BLOCKCHAIN-INTEGRATED SMART GRID ARCHITECTURE WITH FBG SENSING AND EKF FOR FAULT AND ANOMALY DETECTION

by

SURAH ADEL AL DAKHL

A dissertation submitted in partial fulfillment of the
requirements for the degree of

DOCTOR OF PHILOSOPHY IN ELECTRICAL AND COMPUTER ENGINEERING

2025

Oakland University
Rochester, Michigan

Doctoral Advisory Committee:

Mohamed Zohdy, Ph.D., Chair
Jia Li, Ph.D.
Ryan Monroe, Ph.D.
Darrell Schmidt, Ph.D.

© Copyright by Surah Adel Al Dakhl, 2025
All rights reserved

Dedication

This work is dedicated to my loving and supportive parents, whose unwavering encouragement and belief in me have been the foundation of my academic journey. Their guidance, sacrifices, and unconditional love have shaped me into the person I am today.

To my wonderful husband, whose patience, understanding, and unwavering support have been my anchor throughout this challenging yet fulfilling PhD journey. Your encouragement and steadfast belief in my dreams have given me the strength to persevere and achieve my goals.

To my beloved family, whose constant love and motivation have been a source of strength and inspiration. Your support, whether through kind words, reassurance, or simply being there, has played a vital role in this accomplishment.

This achievement is as much yours as it is mine. Thank you for walking this path with me.

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to my advisor, Dr. Zohdy, for his invaluable guidance, mentorship, and support throughout my PhD journey. His expertise, insightful feedback, and encouragement have been instrumental in shaping my research and helping me navigate the challenges of this academic endeavor. His unwavering belief in my abilities has been a source of motivation, and I am truly grateful for the knowledge and inspiration he has imparted to me. Thank you, Dr. Zohdy, for your dedication and for being an exceptional mentor.

Surah Adel Al Dakhl

ABSTRACT

BLOCKCHAIN-INTEGRATED SMART GRID ARCHITECTURE WITH FBG SENSING AND EKF FOR FAULT AND ANOMALY DETECTION

by

SURAH ADEL AL DAKHL

Adviser: Mohamed Zohdy, Ph.D.

The smart grid has emerged to address the shortcomings of one-way existing grid systems and is the next generation power grid infrastructure that applies smart ICT (Information Communication Technology) to existing grid. The Smart Grid is expected to greatly improve the efficiency and reliability of future power systems with the demand for renewable energy resources. However, because major power facilities are interconnected through communication networks, Smart Grid's cyber security is becoming an important issue. Cyber-attacks by malicious intruders can lead to serious incidents such as massive outages and the destruction of power network infrastructure, since cyber-attacks can damage energy data, starting with personal information leakage from grid members. Therefore, as a solution to this issue we will suggest a secure smart energy management system based on the blockchain. The combination of blockchain technology, optical fiber sensors, and Kalman filters in smart grids holds great potential for the future of power transmission and distribution systems. Blockchain offers secure protection against cyber threats and unauthorized access, while optical fiber sensors

provide real-time monitoring and control of electrical energy flow. The integration of these technologies leads to improved transparency in energy generation, distribution, and consumption. Extended Kalman filters are utilized to identify and minimize uncertainties in data collected from optical fiber sensors, thereby enhancing the accuracy of information used for energy management and grid control. This integration promises increased security, enhanced reliability, improved efficiency, and greater flexibility in energy management. This paper presents a comprehensive examination of the benefits and limitations of integrating blockchain technology, optical fiber sensors, and Kalman filters in smart grids.

TABLE OF CONTENTS

TABLE OF CONTENTS—Continued

TABLE OF CONTENTS—Continued

TABLE OF CONTENTS—Continued

TABLE OF CONTENTS—Continued

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES—Continued

CHAPTER ONE

INTRODUCTION

As a result of the large-scale blackout in the world for many years and the damage caused by them, interests surrounding efficient management of energy resources to overcome the power shortage has increased. In addition, it is necessary to reduce environmental pollution caused by the use and depletion of limited fossil fuels such as petroleum and coal. In addition, a system for efficient use and management of renewable energy such as wind and solar power generation is needed.

The Smart Grid, which is an infrastructure that minimizes various damages while maximizing energy efficiency based on problems such as power grid paralysis, unbalanced supply/demand of energy resources, environmental pollution, and use of renewable energy, becomes an issue. The Smart Grid, which emerged for efficient and reliable energy management, is the next generation power grid infrastructure, also known as the intelligent grid. The Smart Grid is an infrastructure for automatic control, high power conversion, optimized energy demand management, and renewable energy management technology that uses smart ICT (Information Communication Technology) to power grid in order to solve the disadvantages of existing unidirectional grid system [1, 2]. The Smart Grid has the advantage that it can work as an optimal energy management system to exchange information in real time by connecting the electricity production and distribution facilities and power consumers to the network. However, since there are security threats to energy data generated by grid members and processes,

and the consequences of these threats are very lethal, efforts are needed to identify and resolve them.

Smart grids, which use advanced technology to monitor and control the flow of electrical energy, have been proposed as a solution to these security issues. The integration of blockchain technology, optical fiber sensors, and Kalman filters is a crucial aspect of this transformation. Blockchain technology offers a secure platform for smart grids, protecting against cyber threats and unauthorized access. Optical fiber sensors provide real-time monitoring and control of electrical energy flow, contributing to grid stability. Furthermore, the integration of these technologies enables real-time visibility into energy generation, distribution, and consumption. Kalman filters play a role in identifying and reducing uncertainties in data collected from optical fiber sensors, resulting in improved accuracy of information used for energy management and grid control. This integration leads to increased security, enhanced reliability, greater efficiency, and more flexibility in energy management. This paper explores the benefits and limitations of integrating blockchain technology, optical fiber sensors, and Kalman filters into smart grids. Smart grids have become increasingly important for the reliable and efficient delivery of electricity to consumers. Fault detection is a critical component of smart grid systems, as it helps to ensure the stability and reliability of the grid. However, traditional fault detection methods can be limited by measurement uncertainties, security risks, and lack of transparency. The use of optical fiber sensors and blockchain technology can help to enhance the reliability and security of fault detection in smart grids.

Therefore, we propose a secure smart energy management solution using blockchain technology. The blockchain is a distributed data processing technology in which all users participating in a network distribute and store data [3]. The blockchain is a kind of database in which data is encrypted with a hash and stored in a block, which is then connected to a previous block in a chain form. Therefore, modifying the contents of the block is difficult because all nodes of the blockchain must be modified [4]. We will build a secure blockchain-based smart energy management system using such reliability of blockchain. In this thesis, we will propose this system which will be an outline of the system to be constructed in the future.

1.1 Motivation

The smart grid is considered to be a communication network with control devices, smart meters, automation, computers, and emerging technologies interacting. All of these entities must be able to communicate efficiently with one another, making the smart grid a large heterogeneous network. As a result, the smart grid inherits most of the security vulnerabilities of cyber systems, putting the electric grid at risk of cyber-attacks. Accordingly, security breaches in the smart grid can have detrimental consequences and may impact a country's entire infrastructure, its economy, and its citizens' lives. The smart grid's two most critical vulnerabilities are reporting false data and gaining private information about the user. The former vulnerability involves the active interception of data to drop or alter messages sent by the smart meter to the utility and causes the smart grid to act on demands that do not exist and take wrong shedding decisions and actions.

The latter vulnerability encompasses the passive interception of messages, which could result in a unauthorized gain of private information about the user. This information could engender more severe attacks such as theft. The targeted data can also be sent from the utility to the smart meters. To address these vulnerabilities, we propose a secure-by-construction prevention mechanism that focuses on Blockchain as the underlying technology to secure the two-way communication between the smart meters and the utility servers. In this thesis, we aim to design and implement a fault detection system in a smart grid that incorporates Fiber Bragg Grating (FBG) sensors, Blockchain technology, and uncertainty identification by Extended Kalman Filter.

1.2 Problem Statement

Due to the high risks associated with potential attacks targeting the two-way communication between the Fiber Bragg Grating (FBG) sensors and the utility servers, it is vital to ensure confidentiality, integrity, availability, authorization, authenticity, and nonrepudiation. Normal security measures, which are employed in traditional communication and network systems, fail to secure the complex network that composes the smart grid for various reasons which will be discussed in this work. The technique we focus on for resolving the risk associated with the smart grid is a prevention technique. It relies on Blockchain as a building block, where communicated data is treated as transactions that are encrypted and stored in a distributed fashion to ensure security and privacy. Blockchain prevents any alteration of the communicated data, and through cryptographic techniques, content and message authenticity are secured.

In order to demonstrate the prevention approach, a simulation setup will be used to prove the practicality of the secure communication between smart meters and servers at the utility. We will first set up a group of nodes (computers) in order to create a Blockchain network. The Blockchain protocols and the security protocols will be configured on every node, while tailoring all cryptographic algorithms for a network that is supposedly composed of thousands of nodes. The Fiber Bragg Grating (FBG) sensors and utility will act as nodes – generators of transactions. We will then perform actual testing on a Blockchain that will be implemented. Algorithm and protocol refinement will be carried out according to how resilient the network is. This setup aims to emulate an AMI and its interaction with the energy management system (EMS) which supports monitoring, controlling, and optimizing the performance of the electric grid. Mitigating uncertainties in the grid environment, encompassing sensor imperfections, environmental fluctuations, noise, and measurement mistakes. Developing strategies that utilize Extended Kalman Filter to analyze and mitigate uncertainties for improved system reliability and robustness.

The existing electrical grid infrastructure faces significant challenges in terms of security, reliability, and transparency. We have found four aspects that needs improvement in the terms of fault detection and uncertainty analysis.

1. **Security and Transparency:** Designing a secure and transparent grid security system using Blockchain to ensure tamper-proof transaction records, secure communication, and real-time visibility into grid activities.

2. Reliable Improved Communication: Install Fiber Bragg Crating (FBG) sensors at various points in the grid, such as substations and power distribution points, to monitor and control the flow of electrical energy in real-time. These sensors should be capable of sending and receiving data in real-time.

3. Real-time Fault Detection: Developing an effective real-time fault detection mechanism using FBG that can adapt to dynamic changes in the grid state, identify anomalies promptly, and trigger appropriate responses.

4. Uncertainties Analysis: Addressing uncertainties in the grid environment, including those arising from sensor inaccuracies, environmental variations, noise and measurement errors. Developing strategies that utilize Extended Kalman Filter to analyze and mitigate uncertainties for improved system reliability and robustness.

1.3 Thesis Contribution

The inherent security risks in Smart Grids are quite complex owing to the integration of legacy power networks and advanced information networks such that there are numerous challenges that are required to be addressed in a holistic way. Further, due to the wide distinction in operating and security environment of these tightly coupled cyber-physical networks, the security requirements are very stringent. Hence, security risk management plays a pivotal role in the assessment of risks, threats, and vulnerabilities that may have a tremendous impact on the security and reliability of Smart Grids. This thesis put forwards the following contributions:

1. **Enhanced security:** Blockchain technology provides a secure and transparent platform for the smart grid system, protecting it against cyber threats, faults, and unauthorized access. This contributes to the overall security of the smart grid system.
2. **Improved reliability:** Optical fiber sensors provide real-time monitoring and control of electrical energy flow, enabling the efficiency and accuracy of the fault detection process. The integration of these sensors contributes to the overall reliability of the smart grid system.
3. **Increased efficiency:** The integration of blockchain technology and optical fiber sensors enables real-time monitoring and control of energy generation, distribution, and consumption. This contributes to the overall efficiency of the smart grid system.
4. **Robustness and Resilience:** Smart grid systems need to be robust and resilient to uncertainties and disturbances to ensure uninterrupted power supply and grid resilience. By effectively managing uncertainties through the EKF, smart grid operators can enhance the robustness of the system, mitigate potential risks, and improve the overall performance and stability of the grid under varying operating conditions.
5. **Greater flexibility in energy management:** Kalman filters reduce the uncertainties in data collected from optical fiber sensors, enabling grid operators to make more informed decisions about energy management and distribution. This contributes to the overall flexibility in energy management.

1.4 Objectives

The objective of this thesis is to design and implement a fault detection system in a smart grid that incorporates optical fiber sensors, blockchain technology, and uncertainty identification by EKF. The proposed system will enhance the reliability and security of fault detection in the smart grid, providing improved stability and efficiency to the grid. The following steps will be taken to achieve the objective of this thesis:

1. **Optical fiber sensor deployment:** Install optical fiber sensors at various points in the grid, such as substations and power distribution points, to monitor and control the flow of electrical energy in real-time. These sensors should be connected to the smart grid system and be capable of sending and receiving data in real-time.
2. **Design of the Blockchain Network:** A blockchain network will be designed specifically for the smart grid system, incorporating optical fiber sensors and the fault detection algorithm. The blockchain network will provide a secure and tamper-proof record of the data collected by the sensors.
3. **Integration with Optical Fiber Sensors:** The optical fiber sensors will be integrated with the blockchain network, allowing for the secure storage and sharing of data collected by the sensors. The data collected by the sensors will provide valuable information about the physical state of the grid, which will be used for fault detection.
4. **Implementation of Smart Contracts:** Smart contracts will be implemented on the blockchain network to automate workflow processes in the fault

detection system. The smart contracts will be triggered by events in the grid, such as faults detected by the sensors, and will execute predetermined actions, such as sending notifications to stakeholders.

5. **Modeling the System:** The fault detection system will be modeled as a state-space model, including the optical fiber sensors and the fault detection algorithm. The state-space model will provide a mathematical representation of the system, which will be used for state estimation.
6. **Estimating the State of the System:** The EKF will be used to estimate the state of the system, including the physical changes in the grid that are indicative of faults. The EKF will incorporate measurement uncertainties from the optical fiber sensors, such as noise and measurement errors, in the state estimation process.
7. **Updating the Model:** The EKF will continuously update the state-space model based on the latest data from the optical fiber sensors. The updated model will provide improved accuracy in the fault detection process.
8. **Identifying Uncertainties:** The EKF will identify uncertainties in the state estimate, providing information about the confidence in the fault detection process. This information can be used to improve decision-making in response to faults in the grid.

1.5 Structure of Thesis

This thesis is organized into several chapters, beginning with the introduction in Chapter 1. Chapter 2 provides essential background information on both traditional and

smart grids. It introduces the Smart Grid as the next-generation power grid infrastructure and highlights its key characteristics through comparison with conventional grid systems. Chapter 3 explores the advantages of integrating FBG sensor into the Smart Grid. These sensors enable real-time monitoring of grid performance, thereby enhancing the accuracy, responsiveness, and efficiency of the system. Chapter 4 reviews existing work on blockchain implementations for securing communications within the Smart Grid. It introduces blockchain technology and presents the proposed blockchain-based system, emphasizing its potential to mitigate cyberattacks. This chapter also addresses the importance of enhancing cybersecurity in smart grid infrastructures. Chapter 5 focuses on identifying system uncertainties using the Extended Kalman Filter (EKF), demonstrating how EKF contributes to improved security and reliability in Smart Grid operations. Chapter 6 describes the simulation setup, detailing its components, architecture, developed scenarios, implemented smart contracts, user interface, recorded results, achieved security properties, and identified limitations. Finally, Chapter 7 summarizes the research contributions and outlines future directions and opportunities for continued development in this area.

CHAPTER TWO

BACKGROUND

This segment will explore power grid challenges and smart grid benefits based on existing research.

Contemporary electrical systems typically generate power more than anticipated demand. Due to the complexity of predicting real-time consumer electricity usage, extra energy is produced to ensure an adequate supply if consumption surpasses expectations. This approach necessitates not only fuel for power generation but also additional power facilities, resulting in increased construction expenses. Moreover, the excess electricity, which is often wasted, decreases energy efficiency while simultaneously increasing environmental pollution from fossil fuel combustion. Furthermore, as fossil fuel reserves diminish, innovative methods of electricity generation from renewable sources like wind and solar have been developed. Consequently, a novel energy framework is necessary to efficiently oversee and monitor various forms of electrical energy in real-time.

2.1 Traditional grid system

The demand for electrical energy grew significantly from the 1970s to the 1990s, leading to an increase in the number of power plants since the initial grid installation in 1886. This growth can be attributed to global urbanization and infrastructure expansion. The current grid system follows a rigid hierarchical structure, with power plants at the apex supplying electricity to consumers at the base [1]. This system relies on fossil fuels for centralized power generation, characterized by unidirectional flows of electrical

energy and data. Consequently, the existing grid is unable to gather and analyze real-time information about customer services, resulting in substantial power waste and excess due to its hierarchical nature.

The electrical power system infrastructure is experiencing a disparity between the escalating demand for electricity and the constrained available supply. There is mounting apprehension regarding suppliers' ongoing capacity to fulfill new and increasing electrical requirements. Integrating and implementing renewable energy sources (RES) into the outdated, conventional power system infrastructure presents challenges. These emerging needs and advancements create numerous obstacles for the operation of generation, transmission, and distribution systems. Furthermore, the distribution system is ill-equipped to manage periods of high-power usage. Excessively old and thermally overloaded transformers are at risk of failure, potentially disrupting the electricity supply. These issues, combined with the persistent limited capital investment in new transmission systems, necessitate the creation of innovative, cost-effective intelligent power systems and infrastructure.

The conventional power grid links various power system components to facilitate the transfer of electricity from generation points to end-users. It utilizes electromechanical infrastructure, unidirectional distribution, and sensors. Its centralized nature means power is generated from a unique location. These features prevent the traditional grid from obtaining real-time data about the condition of its equipment and precise consumption rates. Consequently, it is unsuitable for meeting increasing demand and incorporating renewable energy sources like wind and solar.

In contrast, the smart grid is emerging as a natural successor to the traditional power grid, employing digital infrastructure to enhance communication. Smart grids have been developed as a solution to many of the limitations associated with the conventional electrical grid system.

2.2 Issues facing the power grid

The electrical power system has undergone more than a century of evolution. Throughout its growth and expansion, it has become the world's most intricate electrical infrastructure, with the United States alone boasting over 14,000 transmission substations and 4,500 major distribution substations. Despite this impressive scale, the current electrical infrastructure is facing significant challenges, including aging components, outdated technology, insufficient funding, and excessive strain. Today's power grid relies on 19th-century systems dating back to Edison's era and 20th-century equipment from Westinghouse to meet the demands of a 21st-century economy [5]. The power industry is now confronted with substantial hurdles and must address several critical issues, which will be explored in the following sections.

2.2.1 Efficiency Issue

We have had our electricity grid for a long time. Sixty percent of the circuit breakers are 30 years or older, while over seventy percent of the transformers and transmission lines are 25 years or older [6]. As the electricity system ages, the transmission lines' resistance rises. As a result, the grid loses more electricity due to heat. As the power grid continues to grow, it has become more intricate and expansive than it was previously, making it more challenging to obtain information about the power

system's state. Utility companies constantly need to generate excess power in order to have a sufficient margin in fulfilling the power needs. This is to ensure that there is enough electricity to satisfy all the customers' energy demands. As a result, the excess electricity is wasted on the grid. Consequently, the cost of the garbage falls on all the clients. Likewise, the wider distribution and heightened complexity of the electrical system make it more challenging to optimize electricity delivery. There are currently around 130 control centers in the United States that oversee the whole electrical grid. These facilities are remote and run independently of one another. As a result, their inability to collaborate well leads to low power delivery efficiency [5]. For instance, it is conceivable that certain regions may have high power demands but not enough power plants to supply the necessary energy. In contrast, in some other areas, the power providers produce excess electricity—which is frequently wasted—to satisfy the peak energy demand of their consumers. Consequently, it causes power to be wasted in certain areas and to be absent in others. Therefore, it is essential to address the issue of the power supply system's low efficiency. In addition, the explosion of renewable energy and its implementation (in hybrid cars) open new sources of energy. There is no reason hydropower in Washington State and wind power in Texas cannot be combined. Nevertheless, these novel sources of electricity are not adequately supported by the current power systems. It is now more important than ever to figure out how to use these new energy sources efficiently.

2.2.2 High-Cost Issue

The cost of producing power throughout the day is significantly higher than that of doing so at night. Indeed, the cost of producing electricity at peak demand can increase by a factor of one hundred [5]. The majority of customers use expensive power throughout the day because power companies have no control over how their customers use electricity. Consequently, the cost of producing electricity power is high. Furthermore, in order to meet peak power demands, power plants must maintain hot standby, which requires them to burn coal or other fossil fuels in order to maintain the generator operating at synchronous speed even in the absence of high power demand. The cost of hot standby will rise sharply if additional power plants are constructed in the present. The limited availability of coal and fossil fuels makes it imperative to think of innovative solutions to lower the high cost of generating electricity.

2.2.3 Reliability Issue

The global power system has become more complex due to increasing interconnections and the growth of the power grid. In addition, an extensive amount of outdated transmission cables and equipment are still in use. As a result, the power system becomes harder to manage than it was previously, making failures—even catastrophic ones—more likely. For instance, in just two months in 2003, there were multiple blackouts that affected a large number of consumers worldwide [7, 8, 9]. On August 14, 2003, the outages in the Northeast United States and Canada impacted almost fifty million people. Restoring power to New York City and the other impacted areas took more than a day. It's regarded as one of the worst blackouts in these nations' history; On

August 28, 2003, blackouts in London disrupted rush hour travels and resulted in a roughly 50-minute power outage that affected roughly 20% of the city's demand (734 MW).

The more complex power infrastructure and unsteady older equipment are the cause of the blackout. Because of the high sensitivity of these aged components, it becomes more difficult to coordinate backup protection throughout the entire system and results in greater disruptions. Power utilities and customers always bear the heavy financial burden of blackouts, even though they are still rare occurrences. Therefore, it is imperative that we give the reliability issue more consideration currently. Power system development has spanned over a century, as previously said. In the last century, however, not much has changed. Instead of using microprocessors in the digital age, our electric grid still makes use of electro-mechanics from the 1960s and 1970s. Certain issues that once seemed quite trivial are now urgent due to the power system's continued expansion and complexity. As a result, changes to the power grid that can handle these issues are required. In addition, it will be a massive, intelligent system that is networked and linked from top to bottom, down to billions of individual gadgets. That is the intelligent grid, which is the electrical grid of the future.

2.3 Architecture of Smart Grid

"Smart" and "Grid" are compound words that stand for electric grid, transmission line network, substation, transformer. Together, they constitute the term "smart grid." By utilizing intelligent information and communication technologies within the current grid, the Smart Grid improves "situational awareness" with regard to the condition of the grid

[10]. Put another way, it is a system that allows both the power provider and the customer to exchange real-time information in order to intelligently enhance energy efficiency. The current grid was designed to produce, distribute, and sell electricity in a one-way manner to consumers; however, by connecting consumers and electricity production and distribution facilities to the network, the Smart Grid can facilitate real-time information exchange and potentially offer optimized energy management [11].

Once again, the definition of the Smart Grid is a system that integrates data from the generation, transmission, substation, distribution, and consumption of energy using cyber security communication technology and computer intelligence employing information and communication technology (ICT) to actualize a two-way secure system [12]. Because of this, users of the Smart Grid can increase the resilience, efficiency, dependability, and transparency of their energy management systems while also saving energy and paying less for usage. By doing this, the Smart Grid will be able to address issues that need to be resolved internationally, such as reducing environmental pollution, limiting the use of fossil fuels, and optimizing the use of renewable energy sources. The utility company, transmission and distribution companies, and consumers are the various entities that make up smart grids. Numerous sensors are used to identify issues and

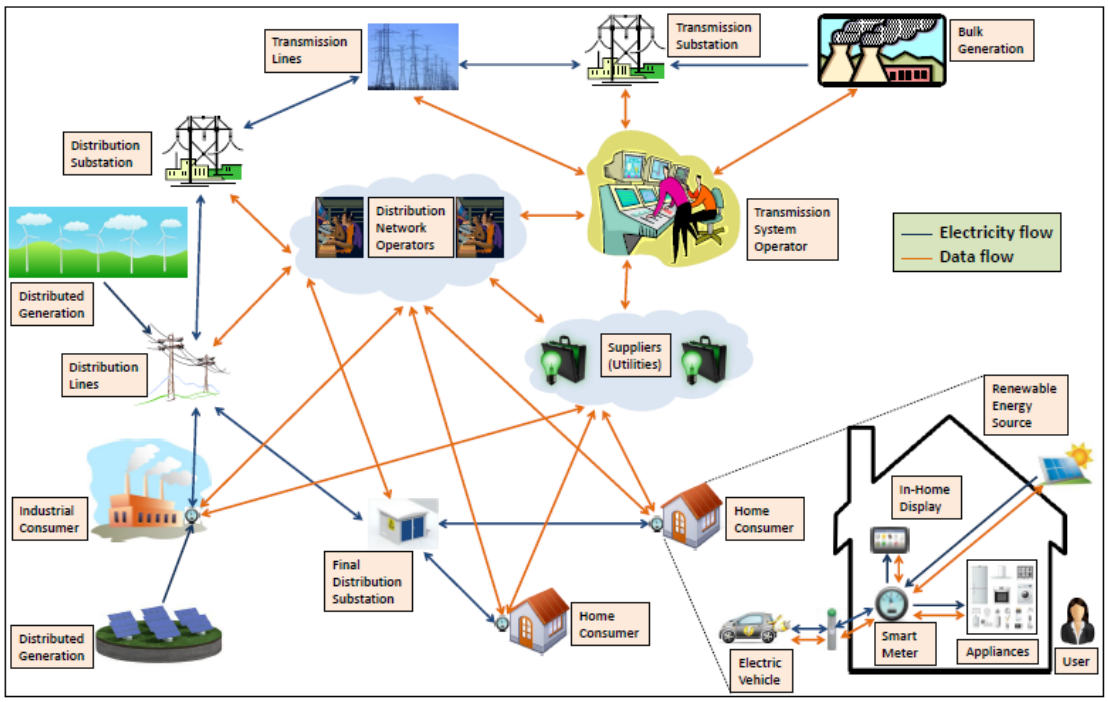


Figure 1:A typical smart grid architecture [13]

redirect electricity as necessary. The adoption of advanced smart meters, which enable more effective data tracking at the customer side, is a crucial component of the smart grid. Since these are the elements covered in this thesis, the meter data management system, supported by the utility, the smart meter, the communication network, and the advanced metering infrastructure are discussed in this part.

1. **Meter Data Management System and Utility:** The smart meter data that is provided by smart metering systems and gathered via the Advanced Metering Infrastructure (AMI) is managed by the meter data management system on the utility side. Data management and long-term data storage are topics covered by the MDMS. It gathers, purifies, stores, and processes the data in order to evaluate it for billing, demand response, and demand side management. Given the

importance of the data to the utility's load or outage management programs, these storage facilities must be earthquake resistant. Concepts like cloud computing and virtualization are used since protecting this data is expensive.

2. **Smart Meter:** Energy consumption meters, sometimes known as smart meters, are used as smart grid entry points. At certain predetermined periods, smart meters can report the electricity data back to the utility. Smart meters and devices track and collect data on power usage. The time at which this data was measured is indicated by its time stamp. The distinct meter identifier is also included in the data. An MDMS can communicate with a smart meter and the smart meter can communicate with the MDMS. The smart meter accepts and uses the data it receives from the MDMS, which we call load balancing data. The new smart meters have replaced the outdated analogue meters, resulting in more accurate data measurements from the customers. Adaptive billing is made possible by setting up various billing systems. Based on the utility control data, this may encourage customers to change how much energy they use. The in-home display (IHD) gadgets give users greater control over how much energy they use. Six categories list the characteristics that a smart meter ought to have [14].

    • *Quantitative measurement:* It includes measuring the data accurately.

    • *Control and calibration:* This includes the capacity to adjust to changes inside the network.

    • *Communication:* It includes the transfer and reception of pertinent data.

• *Power management:* This includes a system's capacity to continue operating even in the event of a power outage.

• *Synchronization:* It includes quick and dependable data transmission.

• *Display:* This includes the capability for the clients to see their statistics regarding electricity usage.

3. **Communication Network:** The communication channel is the way by which data can be sent from smart meters to the utility and vice versa. Either a wired or wireless communication path is possible. In our work, we concentrate on the Internet as the primary wireless communication channel between the utility and its customers. As will be discussed in chapter 4, our blockchain-based solution can help to reduce some of the vulnerabilities and attacks that the communication network confronts.
4. **Advanced Metering Infrastructure:** In order to implement advanced metering, two-way communication, a utility, and smart meters are required. Both the utility and the customers have benefited from the usage of AMI in data processing, administration, and visualization. The smart meters' electrical data is transmitted to the utility company by the AMI. The route for safe information flow should be provided via the AMI communication network. Demand side management and the incorporation of green technology are made possible by the usage of AMI. Smart meter systems decrease outages and financial and electrical losses by offering effective control and monitoring of the power system as well as real-time decision-making for operations. While smart meter systems do not require any

manual intervention—the utility and smart meters interact via the AMI—conventional energy metering systems needed manual data collecting and invoicing. The utility is able to effectively regulate the demand for electricity thanks to the collection of consumer electrical data. Thus, AMI is essential to the smooth integration of various components and technologies that communicate with one another at various Smart Grid domains. Additionally, several networks that correspond to the domains listed in the NIST conceptual reference model—which is discussed in the following subsections to help with understanding security requirements—are included in the Smart Grid communication infrastructure.

