623173, 2019, doi: 10.1109/TSG.2018.2819663.

[73] M. Usman, M. R. Asghar, I. S. Ansari, and F. Granelli, “Towards bootstrapping trust in d2d using pgp and reputation mechanism,” in Communications (ICC), 2017 IEEE International Conference on. IEEE, 2017, pp. 1–6.

[74] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, “RSMA: Reputation System-Based Lightweight Message Authentication Framework and Protocol for 5G-Enabled Vehicular Networks,” IEEE Internet Things J., vol. 6, no. 4, pp. 6417–6428, 2019, doi: 10.1109/JIOT.2019.2895136.

[75] Triantaphyllou, Evangelos. "Multi-criteria decision making methods." Multi-criteria decision making methods: A comparative study. Springer, Boston, MA, 2000. 5-21.

[76] Busygin, Alexey, et al. "Floating Genesis Block Enhancement for Blockchain Based Routing Between Connected Vehicles and Software-defined VANET Security Services." Proceedings of the 11th International Conference on Security of Information and Networks. 2018.

[77] https://www.esri.com/about/newsroom/blog/german-cybersecurity-experts-use-gis/