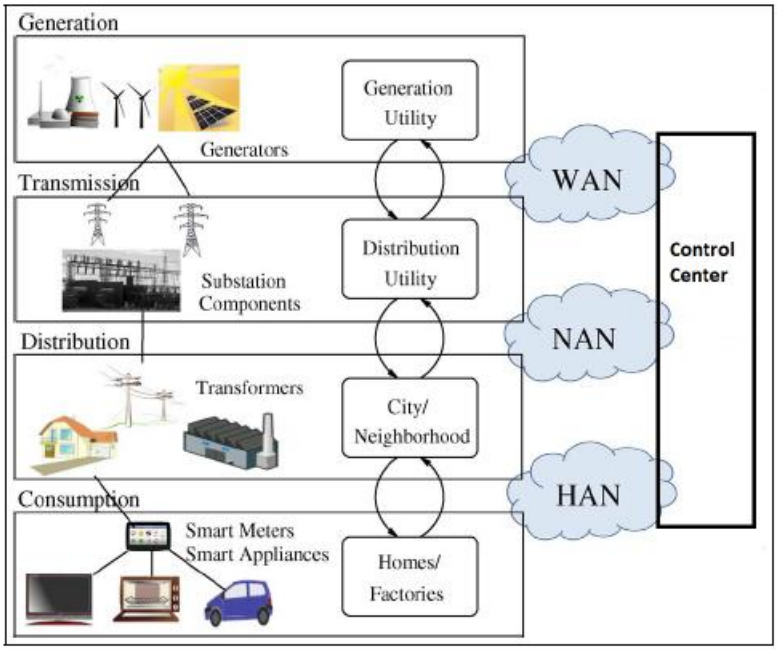


Figure 2: Architecture of Smart Grid [15]

2.3.1 Home Area Network (HAN)

The term "home area network" (HAN), which is also used to refer to "premise area network" (PAN) or "building area network" (BAN) [15, 16], refers to the Smart Grid's customer domain, which includes smart meters and household equipment. In order to gather and analyze consumption data and provide control signals to home appliances for energy efficiency, smart meters communicate with them. As a result, by using smart meters to collect data from smart appliances like lights, heaters, TVs, and so on, this enables demand side control at client locations [17]. With constrained power and bandwidth, wireless communication is the norm in HANs among various smart devices [17, 18]. Therefore, there is still study to be done on choosing the optimal technology for these kinds of wireless networks. Wi-Fi, Zigbee, and BACnet are among the several wireless technologies that are being considered for these kinds of networks [19]. Because of its affordability and simplicity of implementation, ZigBee standard can be a good choice [17]. Nonetheless, there is still a need to handle the security of sensitive data that is shared among many devices on such a wireless network.

2.3.2 Neighborhood Area Network (NAN)

This network links several HANs together and is equivalent to the Smart Grid's distribution domain. This network consists of many mesh-topped smart meters connected to each other. This network's main function is to combine data from all smart meters and aggregate it using "data aggregator units" (DAU), which then sends the collected metered data to utilities as a whole. A NAN gateway serves as the DAU's interface between the wide area network (WAN) and the home area network (HAN) [16]. This network uses a

combination of wired and wireless technologies to cover large areas up to ten square miles at a data rate of roughly 1 Mbps. Ethernet and optical fiber cable (OFC) are workable options for wired access, while WiMAX, LTE, 3G, and 4G are the most widely used options for wireless connectivity [17].

2.3.3 Wide Area Network (WAN)

These networks link several NANs that correspond to the distribution domain of smart grids and match the transmission domain of smart grids. These networks serve as a backhaul for enterprise networks that correspond to the generating and operation domains of the Smart Grid by bridging the gap between HAN, NAN, and utility firms. These networks are mostly used for the monitoring and management of transmission and distribution networks that are dispersed throughout large geographic areas [17]. High throughput, high dependability, and high efficiency can be achieved by combining different communication technologies, such as satellite, cellular networks, leased lines, and optical fiber communication.

2.3.4 Enterprise Networks

These networks, which include "Supervisory Control and Data Acquisition (SCADA)" and "Wide-Area Measurement System (WAMS)", among other measurement systems, are in line with the development and use of smart grids [16, 20, 21]. These networks' main function is to oversee and manage the whole electrical grid in order to guarantee excellent transparency and dependability for all measurements throughout a wide geographic area. This reduces room for error, improving decision-making abilities in a real-time setting. In order to accomplish the same, this network makes use of a

variety of synchronous phasors that communicate with one another in order to synchronously gather data using the global positioning system (GPS) in order to assess the general health of the grid. These networks are also used by a number of applications for billing, outages, and managing metering data [16, 22]. Thus, this network relies on very high bandwidth optical fiber connectivity and leased lines to support these applications effectively.

2.3.5 External Networks

This network is in charge of communicating with retailers, regulators, and service providers since it aligns with the markets and service area of smart grids. This network's main functions include improving customer service, billing, and energy management as well as serving as a platform for the creation of domestic goods to satisfy future demand for smart grid technologies [16, 20]. To fulfill the demand-supply chain for electricity, efforts have been undertaken to establish a safe, dependable, and failproof communication channel between the external market and service providers. Furthermore, this network uses a lot of Internet protocol (IP), and most communication takes place online, which poses major security risks for data integrity and confidentiality [16, 20, 23].

2.4 Advantages of smart grid

The smart grid is described in this paragraph along with answers to frequently asked questions about what it is and how it may help us [7, 8, 9]. Customers and the grid can both monitor and control energy consumption in real time thanks to this sophisticated and interactive power grid. It is the electricity grid's evolution. Its application will be more beneficial to people.

The following benefits are provided by the smart grid.

2.4.1 More efficiency and low cost

Utility companies can regularly collect customer data through the use of smart meters thanks to their installation and the link between customers and the firms. Customers can also quickly and easily obtain information on their usage. It converts the electricity grid into an interactive, two-way system. Power providers can more accurately forecast the energy demand in the grid and manage the supply of power in real time because to the interactivity. Therefore, there is no longer a need to produce excessive amounts of electricity, which minimizes grid power waste and increases power supply efficiency while maintaining safety measures against power grid overload.
Remember that extra energy is especially costly during peak demand periods because a significant portion of the power is generated by thermal power plants, which use pricey fuels like coal and natural gas. In addition, time-based pricing will be possible with the use of smart grid. Customers will receive a variable utility tariff that varies in real time based on fuel consumption. In order for them to modify their power usage in accordance with the current price. As a result, it will alter how the clients use power.

2.4.2 More reliable, more green

The electricity grid is made more dependable in the smart grid by applying sophisticated control algorithms and quick system state feedback. It is stable enough to manage a broad range of power sources and storage systems. Remember that renewable energy sources like wind and sun are constantly erratic. Previously, integrating renewable energy with the electrical system was challenging. However, with a smart grid, renewable

energy may be quickly and easily added to the power grid and coordinated with other dispersed power plants to boost redundancy in the power supply. As a result, it promotes the use of more renewable energy in the production of electricity, which lowers greenhouse gas emissions and improves environmental friendliness. As the number of hybrid and electric cars rises, smart grid technology is able to manage these vehicles to act as backup power and batteries for the grid, strengthening it against the impact of consumer demand fluctuations. The control center can coordinate client power usage to minimize negative effects on the power system thanks to its interactive capability.

For instance, a lot of the machinery in industries has a lot of motors. A motor's start current is five to seven times higher than usual. The start current of these devices will significantly affect the grid if they start at the same time. Factories need to spend a lot of money modernizing the infrastructure in order to decrease these kinds of effects. To minimize the impact on the grid, the control center in a smart grid can intelligently govern the order in which machines start up. This reduces the overall start current. It will therefore also save the expense of making an infrastructure investment. Additionally, the smart grid's capacity to respond swiftly to power fluctuations and use sophisticated management algorithms allows it to coordinate power generation, distribution, and client activity protection. Consequently, the smart grid's stability margin will rise, improving its resistance to disruption and lowering the likelihood of a blackout. As a result, the smart grid is less expensive, more resilient, dependable, and more efficient.

2.4.3 Integration of Renewable Energy Sources

For renewable energy sources to be smoothly incorporated into the current energy infrastructure, smart grids are necessary. They provide a consistent and dependable power supply by allowing for the real-time monitoring and management of energy generation and consumption, which balances the erratic output of renewable sources with demand. Demand response programs allow users to modify their electricity use in response to the availability of renewable energy, while energy storage system integration improves grid flexibility by making the best use of excess renewable energy. Smart grids can also assist decentralization through microgrids, which can integrate renewable sources at lower sizes, and maximize transmission while minimizing losses. In addition, they control how electric cars charge and facilitate vehicle-to-grid technology, which improves grid efficiency and stability even further. Given the circumstances, smart grids offer the intelligence and adaptability required to successfully integrate renewable energy, accelerating the shift to a more robust and sustainable energy system.

2.5 Security Objectives and Requirements of Smart Grid Architecture

The foundation of Smart Grids is fundamentally based on "information and communication technology (ICT)" [24, 25, 26]. Upon examination of the Smart Grid architecture in section 2.3, it becomes apparent that these systems are susceptible to numerous security vulnerabilities associated with advanced technology. Consequently, Smart Grids represent a potentially attractive target for malicious actors seeking to exploit system vulnerabilities for illicit purposes [24, 25, 23]. To establish a secure Smart Grid, it is imperative to comprehend the fundamental security objectives and essential

security requirements. The subsequent sections are dedicated to elucidating these critical aspects for the reader.

2.5.1 Key Security Objectives

As cyber threats escalate, numerous organizations, including the Electric Power Research Institute (EPRI), NIST, and Smart Grid Interoperability Panel (SGIP), have conducted extensive research on evolving security objectives and requirements for Smart Grids [24]. NIST has developed an analytical framework focusing on cybersecurity risk analysis in Smart Grids [20]. This framework identifies availability, integrity, and confidentiality as the primary cybersecurity objectives for Smart Grids, which are described as follows:

1. **Availability:** This concept ensures that authorized parties can access resources when required, while preventing adversaries from denying access to authorized users [24]. Availability is considered the most critical security objective for the continuous operation of Smart Grids. Unlike conventional IT networks where data integrity is the highest priority, availability takes precedence in Smart Grids. This is because Smart Grids are critical infrastructures where restarting the power system is not advisable, as it can significantly impact sensitive operations such as power generation, transmission, and distribution [22]. In contrast, restarting servers or applications in conventional IT networks has a less significant impact.
2. **Integrity:** In Smart Grid networks, integrity involves preventing unauthorized modification of critical data from sensory devices, smart meters, and other system

components by adversaries, as the impact can be severe. Protecting such critical data is essential to prevent disruption of network command and control, which could impair the decision-making capabilities of intelligent devices [24]. Data integrity is a secondary security objective for Smart Grids and can be analyzed from both customer and utility perspectives. In the customer domain, it concerns the protection of metering and billing data, while in the utility domain, it relates to operational data responsible for command and control of the entire grid [27].

3. **Confidentiality:** Confidentiality is a key security objective for Smart Grids, focusing on preventing unauthorized disclosure of sensitive data and access to critical system components. This objective is particularly relevant in the customer domain, as a compromise could lead to privacy intrusion, enabling attackers to predict customer behavior patterns by accessing power usage and billing information [18]. Confidentiality is also crucial for utilities, as a breach could result in the disclosure and misuse of proprietary information. Meeting this security objective is essential for maintaining a secure Smart Grid.

2.5.2 Key Security Requirements

Smart Grid security necessitates a holistic approach, considering both power and IT systems concurrently rather than independently [22]. Given the extensive and dynamic nature of Smart Grid security, organizations such as the Smart Grid Interoperability Panel (SGIP), Cyber Security Working Group (CSWG), and NIST have identified critical security requirements, categorizing them into four primary domains: physical security,

data security, network security, and security management [24, 25, 20]. These categories are elucidated as follows:

1. **Physical Security:** This aspect encompasses the protection of Smart Grid devices from theft, sabotage, and tampering. Smart meters are particularly susceptible to such threats, necessitating advanced protective measures at customer locations to ensure overall grid reliability [28, 24, 23, 18].
2. **Data Security:** This category primarily addresses customer data privacy, secure data storage, regular critical data backup, and efficient data recovery mechanisms. Consumer data privacy is of paramount importance in Smart Grids, as the information exchanged between smart meters and utilities could potentially enable adversaries to discern behavior patterns, such as television viewing or laundry habits, through the analysis of metering data [18].

3. **Network Security:** Network security encompasses the protection of wireless networks, command and control networks, and real-time measurement systems against eavesdropping, state manipulation, and data injection attacks [29, 25, 18]. It also involves safeguarding against unauthorized access, ensuring that only authenticated users can access the network. However, the selection of appropriate security mechanisms for Smart Grids requires careful consideration due to the presence of devices with limited memory and processing capabilities, potentially rendering traditional cryptographic schemes unfeasible [15, 23, 18].

Table 1: Comparison between ICS and IT Security Environments (Adapted from [22])

Security Characteristics	Industrial Control System (ICS)	Information Technology (IT) System
Physical Security	Less secure when far-flung and unmanned.	More secure. System housed in facility and server room.
Connection Speed	Slow. Use of serial links and dial-up connections.	Fast. Use of high bandwidth broadband connections.
Latency	Very low. Varying from milliseconds to seconds.	Medium to High. Depends upon application.
Availability	Very High (24 x 7).	Not much critical. Huge server backups and redundancy.
Confidentiality	Less critical compared to availability and integrity.	Highly critical. Primary security objective.

4. **Security Management:** This domain focuses on the development and implementation of security policies, employment of risk management frameworks, conduct of periodic audits, and establishment of accountability. Audits can effectively detect and prevent security breaches through proper log analysis. Additionally, the assignment of clear accountability to personnel handling critical data is essential for maintaining proper security protocols.

2.6 Security Challenges in Smart Grid

Implementing security mechanisms in Smart Grids presents several significant challenges in meeting key security requirements. The following issues are particularly noteworthy:

1. **Operating Environments:** Smart Grids represent an integration of operational technology (OT) and information technology (IT) systems [22], resulting in substantial differences in their operational settings. Table 2.1 illustrates the primary distinctions between the security features of ICS and IT systems.
2. **Interconnectivity of Diverse Networks:** Smart Grid communication infrastructure comprises a heterogeneous mix of networks, including wired, wireless, cellular, and power line cable, each functioning with its own protocols and standards [16]. Ensuring interoperability among these diverse networks while adhering to security policies poses a significant challenge.
3. **Heavy Reliance on Wireless Technology:** The customer and distribution domains of Smart Grids predominantly utilize wireless technologies such as ZigBee, Wi-Fi, and WiMAX. Consequently, these networks are susceptible to various types of attacks, as they can be more readily intercepted by adversaries compared to wired networks [28, 16, 20, 23, 18].

CHAPTER THREE

OPTIC FIBER BRAGG GRATING SENSING IN SMART GRIDS

3.1 Fiber Bragg Grating Sensing Technology (FBGST)

Fiber Bragg Grating (FBG) is a term that encompasses the fundamental principles of this sensing technology. The term "fiber" denotes the medium and structure, while "Bragg" refers to Bragg's law, which forms the basis of the sensing concept. "Grating" describes the permanent modification in an optical fiber core that creates the FBG structure. The development of FBGST commenced in the late 1970s, shortly after the invention of fiber optic technology [30]. In 1978, researchers at the Canadian Communications Research Centre observed the initial instance of grating formation within an optical fiber core. This phenomenon occurred unexpectedly when the fiber core was exposed to argon-ion laser radiation for an extended duration. Consequently, the light transmitted through the optical core gradually attenuated and was reflected back, which was attributed to the formation of the grating [31]. The significant breakthrough in Fiber Bragg Grating (FBG) development was documented in 1989 by researchers at the United Technology Research Centre in the United States. They successfully created a permanent FBG by directly inscribing it into an optical fiber core using coherent ultraviolet (UV) light interference patterns [32].

Within the fiber optic sensing family, the Fiber Bragg Grating Sensor (FBGS) has emerged as the most widely utilized. FBGSs have established a distinct market presence and have been commercially available since the early 2000s. Initially, FBGs were

primarily employed as wavelength filters in the communications industry, where fiber optic technology is well-established [33]. Recently, however, sensing engineers have demonstrated increased interest in FBG technology. This growing attention is attributed to the unique characteristics of FBGSs, including their compact size, immunity to electromagnetic interference, high sensitivity, capability for distributed and multi-physical sensing, and resistance to harsh environments. These features render FBGSs a promising solution for a broad range of sensing applications. Consequently, there has been a significant increase in the development of FBGST-based techniques for contemporary sensing applications in recent years [34, 35].

3.2 FBGS structure

A Fiber Bragg Grating Sensor (FBGS) is a brief section inscribed into the core of a single-mode optical fiber (SMF) [36]. It is generated along the length of the optical fiber core, where a modulated periodic refractive index is produced in the SMF core when it is exposed to a UV light interference pattern [33].

The structure of an FBGS imprinted in an SMF is illustrated in Fig 3. A typical SMF consists of a cylindrical glass core with a diameter ranging from 4 to 9 μm. This core is surrounded by a cladding glass layer measuring 125 μm in diameter. The function of the cladding layer is to ensure that light propagates exclusively within the fiber core. This is achieved by introducing dopants such as germanium into the core, resulting in a core with a higher refractive index (core n_0) compared to the cladding (cladding n_1) [33, 34]. The outermost layer of the SMF is the coating layer, typically composed of acrylate or polyimide, which functions to protect the fiber.

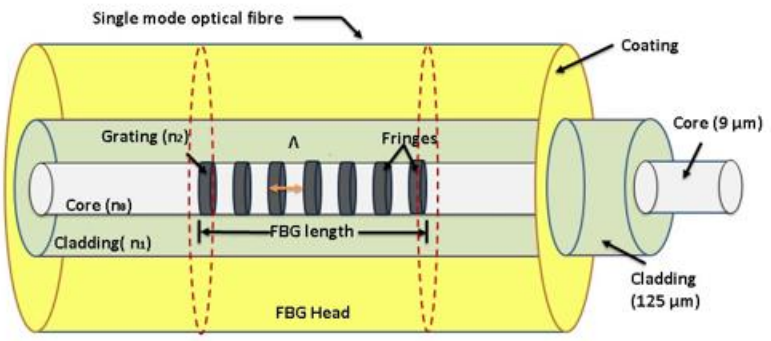


Figure 3: Fiber Bragg Grating sensor structure [33]

The sensing area on the SMF core, defined by the FBGS length, typically ranges from 3 to 20 mm [36]. This length is determined by the quantity of grating fringes and their spacing (grating period Λ), as illustrated in Fig 3. The number of grating fringes can reach several thousand, with the grating period measuring in the hundreds of nanometers [30]. These factors influence the characteristics of the FBG reflected light, which will be examined in the subsequent section. The grating area exhibits a higher refractive index (grating n_2) compared to the core, resulting from the manufacturing process.

Various FBG structures exist, including uniform grating, chirped grating, and superstructure grating FBGs [37]. However, this research exclusively utilizes the uniform FBG structure type, depicted in Fig 3. This selection is based on its straightforward structure and fabrication process, as well as its general applicability for sensing applications [38].

When exposed to broadband light, the fiber's gratings reflect a specific light spectrum, known as the Bragg wavelength (λ_B), which undergoes a shift in response to changes in thermal and mechanical conditions affecting the sensing head. The grating

structure determines which light wavelength is reflected according to the Bragg condition, while permitting the remaining light spectrum to pass through the FBG head. Figure 4 illustrates the operational principle of an FBG sensor, with λ_B representing the calculated peak mid-point of the reflected wavelength. Provided that other relevant application requirements are met, the FBG head can primarily function as a thermal and/or mechanical sensing device by monitoring the reflected spectrum. This approach offers several advantages, including immunity to electromagnetic interference (EMI), compact size, and flexibility.

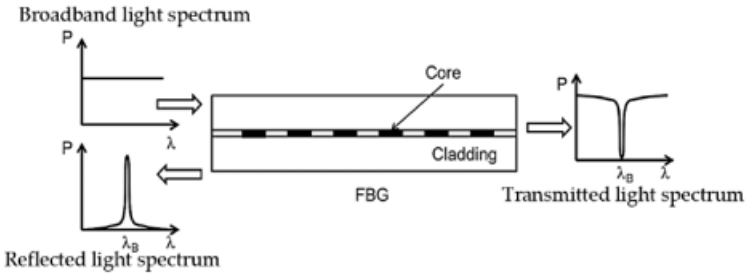


Figure 4: Operating principles of FBG.

In fiber Bragg grating (FBG) sensing applications, a specific light wavelength is reflected from a particular fiber location subjected to physical stimuli such as temperature or strain. The reflected wavelength is observed and quantified utilizing a dedicated optoelectronic interrogator. This device subsequently converts the measured wavelength into a physical quantity based on pre-established calibration for the relationship between wavelength and physical excitation [39,40]. The interrogator's primary functions encompass illuminating the fiber and accurately detecting and monitoring the reflected Bragg wavelength(s). Various techniques are employed to effectively track changes in λ_B,

contingent upon the specific sensing application's requirements. Key characteristics sought in FBG sensing interrogators include high resolution and accuracy (typically within picometers), multiplexing capability, and reasonable cost.

Furthermore, calibrating the wavelength shift to the physical measurement is crucial for enabling FBG sensing applications [41,42]. This process involves exposing the sensor to a controlled range of the target physical quantity and characterizing the relationship between the reflected wavelength and the physical measurement value. While calibration is ideally performed on unattached FBG fibers, some applications necessitate in situ sensor calibration, which can be challenging due to the sensor's embedding within a device and the utilization of any required bonding media between the sensor and device structure.

3.3 Fabrication of a FBGS

This section delineates the prevalent methodologies for fabricating a typical FBGS and examines the critical parameters for its production. The FBGS manufacturing process involves inducing permanent, periodically modulated reflective indexes in a segment of the fiber core [37]. Since the initial discovery of grating formation, ongoing research has led to significant advancements in commercializing the fabrication process [36]. The developed techniques address market demands for sensing applications, including production adaptability, measurement scope, cost-effectiveness, and superior physical and optical properties.

3.3.1 Fabrication techniques

The standard approach for inscribing Bragg gratings in a localized section of a fiber's core utilizes a coherent UV light interference pattern projected onto the fiber. Two primary methods exist for inscribing an FBGS using an external coherent UV light interference pattern:

1. **Two-beam interferometer technique:** This technique, first introduced by Meltz in 1989 [32], was the initial practical method for externally fabricating an FBGS in SMF. It employs an ultraviolet laser light source split into two beams by a beam splitter. These beams are subsequently absorbed and reflected using two side mirrors, as illustrated in Fig 5. The reflected light produces coherent interfering UV beams focused on the SMF section to be inscribed. Also known as the transverse holographic technique, this method exploits the fiber cladding's transparency to ultraviolet light, while the core strongly absorbs it [43]. A significant advantage of this approach is the ability to create FBGSs with specific Bragg wavelengths (λ_B). This is achieved by varying the grating period (Λ) of the fabricated FBGSs by tuning the angle (φ) between the split UV beams and the perpendicular axis of the fibre core, which is expressed as [36]:

$$\Lambda = \frac{\lambda_{uv}}{\varphi} \quad 1$$

where: Λ is the FBGS's grating period, λ_{uv} is the wavelength of the UV light, and φ is the tuneable angle. The disadvantage of this technique is the difficulty of accurately aligning the split UV beams on the inscribing area [121].

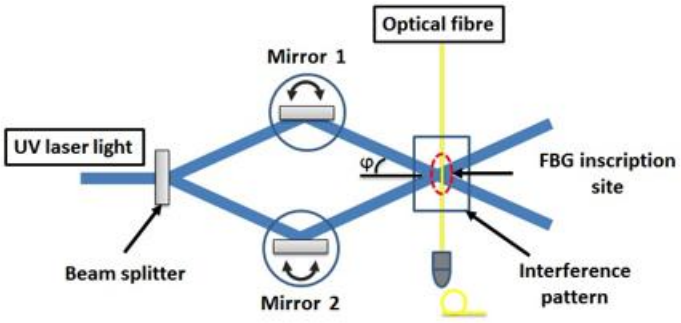


Figure 5: A schematic diagram of the two-beam interference configuration [33]

2. **Phase mask technique:** In 1993, Hill [44] introduced a novel approach for fabricating Fiber Bragg Grating Sensors (FBGS). This method utilizes a phase mask constructed from a transparent material, such as silica glass. The phase mask exhibits etched square wave patterns, as illustrated in Fig 6. Positioned in close proximity to the optical fiber, the phase mask interacts with an incident UV light beam to generate coherent interference patterns. These patterns subsequently modify the refractive index of the fiber's core [44]. However, this technique presents a limitation: each specific Bragg wavelength necessitates its own unique phase mask.

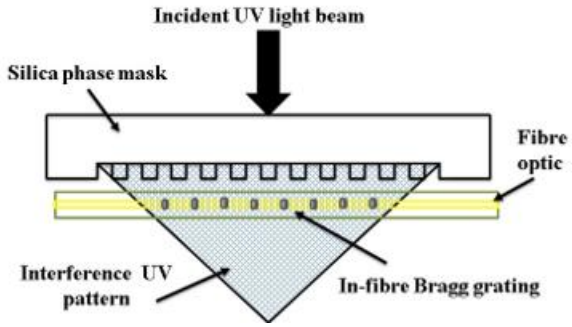


Figure 6: A schematic diagram of the phase-mask technique [36]

In 1996, Dockney [36] introduced an alternative configuration for the phase mask technique, as depicted in Fig 7. This modified version incorporated two adjustable parameters to expand the range of Bragg wavelengths for inscribed FBGs. The first parameter involved increasing the distance between the phase mask and optical fiber, while incorporating two mirrors to adjust the interference beam angles. The second parameter utilized a movable lance positioned between the phase mask and UV laser source, enabling the tuning of UV light wavelengths incident on the phase mask [30]. At present, the phase mask technique is the predominant method for manufacturing FBG sensors. Its prevalence is attributed to its simplicity, practicality, and potential for automation, which enhances production efficiency.

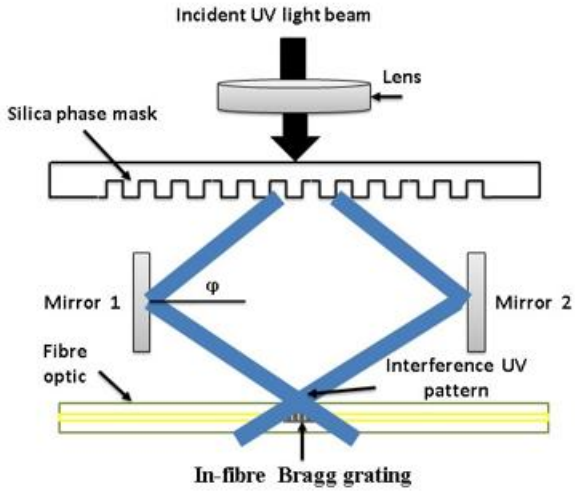


Figure 7: Modified phase-mask technique [30]

3.4 FBGS sensing principles

The preceding sections have addressed the fabrication and analysis of FBGSs embedded in SMF. This section will elucidate the sensing principle of FBGSs. The operational mechanism of a FBGS is illustrated in Fig 8. In essence, a FBGS functions as

a light filter, employing the Bragg reflection theory for its filtering process. When a broadband light source illuminates an optical fiber containing a FBG head (Fig 8.a), the light typically propagates through the fiber until it encounters the FBG head (Fig 8.b). At this juncture, the FBG head reflects a specific wavelength of the incident light (the one that satisfies the Bragg condition). The remaining light wavelengths traverse the FBG head unaltered, as depicted in Fig 8.c.The reflected Bragg wavelength changes with the variation of the FBGS structure parameters (grating period Λ and refractive index $n_{eff,}$) upon being subjected to external forces and/or temperature changes. The subsequent sections will provide a more detailed explanation of the effects resulting from mechanical and/or thermal stimulation.

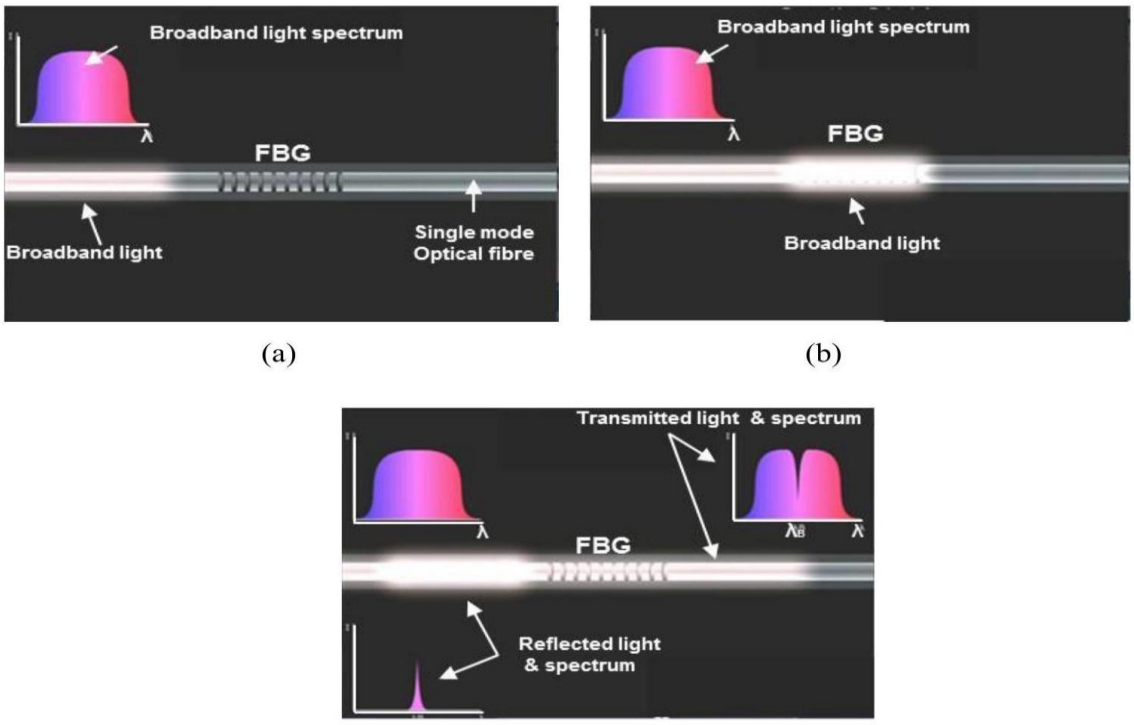


Figure 8: Working principle of FBGS [45]

The integration of advanced interrogation methods featuring multiplexing capabilities with the ability to embed multiple FBG heads in a single-mode fiber (SMF) enables FBGST to offer a significant advantage for distributed sensing applications. Multiple FBGSs within an SMF can be interrogated, as these sensors are designed with distinct Bragg wavelengths to prevent spectral overlap [46]. An optical fiber containing several FBG heads is designated as an FBG array sensor (FBGAS). The operational principle of an FBGAS is illustrated in Fig 9: broadband light illuminates the array, and specific wavelengths are reflected by each FBG sensing head. As demonstrated in Fig 9.a, individual FBG heads reflect particular light spectra corresponding to their engineered Bragg wavelengths [47]. The array can be configured to measure a single physical parameter such as temperature, with all FBG heads functioning as temperature sensors, or as multi-parameter sensors where different FBG heads measure various physical quantities including temperature, strain, pressure, and force (as depicted in Fig 9.b).

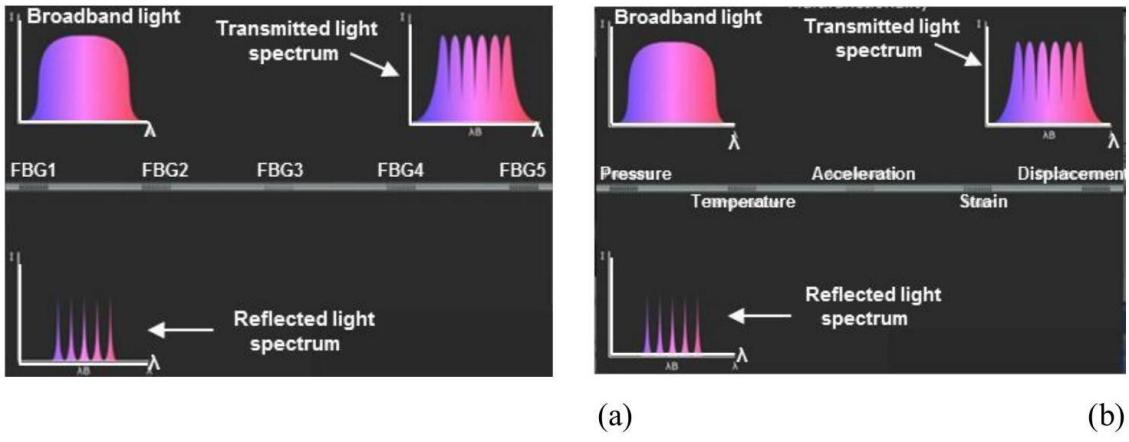


Figure 9: Operating principle of the FBG array sensor [45]

The reflected λ_B varies as a function of the FBGS structure parameters (grating period and refractive index). The FBGS's parameters fluctuate when subjected to variations in strain and/or temperature [48]. Hence, examining the variations of the reflected λ_B allows the sensing capability to be achieved. The reflected λ_B relative rate of change due to changes in the FBG structure parameters can be defined in terms of the acting thermal and/or mechanical excitation as [36]:

$$\frac{\Delta\lambda_B}{\lambda_\mathrm{B}} = \overbrace{2\left(\Lambda\frac{dn_{eff}}{d\varepsilon} + n_{eff}\frac{d\Lambda}{d\varepsilon}\right)\Delta\varepsilon}^{A} + \overbrace{2\left(\Lambda\frac{dn_{eff}}{dT} + n_{eff}\frac{d\Lambda}{dT}\right)\Delta T}^{B} \quad 2$$

where: $\Delta\lambda_B$ is the shift in the Bragg wavelength, λ_B is the base Bragg wavelength, ε is the strain and T is the temperature. The term A in Eq. 2 signifies the Bragg wavelength shift caused by elastic-optic effect due to strain. Term B in Eq. 2 describes the Bragg wavelength variation due to thermo-optic and thermal expansion effects caused by temperature variation [49, 34]. Eq. 2 can be simplified and rewritten as:

$$\frac{\Delta\lambda_B}{\lambda_\mathrm{B}} = k_\varepsilon\Delta\varepsilon + k_T\Delta T \quad 3$$

where: k_ε and $k_{T\text{ are the}}$ FBGS sensitivity factors to strain and temperature, respectively.

3.4.1 FBGS temperature sensing dependency

When a FBGS structure is subjected to temperature variation, the reflected λ_B is shifted and corresponds to the subjected temperature variation, as illustrated in Fig 2.11. The temperature response of λ_B is due to the optical fibre temperature dependency effects. Two primary factors contribute to the observed effect. The initial impact stems from alterations in the grating interval, which result from thermally induced longitudinal

expansion of the optical fiber. The secondary factor is the thermo-optic phenomenon, arising from the temperature-dependent nature of the effective refractive index. This analysis assumes the absence of mechanical stimulation and considers only thermal excitation acting upon the FBG sensor. the first part of Eq. 3 can be ignored and the variation in λ_B due to temperature expressed as [46]:

$$\Delta\lambda_B / \lambda_B = k_T \Delta T = (\alpha + \xi)\Delta T \quad 4$$

where: α represents the longitudinal thermal expansion coefficient and ξ is the thermooptic coefficient. In a standard optical fibre made of silica, α is $\approx 0.55 \times 10^{-6}/$ $^{\circ}\mathrm{C}$ and ξ is $\approx 6 - 9 \times 10^{-\ 6}/\ ^{\circ}\mathrm{C}$ [46]. The thermal expansion coefficient of optical fibres is very minor. Thus, the shift in λ_B when a FBGS is subjected to thermal excitation largely depends on the change in n_{eff}. Nevertheless, the effect of the thermal expansion coefficient can be utilized to boost the temperature sensitivity of Fiber Bragg Grating Sensors (FBGS). This enhancement is possible by encasing an FBG temperature sensor in a material with a high coefficient of thermal expansion.; in this case α in Eq. 4 is the packaging material thermal expansion coefficient [50].

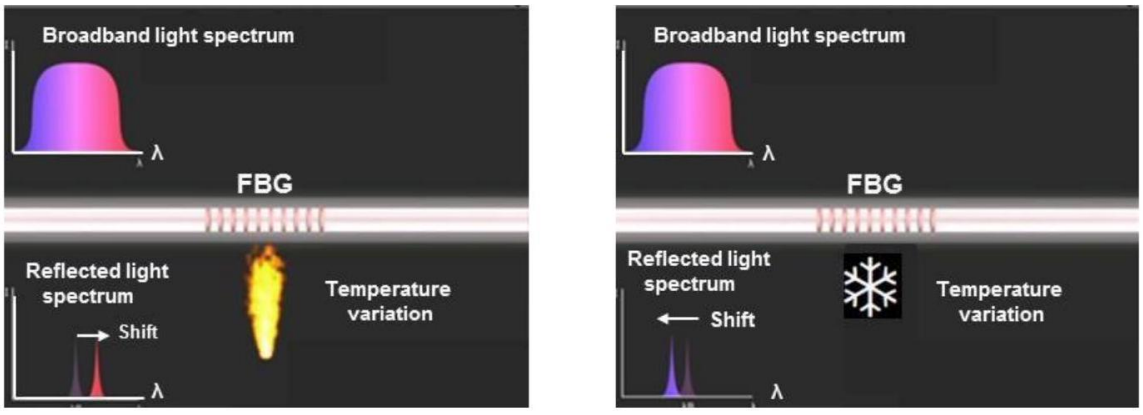


Figure 10: FBG temperature sensor operating principle [45]

The temperature sensitivity of a standard FBGS with $\lambda_B \approx 1550$ nm can be estimated from Eq. 4. For 1 °C of temperature change, the temperature sensitivity can be $\approx 10 - 14\text{pm}/\,^{\circ}\text{C}$. [51]. The temperature measurements range of FBGS is limited by the fiber type, coating and packaging (in case of packaged FBGSs). Generally, fibers with an acrylate coating can operate within a - 20 to 80°C temperature range, and fibres with a polyamide coating can operate within a -50 to 300°C temperature range [52]. However, the use of FBG thermal sensors for high temperature measurements, above 600°C, has also been recently reported in literature [53, 54].

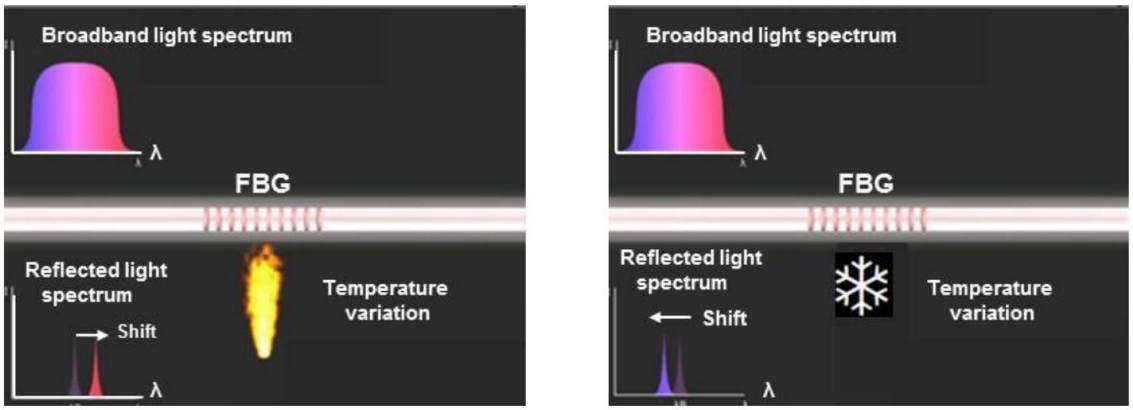


Figure 11: FBG temperature sensor operating principle [45]

3.4.2 FBGS strain sensing dependency

An FBG strain sensor is based on monitoring the λ_B shift due to an applied strain. The shift in λ_B is due to the change in the grating spacing Λ (elongation of the optical fibre) and the change in in n_{eff} (fiber photo-elastic effect) [34, 46]. Fig 12 shows the reflected λ_B shift and the change in the grating spacing (expansion or contraction) of FBGS when it is subjected to external strain. Assuming constant temperature, the variation in λ_B due to strain can be expressed as [36]:

$$\Delta\lambda_B/\lambda_B = k_\varepsilon \Delta\varepsilon = (1 - P_e)\Delta\varepsilon \quad (5)$$

where $\Delta\varepsilon$ is the axial strain and P_e is the photo-elastic coefficient of the fibre, which can be calculated as [36]:

$$P_e = \left(\frac{n_{eff}^2}{2}\right)[P_{12} - v(P_{11} + P_{12})] \approx 0.22 \quad (6)$$

P_{11} and P_{12} are the strain optic tensor coefficients and v is the Poisson's ratio. From Eq. 4 and Eq. 6 , the FBGS strain sensitivity for a standard fiber optic with $\lambda_B \approx 1500$ nm is $\approx 1.2\text{pm}/\mu$ strain [52]. FBGSs can measure strain up to $\pm 10000 \mu\text{strain}$ [33].

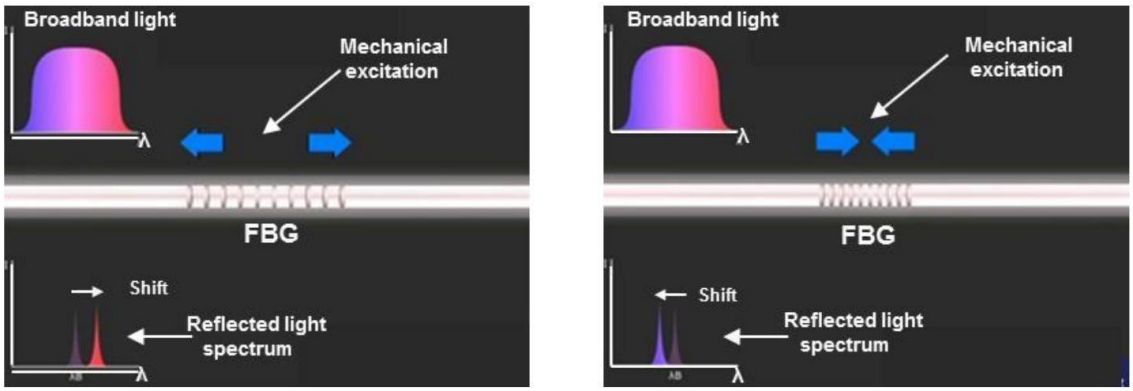


Figure 12: FBG strain sensor operating principle [45]

3.4.3 Temperature-strain cross-sensitivity in FBGSs

As previously discussed, the displacement in the reflected λ_B of FBGSs can be induced due to any change in the strain or the temperature the sensor is exposed to. The interdependence of strain and temperature on FBGS output is evident from Eq. 3. To obtain accurate measurements of strain and/or temperature, either individually or simultaneously, it is imperative to differentiate between the effects of these two factors on the reflected light spectrum [33]. When measuring temperature exclusively, an FBGS

must be isolated from external mechanical forces, which can be achieved through appropriate packaging design. However, it is essential to exercise utmost caution when designing the packaging for an FBG temperature sensor, as it can significantly influence the sensor's accuracy and sensitivity [51, 55].

Researchers have documented various methods for measuring strain using FBGSs. One straightforward approach involves utilizing an additional FBG temperature sensor (an FBGS protected from mechanical forces) to compensate for the strain measurements obtained from the FBG strain sensor. This additional FBGS should be positioned in the same thermal environment as the active FBG strain sensor. The temperature-induced error in strain measurement can be corrected in real-time by subtracting the measured wavelength shift of the FBG temperature reference sensor from that of the FBG strain sensor, as follows:

$$\frac{\Delta\lambda_{\mathrm{B-\ corrected}}}{\lambda_{\mathrm{B}\varepsilon}} = \frac{\Delta\lambda_{\mathrm{B}\varepsilon}}{\lambda_{\mathrm{B}\varepsilon}} - \frac{\Delta\lambda_{\mathrm{B}T}}{\lambda_{\mathrm{B}T}} \quad 7$$

where $\Delta\lambda_{\mathrm{B}\varepsilon}$ is the induced wavelength shift in the active strain sensor and $\Delta\lambda_{\mathrm{B}T}$ is the induced shift in the additional temperature sensor. Although this technique typically yields precise measurements, it is associated with the disadvantage of increasing the overall cost of the sensing system due to the necessity for an additional sensor.

3.4.4 FBG multi-physical sensing

While an FBG head exhibits inherent sensitivity to variations in strain and/or temperature, as previously discussed, it can be further adapted to create sensors capable of detecting additional physical properties. These include stress, pressure, force, magnetic and electrical fields, voltage, current, acceleration, and displacement [33, 36, 46, 56-59].

This versatility is achieved through the application of specific coatings and packaging designs for FBGSs. The capacity of FBGST to sense multiple physical properties is significant. However, this research primarily focuses on investigating the thermal sensing capabilities of FBGSs for use in real-time temperature monitoring applications within electric machines, and consequently, the multi-physical sensing aspect is beyond the scope of this thesis.

3.5 The Advantages of FBGSs

1. **Size:** A Fiber Bragg Grating Sensor (FBGS) comprises a modified segment within a standard single-mode optical fiber core, measuring approximately 125 μm in diameter and typically extending several millimeters in length [60]. The compact dimensions and low mass of FBGSs render them suitable for integration into challenging locations with minimal mass impact [61]. These characteristics are particularly significant for contemporary electrical machines (EMs), where mass and size constraints are critical factors in applications such as aerospace and transportation. Capitalizing on this attribute, FBGSs provide unique opportunities for real-time thermal and mechanical monitoring of internal EM component structures.
2. **Uniquely self-coded:** The central Bragg wavelength λ_B functions as a distinct identifier for each FBGS [60]. This methodology facilitates sensor identification and mitigates potential ambiguity in measurement interpretation.
3. **Multiplexing:** Multiple FBG heads can be inscribed on a single optical fiber, creating an FBG array that facilitates simultaneous interrogation. Moreover,

several FBG arrays with multiple sensing points can be concurrently interrogated utilizing a multi-channel interrogator unit. This capability is essential for sensing applications, as it can significantly reduce the dimensions of the sensing system, mitigate wiring complications, and alleviate installation challenges [43, 62]. The multiplexing feature is particularly noteworthy as it enables the development of a distributed sensing system. In principle, a single fiber can incorporate a substantial number of sensing points, resulting in a sensing array that, when integrated into a machine structure, can provide valuable real-time monitoring data.

4. **Electromagnetic/electrical immunity:** The FBGS structure exhibits dielectric properties, rendering it non-conductive and resistant to electrical and electromagnetic interference. This characteristic establishes FBGSs as an optimal choice for integrated sensing applications in constrained environments with high electrical and electromagnetic activity, where conventional sensors may malfunction or encounter measurement challenges. This attribute facilitates the secure and reliable incorporation of FBGSs in direct contact with operational electric and/or electromagnetic components (such as stator windings, stator core, and magnets) within EMs [30, 63].
5. **Multi-physics sensing:** FBGST utilizing transducers can be engineered to detect various physical parameters, including stress, force, magnetic and electrical fields, voltage, current, and displacement [33, 36, 46, 56-59]. Through the integration of multi-physics sensing capabilities with multiplexing functionality, a

comprehensive sensing system for EMs can be developed. This system would monitor critical parameters for EM health assessment, such as temperature, vibration, forces, and magnetic field. The implementation of such an integrated system could significantly reduce the monitoring system's spatial requirements and, consequently, its associated costs.

6. **Working in harsh conditions:** FBGSs exhibit resilience and functionality in adverse environments, including those characterized by corrosive elements or high-pressure conditions. Moreover, an FBGS functions as a passive sensor, necessitating no electrical input for operation, thereby ensuring safe utilization in potentially hazardous or explosive settings [30, 61].
7. **Distance sensing:** The placement of FBGSs can be situated up to several kilometers from the interrogation unit. This capability is attributed to the fact that optical fibers function as efficient single carriers, whereas other electrical sensors necessitate signal amplification for long-distance sensing. This characteristic proves advantageous in scenarios where EMs are located at a substantial distance from their control and operating units [30].
8. **High sensitivity:** The FBGS demonstrates high sensitivity to both strain and temperature, with sensitivity coefficients of approximately 1.2 pm/μ strain and 10-14 pm/ºC, respectively [36, 52].
9. **Long-term stability:** FBGSs offer robust and enduring solutions. In the telecommunications sector, these sensors have obtained commercial certification for a minimum operational lifespan of 25 years through the Telcordia program.

This certification is predicated on various assessments, including temperature cycling, high temperature storage, and humidity exposure, among others [52, 64].

10. **Rotary sensing:** Rotating components in electric machines (EMs), such as rotors, can accommodate Fiber Bragg Gratings (FBGs). This integration is facilitated through the connection of rotating FBG heads to interrogation units via a fiber-optic rotary joint (FORJ) device [65, 66]. This capability represents a significant advancement in electric machinery applications, as it addresses previous challenges in rotor parameter sensing, which was often avoided due to issues with signal transmission, implementation complexities, and reliability concerns.

3.6 The disadvantages of FBGSs

1. **Standard:** Currently, no established standard exists for FBG sensing applications.
2. **Cross-sensitivity:** Conducting concurrent and separate measurements of strain and/or temperature necessitates additional compensatory measures, which increases the system's complexity and cost [67]. This challenge is particularly pronounced in sensing applications for EMs, as these are inherent sources of thermal and mechanical stimulation. Consequently, achieving distinct or simultaneous measurements in this context presents significant difficulties.
3. **Installation:** FBGSs are fragile and easy to break. Therefore, careful handling and installation is required [68].
4. **Weak market:** FBGSs are susceptible to damage due to their fragile nature. Therefore, extreme caution is necessary during their handling and installation processes [61].

5. **Cost:** While FBGSs are relatively cost-effective sensors, their interrogation systems are associated with a substantial financial investment, typically ranging from several thousand dollars, contingent upon performance requirements [33]. This high cost is presently considered a limitation from an industrial perspective. However, FBGST remains an evolving technology, and its cost is anticipated to decrease over time. The multifaceted nature of FBG sensing systems, in conjunction with their multiplexing capabilities, has the potential to significantly reduce the overall scale and expense of monitoring systems. Furthermore, FBG sensing offers numerous advantageous monitoring and performance enhancements for EMs that would be challenging to achieve through alternative sensing or design methodologies. Despite its current high cost, this technology has already found applications in aerospace [69] and wind turbine [70] industries, where its features have contributed to the development of more effective condition monitoring systems.

Research indicates a correlation between cost, market, demand, and manufacturing competition. A recent study on the global FBGS market through 2017 demonstrates the technology's rapid market growth [35]. FBGST has recently found practical applications in critical industries such as aerospace, oil and gas, medical, and energy sectors, where its features are essential [35, 52, 71]. Moreover, the increasing number of publications on FBGST applications across various fields reflects the growing demand for research in this area. The report [35] also highlights an increase in technology manufacturers worldwide. Currently, competition in manufacturing extends beyond established FBGST developers

such as Micron Optics [71], FBGS [72], and Smart Fibers Limited [52], to include globally recognized sensing and instrumentation companies such as HBM [54] and National Instruments [73].

3.7 FBG Sensing Application in Smart Grid

3.7.1 FBG sensing for fault detection

In the smart grid, fault detection plays a vital role in maintaining grid stability and reliability. Optical fiber sensors are one method employed for identifying faults, as they can detect alterations in the fiber's physical properties, including temperature, strain, and vibration. The information gathered by these sensors can be utilized to identify potential issues within the grid. For instance, an anomalous temperature increase detected in a specific grid area might indicate a possible fault.

Power systems are commonly monitored using current transformers (CTs) and potential transformers (PTs), which transmit fault current/voltage data to relay and control rooms at substations. Relays send trip signals to breakers when current/voltage in a particular line exceeds preset limits. If a primary relay fails, a backup breaker will clear the fault based on predetermined rules. Traditional iron-based CTs are susceptible to saturation and hysteresis. Most relays make decisions based on the root mean square (rms) value of fault current detected by the CT. CT saturation can cause the sensed rms value to be significantly lower than the actual value, potentially preventing relay tripping and leading to system instability.

Optical current transformers (OCTs) are gaining prominence in power systems due to their superior transient response, improved accuracy, and wider bandwidth compared to

conventional CTs, attributed to their lack of an iron core [74]. OCTs are compact, lightweight, cost-effective, and resistant to electromagnetic interference (EMI) [75]. Several Faraday effect current sensors have been successfully implemented [76,77]. Although OCTs can measure high currents without saturation, the absence of suitable fault detection and classification algorithms hinders their application in power systems. Previous studies have examined the impact of faults on FBG wavelength shifts [78]. A smart grid system can experience several typical fault types:

1. **Overvoltage or undervoltage:** A voltage fault occurs when the electrical potential in the power system deviates beyond its standard operational parameters. Multiple factors can precipitate this phenomenon, including equipment malfunctions, excessive power demands, or disruptions in the electricity supply.

2. **Short circuits:** A short circuit constitutes an electrical fault wherein two points in the electrical grid with differing voltage potentials become directly connected. This phenomenon can result in equipment damage and disruptions to the power supply.

3. **Open circuits:** A discontinuity in the electrical connection between two points within the power grid is referred to as this type of fault. Such interruptions can result in power outages and potential damage to electrical equipment.

4. **Ground faults:** A ground fault is characterized by the flow of electrical current through the earth. Such faults possess the potential to damage equipment and compromise the stability of the electrical grid.

5. **Transients:** A transient fault occurs when the voltage or current in the electrical grid experiences an abrupt and momentary fluctuation. These transients have the potential to damage equipment and result in interruptions to power delivery.

6. **Oscillations:** This fault type is characterized by a sustained oscillation in the voltage or current magnitude within the electrical grid. These fluctuations have the potential to cause damage to equipment and compromise the stability of the grid.

7. **Stuck Relays:** This type of fault occurs when the relay is not switching on or off as per the command.

8. **Misoperations:** This type of fault occurs when the protection system operates on a healthy part of the system.

9. **False tripping:** A malfunction of this nature arises when the protective mechanism activates on a properly functioning segment of the system, causing the circuit breaker to disconnect.

Benefits of Using Optical Fiber Sensors for Smart Grid Fault Detection:

1. **Real-time data:** Real-time data pertaining to the electrical grid's performance can be acquired through the utilization of optical fiber sensors. These sensors measure physical parameters such as temperature, pressure, and strain, which facilitate the identification and analysis of potential grid anomalies or malfunctions. The acquired data is subsequently recorded and stored on the

blockchain, ensuring that all participants have access to accurate and current information regarding the grid's operational status.

2. **Increased accuracy:** The utilization of optical fiber sensors can enhance the precision of acquired data, as these instruments are capable of measuring physical parameters with high accuracy.

3. **Improved security:** Optical fiber-based sensors can be utilized to monitor physical infrastructure and detect potential tampering attempts, thereby contributing to the prevention of unauthorized access and potential attacks on the electrical grid.

4. **Peer-to-peer energy trading:** Optical fiber sensors can facilitate peer-to-peer energy trading by providing real-time information on energy generation and consumption. This data enables individuals and organizations to make informed decisions regarding the acquisition and distribution of energy.

5. **Reliability:** Owing to their immunity to electromagnetic interference and capacity to operate over extensive distances, optical fiber sensors offer a reliable solution for monitoring the smart grid.

6. **Durability:** The resilience and durability of optical fibers enable them to withstand adverse conditions, rendering them suitable for prolonged utilization in diverse outdoor applications.

7. **High Sensitivity:** The smart grid's faults can be effectively detected utilizing optical fiber sensors due to their exceptional sensitivity to physical alterations.

8. **Immunity to electromagnetic interference:** Due to their resistance to electromagnetic interference, optical fiber sensors are particularly suitable for smart grid applications.

9. **Low maintenance:** Fiber optic sensors are characterized by low maintenance requirements and extended operational lifetimes.

CHAPTER FOUR

BLOCKCHAIN IN SMART GRIDS

4.1 Blockchain Technology

Blockchain technology, first introduced in [79], is a form of distributed ledger or database technology [80], [81], [82] those functions as a consensus-based system of replicated, shared, and synchronized digital information [83]. This technology serves as a secure, decentralized, and trusted cyber infrastructure, enabling multiple network entities to generate, maintain, and store a chain of blocks. It incorporates fault-tolerant consensus algorithms, smart contracts, public-key cryptography, peer-to-peer networks, and database management technologies, resulting in a cost-effective, secure, and efficient operational management system [84].

As depicted in Figure 13, each block in a blockchain records various data or transaction entries. A data record or transaction represents a message transmitted from one node to others within the network. Every transaction contains the recipient's address, transaction data payload, and a transaction value. The sender's private key is utilized to sign transactions, and the network's state is modified exclusively by these signed transactions [82].

A blockchain block can contain various elements such as a timestamp, nonce, Merkle tree (a type of hash tree) [85], hash, and smart contract scripts [86],[87]. The Merkle Tree functions to efficiently summarize and verify extensive data sets within a block, rendering it suitable for devices with limited storage capacity that require rapid

searching and verification of data without storing the entire blockchain. Each block's timestamp, indicating its creation time [89], introduces variability to the block hash and enhances the blockchain's resistance to tampering. The block's hash, a cryptographic representation, links all blocks together, with each block referencing its predecessor's hash. Both the hash and Merkle Tree ensure data integrity by enabling verification of the block's unaltered content [81]. Network nodes continuously append newly validated blocks to their local chains at predetermined intervals. Consequently, blockchain data is distributed across numerous locations, nations, and institutions globally, accessible to all network participants. Modifying any block's content necessitates changing all corresponding data due to the interconnected hash mechanism. In a linear chain structure, blocks connect only to their immediate predecessor. When blocks reference multiple previous blocks, the structure is termed a Directed Acyclic Graph (DAG) [83]. The redundancy created by blockchain technology contributes to its resilience against single point failures and cyber-attacks [90].

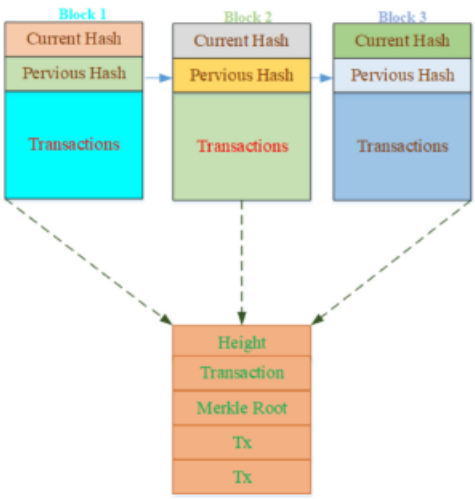


Figure 13: A block construction in blockchain

4.1.1 Network

In a centralized network, a single entity functions as the primary point of contact for information exchange. Conversely, a decentralized network comprises multiple central authorities that maintain copies of resources, addressing the vulnerability of a single point of failure inherent in centralized systems. A distributed network, however, entirely eliminates centralization, granting full access to all participants. Blockchain technology exemplifies a distributed network, wherein every node possesses access to all available information. The blockchain operates as a fully decentralized system, thus eliminating the necessity for a trusted intermediary.

4.1.2 Ledger

A database serves as a repository for managing, storing, editing, and accessing data at any time. In contrast, a blockchain ledger functions similarly to a database in terms of data storage and accessibility, but it does not allow for data modification. This

characteristic makes the ledger append-only, ensuring its integrity and immutability. Every node within the blockchain network maintains a synchronized copy of the ledger, which is distributed across the network. The ledger records transactions that are generated and authenticated by various blockchain nodes. These transactions are incorporated into the ledger through a mining process**.**

4.1.3 Consensus Mechanism

The establishment of trust within a network is facilitated through the consensus mechanism, a critical component of blockchain technology. This process entails a group of validators reaching an agreement on the validity of a block. Both public and private blockchains employ consensus algorithms. In public blockchains, all nodes are permitted to participate in the process, whereas private blockchains restrict participation to selected nodes. The limited number of validators in private blockchains results in a more streamlined consensus mechanism and enhanced network performance [83]. The components of a transaction block and consensus algorithms may vary based on the specific requirements of blockchain applications. Several prominent consensus mechanisms exist and are widely implemented in various blockchain systems.

1. Proof of Work (PoW): (PoW) was initially implemented in Bitcoin and is regarded as the original public blockchain consensus mechanism [79]. In PoW systems, consensus nodes participate in a competition to solve a computationally challenging puzzle, known as the PoW problem, which is difficult to solve but straightforward to verify. The node that successfully solves the puzzle appends the solution to a new block and propagates it across the network for verification

by other nodes. This process of solving the puzzle and validating the block is termed mining. While PoW aims to mitigate various cyber-attacks, it is vulnerable to a 51% attack, wherein malicious actors controlling over half of the network's processing power can potentially compromise the system. Furthermore, PoW faces challenges such as low throughput, high latency, and excessive energy consumption, limiting its applicability in other blockchain applications [83], [91], [92].

2. Proof of Stake (PoS): (PoS) [93], [94], [95] serves as an alternative to Proof of Work (PoW), aiming to address the prevalent limitations of PoW. In PoS-based blockchain systems, block validation typically supersedes mining. The system employs a stochastic selection process for validators to generate new blocks, with the probability of a node being selected to validate the subsequent block correlating to the quantity of stakes or assets it possesses. However, this approach inherently favors the most affluent validators, who effectively govern the blockchain, resulting in an inequitable PoS mechanism [83], [92].

3. Delegated Proof of Stake (DPoS): DPoS [96] DPoS represents a modification of PoS. The key distinction between these two systems lies in their democratic approach: PoS employs direct democracy, whereas DPoS utilizes delegated democracy. In the DPoS system, block generation and validation are restricted to a limited group of chosen delegates. Due to the reduced number of nodes involved in the validation process, DPoS operates at a higher speed compared to PoS.

4. Leased Proof of Stake (LPoS): The LPoS [97] system enables participants to rent out their assets to other users. This process can enhance the chances of the borrowing participants being chosen as validators. By increasing the number of eligible voters, the network can reduce the likelihood of a single group of nodes gaining control over the blockchain system.

5. Proof of Activity (PoAc): PoAc [98] combines elements of PoW and PoS. Initially, new block creators function as miners, employing the PoW mechanism to protect against security threats and earn rewards. Once these miners accumulate sufficient coins (assets), they switch to the PoS mechanism for publishing new blocks [99], [100]. PoAc guarantees that reward tokens are distributed punctually.

6. Proof of Burn (PoB): (PoB) [101] serves as an alternative to Proof of Work (PoW) and Proof of Stake (PoS) consensus mechanisms. In PoB, nodes can become authorized validators by destroying their own coins or assets through sending them to verifiable, public, and unspendable addresses. This process enables nodes to generate new blocks and receive rewards, with the burned coins viewed as an investment. Unlike PoW and PoS, PoB does not require substantial energy consumption. The cryptocurrency Slimcoin [102] utilizes PoB as its underlying consensus mechanism.

7. Proof of Inclusion (PoI): The Merkle tree root [85] within a block serves as evidence for record inclusion. It allows nodes to confirm individual records without examining and contrasting the entire chain. When two nodes' blockchains

share an identical Merkle tree root, it indicates that their blocks are verified and in agreement. The Ethereum blockchain, as described in [86], employs PoI.

8. Proof of Elapsed Time (PoET): PoET [103] was developed to address the challenges associated with the high energy consumption of PoW. Rather than employing computationally intensive tasks, PoET utilizes proof of elapsed time. The system randomly selects the subsequent block publisher from all validators, who request a random waiting period from their enclaves. The validator with the shortest wait time for a specific block is designated as the leader and is authorized to publish the new block upon completion of their waiting period. The system relies on trusted hardware to generate the time. Hyperledger Sawtooth [104] implements the PoET consensus mechanism.

9. Proof of Authority (PoA): Proof of Authority (PoA) [105] is specifically engineered for permissioned blockchains, utilizing a participant's identity as the stake. Participants must verify their identity within the network before gaining the authority to issue blocks. The system relies on pre-selected, trusted authorities for block publication. This approach facilitates the identification of malicious actors and enables efficient communication of such activities to other nodes. The Parity Ethereum platform [106] is built upon the PoA concept.

10. Proof of Reputation (PoR): Proof of Reputation (PoR) [107] represents an enhanced and more robust version of Proof of Authority (PoA), utilizing a blockchain consensus mechanism that relies on participant reputation to ensure network security [108]. In the PoR system, any node attempting to deceive the

network would face substantial monetary penalties and reputational damage. The implementation of PoR occurred in [109].

4.1.4 Cryptographic Techniques

To ensure data security during transfers between parties, various cryptographic methods have been developed. These techniques aim to maintain confidentiality, integrity, authenticity, and privacy of information, while also preventing unauthorized access and misuse by malicious actors. This thesis employs several key concepts, including hash functions, digital signatures, and asymmetric cryptography, which are briefly delineated.

1. **Hash Function:** In cryptography, a hash function is utilized to maintain data integrity. The blockchain's tamper-resistant nature is achieved through the linkage of blocks containing data hashes. Prior to transmission, transactions undergo hashing as well. This process enables miners to verify the authenticity of each transaction.
2. **Digital Signature:** Cryptographic authentication of data is accomplished through the utilization of digital signatures. When initiating a transaction, the user can apply their private key to sign it. Prior to incorporating the transaction into the blockchain, the recipient can verify its authenticity by employing the creator's public key.
3. **Asymmetric Cryptography:** Asymmetric cryptography functions as a mechanism for ensuring data confidentiality. In this methodology, the entity initiating a transaction can encrypt the information utilizing their public key.

Subsequently, the recipient of the transaction can decrypt the information employing their private key.

4.2 Blockchain Types

Blockchain technology can be categorized into two primary classifications: private and public blockchains. Additionally, there exists a significant variant known as consortium blockchain.

4.2.1 Public Blockchain

A public blockchain is an open, decentralized ledger system that permits unrestricted access. Participants can freely join the network without requiring authentication from other users [89]. Each node possesses the authority to generate blocks, view all records within the network, validate transactions for incoming blocks, and store blocks, thereby ensuring complete transparency and openness for all participating nodes. While individual nodes in a public blockchain are not inherently trustworthy, the system as a whole is considered reliable and more secure than private alternatives. This enhanced security is achieved through sophisticated cryptographic encryption methods, a consensus mechanism that validates all transactions and blocks, a larger network size, and distributed record-keeping, which collectively deter potential malicious actors.

Public blockchains typically comprise extensive networks with numerous nodes. The requirement for each node to verify transactions and perform proof-of-work calculations results in time-consuming processes, leading to low TPS (Transactions Per Second) and increased energy consumption [81]. The slow transaction processing and completion rates of public blockchains also contribute to scalability challenges. The most

fundamental application of public blockchain technology is in the mining and exchange of cryptocurrencies, such as Bitcoin and Ethereum [110].

4.2.2 Private Blockchain

A private blockchain is a restricted network typically established within an organization, permitting only designated members to participate. The controlling entity manages security, authorization, and access. Due to the limited number of nodes, private blockchains achieve higher transaction processing speeds (TPS) and consume less energy. The consensus process for blocks and the addition of new transactions occurs expeditiously [111]. The relatively small scale of private blockchains contributes to their favorable scalability. However, the necessity for trust among nodes when sharing confidential information within the network increases the potential for security breaches. Private blockchains necessitate a control unit and Identity Access Management (IAM) system to oversee and regulate permissions, which contravenes the principle of decentralization and contradicts the fundamental concept of blockchain technology. These private blockchain networks find applications in voting systems and supply chain management [110], with Hyperledger Fabric serving as an exemplar [112].

4.2.3 Consortium Blockchain

A consortium blockchain is a partially decentralized system governed by multiple organizations [110]. It integrates elements of both public and private blockchains, incorporating open consensus mechanisms from public systems and centralized control from private ones. Organizations typically utilize consortium blockchains to establish

comprehensive platforms for data sharing among various stakeholders [113], [114]. Table 1 presents a summary of the primary characteristics of these blockchain classifications [81], [89], [111], [115].

Table 2: Different Features of blockchain Classifications

Item	Public		Private	Consortium
Join	Permissionless		Strictly Permissioned	Permissioned
Governance	None		Managed by one administrator	Managed by a set of participants
Access right	Any node can read, write, leave, and join		Only authorized nodes	Only a set of authorized nodes
Anonymity	Yes		No	No
Nodes	Not trusted		Trusted	Trusted
Consensus mechanism	Proof of Work (PoW), Proof of Stake (PoS)		Multi-part voting	Strictly preapproved node's voting
Cryptocurrency	Bult-in cryptocurrency		No	No
Security performance	High security. 51% attack tolerance, hard to tamper, no finality		Low security. 33.33% attack tolerance, could be tampered, enabled finality	High-end security
Transactions per second (TPS)	Bitcoin 7 TPS; Ethereum network 15 TPS		VISA 24,000 TPS	1000 - 2000 TPS
Computation complexity	High		Low	Middle
Decentralization level	Highly decentralized		Highly centralized	Semi-centralized
Transaction Validation	Incentive-based mining by any node		List of authorized validators, no incentive required	
Energy consumption	High		Low	Middle
Scalability	Low		High	Middle

4.3 Ethereum

Ethereum functions as a public, open-source computing platform and operating system predicated on blockchain technology, with an emphasis on smart contract functionality. It operates as a state machine driven by transactions, wherein each transaction modifies the blockchain's state. Upon verification and incorporation into a block, a transaction becomes an integral part of an immutable record. This immutability ensures the Ethereum blockchain's resistance to unauthorized alterations. Additional features encompass the capability to scrutinize data and monitor its entire lifecycle. Ethereum serves as a programmable foundation for the execution of decentralized applications (DApps) on a distributed network. These DApps, which operate within the Ethereum network, utilize smart contracts as their core functionality.

4.3.1 Account

The Ethereum blockchain network comprises two distinct account types. The first is the externally owned account (EOA), which functions as the user's Ethereum account and contains both a public and private key. EOAs possess the capability to send, sign, and receive transactions. The second type is the contract account, which represents the address of a deployed smart contract. Contract accounts are restricted to receiving transactions and executing smart contract code.

Every Ethereum EOA is associated with a key pair consisting of a public and private key. It is imperative to maintain the security of the private key. The public key is derived from the private key, and the account's address is generated by extracting a

portion of the public key's hash. Notably, the public key cannot be utilized to derive the private key.

The private key of an Ethereum account plays a crucial role in signing transactions, thereby verifying their authenticity. This signature process ensures that transactions cannot be altered subsequent to their issuance.

4.3.2 Smart Contracts

A smart contract functions analogously to a traditional agreement between two parties, with the primary distinction being its digital nature and automated enforcement. This computerized agreement implements contract terms, negotiations, and execution through code, which automatically initiates predetermined actions when specific conditions are met. The decentralized and transparent nature of smart contract transactions, coupled with the absence of intermediaries, renders them an attractive, conflict-mitigating tool. Smart contracts exhibit several advantageous properties. Their transparency is ensured through public accessibility, which in turn fosters trust as all interactions with the contract are recorded and visible to all parties. By utilizing smart contracts for transaction processing, the time typically required for third-party involvement is eliminated. Transactions are executed successfully when conditions are satisfied, or they fail if not, thereby mitigating potential issues associated with intermediary participation, including human error. Furthermore, the exclusion of third-party entities results in cost reduction.

The implementation of smart contracts guarantees various benefits. Their open availability ensures transparency, as they are accessible to all interested parties. This

visibility of all contract interactions establishes their credibility. Smart contract-based transaction processing reduces the time typically required for tasks involving third parties. If conditions are met, transactions proceed; otherwise, they fail. This streamlined process eliminates problems that can arise from third-party involvement, such as human errors. Additionally, removing intermediaries leads to decreased expenses.

Solidity, currently the predominant language for developing smart contracts, can be utilized to compose these contracts. Upon compilation into Ethereum Virtual Machine (EVM) bytecode, referred to as ABI (Application Binary Interface), the contract can be implemented on the platform. The Ethereum network, the preeminent blockchain platform for smart contract creation and deployment, is employed to deploy these contracts to ensure specific conditions are met between parties. The deployment of a contract on Ethereum constitutes a transaction that generates a contract address. Analogous to an Ethereum account, a smart contract possesses its own Ethereum address, which other nodes utilize to interact with it. Upon deployment, these contracts are securely stored in the state storage of each network node's ledger, rendering them tamper-resistant akin to other distributed ledger transactions. Once deployed, the contract cannot be altered.

To implement changes, it is necessary to delete the contract, rectify the issue, and redeploy it. Any account within the blockchain network can access the deployed contract using its address. All contract details are accessible, including transaction senders and recipients, transaction data, executed bytecode, and the state of each variable stored in the contract. Similar to other Ethereum addresses, smart contracts possess a balance. They

can receive either through transactions (utilizing a Solidity payable function), thereby increasing their balance, and can also send ether, consequently decreasing their balance. Smart contracts must be deterministic, consistently producing the same output given identical input. They must also be terminable, concluding their function execution within a specified time limit. Furthermore, smart contracts must be isolated, with their function execution separated from the entire ecosystem to prevent adverse side effects.

4.3.3 Decentralized Application

A decentralized application, or DApp, is a novel form of software that is not under the control of a single entity, as its nomenclature suggests. In contrast to centralized applications, DApps operate on a peer-to-peer computer network. While not all decentralized applications function on blockchain networks, the ones under discussion do. The fundamental logic of these blockchain-based DApps is encapsulated in smart contracts. These applications built on blockchain technology ensure data immutability and indelibility. The source code of the smart contract, which constitutes the core logic, is publicly accessible to all blockchain users. Ethereum serves as a platform for developers to code smart contracts, which function as blueprints for decentralized applications. The Ethereum blockchain hosts various categories of DApps, including those for currency exchange, identity management, energy management, health management, and additional domains. Other platforms such as EOS, Tron, and Hyperledger also facilitate the creation of decentralized applications. To develop a DApp, a programmer must create, test, and deploy a smart contract, which will govern the application's functionality on the blockchain network.

The decentralized application (DApp) inherits key characteristics from its underlying smart contract: immutability, transparency, and absence of centralized control. With the back-end established by the smart contract, attention must be directed toward developing the DApp's front-end. This user interface can be constructed using fundamental web technologies such as HTML, CSS, and JavaScript, or more advanced frameworks such as React or Angular. The web3 JavaScript library, which will be examined further in this thesis, enables users to interact with Ethereum's blockchain and its deployed smart contracts. Thus, a DApp comprises three main elements: the smart contract serving as the back-end, the web3 library functioning as an intermediary, and the user-facing front-end. It is noteworthy that while web3 is a prevalent choice, it is not the sole method for facilitating interaction with Ethereum.

4.3.4 Ethereum Virtual Machine

The Ethereum Virtual Machine (EVM) functions as an execution environment for smart contract code. Prior to execution, smart contracts must be transformed into bytecode that the EVM can interpret and execute. Each Ethereum node hosts the EVM, which exhibits Turing Completeness, enabling it to resolve any program it executes. The EVM is essential due to the isolation property of smart contracts, which renders interactions potentially hazardous. Without isolation of smart contract interactions, the entire system could be compromised. The EVM provides a sandboxed environment, ensuring security and isolation.

4.3.5 Transaction

Transactions on the Ethereum network can encompass various operations, including Ether transfers, smart contract deployment, or interactions with existing contracts. Upon execution, transactions record data on the blockchain, modifying the Ethereum state. These transactions are immediately visible to all network nodes. Smart contracts contain functions that can be accessed by different Ethereum nodes. Interaction with a smart contract can occur through two methods: a "call" method, which does not consume gas or alter the Ethereum state, merely returning a value; or a "send" method, which modifies the state and utilizes gas.

A transaction comprises several components. The "nonce" indicates the sender's previous transaction count. The "to" field specifies the recipient's Ethereum address, while the "from" field denotes the sender's address. The "value" represents the quantity of Ether being transferred. The "gasLimit" establishes the maximum gas consumption for the transaction, and the "gasPrice" determines the cost per gas unit. An optional "data" field serves multiple purposes: it may contain binary payload for Ether transfers between accounts or contracts, smart contract bytecode for deployment, or the hexadecimal representation of a function call with its parameters for contract interactions.
In the process of deploying a smart contract, the transaction will be characterized by the absence of a "to" field. Conversely, all other transactions incorporate a "to" field containing the intended Ethereum address. Upon finalization of the transaction, the initiating account will authenticate it through a signature using its private key. The

transaction's validity can be verified utilizing the public key of the transaction's originator.

4.3.6 Storage

Ethereum operates as a state machine, enabling transactions to modify the network's state. The platform employs a trie structure to store and manage data. Specifically, Ethereum utilizes the Merkle Patricia Trie, which incorporates elements from both the Merkle tree and the Patricia trie.

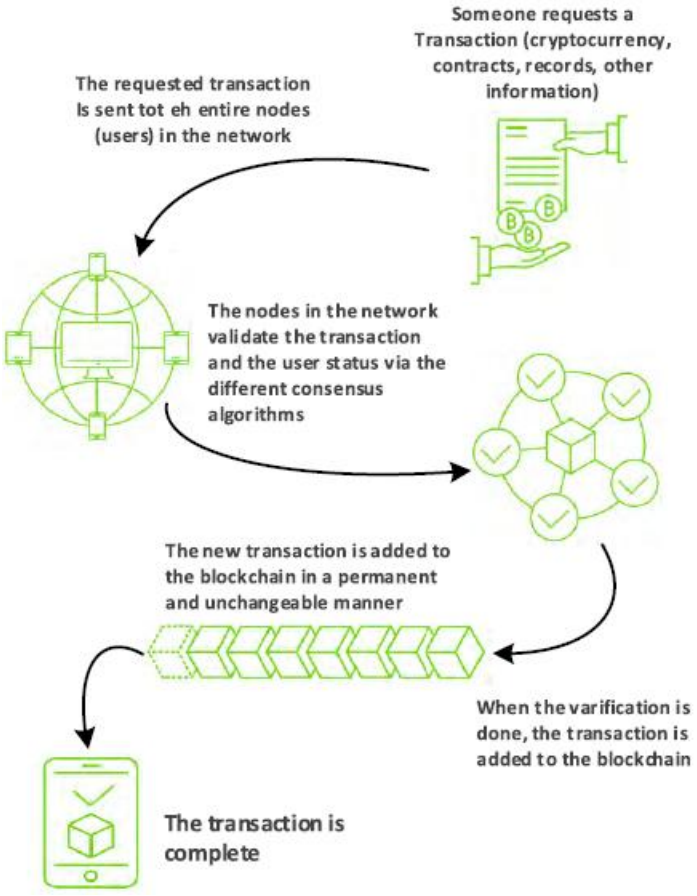


Figure 14: Blockchains transactions steps.

4.4 Framework of Blockchain-Enabled Technology

Blockchain technology is predicated on several fundamental principles that operate in concert to establish a robust network. These encompass a decentralized database, peer-to-peer transmission, transparency, immutability, and computational logic. The decentralized database facilitates access to transaction records for all network participants without centralized control. Peer-to-peer (P2P) transmission enables direct interactions between participants, with each transaction disseminated across the entire network, ensuring equitable information access. Transparency is achieved through unique alphanumeric addresses, allowing all participants to view network data. The immutability of records precludes data alteration once entered, mitigating the risk of fraud. Computational logic links transactions to programmable rules, triggering network responses when new transactions are added. Some researchers characterize blockchain as a distributed transaction database operating on a peer-to-peer (P2P) communication network, connecting dispersed nodes into a comprehensive system with its own protocol for node communication and discovery (see Figure 15) [116].

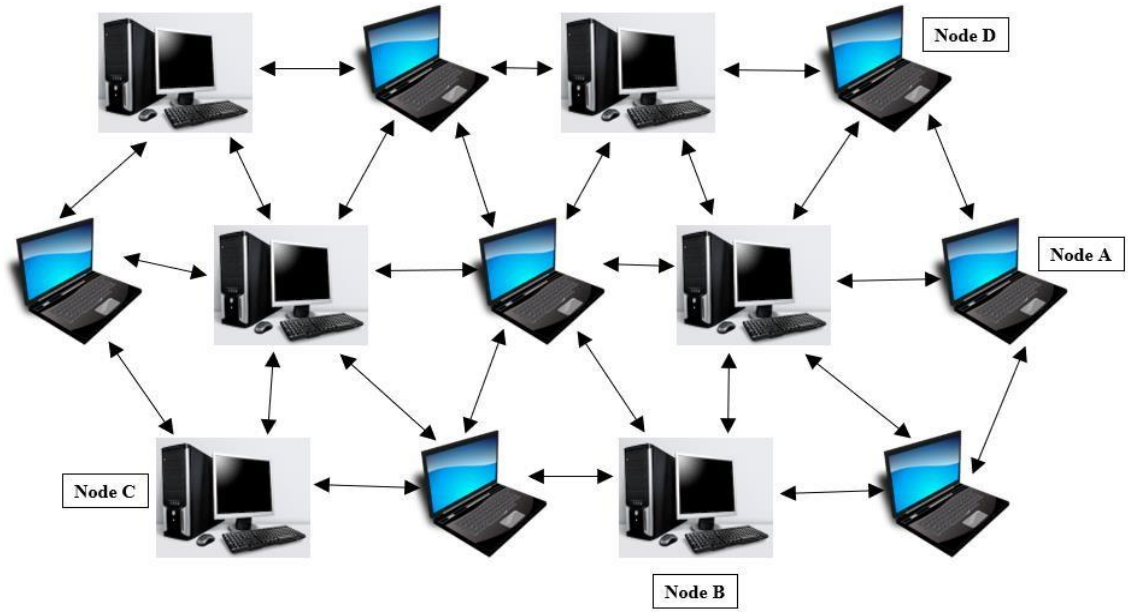


Figure 15: Blockchain network showing how information is interconnected between the nodes of a block in the network [116]

In Figure 15, a node represents a physical or virtual machine, such as a computer or laptop, that communicates with other nodes utilizing TCP/IP and UDP protocols. Within the network, users are identified by their public key addresses. Nodes recognize users through their IP addresses, while users can refer to one another using public keys. Users can conduct transactions (Tx) and cryptographically sign messages utilizing their private keys to ensure other parties of their legitimate intentions within the network. Each node contains an inherent scripting language (also known as smart contracts) that is activated by specific transaction events, storing activities in conventional databases and executing additional business logic triggered by any transaction. Although blocks share certain similarities and are interconnected, the distributed ledger enables blockchain to

operate in a decentralized manner, as information is not stored in a single central repository.

As illustrated in Figure 15, when Node A in Community A purchases 10 energy units from Node B for $150, this exchange is recorded as Transaction T1. The blockchain network ensures transparency by disseminating T1's details to all nodes, enabling every user to view the transaction. Node C subsequently incorporates T1, along with other recent transactions, into the blocks linked to Block A within the blockchain system. The interconnected nature of nodes within a block mitigates data loss in the event of a computer failure. Users can be assured that their information remains accessible through other computers in the network, thus eliminating the risk of a single point of failure [116]. Blockchain technology commonly employs hashing, which converts input strings of any length into fixed-length outputs utilizing the sha256 algorithm [117]. The hash of each block is derived from the previous block's hash, establishing a continuous chain in the system.

While blockchain technology currently faces certain technical limitations, including capacity, latency, and query capabilities, these challenges are likely temporary and may be resolved through future advancements [118]. The blockchain system comprises two code layers: the fabric layer and the application layer, as depicted in Figure 16.

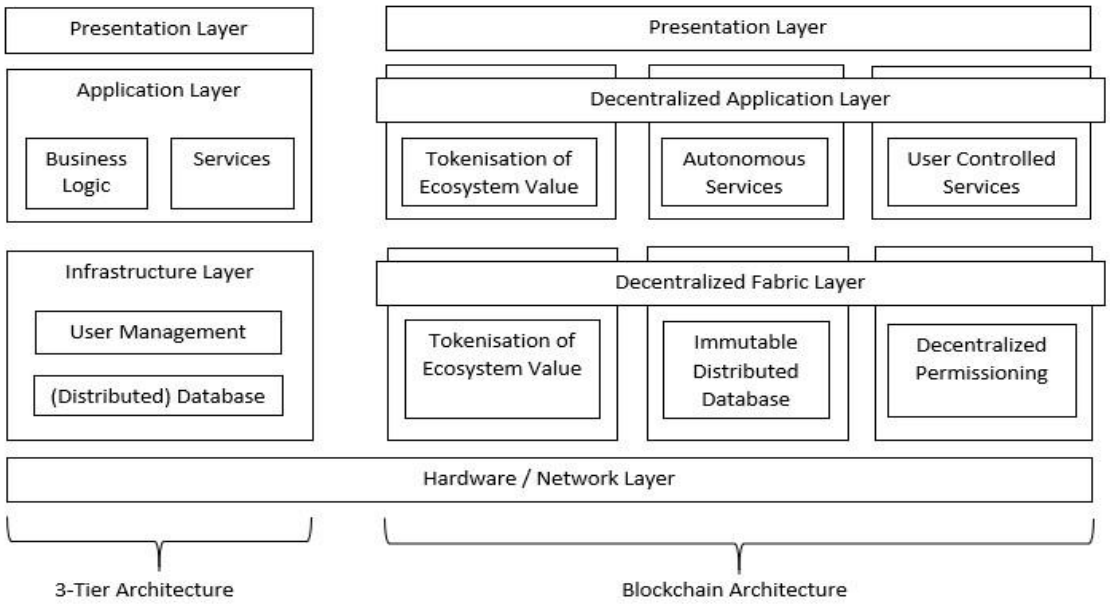


Figure 16: Layers of the blockchain network.

Figure 16 illustrates that the initial layer, designated as the fabric layer, encompasses the communication layer, public key infrastructure, and data structures essential for blockchain development and support. This layer additionally facilitates the execution of smart contract codes. The second layer, termed the application layer, contains the code that governs the application services' logic, ensuring proper system functionality. This code integrates users into the system, subjecting programmers to system control. Upon the application layer becoming publicly accessible, fabric layer developers relinquish control over application layer events, resulting in a decentralized blockchain network.

The fabric layer incorporates an integrated module that enables various user types to possess distinct authorization levels. Distribution companies, transaction-executing users, and the grid are allocated specific permission ranges within the system. A super

client with comprehensive rights control oversight exists, facilitating user differentiation through the management module. This configuration promotes complete transparency among all users involved in transactions and smart contract codes of other blockchain system participants. Privacy concerns arise solely in instances where a group of authorized users can view and verify transactions and blocks. Distribution companies are granted specific permissions to monitor and track their distribution lines when users intend to utilize their channels for energy transactions among themselves and with the grid.

4.5 Mechanism of Smart Contract in a Blockchain-Based Technology

Smart contracts comprise programming code segments that transform the entire blockchain network into a functional system accessible to users. If a portion of the scripting language fails to execute, it results in the failure of the entire transaction, preventing the progression to the next state. To prevent system malfunction, execution time is limited by requiring payment, as an infinite program execution would impede the entire blockchain system. Consequently, smart contracts necessitate external mediation for self-execution to function for users. Each node, representing an individual user, possesses a unique address and specific energy storage characteristics within the blockchain network. The profit percentage for each seller correlates directly with the quantity of surplus energy they contribute to the network at any given time [119].

The majority of literature reviewed in this study focuses on blockchain technology utilizing a bidding system method. This creates an inequitable environment for multiple nodes competing for the same amount of energy from a particular solar PV

energy producer willing to trade. Sellers have the autonomy to adjust their demand as they deem appropriate, while buyers remain unaware of their competitors bidding for the same available energy through other energy trading platforms in the blockchain network. Only the highest bidder can secure access to the traded energy [119]. The smart contract employed for such bidding platforms adheres to the sequential steps outlined in Figure 17 [119]. Figure 17 illustrates that all nodes receive notification when each auction cycle is set to commence, enabling buyers to acquire information about the energy units available in the block. This notification follows the compilation of data from sellers, who provide information on their excess energy for sale. Subsequently, the system establishes a deadline for buyers to submit bids, awaits the conclusion of this period, evaluates the bids, and then declares the highest bidder as the winner. The buyer then transfers the agreed-upon fee to the seller for the energy unit. This entire process occurs without third-party involvement to prevent fraudulent activities within the blockchain system.

However, the bidding process may result in excessively high bid values, leading to intense competition among buyers. This scenario can arise following downtime from a disaster, which impacts the behavior of network nodes. Sellers might exploit buyers' vulnerabilities by offering energy at prices significantly above the standard rate. This situation disadvantages less affluent individuals who may be unable to outbid their more financially capable competitors. If these individuals fail to succeed in the bidding system, they are compelled to purchase energy from the standard grid at higher rates or forgo electricity. Consequently, the objective of providing affordable energy to all remains unfulfilled. This indicates that the bidding system tends to favor more affluent

participants, potentially leaving others without access to energy when generation is insufficient.

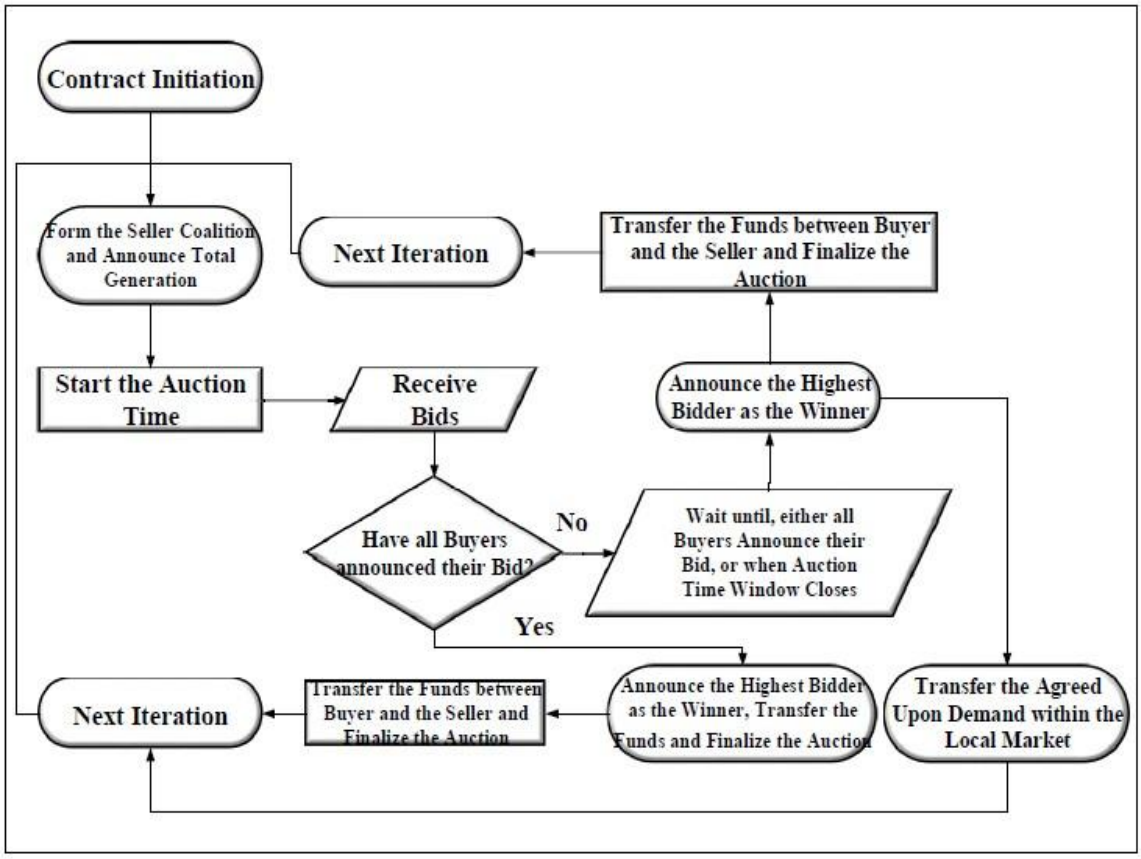


Figure 17: Smart contract algorithm.

In light of these issues, this thesis will focus on implementing a fixed rate for energy trades within the blockchain platform, rather than a bidding system. By establishing a standard rate to govern the energy-trading platform's operations, all individuals can access and purchase energy regardless of the season. Moreover, this approach prioritizes energy availability and reliability over competition among energy buyers and sellers. Thus, this study aims to develop a more equitable approach that accommodates both affluent and less privileged individuals.

4.6 Blockchain Contribution in Smart Grid

This section primarily focuses on examining the potential applications of blockchain technology in smart grid systems. We commence by providing a comprehensive overview of the anticipated future smart grid infrastructure. Subsequently, we analyze the key characteristics of blockchain and discuss how it can address security, privacy, and trust concerns in smart grids. This analysis aims to elucidate the compelling rationale for integrating blockchain technology into smart grid systems.

4.6.1 Moving towards Decentralized Smart Grid System

The introduction section elucidated the smart grid concept, which represents an innovative grid infrastructure utilizing digital computation and communication technologies to transform and enhance the traditional legacy grid into a more precise, efficient, and intelligent energy access and delivery network. These advancements have been driven by the pressing issue of climate change and the necessity for sustainable energy sources. The primary objective of these improvements is to restructure the energy landscape by incorporating and leveraging more renewable and distributed energy resources while reducing dependence on fossil fuel-based generation. In contrast to the conventional legacy grid, which supplies consumers through extensive transmission lines, the smart grid paradigm brings energy producers and consumers into closer proximity by implementing independent distributed renewable energy producers.

Recently, the energy Internet (EI) concept [120–127] has emerged as an enhanced iteration of the smart grid system. The EI is characterized by the application of Internet technologies to develop the next-generation smart grid by integrating information,

energy, and economics. It aims to provide significant opportunities for seamlessly incorporating various clean and renewable energy sources into the grid while fostering increased interactions among different power grid components to create a fully autonomous and intelligent energy network. The fundamental principle of the EI is its capacity to share both energy and information, analogous to data sharing on the Internet. The typical elements in this system include traditional generation units, micro-grids, distributed energy resources (DERs), community-generated energy networks, energy storage units, electric vehicles (EV), vehicle to grid (V2G), cyber-physical systems, prosumers, service providers, and energy markets.

While the smart grid and energy Internet aim to accommodate both distributed and centralized energy generation, a significant limitation of the current design is its centralized structure. In this configuration, energy generation, transmission, distribution networks, and markets are partially dependent on centralized or intermediary entities. These central entities monitor, collect, and analyze data, providing control signals to all components of the smart grid. Energy is typically transmitted over long distances to reach end-users through the distribution network. However, the increasing integration of renewable energy sources and the rapidly growing number of grid elements have raised concerns about the current smart grid design. These issues include limited scalability and expandability, substantial computational and communication burdens, vulnerability to availability attacks, and inadequacy in managing future power systems with numerous components.

Table 3: A Brief Comparison between the Smart and Future

Smart Grid	Future Decentralized Smart Grid
Transformed into utilizing more renewable energies and integrating with centralized grids	Moving towards building a decentralized system by integrating various distributed energy resources
Generally, focus on the integration of advanced sensing and control technologies into traditional grid	Basically, refer to real-time monitoring, auto-adjust controlling and optimization
Relied on intermediaries and centralized markets	Support a number of users to generate their own energy and share surpluses through peer-to-peer
Utilized advanced communication technologies	Dominated by energy Internet to realize Internet-like seamless energy and information sharing
Come up with bi-directional communications	Support advanced plug-and-play functionalities
Heavy computational and communicational costs	The costs are distributed among the entities over the network
Less option to expand the network	Have the option to expand fast and large number of connectivity
Would be affected by a single point of failure	Have resiliency against single point of failure
Integrated with only electric energy networks	Integrated with other energy networks as well
Dependent always on the regional system control	Allows the smooth access of massive distributed energy resources

Consequently, there is a trend towards decentralization in smart grid systems to introduce more dynamic, intelligent, and proactive features. The grid infrastructure itself is evolving towards a fully automated network with decentralized topologies, enhancing interactions among all smart grid components in a dynamic manner. The connectivity and accessibility offered by the Energy Internet (EI) further contribute to a more economical, efficient, and reliable operation of the smart grid system.

4.6.2 Motivations of Applying Blockchain in SG

Security, privacy, and trust are critical components of any system, including the future smart grid. The smart grid should incorporate various security measures [127–128], such as: preventing unauthorized access to information, implementing robust cryptographic methods, safeguarding against data modification, restricting access to authorized entities, ensuring rightful access, providing non-repudiation, developing resilient networks resistant to availability attacks, enhancing monitoring capabilities, employing advanced privacy protection techniques, and fostering trust, transparency, and democracy among all participants.

Nakamato's work in [128] addresses the challenge of establishing trust in distributed systems by introducing a novel consensus mechanism, which has made Bitcoin the most successful blockchain application to date. This success is attributed not only to the consensus mechanism but also to the utilization of cryptographically protected data structures, digital signatures, timestamps, and reward schemes. In blockchain applications, consensus mechanisms primarily focus on establishing trust, while various cryptographic techniques address fundamental security requirements such as

confidentiality, integrity, authentication, authorization, non-repudiation, and privacy. It is noteworthy that while the concepts of consensus mechanisms and blockchain originated in cryptocurrency applications, developing a blockchain-based decentralized system does not necessarily require the construction of a cryptocurrency.

Currently, the majority of solutions in the smart grid rely on centralized models, where components depend on centralized platforms or intermediaries for services such as billing, monitoring, bidding, and energy trading. Although these solutions are mature and functional, they face several challenges. As previously mentioned, the smart grid is facilitating the integration of numerous EVs, DERs, prosumers, and cyber-physical systems. Consequently, the grid topology is evolving from a centralized structure to a decentralized, fully automated network that allows for greater interaction among components. Furthermore, the smart grid market is transitioning from a centralized producer-governed network to a decentralized, interactive prosumer network, facilitated by the EI concept.

Blockchain technology can play a crucial role in enabling the transition to decentralized systems. This is because blockchain possesses distinctive features that make it particularly suitable for supporting this move away from centralization.

1. **Decentralization:** Blockchain networks typically operate through a system of distributed nodes utilizing consensus protocols. This structure facilitates peer-to-peer functionality without reliance on a central authority for management or authorization.

2. **Scalability:** The decentralized nature of blockchain networks enables their expansion as additional nodes join. This growth potential is inherent in the peer-to-peer structure of the network.
3. **Trustless but Secure:** Blockchain networks operate without the necessity for trust between parties yet maintain security. Nodes interact directly without intermediaries, and all transactions are secured using asymmetric cryptography. Unlike traditional systems, blockchain eliminates the requirement for implicit trust in specific entities.
4. **Immutability:** Blockchain technology employs cryptographic methods and maintains a globally synchronized ledger across nodes. This structure ensures that block contents remain unalterable unless a majority of nodes become compromised.
5. **Transparency and Auditability:** The inherent structure of blockchain networks provides high transparency. Network nodes can verify record authenticity and confirm that blocks remain unaltered. This transparency extends to auditability, as all records are accessible to every node on the network.
6. **Resiliency:** The blockchain architecture offers a robust and fault-tolerant network. Its decentralized structure, lacking a single point of failure, allows for efficient identification and recovery from faults or malicious activities. This resilience is further enhanced by each node storing the entire blockchain locally.

7. **Secure Script Deployment:** The immutability and decentralization of blockchain enable secure script deployment, also known as smart contracts. These contracts, stored on the blockchain, can execute automatically based on predefined criteria without human intervention, intermediaries, or central authorization.

These features, combined with advanced cryptographic security benefits, position blockchain as a promising alternative to conventional centralized systems. It offers improvements in security, privacy, and trust while facilitating the transition to a more decentralized and resilient system architecture.

Table 4: Summary of the Common Security, Privacy and Trust Objectives and Descriptions of How Blockchain can

Objective	How Blockchain can Achieve
Confidentiality	Usually, the records are not encrypted in public blockchain; Cryptographic techniques
Integrity	Cryptographically protected data structure by hash function, Markel tree, nonce (numbers used once) and time-stamps; Manipulated records can be detected and prevented decentralized access
Authentication	Signed records inside the blocks by users individual private keys so that it can be verified that only the valid user sent it
Auditability	Publicly available records/transactions in public blockchain
Authorization and Access Control	User-defined authorization and access control relied on smart contract; Attribute certificates
Privacy	Pseudo-anonymization by using hash functions to keep secret identities, Zero-knowledge proof
Trust	Consensus algorithms, Trust is not placed on central entities/intermediaries rather it is distributed among the entities in the network
Transparency	Complete transparency by maintaining an immutable distributed ledger including all records, transactions, events, and logs
Availability	Distributed architecture with allowing multiple entities to establish connections with others and to replicate full copy of the blockchain
Automaticity	Blockchain and smart contract offers automaticity where the entities can communicate and exchange values in peer-to-peer way by blockchain and execute actions automatically by smart contract

4.7 Examples of applying Blockchain to secure Smart grids

4.7.1 Safeguarding power grids from hacking and malicious activities

Blockchain technology provides a secure identification service through public/private encryption with key access. This feature necessitates that individuals attempting to enter a system verify their credentials for authentication, thereby allowing them to access and operate on the network. The power grid can be effectively protected if key access codes are maintained securely, rendering blockchain an essential technology for grid safety [129].

4.7.2 Serving as the foundation for secure and efficient smart city infrastructure

Recent years have witnessed significant urban migration, resulting in severe shortages of basic amenities in cities. This phenomenon is attributed to resources failing to keep pace with rapid population growth and urbanization. Governments have responded by proposing smart city solutions, incorporating innovative technologies and infrastructure to efficiently address the needs of expanding populations [130]. Blockchain's secure identification, authorization, and access control features enable it to record and store transactions immutably, facilitating seamless and cost-effective data exchanges between distributed entities. This technology provides the requisite security for a smart city to function, interconnecting devices and services throughout the urban environment [131].

4.7.3 Establishing a peer-to-peer energy trading environment

Energy trading has become a prominent topic among researchers and industry leaders with the emergence of microgrids and distributed generation. Blockchain plays a crucial role in this field by mitigating fraudulent activities. To ensure the integrity of energy market trading, a proof of origin certificate is issued. Implementing blockchain in energy market transactions reduces the time and effort required. As traditional energy sources rapidly deplete, governments worldwide are exploring alternative renewable energy sources such as solar and wind. These smaller energy-generating grids need to feed back into the main grid for consumer purchase [132]. Notably, electricity consumers are now also producers. A blockchain-based system offers an efficient peer-to-peer trading mechanism for localized housing complexes that generate energy. Data is automatically managed through a peer-to-peer topology after being stored in a public ledger, with all network copies reflecting any changes to the ledger. Blockchain technology involves transmitting data transactions as blocks through nodes in the Smart Grid network. These blocks are interconnected, with each device containing address information of the previous device [133].

4.7.4 Handling electricity certificates

The power grid generates electricity through various methods. Monitoring the production of clean energy and differentiating energy certificates proved challenging to manage. Traditional approaches to electricity certificate management were also complex. When renewable facilities produce electricity or meters output data, it is recorded in spreadsheets and forwarded to registry providers. After certificate generation, brokers

facilitate transactions between certificate buyers and sellers, with third-party verification. This process is costly and susceptible to accounting errors [130]. The main areas where extensive research and application of blockchain technology in smart grids occurred include:

4.7.5 Blockchain's role in Electric Vehicles

The integration of electric vehicles (EVs) with smart grids has been a significant focus in recent years. EV charging is the primary concern in smart grid connectivity. Unplanned charging of EVs can severely strain the power grid. Various solutions, including blockchain technology, have been proposed to address this issue. Liu et al. and Su et al. suggested an EV integration scheme based on blockchain, which resulted in reduced power fluctuations and charging costs. Researchers recommended incorporating blockchain to enable EVs to locate nearby charging stations that compete for charging opportunities. Utilizing blockchain in EV charging ensures optimal location and pricing for users while maintaining system security and privacy.

4.7.6 Blockchain in Cyber-Physical Systems

Smart grid implementation introduced vulnerabilities, making various components of the cyber-physical smart grid susceptible to manipulation or attacks. Cyber-physical attacks manifest in different forms and impacts, such as 1) time synchronization attacks 2) GPS spoofing attacks and 3) Denial-of-Service (DOS) attacks. A critical cyber-physical system attack is the False Data Injection (FDI) attack, where attackers manipulate or inject false data into measurements or control signals to alter power grid dynamics. These attacks pose significant risks to grid operations due to their

detection challenges. Literature classifies FDI attack countermeasures into protection-based and detection-based schemes. Protection-based schemes aim to safeguard power grid measurements from manipulation by increasing measurement redundancy. However, these schemes have limitations in effectiveness across varying grid operating conditions and require extensive measurement redundancy. Detection-based schemes employ the Bayesian framework to identify FDI attacks that appear as anomalies among measurements [134].

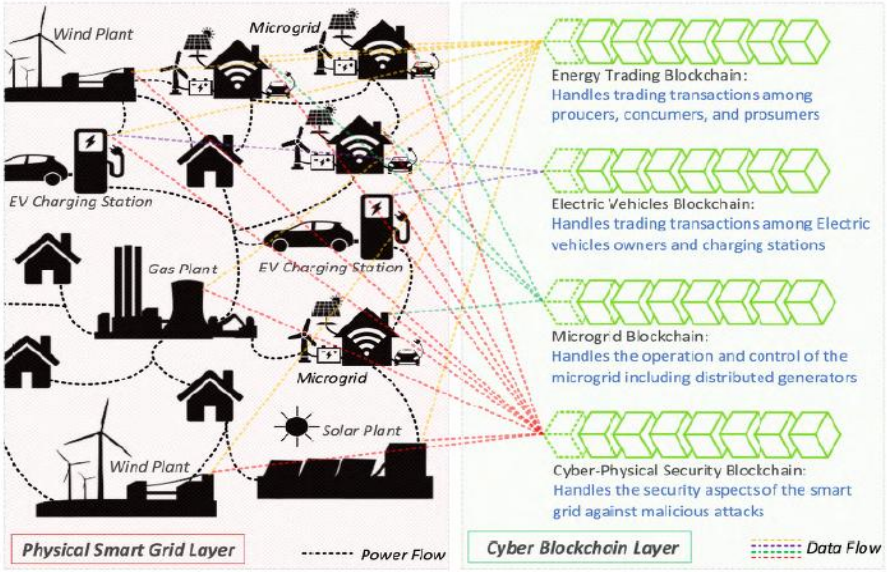


Figure 18: Blockchain as a new cyber layer of smart grids.

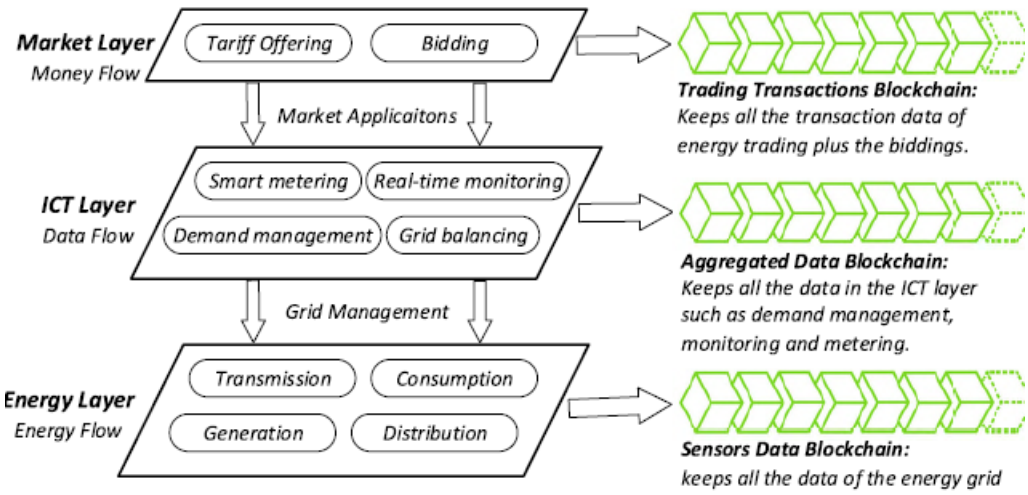


Figure 19: Blockchain applications framework in smart grid security and data protection.

4.8 Constrains and Shortcomings

While blockchains possess remarkable features, several limitations must be taken into account:

1. **Increased operational costs:** In accordance with the principles of supply and demand, nodes require greater compensation for executing transactions in a business environment.
2. **Reduced ledger size:** This may compromise the blockchain's security and immutability, as well as the integrity of all stored data.
3. **Extended transaction processing times:** Even in the absence of intermediaries, transaction processing times may exceed those of conventional methods.
4. **Network speed and transaction fees:** Despite initial assertions of being "almost free," blockchain technology now incurs substantial transaction costs.

Furthermore, its computational power and response time are insufficient to meet the requirements for high-frequency transactions and smart grid management.

5. **Potential for human error:** Although blockchain is a highly secure technology, the risk of errors persists when human involvement is present.
6. **Inefficiency:** To maintain consensus across the blockchain, each node must verify transactions. This process is inefficient as every node duplicates efforts to reach the agreed-upon consensus.

4.9 System Model

The proposed design comprises four distinct layers: the data input layer, the blockchain layer for data collection, verification, and storage, the communication layer, and the receiving layer, which encompasses the control center, billing center, and common receivers. The Public Key Infrastructure (PKI) extends across all four layers, as depicted in Figure 20. Within the blockchain layer, various information groups are represented by colored circles.

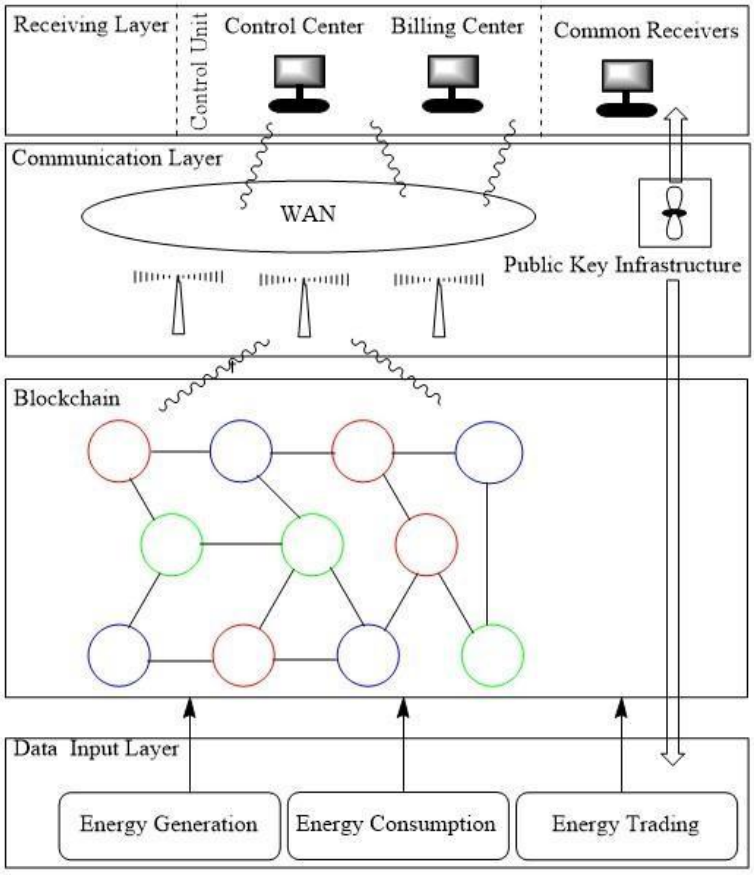


Figure 20: System Model

1. **Input data layer:** This layer encompasses all data sources, including smart meters, phasor measurement units (PMUs), and user-operated computers for entering energy purchase details. It serves as the origin point for all new transactions. Each transaction comprises an encrypted core message, group signature, encrypted sender's public key, and information type. Upon creation, transactions are disseminated across the entire network.
2. **Blockchain layer:** Transaction auditing, validation, and blockchain storage occur in this layer. Once a block is deemed valid, it is broadcast to the network for processing by subscribers and receivers.

3. **Communication layer:** This layer facilitates the transmission of all requisite information throughout the network.
4. **Reception layer:** This layer is divided into two segments: general customers (e.g., users receiving trading information) and management departments (e.g., control and billing centers). The control center oversees group registration and power distribution.
5. **Public Key Infrastructure (PKI):** PKI generates public-private key pairs for all participants, including each information group. Every group receives a group message and two sets of public-private keys: one for publishers (PUgp-PRgp) and another for subscribers (PUgs-PRgs).

4.9.1 System Initialization

Key Generation and Group Membership:

1. Every participant in the system needs to obtain a set of public-private keys. For those receiving, we utilize PUr-PRr.
2. Publishers will be provided with the control center's public key (PUc), the group message, the private key of the group publisher (PRgp), the public key of the receiver (PUr), and the public key of the subscriber (PUgs).
3. Receivers will be given the group message, the public key of the group publisher (PUgp), and the private key of the group subscriber (PRgs).

4.10 System Smart Contract

4.10.1 Transaction Creation

1- **Transaction creation:** The sender's account is encrypted by the control center's public key. The core data, time stamp, and energy consumption or energy ordering information are encrypted. If this transaction is for an individual receiver, this transaction will be encrypted by the receiver's public key first, then encrypted by the subscriber's public key. If this transaction is for group subscribers, it will be only encrypted by the group subscriber's public key. The transaction's signature will be created by using the group message and the publisher's private key. The transaction ID will be created by hashing the sender's account, core data, signature, and group number.

2- **Sub Functions:** We use Golang to implement consumer transaction forming and sending. Our implementation includes the following functions: create public-private key, create signature, verify signature, read consumer information, encrypt message, decrypt message, broadcast transaction, receive information, and append message.

3- **Transaction components:** A transaction includes information group number, transaction hash, encrypted core information, encrypted sender's account, and transaction signature.

4.10.2 Consensus Contract

The consensus nodes constantly check on transactions. When they receive a transaction, they check the transaction's group and verify the signature. If the group is

correct and the signature is valid, this transaction will be saved locally. Otherwise, the transaction will be discarded. If it is consensus time, the nodes. start to elect a leader and broadcast their proposals. Each node calculates its votes. If it receives the most votes, it will know it is the leader and it will pack its local transactions and broadcast it. When the non-leader nodes receive the block, they start to compare the block's transactions with their local transactions one by one. If any transaction's group, signature, or the data fails during the comparison, the consensus will fail, and consensus procedure will be ended. If all the transactions in the block are the same as the local transactions, the consensus is passed. Each node broadcasts its consensus result and waits for other's results. If a node received two thirds passing notifications from the members, it will permanently save the block to its blockchain and delete its local transactions. When the leader receives two thirds passing notification, it will save the block to its blockchain and broadcast the final block to the subscribers/receivers.

4.10.3 Receive Contract

When a subscriber receives the final block sent by the group leader, it will go through the block's transactions one by one. If the subscriber finds that a transaction belongs to the right group, the signature is valid, and it decrypts the data with the group receiver's private key correctly, it will process this transaction according to its groups, such as energy consumption or energy order. If the first data decryption failed, the specific receiver's private key will be used to decrypt this data. If the second decryption is successful, this transaction will be processed accordingly. If both decryptions failed,

this transaction will be discarded. If the subscriber is the controller, it can decrypt the transaction with sender's public key also and will know who sends this transaction.

4.11 System Analysis

4.11.1 Security Analysis

Confidentiality, integrity, and availability constitute the three fundamental security requirements. The system design incorporates encryption of the user's public key and essential information, permitting access only to authorized users possessing the appropriate private keys. For instance, nodes within an information group can authenticate a transaction's origin and compare core data without revealing its contents. Subscribers or recipients can decrypt the publisher's core data utilizing their group private key and/or individual private key. The control center exclusively possesses the capability to decrypt a user's public key, which functions as the publisher's identity. This approach preserves the publisher's anonymity while ensuring data confidentiality and integrity. The blockchain environment incorporates multiple nodes within each information group, mitigating the risk of single point failure and thereby ensuring resource availability. The subsequent section examines common security attack scenarios:

1. **Denial of Services (DoS) Attack:** The system architecture stores all transactions prior to processing them through information group nodes at predetermined intervals. The rate of service requests is constrained by the processing time interval [135], and the majority of information transmitted in the energy network adheres to a set frequency. Any anomalous transaction frequency triggers a system alert.

2. **Single Data Point Failure:** Network design divides nodes into distinct information groups. Each group comprises a minimum of three nodes, providing redundancy to mitigate single point failure.
3. **Content Poisoning Attack:** During the consensus process, alterations to a node's information are detectable by other nodes.
4. **Data manipulation in Data Input Layer:** Smart contracts automatically generate the majority of transactions, such as energy consumption and availability, eliminating the necessity for human intervention. Smart meters and PMUs are secured both physically and digitally, rendering it challenging to alter core data or create fraudulent transactions. While the creation of a fraudulent energy trading transaction is feasible, users would promptly identify it through control center confirmations or billing information.
5. **Forged transaction:** To fabricate a transaction, an attacker would require access to the control center's public key, the group subscriber's public key, the receiver's public key, and the group message. The probability of obtaining all these elements is exceedingly low unless they are stored together and compromised simultaneously.
6. **Null transaction block:** To prevent an adversary from transmitting blocks when no transactions exist in a time slot for certain information groups, the selected master will transmit a null transaction block to report its group's status if no transactions require processing. The

system is alerted if multiple nodes broadcast a block for the same information group within the same time frame.

4.11.2 Privacy

1. **Privacy of identity:** The control center's public key encrypts all senders' public keys. Only the control center possesses the capability to reveal a user's identity. This methodology ensures the protection of the publisher's confidentiality and sources of information.
2. **Privacy of data:** The publisher's information undergoes dual encryption: initially utilizing the receiver's public key for individual transactions, followed by encryption with the group's public key. Only intended recipients or subscribers possess the ability to decrypt the data using the appropriate private keys.
3. **Privacy of information origin:** Each transaction's signature is generated through the utilization of the group message and the publisher's private key. Consensus nodes, receivers, and subscribers can verify a transaction's validity using the identical group message and the group publisher's public key. All publishers within a group employ identical group messages and publisher private keys. Through the combination of transactions, group messages, and the publisher's private key, the transaction's source remains concealed from potential threats.

4.11.3 Scalability Analysis

The consensus process in each blockchain necessitates time to ensure all participating nodes receive and respond to messages from other nodes. This adaptation adversely affects network throughput. Our system, however, categorizes blockchain transactions into distinct groups, enabling these separate information sets to achieve consensus concurrently. Consequently, a greater number of transactions can be processed within any given time frame compared to existing blockchain systems. Furthermore, since fewer nodes are involved in each group's consensus, the time required for consensus within each group is reduced, further enhancing network throughput.

4.11.4 Reduced Storage Redundancy

Consider a network with n nodes. In a scenario where the blockchain information is not categorized or segmented, forming a single information group, all n nodes will store identical transactions, resulting in a storage redundancy of n. However, if the blockchain's data is divided into k distinct groups, the redundancy decreases to n/k.

4.11.5 Enhanced Search Efficiency

By storing distinct information in separate blockchains according to their type, the system can perform more efficient searches for specific transactions. This is because it only needs to examine the relevant blockchain, resulting in faster query times.

4.12 Conclusion

The proposed design incorporates information-centric blockchain technology to enhance security in smart grids. The conducted implementation has demonstrated the

feasibility of the approach, which effectively conceals the sender's identity, obscures transaction origins, and ensures data confidentiality. However, the current implementation relies on a simplified model with limited data. To fully validate the design, a more comprehensive implementation and rigorous testing process are required.

CHAPTER FIVE

THE ROLE OF EXTENDED KALMAN FILTER (EKF) IN MANAGING UNCERTINTIES IN SMART GRIDS

This chapter focuses on developing the Extended Kalman filter (EKF) technique for nonlinear power system models. To achieve reliable and effective uncertainty detection, it is essential to consider the impact of load variations and the fluctuations in system states before and after an attack. The method establishes the limits for state variable output interval estimates, necessitating precise quantification.

5.1. Extended Kalman Filter

The Kalman filter, primarily designed for linear systems, encounters limitations in real-world power systems, which are predominantly non-linear. Developed by Rudolf E. Kalman, this algorithm is a derivative that facilitates the estimation of states in dynamic, linear systems utilizing time series data. For power system state estimation, the Extended Kalman Filter (EKF) functions as an adaptation of the original Kalman filter. In the EKF approach, the model undergoes linearization at each time step, centered around the current operational mean and covariance.

The Extended Kalman Filter (EKF) operates through two primary stages: prediction and update.

1. **Prediction Phase:** During this phase, the EKF utilizes a nonlinear system model to forecast the grid's future state based on its current condition and any control

inputs. This projection is achieved by propagating the state through the nonlinear model, which considers factors such as generation plans, consumption patterns, and grid component performance. The projected state represents the most accurate estimate of the system's behavior prior to the incorporation of new measurements.

2. **Update Phase:** In this phase, the EKF compares the projected state with actual data acquired from sensors distributed across the grid. These measurements may encompass information on voltage levels, current flows, power outputs, and phase angles. The discrepancy between the projected and measured values, termed the residual or innovation, is utilized to refine the state estimate, thereby enhancing its accuracy. Additionally, the EKF generates an error covariance matrix that quantifies the uncertainty associated with the updated state estimate.

5.2 Dynamic process

Consider the following nonlinear system, described by the difference equation and the observation model with additive noise:

$$\mathrm{x}_k = \mathrm{f}(\mathrm{x}_{k-1}) + \mathrm{w}_{k-1} \quad (1)$$

$$\mathrm{z}_k = \mathrm{h}(\mathrm{x}_k) + \mathrm{v}_k \quad (2)$$

The initial state x_0 is a random vector with known mean:

$$\mu_0 = E[\mathrm{x}_0] \quad (3)$$

and covariance

$$\mathrm{P}_0 = E[(\mathrm{x}_0 - \mu_0)(\mathrm{x}_0 - \mu_0)^T] \quad (4)$$

For the subsequent discussion, we consider that the random vector represents model uncertainties, while signifies measurement noise. These two elements are characterized as temporally independent (white noise) and zero-mean random sequences with known covariances. Additionally, both and are uncorrelated with the initial state x_0.

$$E[\mathrm{w}_k] = 0 \; E[\mathrm{w}_k \mathrm{w}_k^T] = \mathrm{Q}_k \; E\left[\mathrm{w}_k \mathrm{w}_j^T\right] = 0 \text{ for } k \neq j \; E[\mathrm{w}_k \mathrm{x}_0^T] = 0 \text{ for all } k \quad (5)$$

$$E[\mathrm{v}_k] = 0 \; E[\mathrm{v}_k \mathrm{v}_k^T] = \mathrm{R}_k \; E\left[\mathrm{v}_k \mathrm{v}_j^T\right] = 0 \text{ for } k \neq j \; E[\mathrm{v}_k \mathrm{x}_0^T] = 0 \text{ for all } k \quad (6)$$

Also the two random vectors w_k and v_k are uncorrelated:

$$E\left[\mathrm{w}_k \mathrm{v}_j^T\right] = 0 \text{ for all } k \text{ and } j \quad (7)$$

Vectorial functions $\mathrm{f}(\cdot)$ and $\mathrm{h}(\cdot)$ are assumed to be C^1 functions (the function and its first derivative are continuous on the given domain).

Dimension and description of variables:

x_k	$n \times 1$	− State vector
w_k	$n \times 1$	− Process noise vector
z_k	$m \times 1$	− Observation vector
v_k	$m \times 1$	- Measurement noise vector
$\mathrm{f}(\cdot)$	$n \times 1$	- Process nonlinear vector function
$\mathrm{h}(\cdot)$	$m \times 1$	- Observation nonlinear vector function
Q_k	$n \times n$	- Process noise covariance matrix
R_k	$m \times m$	- Measurement noise covariance matrix

5.3 EKF derivation

Assuming the nonlinearities in the dynamic and the observation model are smooth, we can expand $\mathrm{f}(\mathrm{x}_k)$ and $\mathrm{h}(\mathrm{x}_k)$ in Taylor Series and approximate this way the forecast and the next estimate of x_k.

5.3.1 Model Forecast Step

Initially, since the only available information is the mean, μ_0, and the covariance, P_0, of the initial state then the initial optimal estimate x_0^a and error covariance is:

$$\mathrm{x}_0^a = \mu_0 = E[\mathrm{x}_0] \quad (8)$$

$$\mathrm{P}_0 = E[(\mathrm{x}_0 - \mathrm{x}_0^a)(\mathrm{x}_0 - \mathrm{x}_0^a)^T] \quad (9)$$

Assume now that we have an optimal estimate

$$\mathrm{x}_{k-1}^a \equiv E[\mathrm{x}_{k-1} \mid \mathrm{Z}_{k-1}] \quad (10)$$

with P_{k-1} covariance at time $k-1$. The predictable part of x_k is given by:

$$\begin{aligned} \mathrm{x}_k^f &\equiv E[\mathrm{x}_k \mid \mathrm{Z}_{k-1}] \\ &= E[\mathrm{f}(\mathrm{x}_{k-1}) + \mathrm{w}_{k-1} \mid \mathrm{Z}_{k-1}] \\ &= E[\mathrm{f}(\mathrm{x}_{k-1}) \mid \mathrm{Z}_{k-1}] \end{aligned} \quad (11)$$

Expanding $\mathrm{f}(\cdot)$ in Taylor Series about x_{k-1}^a we get:

$$\mathrm{f}(\mathrm{x}_{k-1}) \equiv \mathrm{f}(\mathrm{x}_{k-1}^a) + \mathrm{J}_\mathrm{f}(\mathrm{x}_{k-1}^a)(\mathrm{x}_{k-1} - \mathrm{x}_{k-1}^a) + \text{ H.O.T.} \quad (12)$$

where J_f is the Jacobian of $\mathrm{f}(\cdot)$ and the higher order terms (H.O.T.) are considered negligible. Hence, the Extended Kalman Filter is also called the First-Order Filter. The Jacobian is defined as:

$$\mathrm{J}_\mathrm{f} \equiv \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} & \cdots & \frac{\partial f_n}{\partial x_n} \end{bmatrix} \quad (13)$$

where $\mathrm{f(x)} = (f_1(\mathrm{x}), f_2(\mathrm{x}), \dots, f_n(\mathrm{x}))^T$

and $\mathrm{x} = (x_1, x_2, \dots, x_n)^T$. The eq.12 becomes:

$$\mathrm{f}(\mathrm{x}_{k-1}) \approx \mathrm{f}(\mathrm{x}^a_{k-1}) + \mathrm{J_f}(\mathrm{x}^a_{k-1})\mathrm{e}_{k-1} \qquad 14$$

where $\mathrm{e}_{k-1} \equiv \mathrm{x}_{k-1} - \mathrm{x}^a_{k-1}$.

The expected value of $\mathrm{f}(\mathrm{x}_{k-1})$ conditioned by Z_{k-1} :

$$E[\mathrm{f}(\mathrm{x}_{k-1}) \mid \mathrm{Z}_{k-1}] \approx \mathrm{f}(\mathrm{x}^a_{k-1}) + \mathrm{J_f}(\mathrm{x}^a_{k-1})E[\mathrm{e}_{k-1} \mid \mathrm{Z}_{k-1}] \qquad 15$$

where $E[\mathrm{e}_{k-1} \mid \mathrm{Z}_{k-1}] = 0$.

Thus, the forecast value of x_k is:

$$\mathrm{x}^f_k \approx \mathrm{f}(\mathrm{x}^a_{k-1}) \qquad 16$$

Substituting (14) in the forecast error equation results:

$$\begin{aligned} \mathrm{e}^f_k &\equiv \mathrm{x}_k - \mathrm{x}^f_k \\ &= \mathrm{f}(\mathrm{x}_{k-1}) + \mathrm{w}_{k-1} - \mathrm{f}(\mathrm{x}^a_{k-1}) \\ &\approx \mathrm{J_f}(\mathrm{x}^a_{k-1})\mathrm{e}_{k-1} + \mathrm{w}_{k-1} \end{aligned} \qquad 17$$

The forecast error covariance is given by:

$$\begin{aligned} \mathrm{P}^f_k &\equiv E\left[\mathrm{e}^f_k(\mathrm{e}^f_k)^T\right] \\ &= \mathrm{J_f}(\mathrm{x}^a_{k-1})E[\mathrm{e}_{k-1}\mathrm{e}^T_{k-1}]\mathrm{J}^T_{\mathrm{f}}(\mathrm{x}^a_{k-1}) + E[\mathrm{w}_{k-1}\mathrm{w}^T_{k-1}] \\ &= \mathrm{J_f}(\mathrm{x}^a_{k-1})\mathrm{P}_{k-1}\mathrm{J}^T_{\mathrm{f}}(\mathrm{x}^a_{k-1}) + \mathrm{Q}_{k-1} \end{aligned} \qquad 18$$

5.3.2 Data Assimilation Step

At time k we have two pieces of information: the forecast value x_k^f with the covariance P_k^f and the measurement z_k with the covariance R_k. Our goal is to approximate the best unbiased estimate, in the least squares sense, x_k^a of x_k. One way is to assume the estimate is a linear combination of both x_k^f and z_k[136]. Let:

$$\mathrm{x}_k^a = \mathrm{a} + \mathrm{K}_k \mathrm{z}_k \tag{19}$$

From the unbiasedness condition:

$$\begin{aligned} 0 &= E[\mathrm{x}_k - \mathrm{x}_k^a \mid \mathrm{Z}_k] && (20)\\ &= E\left[\left(\mathrm{x}_k^f + \mathrm{e}_k^f\right) - (\mathrm{a} + \mathrm{K}_k \mathrm{h}(\mathrm{x}_k) + \mathrm{K}_k \mathrm{v}_k) \mid \mathrm{Z}_k\right] \\ &= \mathrm{x}_k^f - \mathrm{a} - \mathrm{K}_k E[\mathrm{h}(\mathrm{x}_k) \mid \mathrm{Z}_k] \\ \mathrm{a} &= \mathrm{x}_k^f - \mathrm{K}_k E[\mathrm{h}(\mathrm{x}_k) \mid \mathrm{Z}_k] && (21) \end{aligned}$$

Substitute (21) in (19):

$$\mathrm{x}_k^a = \mathrm{x}_k^f + \mathrm{K}_k(\mathrm{z}_k - E[\mathrm{h}(\mathrm{x}_k) \mid \mathrm{Z}_k]) \tag{22}$$

Following the same steps as in model forecast step, expanding $\mathrm{h}(\cdot)$ in Taylor Series about x_k^f we have:

$$\mathrm{h}(\mathrm{x}_k) \equiv \mathrm{h}\left(\mathrm{x}_k^f\right) + \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right)\left(\mathrm{x}_k - \mathrm{x}_k^f\right) + \text{ H.O.T.} \tag{23}$$

where J_h is the Jacobian of $\mathrm{h}(\cdot)$ and the higher order terms (H.O.T.) are considered negligible. The Jacobian of $\mathrm{h}(\cdot)$ is defined as:

$$\mathrm{J_h} \equiv \begin{bmatrix} \frac{\partial h_1}{\partial x_1} & \frac{\partial h_1}{\partial x_2} & \cdots & \frac{\partial h_1}{\partial x_n} \\ \vdots & & \ddots & \vdots \\ \frac{\partial h_m}{\partial x_1} & \frac{\partial h_m}{\partial x_2} & \cdots & \frac{\partial h_m}{\partial x_n} \end{bmatrix} \quad (24)$$

where $\mathrm{h(x)} = (h_1(\mathrm{x}), h_2(\mathrm{x}), \ldots, h_m(\mathrm{x}))^T$ and $\mathrm{x} = (x_1, x_2, \ldots, x_n)^T$. Taken the expectation on both sides of (23) conditioned by Z_k :

$$E[\mathrm{h(x}_k) \mid \mathrm{Z}_k] \approx \mathrm{h}\left(\mathrm{x}_k^f\right) + \mathrm{J_h}\left(\mathrm{x}_k^f\right) E\left[\mathrm{e}_k^f \mid \mathrm{Z}_k\right] \quad (25)$$

where $E\left[\mathrm{e}_k^f \mid \mathrm{Z}_k\right] = 0$.

Substitute in (22), the state estimate is:

$$\mathrm{x}_k^a \approx \mathrm{x}_k^f + \mathrm{K}_k\left(\mathrm{z}_k - \mathrm{h}\left(\mathrm{x}_k^f\right)\right) \quad (26)$$

The error in the estimate x_k^a is:

$$\begin{aligned} \mathrm{e}_k &\equiv \mathrm{x}_k - \mathrm{x}_k^a \\ &= \mathrm{f(x}_{k-1}) + \mathrm{w}_{k-1} - \mathrm{x}_k^f - \mathrm{K}_k\left(\mathrm{z}_k - \mathrm{h}\left(\mathrm{x}_k^f\right)\right) \\ &\approx \mathrm{f(x}_{k-1}) - \mathrm{f}(\mathrm{x}_{k-1}^a) + \mathrm{w}_{k-1} - \mathrm{K}_k\left(\mathrm{h(x}_k) - \mathrm{h}\left(\mathrm{x}_k^f\right) + \mathrm{v}_k\right) \\ &\approx \mathrm{J_f}(\mathrm{x}_{k-1}^a)\mathrm{e}_{k-1} + \mathrm{w}_{k-1} - \mathrm{K}_k\left(\mathrm{J_h}\left(\mathrm{x}_k^f\right)\mathrm{e}_k^f + \mathrm{v}_k\right) \\ &\approx \mathrm{J_f}(\mathrm{x}_{k-1}^a)\mathrm{e}_{k-1} + \mathrm{w}_{k-1} - \mathrm{K}_k\mathrm{J_h}\left(\mathrm{x}_k^f\right)(\mathrm{J_f}(\mathrm{x}_{k-1}^a)\mathrm{e}_{k-1} + \mathrm{w}_{k-1}) - \mathrm{K}_k\mathrm{v}_k \\ &\approx \left(\mathrm{I} - \mathrm{K}_k\mathrm{J_h}\left(\mathrm{x}_k^f\right)\right)\mathrm{J_f}(\mathrm{x}_{k-1}^a)\mathrm{e}_{k-1} + \left(\mathrm{I} - \mathrm{K}_k\mathrm{J_h}\left(\mathrm{x}_k^f\right)\right)\mathrm{w}_{k-1} - \mathrm{K}_k\mathrm{v}_k \end{aligned} \quad (27)$$

Then, the posterior covariance of the new estimate is:

$$
\begin{aligned}
&\mathrm{P}_k \equiv E[\mathrm{e}_k \mathrm{e}_k^T] \\
&= \left(\mathrm{I} - \mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right)\right) \mathrm{J}_\mathrm{f}(\mathrm{x}_{k-1}^a) \mathrm{P}_{k-1} \mathrm{J}_\mathrm{f}^T(\mathrm{x}_{k-1}^a) \left(\mathrm{I} - \mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right)\right)^T \\
&+ \left(\mathrm{I} - \mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right)\right) \mathrm{Q}_{k-1} \left(\mathrm{I} - \mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right)\right)^T + \mathrm{K}_k \mathrm{R}_k \mathrm{K}_k^T \\
&= \left(\mathrm{I} - \mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right)\right) \mathrm{P}_k^f \left(\mathrm{I} - \mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right)\right)^T + \mathrm{K}_k \mathrm{R}_k \mathrm{K}_k^T \\
&= \mathrm{P}_k^f - \mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right) \mathrm{P}_k^f - \mathrm{P}_k^f \mathrm{J}_\mathrm{h}^T\left(\mathrm{x}_k^f\right) \mathrm{K}_k^T + \mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right) \mathrm{P}_k^f \mathrm{J}_\mathrm{h}^T\left(\mathrm{x}_k^f\right) \mathrm{K}_k^T + \mathrm{K}_k \mathrm{R}_k \mathrm{K}_k^T
\end{aligned}
\tag{28}
$$

The posterior covariance formula holds for any K_k. Like in the standard Kalman Filter we find out K_k by minimizing $\mathrm{tr}(\mathrm{P}_k)$ w.r.t. K_k.

$$
\begin{aligned}
0 &= \frac{\partial \mathrm{tr}(\mathrm{P}_k)}{\partial \mathrm{K}_k} \\
&= -\left(\mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right) \mathrm{P}_k^f\right)^T - \mathrm{P}_k^f \mathrm{J}_\mathrm{h}^T\left(\mathrm{x}_k^f\right) + 2\mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right) \mathrm{P}_k^f \mathrm{J}_\mathrm{h}^T\left(\mathrm{x}_k^f\right) + 2\mathrm{K}_k \mathrm{R}_k
\end{aligned}
\tag{29}
$$

Hence the Kalman gain is:

$$
\mathrm{K}_k = \mathrm{P}_k^f \mathrm{J}_\mathrm{h}^T\left(\mathrm{x}_k^f\right)\left(\mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right) \mathrm{P}_k^f \mathrm{J}_\mathrm{h}^T\left(\mathrm{x}_k^f\right) + \mathrm{R}_k\right)^{-1} \tag{30}
$$

Substituting this back in (28) results:

$$
\begin{aligned}
\mathrm{P}_k &= \left(\mathrm{I} - \mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right)\right) \mathrm{P}_k^f - \left(\mathrm{I} - \mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right)\right) \mathrm{P}_k^f \mathrm{J}_\mathrm{h}^T\left(\mathrm{x}_k^f\right) \mathrm{K}_k^T + \mathrm{K}_k \mathrm{R}_k \mathrm{K}_k^T \\
&= \left(\mathrm{I} - \mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right)\right) \mathrm{P}_k^f - \left(\mathrm{P}_k^f \mathrm{J}_\mathrm{h}^T\left(\mathrm{x}_k^f\right) - \mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right) \mathrm{P}_k^f \mathrm{J}_\mathrm{h}^T\left(\mathrm{x}_k^f\right) - \mathrm{K}_k \mathrm{R}_k\right) \mathrm{K}_k^T \\
&= \left(\mathrm{I} - \mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right)\right) \mathrm{P}_k^f - \left[\mathrm{P}_k^f \mathrm{J}_\mathrm{h}^T\left(\mathrm{x}_k^f\right) - \mathrm{K}_k\left(\mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right) \mathrm{P}_k^f \mathrm{J}_\mathrm{h}^T\left(\mathrm{x}_k^f\right) + \mathrm{R}_k\right)\right] \mathrm{K}_k^T \\
&= \left(\mathrm{I} - \mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right)\right) \mathrm{P}_k^f - \left[\mathrm{P}_k^f \mathrm{J}_\mathrm{h}^T\left(\mathrm{x}_k^f\right) - \mathrm{P}_k^f \mathrm{J}_\mathrm{h}^T\left(\mathrm{x}_k^f\right)\right] \mathrm{K}_k^T \\
&= \left(\mathrm{I} - \mathrm{K}_k \mathrm{J}_\mathrm{h}\left(\mathrm{x}_k^f\right)\right) \mathrm{P}_k^f
\end{aligned}
\tag{31}
$$

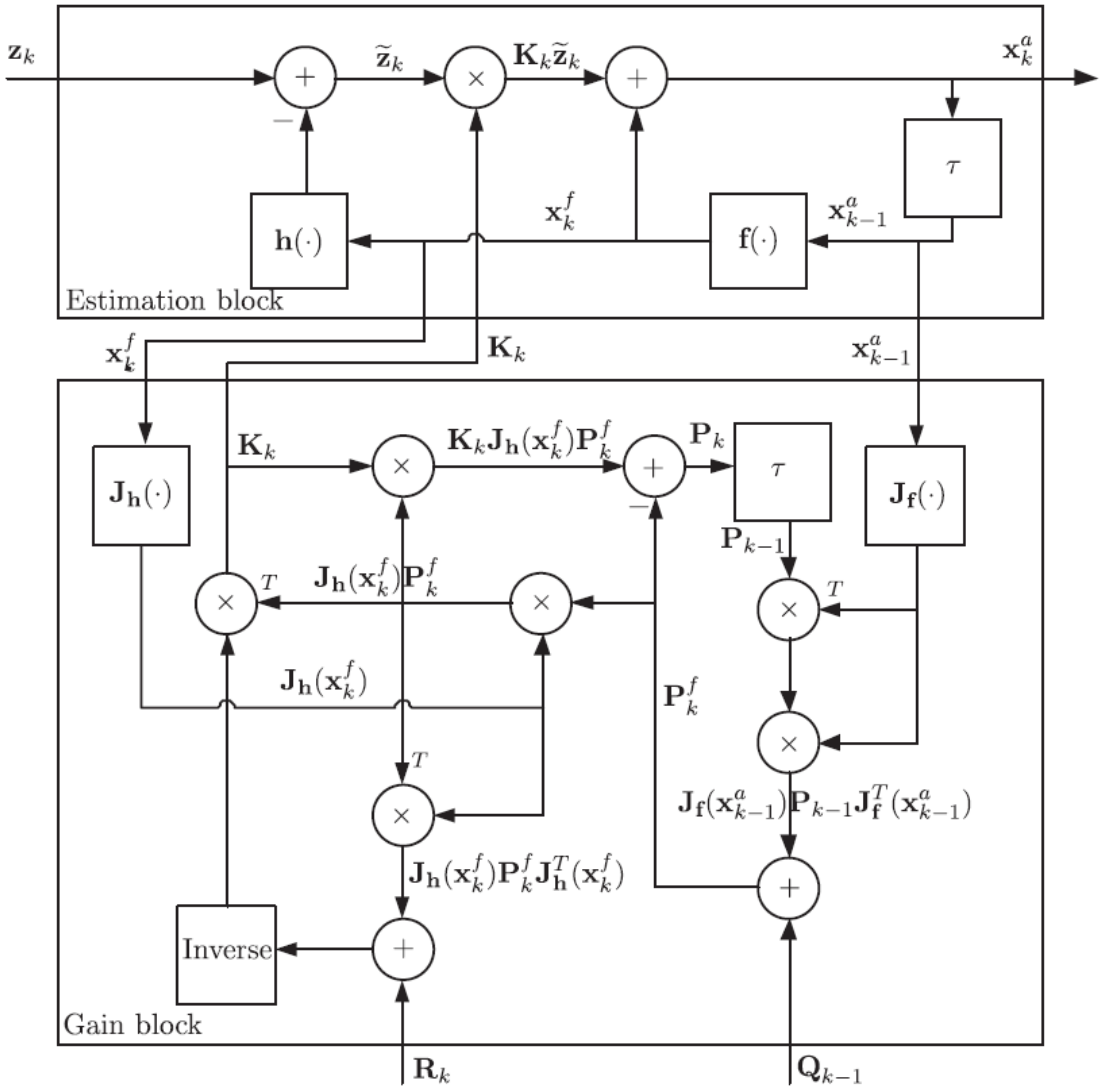


Figure 21: The block diagram for Extended Kalman Filter

5.4 EKF workflow

The Extended Kalman Filter (EKF) operates in a series of well-defined steps. Below is a breakdown of the EKF's key components and workflow:

5.4.1. Initialization

Initial State Estimate: The EKF begins with an initial estimate of the system's state, denoted as $\hat{x}_0$, and an initial error covariance matrix P_0. These values are either known from prior knowledge or set based on assumptions.

5.4.2. Prediction Step

This step forecasts the system's future state based on its current state and a model of its dynamics.

1. **State Prediction:** The system's next state is predicted using a nonlinear model $f(\cdot)$. The predicted state is given by:

$$\hat{x}_{k|k-1} = f(\hat{x}_{k-1}) \quad 32$$

Here, $\hat{x}_{k|k-1}$ is the predicted state at time step k based on the state at time step $k-1$.

2. **Error Covariance Prediction:** The error covariance matrix is predicted using the Jacobian of the system's model (denoted as F_k), which linearizes the system around the current estimate:

$$P_{k|k-1} = F_k P_{k-1|k-1} F_k^T + Q_k \quad 33$$

where Q_k represents the process noise covariance matrix.

5.4.3. Update Step

This step refines the predicted state based on new measurements from sensors or external sources.

1. **Sensor Measurements:** At time k, measurements z_k are obtained. These measurements are related to the system state by a nonlinear observation model $h(\cdot)$:

$$z_k = h(x_k) + v_k \tag{34}$$

where v_k is the measurement noise.

2. **Residual Calculation (Innovation):** The difference between the actual measurement and the predicted measurement, known as the residual (or innovation), is computed:

$$y_k = z_k - h(\hat{x}_{k|k-1}) \tag{35}$$

3. **Kalman Gain Calculation:** The Kalman gain K_k determines how much to adjust the predicted state based on the residual. It is computed as:

$$K_k = P_{k|k-1} H_k^T (H_k P_{k|k-1} H_k^T + R_k)^{-1} \tag{36}$$

where H_k is the Jacobian of the observation model and R_k is the measurement noise covariance matrix.

4. **State Update:** The predicted state is updated using the Kalman gain and the residual:

$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + K_k y_k \tag{37}$$

5.4.4. Covariance Update

The error covariance matrix is updated to reflect the uncertainty in the updated state estimate:

$$P_{k|k} = (I - K_k H_k) P_{k|k-1} \quad (38)$$

where I is the identity matrix.

5.4.5. Repeat

Steps 2 through 4 are repeated at each time step as new measurements are received. The EKF continuously refines its estimate of the system's state and uncertainty over time.

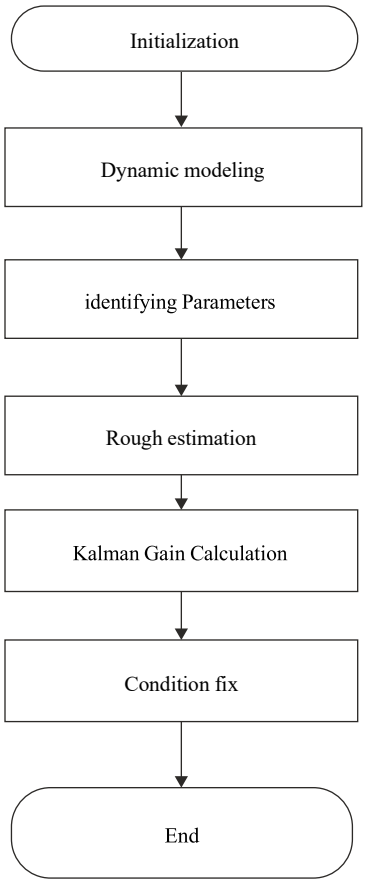


Figure 22: EKF organization chart.

5.5 Application of the EKF in Smart Grids

The Extended Kalman Filter (EKF) finds widespread use in smart grid systems, serving crucial functions in uncertainty management and grid efficiency enhancement. Several primary applications of the EKF in this context are explored in the following discussion:

5.5.1 Dynamic State Estimation (DSE)

The Extended Kalman Filter (EKF) plays a crucial role in smart grids, particularly in dynamic state estimation (DSE). This process involves real-time monitoring of essential

grid parameters, including voltage magnitudes, phase angles, and power flows. In contrast to conventional state estimation methods that rely on linear models and static grid snapshots, the EKF is capable of addressing the nonlinear and dynamic aspects of smart grid operations. By integrating real-time sensor information and considering the nonlinearities in power flow equations, the EKF provides more accurate and up-to-date estimates of the grid's condition. This enhanced accuracy enables grid operators to identify and address disturbances more effectively.

5.5.2 Short-Term Load Forecasting

Predicting electricity demand is essential for maintaining equilibrium between power generation and consumption in the electrical grid. However, the increasing variability in consumer usage patterns has rendered short-term demand forecasting more complex. The Extended Kalman Filter (EKF) can enhance demand prediction by incorporating real-time data from intelligent metering systems, meteorological projections, and historical usage trends into its state estimation calculations. By accounting for the variability of consumer behavior, the EKF produces more accurate demand forecasts, which are critical for optimizing grid management and resource allocation.

5.5.3 Renewable Energy Output Estimation

Grid operators encounter a significant challenge in managing supply-demand imbalances due to the stochastic nature of renewable energy sources. The Extended Kalman Filter (EKF) can be employed to forecast the current output of wind and solar

farms through the analysis of meteorological data and sensor measurements. This precise prediction of renewable energy production enables operators to more effectively manage the fluctuations associated with these sources and optimize their integration into the power grid.

5.5.4 Fault Detection and Diagnosis

Maintaining grid reliability is contingent upon the critical task of identifying and assessing malfunctions in grid components, including transformers, transmission lines, and inverters. The Extended Kalman Filter (EKF) can be employed for fault detection by systematically comparing the anticipated system state with actual sensor readings. Significant deviations from the expected behavior may indicate the presence of a malfunction. Prompt identification of faults enables operators to implement corrective measures before issues escalate, thereby minimizing downtime and reducing maintenance costs.

5.5.5 Grid Synchronization and Control

Synchronization between distributed energy resources (DERs) and the primary grid is essential for maintaining stability in microgrids and distributed generation systems. The Extended Kalman Filter (EKF) serves a critical function in this process by estimating the discrepancies in frequency and phase between DERs and the grid. This crucial information enables system operators to optimize control parameters, ensuring that DERs

remain synchronized with the grid. Such synchronization is imperative for preventing system destabilization resulting from fluctuations in frequency and voltage.

5.6 Uncertainties in Smart Grids

In smart grids, various crucial factors contribute to the presence of uncertainty, potentially impacting the grid's efficiency, reliability, and stability. These factors include:

5.6.1 Variability of Renewable Energy Sources

The variability of renewable energy sources, particularly wind and solar power, presents a significant challenge in contemporary electrical grids. These sustainable energy options are highly dependent on fluctuating environmental conditions, which are inherently difficult to predict with precision. Variations in cloud cover, temperature fluctuations, and changes in wind velocity can significantly affect the energy output of solar installations and wind farms. As a result, the integration of renewable energy into the power grid introduces considerable variability in electricity supply, complicating the critical task of maintaining equilibrium between power generation and consumption.

5.6.2 Demand-Side Fluctuations

The increasing prevalence of distributed energy resources (DERs) and intelligent appliances has resulted in more variable consumer demand patterns. The integration of technologies such as electric vehicles, residential solar installations, and energy storage units has introduced fluctuations in load profiles, challenging conventional load

forecasting methodologies. Furthermore, the extensive implementation of demand response initiatives, which enable utilities to modulate demand based on real-time grid conditions, further exacerbates the unpredictability of power consumption patterns.

5.6.3 Nonlinear Operational Dynamics

The contemporary advanced smart grid incorporates a diverse array of components that exhibit nonlinear and time-varying properties, including inverters, voltage regulators, and distributed generation systems. These nonlinear elements engender complex grid behaviors that present significant challenges in accurate simulation and prediction. For instance, power electronic devices, which are frequently utilized in renewable energy installations, manifest nonlinear characteristics that can exert unpredictable influences on power flow and voltage stability. To ensure the grid's reliable operation, it is imperative to precisely capture and regulate these nonlinear dynamics.

5.6.4 Measurement Noise and Data Integrity

The implementation of advanced sensing technologies, including Phasor Measurement Units (PMUs), smart meters, and voltage sensors, has enabled real-time monitoring of grid conditions. However, the data acquired by these instruments is frequently subject to noise, which can obscure the grid's actual state. Various factors, such as sensor inaccuracies, communication delays, or external interferences, may contribute to measurement noise. To ensure effective state estimation and decision-making in the grid, it is imperative to maintain the reliability and accuracy of sensor data.

5.7 Identifying the uncertainties by using Extended Kalman Filter

In a smart grid system, the process of recognizing uncertainties involves comprehending and quantifying the various sources of variability and unpredictability. This encompasses identifying potential causes of inconsistency and error, such as measurement inaccuracies, power and voltage fluctuations, modeling flaws, and the consequences of cyber-attacks and equipment malfunctions. The primary objective of this identification process is to enhance the smart grid's resilience and security by mitigating the effects of these uncertainties on power distribution and overall grid stability. By obtaining a comprehensive understanding and quantification of uncertainty sources, it becomes feasible to develop more accurate and robust system models, as well as design control and monitoring mechanisms that are more adept at detecting and addressing anomalies.

Typically, the process of identifying uncertainties in a smart grid system involves collecting data from sensors, conducting simulations and analyses, and evaluating the outcomes to determine the origins of variability and unpredictability within the system. The insights gained from this process can subsequently be utilized to develop more effective control and monitoring systems, ultimately improving the overall security and resilience of the smart grid infrastructure. The extended Kalman filter (EKF) functions as a state estimation methodology for identifying uncertainties within smart grid systems. The process of implementing the EKF for uncertainty identification typically encompasses the following steps:

1. **System modeling:** Develop a mathematical representation of the smart grid system, encompassing the interactions between various components and their temporal behaviors.
2. **EKF initialization:** Commence the process by establishing an initial estimate of the system's state, which will serve as the starting point for the EKF's iterative procedure.
3. **Information gathering:** Acquire real-time data from sensors and other monitoring devices within the smart grid system.
4. **State forecasting:** Employ the system's mathematical model to predict its future state based on the current state and system inputs.
5. **Prediction refinement:** Utilize the gathered real-time data to update the state forecast. This involves comparing the predicted state with the actual measurements and adjusting the prediction accordingly.
6. **Uncertainty assessment:** Evaluate the uncertainty in the estimated system state, considering both measurement data uncertainty and system model uncertainty.
7. **Iteration:** Continue the forecasting and refinement steps, using the updated state estimate as the foundation for the subsequent iteration.

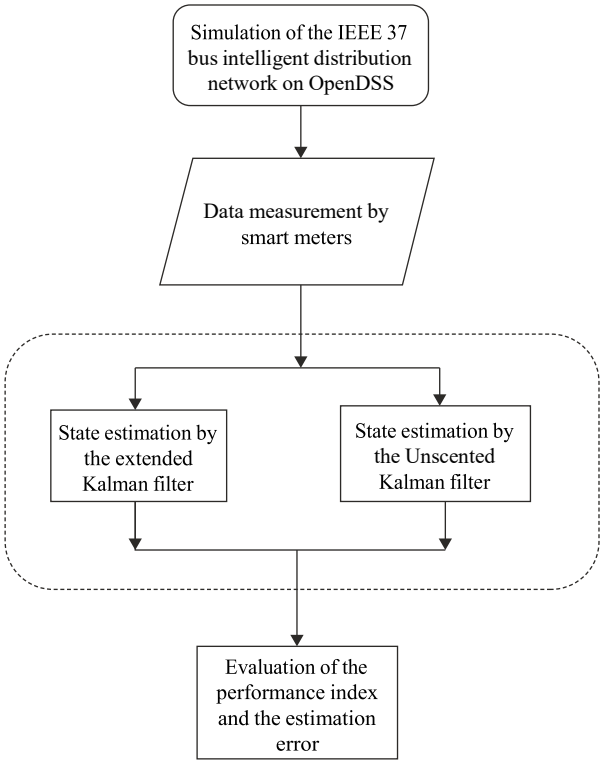


Figure 23: Proposed flowchart for the hybrid state estimation algorithm

5.8 Challenges and Considerations in EKF Implementation

Despite the EKF's notable benefits in handling uncertainties within smart grids, its application comes with several obstacles:

5.8.1 Computational Complexity

Matrix operations in the EKF can be computationally intensive, particularly when applied to large-scale smart grid systems with numerous sensors and devices. As the grid expands, the EKF's computational burden increases, potentially limiting its capacity to deliver real-time estimations. To address this challenge, it may be necessary to implement

the EKF in an efficient manner, potentially through the utilization of parallel computing methodologies.

5.8.2 Model Accuracy

The efficacy of the Extended Kalman Filter (EKF) in estimating system states is dependent upon the accuracy of the predictive model utilized. Inaccurate models, particularly those that inadequately represent the nonlinear behavior of grid elements, may result in suboptimal state estimations and diminish the filter's performance. Therefore, it is imperative to develop accurate models that precisely capture the grid's complexities for successful EKF implementation.

5.8.3 Parameter Tuning

The efficacy of the Extended Kalman Filter (EKF) is contingent upon the appropriate calibration of its process noise and measurement noise covariance matrices. These parameters necessitate meticulous adjustment to ensure the filter accurately estimates the system's state. Insufficiently calibrated filters may exhibit diminished capacity to accurately track the system's true state or potentially manifest instability.

CHAPTER SIX

SIMULATION AND RESULTS

6.1 Introduction

Section 6.1 introduces the chapter contents; Section 6.2 highlights the data gathered, and Section 6.3 highlights the choice of software used in this study. Section 6.4 shows how the MATLAB/Simulink platform was used to analyze how solar photovoltaic (PV) Distributed Generation (DG) was designed and modelled for the Smart Grid using Fiber Bragg Grating Sensors and blockchain technology. Section 6.5 demonstrates how Python and Anaconda programming environments were used to analyze how blockchain could improve the resilience of the smart grid energy system especially when it comes to energy trading.

6.2 Data Collection

For integrating the collected data from measurements of the FBG and conventional sensors, a real-time simulator based on OPAL-RT 4510 was used to interface the measurements with the MG Simulink as designed in Figure 27. It shows the measurements collected from FBG and the conventional sensors were applied to the potential points predefined in the Simulink model via analog input ports of the OPAL-RT. Moreover, the output of the Simulink model was applied to the scopes via analog output channels of the Opal- RT.

6.3 Choice of Software

MATLAB/Simulink, Python programming and Ethereum platform were used to carry out research objectives and answer research questions because of their ability to introduce and manipulate real-time data to suit the focus of study. This software was used to design the model of this study as seen in Figure 27 to simulate and analyze how solar renewable energy could be implemented and traded in the smart grid. Thereafter, the MATLAB/Simulink model was interfaced with Python scripts to simulate the operation of the blockchain energy-trading platform.

6.4 MATLAB/SIMULINK Model

The full model designed in Figure 27 was sectioned into different aspects consisting of solar panels (PV), DC-AC inverter, BOOST converter, smart meter, transformer, grid system, FBG sensors, and Maximum Power Point Tracking (MPPT) Control.

The primary function of solar panels is to harness energy from the sun's Global Horizontal Irradiance (GHL) that reaches the solar collector. To connect the photovoltaic system to the utility grid, an inverter control system is utilized. The energy produced by the PV system and the energy exchanged with the utility grid are measured using a smart meter. To prevent voltage loss, transformers are employed to increase and decrease voltages as needed. Additionally, a storage system is implemented to retain any surplus energy generated during various periods.

For integrating the collected data from measurements of the FBG and conventional sensors, a real-time simulator based on OPAL-RT 4510 was used to interface the measurements with the SG Simulink as designed in Figure 27. It shows the measurements collected from FBG and the conventional sensors were applied to the potential points predefined in the Simulink model (were used at two selected potential points: PV array, and the PCC) via analog input ports of the OPAL-RT. Moreover, the output of the Simulink model was applied to the scopes via analog output channels of the Opal-RT.

Blockchain technology was then used to program energy trading carried out between various nodes (i.e. participants) connected to the proposed blockchain energy trading platform.

Finally, Kalman Filter was implemented into the MATLAB Simulation then cascaded both together in order to detect the uncertainties in the smart grid system and analyzing the system behavior for different operating conditions in this study.

6.4.1 Grid Network Design

A 100-kW PV array is connected to a 25-kV grid via a DC-DC boost converter and a three-phase three-level Voltage Source Converter (VSC). Maximum Power Point Tracking (MPPT) is implemented in the boost converter by means of a Simulink model using the 'Perturb & Observe' technique.

The average model contains the following components.

1. PV array delivering a maximum of 100 kW at 1000 W/m^2 sun irradiance.

2. DC-DC boost converter.

3. 3-level 3-phase VSC.

4. 100-kVA 260V/25kV three-phase coupling transformer.

5. Utility grid.

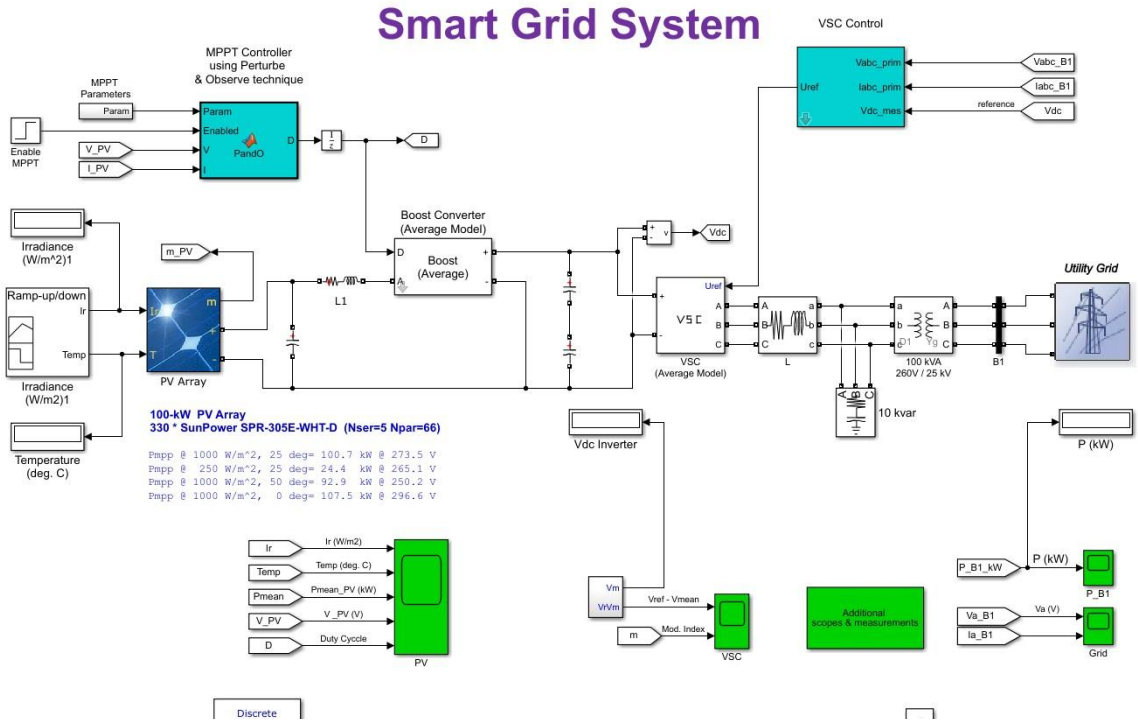


Figure 24: Smart Grid System

In this model the boost and VSC converters are represented by equivalent voltage sources generating the AC voltage averaged over one cycle of the switching frequency. Such a model does not represent harmonics, but the dynamics resulting from control system and power system interaction is preserved. This model allows

using much larger time steps, resulting in a much faster simulation. This algebraic loop is required to get an iterative and accurate solution of the PV model when large sample times are used. This algebraic loop is easily solved by Simulink. The 'Perturb and Observe' MPPT algorithm is implemented in the MPPT Control MATLAB Function block.

6.4.2 Grid Connected Solar Photovoltaic (PV) Model

Grid-connected solar photovoltaic models were designed to ensure the bidirectional flow of energy. The grid-connected decentralized solar photovoltaic distributed generation systems were designed to function in a bidirectional way so that energy could be distributed in both directions between the grid and the respective loads with and without PV systems installed in the various locations. The required capacity of PV Array installed at the DC end of the network were determined by assessing the quantity of loads that would demand for energy from PV generation plants. The SunPower SPR-415E-WHT-D PV Module was selected to design the decentralized solar photovoltaic model. The SunPower SPR415E-WHT-D monocrystalline module was chosen because of its 385.2W PTC ratings and 415W CEC ratings.

No matter how big or small a PV cell is, it produces approximately 0.5-0.6V DC under open circuit conditions (i.e when no load is connected to it). The power and current output of a PV call now depends on its efficiency and surface area. It is also proportional to the amount of light intensity striking the surface of the PV cell. A typical PV cell with a surface area of around 1.26 square meters under maximum

sunlight conditions, will produce a peak power of 170W. Usually the output voltage of each cell is usually low (typically 0.5-0.6V). Several cells are connected in series in the manufacture of a “laminate”. This laminate is then fixed onto a protective weatherproof enclosure. The resulting structure is now a photovoltaic panel or a solar panel. Modules can then be strung together into a photo-voltaic array.

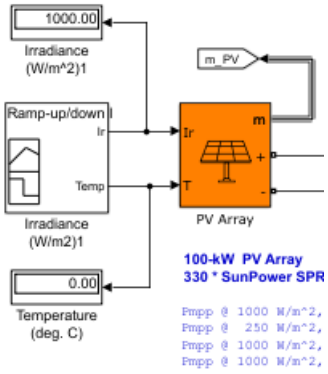


Figure 25: Grid Connected Solar Photovoltaic (PV) Model

6.4.3 Maximum Power Point Tracking (MPPT) Control

In Photo-voltaic converters, the maximum power available is often dependent on the photovoltaic cell characteristics. This value is not always in sync with the maximum power point of the load.

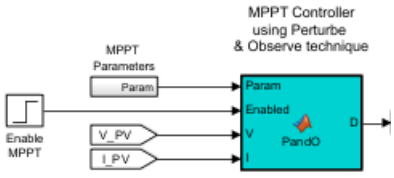


Figure 26: Module of MPPT

When the MPPT control system is used in a photo-voltaic system, the maximum power point of the photovoltaic cells can be maintained (or tracked) and by doing so the size of the photo-voltaic panels can be greatly reduced and the energy released by the photovoltaic cells can be optimized. During the day the sun is always moving from point A to B. This leads to changes in the amount of power that was being absorbed by the PV panels. Henceforth the energy that is being absorbed by the PV panels does not stay constant over time. When this happens, the I-V characteristics of the photovoltaic module will in turn change over time and this will cause the maximum power point of the PV module to also move from time to time. These changes may result in adamant power losses at the same operating point and different conditions.

6.4.4 DC-AC Converters (Inverter)

In this modern day, we hardly come across DC loads. Many loads nowadays (especially domestic loads) all operate on AC power. This poses yet another challenge, as the power output from a PV panel is only DC. This DC output needs to be converted to AC hence the need for the DC-AC inverter. For the purpose of this study, a single-phase full bridge inverter shown below was used: The single-phase full bridge inverter comprises of four switching devices (mosfet) with two of them arranged to form one leg. The input DC voltage is of fixed magnitude coming from the MPPT control. It can only be changed its polarity.

This particular inverter uses a PWM (Pulse Width Modulation) scheme with a switching frequency in the ranges of 2-20 kHz. Inverter is acting as an

interface between the PV panels and loads. During the system design, an inverter was designed by placing the inverter inside the solar PV panel subsystems. The inverter control was designed by integrating Phase-Locked Loop (PLL) and measurements; Maximum Power Point Tracker system (MPPT) that uses a Perturbation and Observation (P&O) algorithm approach; Direct Current (DC) voltage regulator; current regulator; and Pulse Width Modulation (PWM), which were functioning together. Furthermore, the inverter was used to convert DC voltage from the PV energy output to a sinusoidal ac voltage with lesser distortions is produced as the output of this inverter. A low pass filter is implemented during this phase to get the desirable output voltage fundamental frequency of 50Hz. It does so by separating this frequency from its switching frequencies which are in the ranges of kilos.

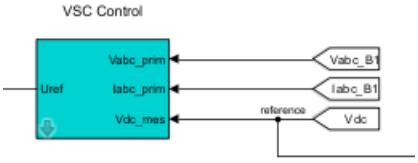


Figure 27: Block of DC to AC Converter

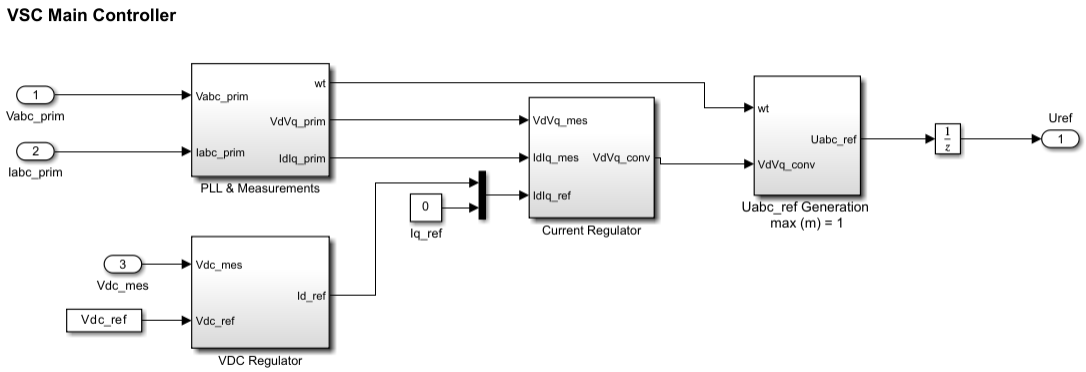


Figure 28: Block of DC to AC Converter

6.4.5 BOOST Converter Design

The Perturbation and Observation (P&O) method was used in this thesis to model the operations of the P&O control systems. This was because a lesser amount of sensor was required when compared to other MPPT algorithms, and it beats the constraints associated with system failure due to unforeseen circumstances or oscillatory stability conditions [137-141]. Furthermore, instead of designing a network for discrete power environments (i.e. not changing), the perturbation was designed to vary, based on changes in power continuously adjusted to new system conditions [141, 142]. The boost converter design in Figure 33 consisted of Maximum Power Point Tracking (MPPT), Pulse Width Modulation (PWM), inductor and capacitor to monitor the solar PV array's maximum voltage and current i.e. V_{max} and I_{max}.

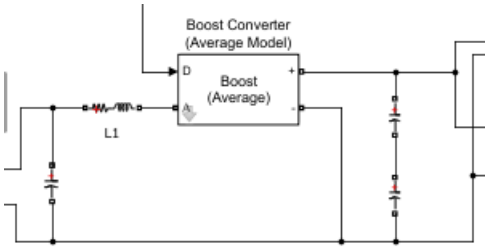


Figure 29: Circuit of the boost converter in the system design.

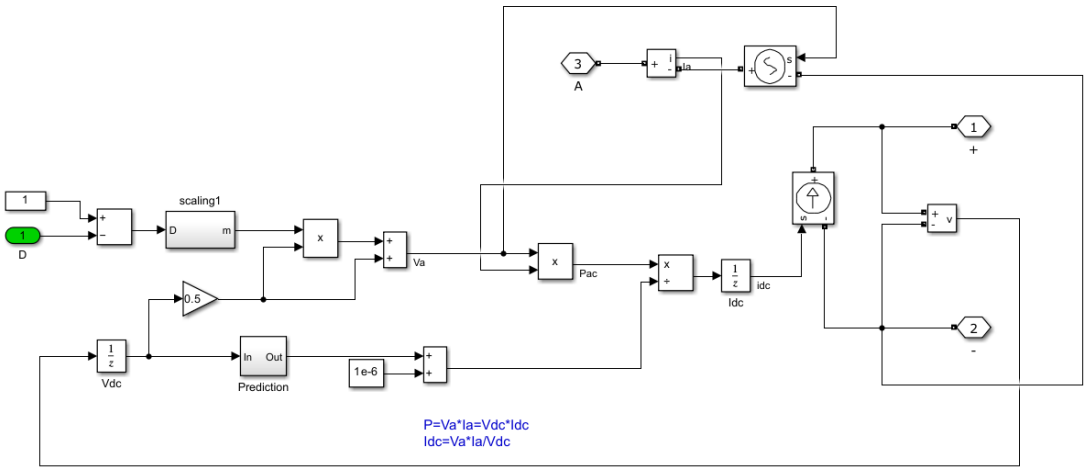


Figure 30: Circuit of the boost converter in the system design

The Phase Locked Loop (PLL) system was used to synchronize the frequency and three phase sinusoidal signals by enabling the Automatic Gain Control (AGC) such that the PLL regulator input (phase error) was scaled based on the magnitude of the input signals. To achieve the best possible outcome, the AGC control was enabled by assigning: a minimum frequency of 45Hz, initial inputs of 0° phase and 50Hz, while the regulator gains $[Kp, Ki, Kd]$ was set to [180, 3200, 1]. Thereafter, a time constant derivative action of 1×10^{-4} seconds (s) and maximum rate of change of frequency of 12Hz/s was set, while a filter cut-off

frequency measurement of 25Hz, with a sample time of zero seconds (s) was set before enabling the automatic gain control icon.

6.4.6 Smart Meter (SCOPE)

The smart meter in the model was designed in the form of MATLAB/Simulink scope. The voltage and current of the distributed generation solar photovoltaic (PV) system was represented as V_{abc}_B1 and I_{abc}_B1 respectively where abc denotes the lines a, b and c of the three phases. The smart meter for the grid's voltage and current was denoted as V_{grid} and I_{grid}, and the voltage and current of the smart meter symbol representing the loads connected to the solar PV generation system were expressed as $VLoad_1$ and $ILoad_1$.

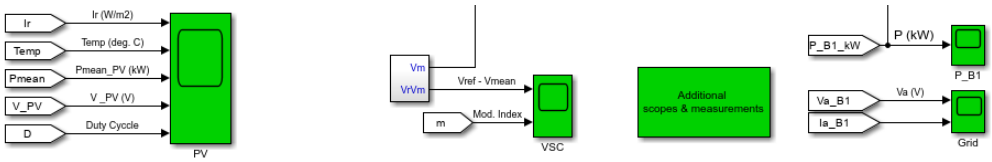


Figure 31: Smart Meter (SCOPE)

6.5 PYTHON Model

During this research, Python programming language was adopted to program the pattern of the blockchain energy-trading marketplace for this study. This was because the Python programming language is what most developers and analysts who work in the Energy Market and Trading (EM&T) industries utilize for their trading platforms and data analysis. Among the various Python programming environments, Anaconda, Jupiter Notebook and Visual Studio Code

Python environments were used for this research because they were used for their user friendliness.

Python programming language was used to import the results of the decentralized solar PV distributed generation networks modelled in the MATLAB/Simulink platform into the Python environment. Thereafter, simulation results from the MATLAB/Simulink platform were then used to program a basic energy-trading marketplace in the Anaconda, Jupiter and Python programming environments.

6.6 Importing MATLAB/SIMULINK Results into PYTHON Environment

The MATLAB/Simulink results were first sent into the MATLAB workspace before saving onto the research computer hard drive. After this, the Python programming language was used to import these results into the Jupiter Notebook environment. The next phase of the program was to ensure that available surplus energy could be made known to all nodes in the blockchain-trading platform.

6.7 Testing the Effect of Sensing Accuracy

This section outlines the findings from the research testing. The primary aim of unit testing was to evaluate the measurement precision between traditional sensors and FBG sensors at key locations. Table 5 provides an overview of the sensors employed in the study and the various test scenarios. To achieve this, data gathered from the experimental setup, including readings from all digital and analog conventional sensors

as well as FBG sensors, was input into the Simulink model depicted in Figure 27. This allowed for an examination of SG performance parameters across different sensing technologies. While the SG contained numerous potential sensor installation points and various physical signals for monitoring and control, this study focused on temperature measurements at two specific locations.

The research utilized two types of conventional temperature sensors and one FBG temperature sensor at two selected points: the PV array and the PCC. Given that high voltage (HV) and electromagnetic interference (EMI) represent the most challenging operating conditions, these were chosen for testing alongside normal operating conditions. The selection of temperature as the measured signal and these specific test conditions was made to effectively evaluate sensor performance in the SG environment.

Table 5: The testing data.

Sensors	Test Cases	Potential Points
FBG Temperature sensors	Normal case	PV array
DS18b20 digital temperature sensor	EMI Effects	PCC
LM35 analog temperature sensor	HV Effects	

6.7.1 Normal Condition at PV Array as an Energy Source

The temperature measurements of the photovoltaic (PV) system under standard operating conditions are presented in Figure 35. The investigation employed four distinct measurement methodologies: infrared (IR), Fiber Bragg Grating (FBG) sensors, LM35,

and DS18b20. The IR temperature sensor, owing to its superior precision, served as the reference standard. An analysis of the temperature trends depicted on the right side of the figure, accompanied by corresponding legends, indicates that the FBG sensors exhibited greater accuracy in comparison to the two conventional sensors.

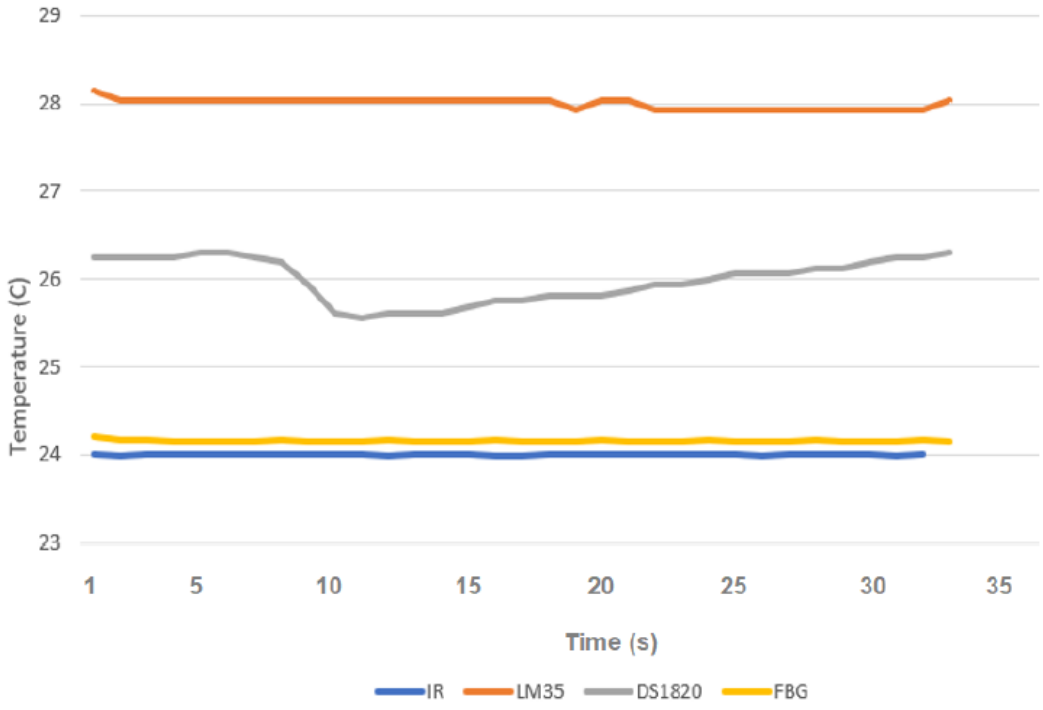


Figure 32: Normal operating conditions at the PV panel

6.7.2 Normal Condition at the PCC

The temperature reading trends from conventional sensors, the IR reference, and the FBG sensor at the point of common coupling (PCC) are illustrated in Figure 36. The graph clearly demonstrates that the FBG sensor provided the most accurate readings, closely aligning with the reference measurements. In contrast, the two conventional sensor types exhibited significant inaccuracies and fluctuations.

Table 6 offers a statistical comparison of readings under normal conditions at the PCC for all sensor types, including conventional sensors, IR reference, and FBG. The data unequivocally shows that the FBG sensor had the smallest standard deviation, indicating the least variation from the mean value and superior accuracy compared to conventional sensors. Furthermore, a quantitative statistical analysis was performed to compare the mean and standard deviation of each sensing technology's readings, as shown in the third and fourth columns of Table 6. The FBG sensor's mean was found to be the nearest to the IR sensor reference mean, while other conventional sensors deviated further.

Additionally, the FBG and reference IR sensors displayed the lowest standard deviation values, signifying minimal fluctuation in comparison to the conventional sensors, which exhibited high deviation. This implies that lower standard deviation corresponds to smaller discrepancies between measured values and mean values.

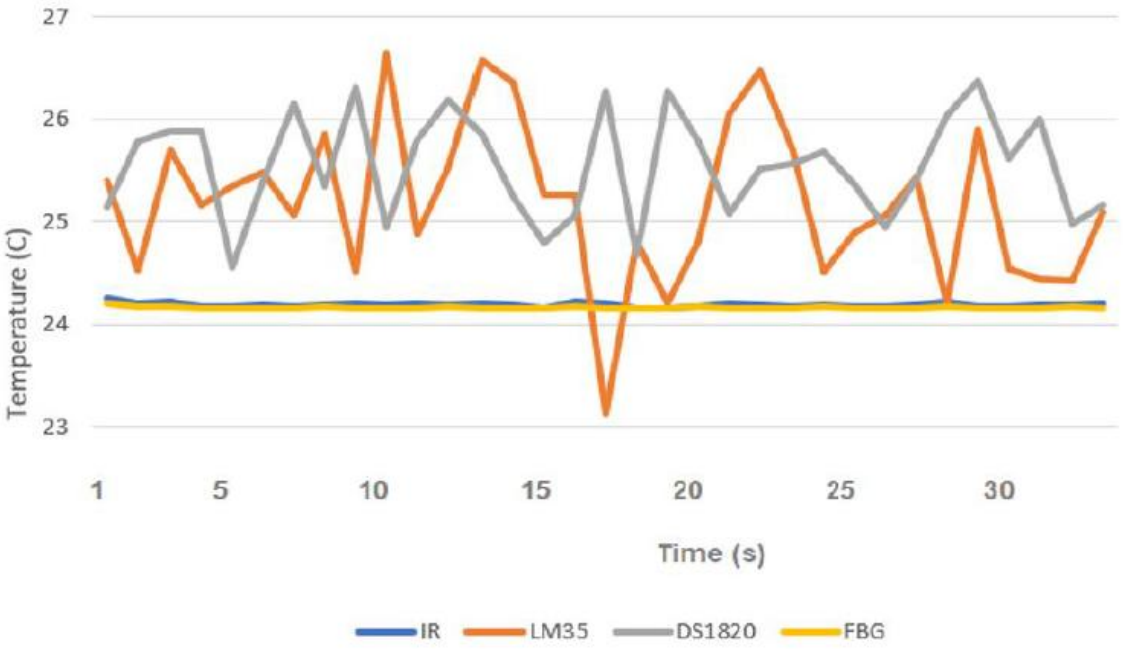


Figure 33: Normal operating conditions at PCC

Table 6: Statistics of the measurements at PCC point

Sensor	min	max	Avg	std
IR	24.15217	24.25836	24.18738	0.021523
LM35	23.12	26.64	25.18818	0.7772
DS1820	24.56	26.38	25.54879	0.512773
FBG	24.14999	24.21119	24.16056	0.011033

6.7.3 Testing the Condition of EMI Effects at the PCC

A comparison of conventional sensors and the FBG sensor under electromagnetic interference (EMI) is illustrated in Figure 37. The results demonstrate that the analog

sensor LM35 was most susceptible to EMI, followed by the digital sensor DS18B20. In contrast, the FBG sensors exhibited the least sensitivity to EMI effects.

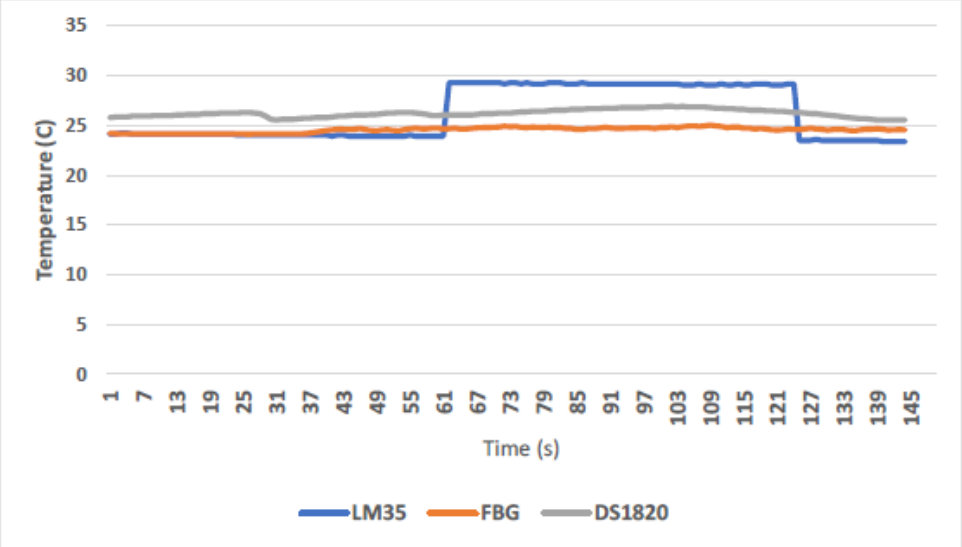


Figure 34: EMI effects on the FBG, LM35, and DS18B20 sensors.

6.7.4 Testing the Condition of HV Effects at the PCC

A comparison between traditional sensors and the FBG sensor under high voltage (HV) conditions at the PCC point is illustrated in Figure 38. The results demonstrate that the analog sensor LM35 was the most susceptible to HV effects, followed by the digital sensor DS18B20. In contrast, the FBG sensors exhibited the least sensitivity to these conditions.

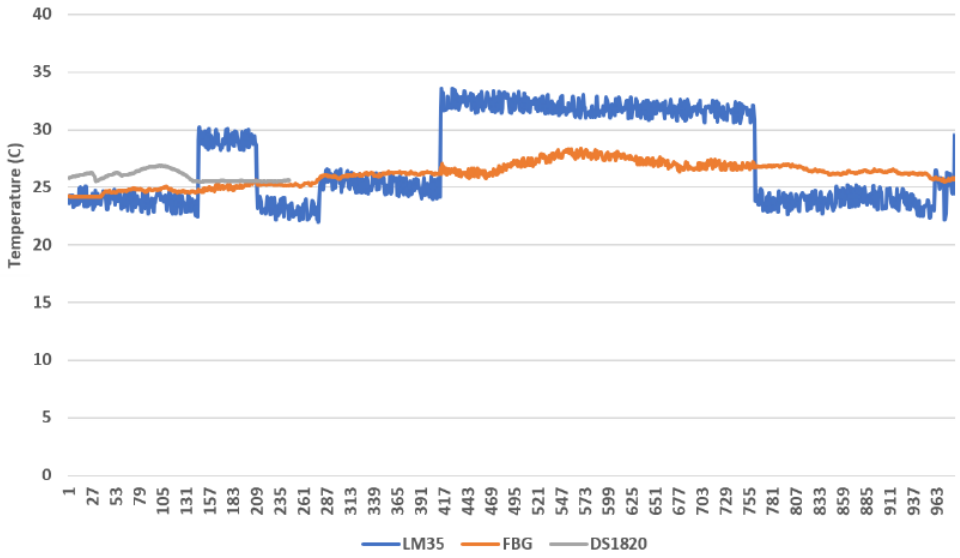


Figure 35: HV effects on the FBG, LM35, and DS18B20 sensors

6.8 Testing the Effect of Sensing Accuracy on the SG Performance

6.8.1 Testing at Normal Condition

Two tests were conducted under normal operating conditions, comparing the PV array output based on temperature measurements from different sensors. The yellow line represented analog sensors, brown represented digital conventional sensors, and blue represented FBG temperature sensors. Figure 39 illustrates a comparative analysis of the average voltage and power output from the PV array under normal operating conditions. The reference values for mean voltage and power were 230 V and 100 kW, respectively, at standard conditions of 25 _C and 1000 w/m2. Significant noise was observed in voltage and power measurements when using conventional sensors, while FBG sensors demonstrated minimal noise.

Furthermore, Figure 40 presents a comparison of the average output power at the point of common coupling (PCC) across different sensor types. Conventional sensors, particularly analog ones, exhibited fluctuations and noise. In contrast, FBG sensors showed minimal noise and superior accuracy. The reference power measurement at the PCC was 147.7 kW.

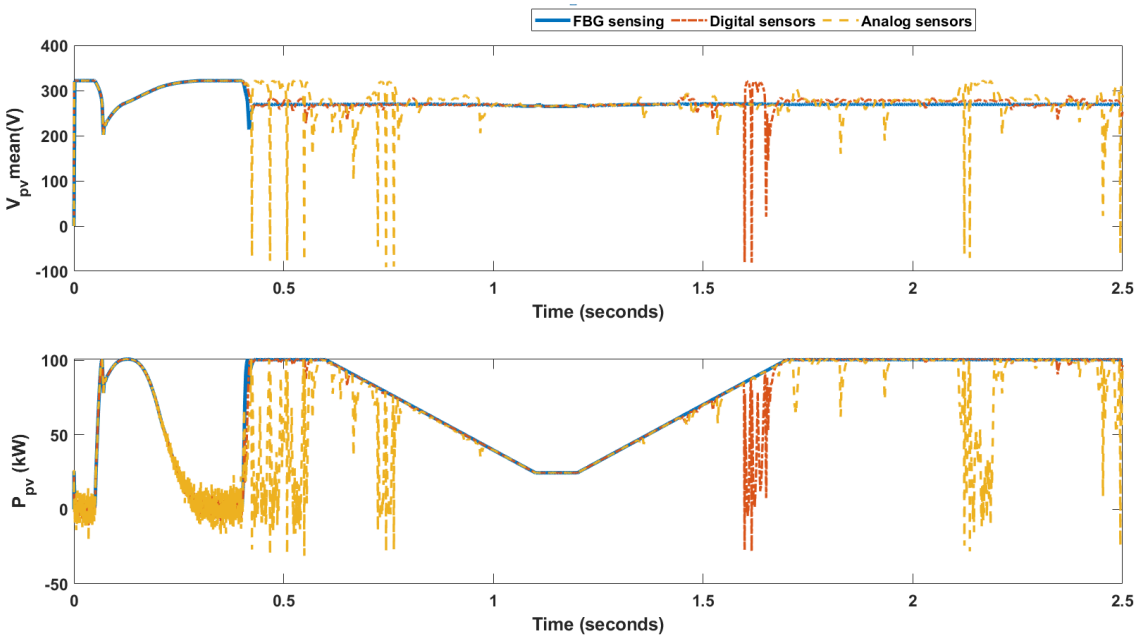


Figure 36: Output metrics at the potential point of PV array output.

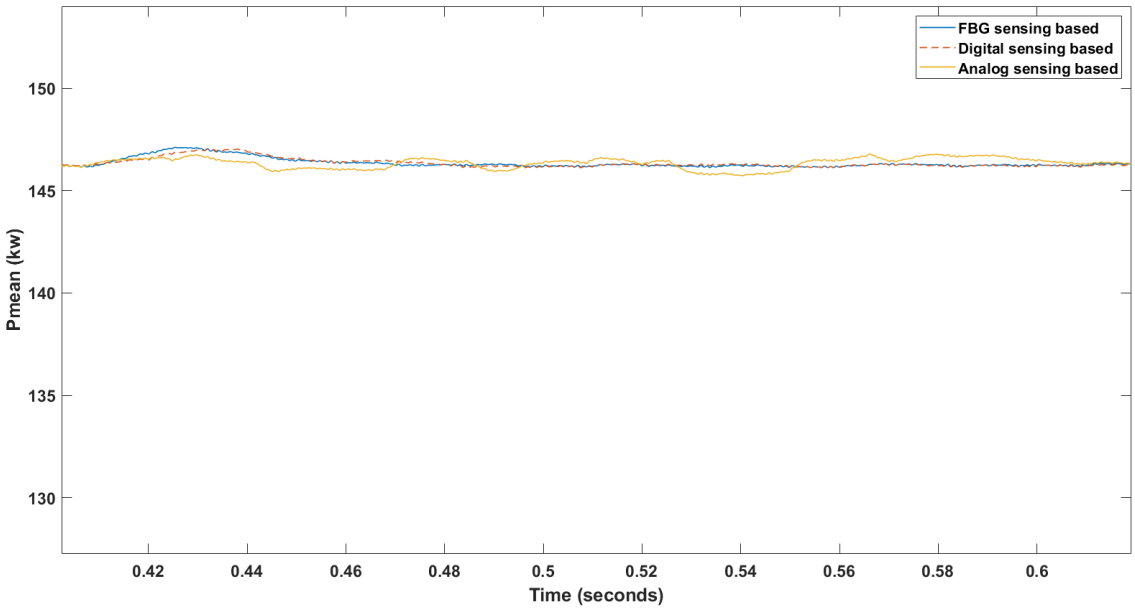


Figure 37: Output metrics at the potential point of PCC output.

A statistical comparison of readings at the PCC point for conventional sensors and FBG under normal conditions is presented in Table 7. The data clearly demonstrates that FBG exhibited the smallest standard deviation, indicating the least variation from the mean value and superior accuracy compared to conventional sensors. The results unequivocally show that FBG provided the most precise measurements and aligned most closely with the reference readings. In contrast, the two types of conventional sensors displayed poor accuracy and significant fluctuations in their measurements.

Table 7: Statistics of the measurements at PCC point.

Sensor type	Min	Max	Avg	Std
LM35	23.12	26.64	25.18818	0.7772
DS1820	24.56	26.38	25.54879	0.512773
FBG	24.14999	24.21119	24.16056	0.011033

6.8.2. Testing under EMI Effects

Two tests were performed under abnormal operating conditions, specifically in the presence of electromagnetic interference (EMI). These tests measured the output from the photovoltaic (PV) array based on temperature readings from different sensors. The results were color-coded: yellow for analog sensors, brown for digital conventional sensors, and blue for Fiber Bragg Grating (FBG) temperature sensors. Figure 41 provides a comparative analysis of the average measured voltage and output power of the PV array under EMI conditions. The data showed that when using conventional sensors, the voltage and power of the PV array exhibited significant noise. In contrast, the noise levels were considerably lower when FBG sensors were employed.

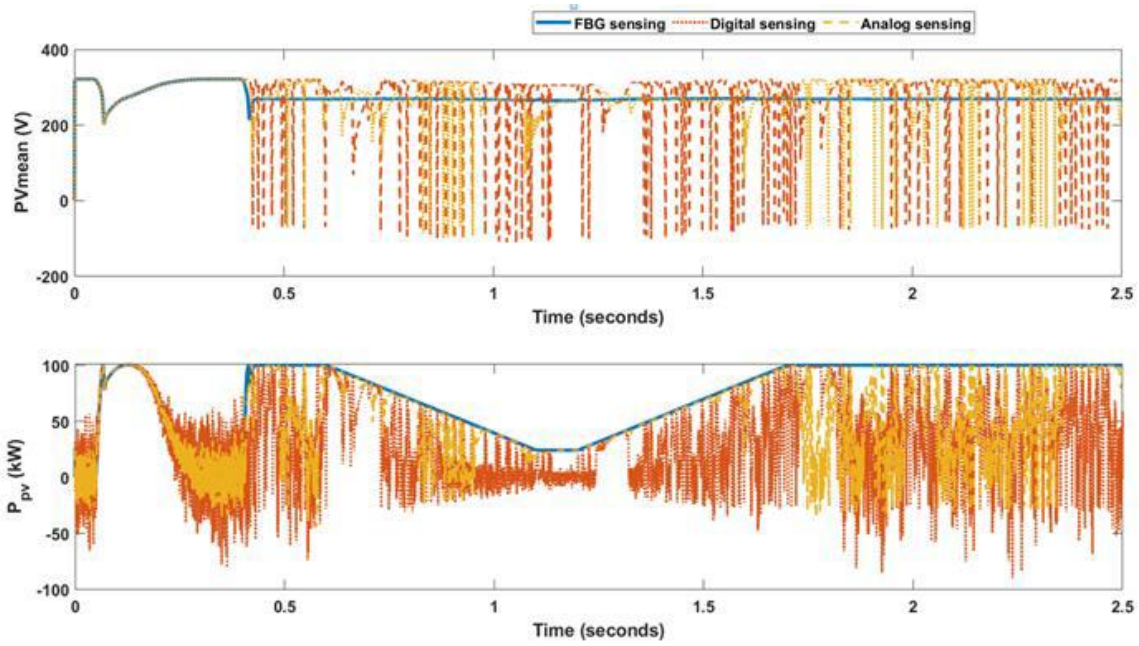


Figure 38: Output metrics at the potential point of PV array output under EMI.

Additionally, Figure 42 illustrates a comparison of the average output power at the point of common coupling (PCC) when using traditional analog and digital sensors versus employing the FBG sensor. In the presence of electromagnetic interference (EMI), conventional sensors, particularly analog ones, exhibited fluctuations and noise. In contrast, the FBG sensors demonstrated minimal noise and superior accuracy.

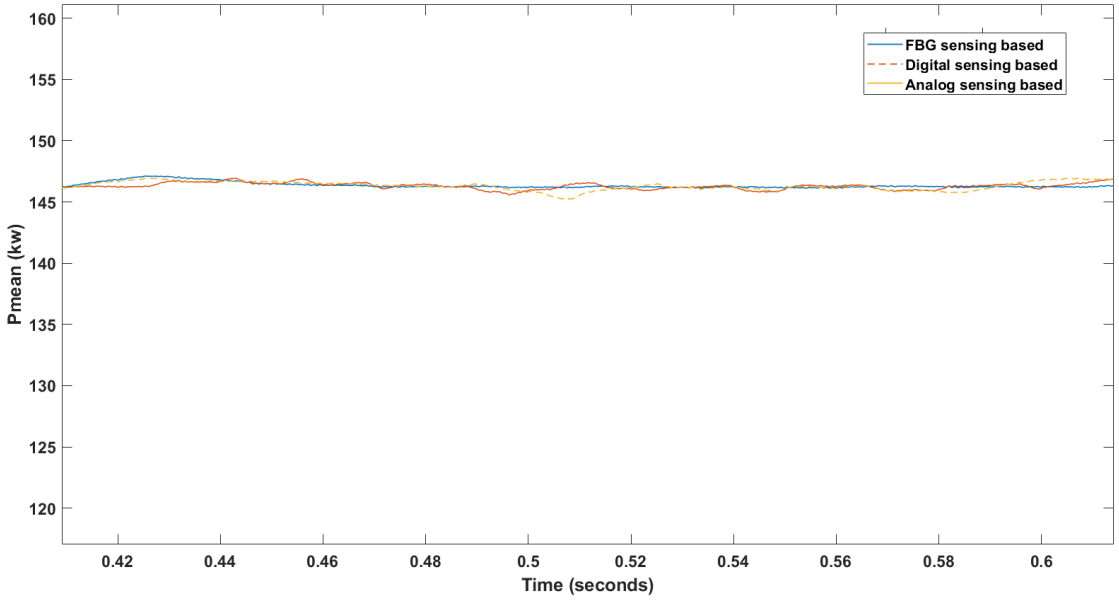


Figure 39: Output metrics at the potential point of PCC output under EMI.

6.9 Blockchain MATLAB Implementation

6.9.1 Block Chain Theory

1. A block serves as a versatile data structure capable of storing various types of information. In most blockchain applications, the data stored typically consists of transaction records. Within MATLAB, a class can be utilized to represent a block.

2. The Block class definition includes several attributes: index (representing the block number), data (containing transaction information), selfHash (the block's unique hash value), previousHash (the hash value of the preceding block), and nounce (a random value indicating mining attempts).

3. The block's function can be called with either 2 or 3 arguments. When provided with two arguments, the resulting Block object is termed a Genesis Block, which represents the initial block in the blockchain. When three arguments are supplied, the third argument corresponds to the hash value of the previous block. The implementation specifics can be found in section 6.1 block.m.

6.9.2 Block.m

Program 6.1: Block

```
1 classdef Block < handle
2
3 properties
4 index % index of block
5 data % transcation data
6 previousHash % the previous hash
7 selfHash % current hash
8 nonce % random number
```

```
9 end
10
11 methods
12 function obj = Block(index, data, previousHash)
13 if nargin == 2 % genesis block!
14 obj.index = index ;
15 obj.data = data ;
16 elseif nargin == 3
17 obj.index = index ;
18 obj.data = data ;
19 obj.previousHash = previousHash;
20 end
21 end
22
23 % The function below converts all data on the block except 'nonce' and
24 % 'selfHash' into characters, which is then used to calculate selfHash.
25 function str = getCombined(obj)
26 str = strcat([num2str(obj.index), obj.previousHash, join(obj.data)]);
27 end
28 end
29 end
```

Listing 1: Block.m

Output 6.1:

```
>> Block(1, 'this is data')

ans =

Block - properties:

index: 1

data: 'this is data'

previousHash: []

selfHash: []

nonce: []

>> Block(1, 'this is data', 'this is previous hash')

ans =

Block - properties:

index: 1

data: 'this is data'

previousHash: 'this is previous hash'

selfHash: []

nonce: []
```

6.9.3 BlockChain.m

Program 6.2: BlockChain

```
1 classdef BlockChain < handle
2
3 properties
4 totalCount % used to record the number of blocks
5 blockArray % this is an object array that used to store the blockchain
6 end
7
8 methods
9 function obj = BlockChain()
10 obj.blockArray =[Block(0, 'Genesis Block')]; % genesis block
11 obj.totalCount = 1 ;
12 obj.calculateGensisBlockHash(); % calculate the hash of genesis block
13 end
14
15 function bc = getLatest(obj) % get the last block on the current
blockchain
16 bc = obj.blockArray(end);
17 end
18
19 function calculateGensisBlockHash(obj)
20 gb = obj.blockArray(1);
21 Opt.Method = 'SHA□256';
22 Opt.Input = 'ascii';
```

```
23 str = strcat(num2str(gb.index), gb.data);
24 disp(str);
25 gb.selfHash = DataHash(str, Opt); % calculate current hash
26 end
27
28 function addBlock(obj, newBlock) % when Miner.m successfully 'digs out' a
block that meets the requirements
29 if obj.validateNewBlock(newBlock) % call this function
30 obj.blockArray(end+1) = newBlock; % and then add this block to this
blockchain
31 end
32 end
33
34 function tf = validateNewBlock(obj, newBlock) % verify that the newly
added block meets the requirements or not.
35 newHash = DataHash([strcat(newBlock.getCombined(), num2str(newBlock.
Nonce))]);
36 if(strcmp(newHash(1:3), '000') && strcmp(newBlock.selfHash, newHash))
37 tf= true;
38 else
39 tf = false;
40 end
41 end
42 end
```

```
43 end
```

Listing 2: BlockChain.m

Output 6.2:

```
>> BlockChain

0Genesis Block

ans =

BlockChain – properties:

totalCount: 1

blockArray: [1×1 Block]
```

6.9.4 Miner.m

Program 6.3: Miner

```
1 classdef Miner < handle
2 properties
3 blockchain
4 end
5
6 methods
7 function obj = Miner(blockchain)
8 obj.blockchain = blockchain;
9 end
10
11 function mine(obj, newData)
```

```
% get the last block on the current blockchain
latestBlock = obj.blockchain.getLatest();
% construct a new block
newBlock = Block(latestBlock.index+1,…
newData,…
latestBlock.selfHash);% find appropriate selfhash
not_found = true;
iter = 1;
Opt.Method = 'SHA□256';
Opt.Input = 'ascii';

tic
while(not_found)
newHash = DataHash([strcat(newBlock.getCombined(), num2str(iter))]);
if(strcmp(newHash(1 : 3), '000'))
newBlock.nonce = iter; % solve violently
newBlock.selfHash = newHash; % if the 155ppropriate selfhash is found
disp(newHash)
obj.blockchain.addBlock(newBlock); % add selfhash to blockchain
break
end
iter = iter + 1;
end
```

```
35 toc
36 end
37 end
38 end
```

Listing 3: Miner.m

6.9.5 TradingTest.m

Program 6.4: TradingTest

```
1 clear; clc;
2 bc = BlockChain;
3 bc; bc.blockArray(1)
4 mining = Miner(bc);
5 disp('============================================');
6 transcation = ['A', 'B', 'MOP', '200'];
7 mining.mine(transcation)
8 bc; bc.blockArray(2)
9 disp('============================================');
10 transcation = ['B', 'C', 'USD', '300'];
11 mining.mine(transcation)
12 bc; bc.blockArray(3)
13 disp('============================================');
14 transcation = ['C', 'A', 'HKD', '700'];
15 mining.mine(transcation)
16 bc; bc.blockArray(4)
```

Listing 4: BlockChain.m

Output 6.4:

```
0Genesis Block

ans =

Block - properties:

index: 0

data: 'Genesis Block'

previousHash: []

selfHash: '075c27741a3506846368fa6e5b3477f85b31ceee71a5

716e2f12b40fa21d23aa'

nonce: []

==========================================

000cfbb745e3d504306b8c435b639d1d

It took 0.562127 seconds.

ans =

Block - properties:

index: 1

data: 'ABMOP200'

previousHash: '075c27741a3506846368fa6e5b3477f85b31ceee71a5

716e2f12b40fa21d23aa'

selfHash: '000cfbb745e3d504306b8c435b639d1d'
```

nonce: 1209

==========

0008fc36bf8a3fac06b898239c5f6ff5

It took 0.114654 seconds.

ans =

Block - properties:

index: 2

data: 'BCUSD300'

previousHash: '000cfbb745e3d504306b8c435b639d1d'

selfHash: '0008fc36bf8a3fac06b898239c5f6ff5'

nonce: 292

==========

000b3d4205a9fcd798805f004e8d9a75

It took 0.946117 seconds.

ans =

Block - properties:

index: 3

data: 'CAHKD700'

previousHash: '0008fc36bf8a3fac06b898239c5f6ff5'

selfHash: '000b3d4205a9fcd798805f004e8d9a75'

nonce: 2940

6.9.6 Simulation of Blockchain Security with Blackhole Attack

This research examines the susceptibility of a (MANET) Network to blackhole attacks by simulating the network using the On-demand Distance Vector routing protocol. The research incorporates blockchain technology to establish node connections and introduces a malicious node to simulate a blackhole attack, potentially disrupting communication. Through visual representation, the simulation showcases the effects of the blackhole attack on routing paths, comparing routes with and without the presence of the malicious entity.

This simulation serves as a tool to explore how routing protocols respond to security threats, providing valuable insights into potential strategies for countering such attacks in MANET networks.

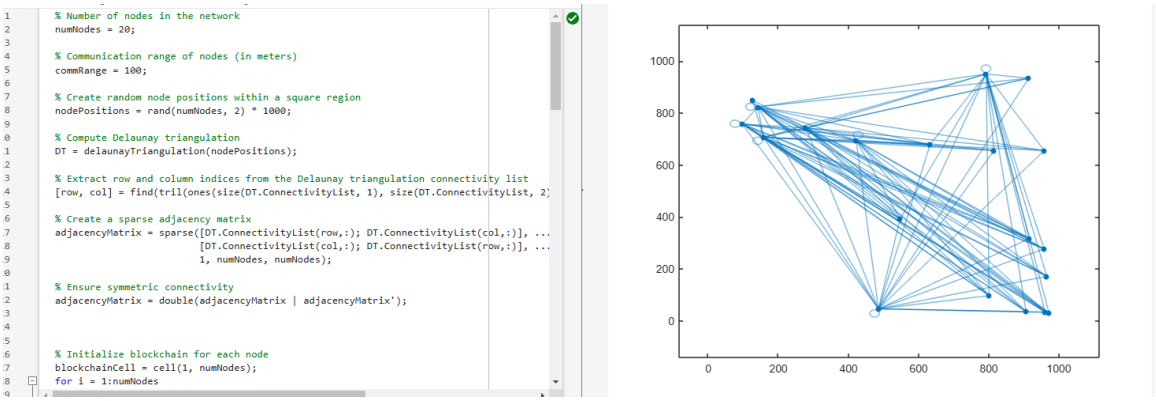


Figure 40: Blockchain with 20 Nodes, 3 Blocks, without blackhole attack

The nodes are visually distinguished by three different colors: red, blue, and green. Let's explain the significance of each color:

1. **Red Nodes:** In routing protocols, the origin and endpoint of data packets are denoted by nodes colored in red. These red nodes, representing the source and destination, play a vital role in the routing process.
2. **Blue Nodes:** Blue-colored nodes on the path indicate those that are not affected by a blackhole. These blue nodes constitute the most direct route between the origin and destination points when no malicious interference is present.
3. **Green Nodes:** In the network simulation, a green-colored node represents the blackhole node. This simulated malicious entity is incorporated into the network to emulate a disruptive force that interferes with communication by either discarding or modifying data packets.

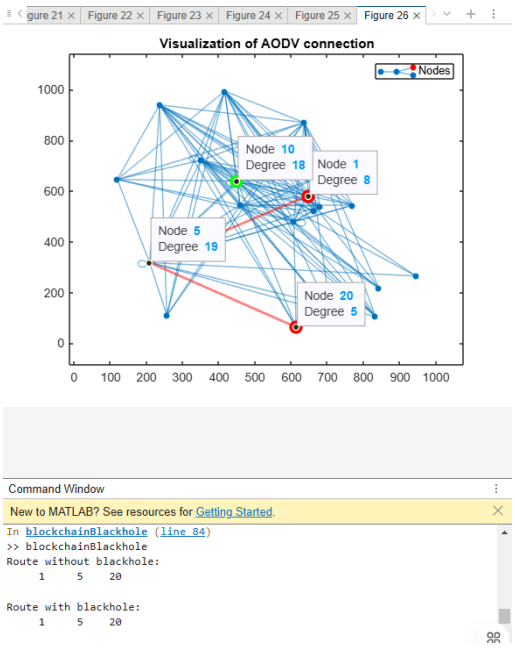
The phrases "Route without blackhole attack" and "Route with blackhole attack" describe the trajectories taken by information packets as they travel from the originating node to the target node in the simulated network environment. These routes are illustrated both when a blackhole attack is absent and when it is present, respectively.

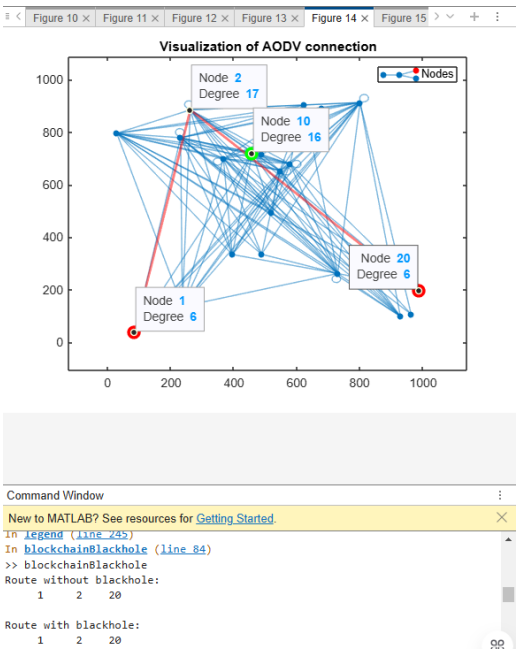
A. Route without blackhole attack:

1. This line indicates the path taken by data packets when there is no blackhole node in the network.
2. In this case, the route consists of two nodes: node 1 (the source node) and node 20 (the destination node).
3. The data packets are successfully transmitted from the source node (node 1) to the destination node (node 20) without encountering any disruption or interference.

B. Route with blackhole attack:

1. This line indicates the path taken by data packets when a blackhole node is present in the network.
2. In this case, the route consists of three nodes: node 1 (the source node), node 20 (the destination node), and node 10 (the blackhole node).
3. The data packets, instead of being routed directly from the source node to the destination node, are diverted through the blackhole node (node 10).
4. This diversion is characteristic of a blackhole attack, where the malicious node intercepts and drops or alters data packets, disrupting communication between legitimate nodes.





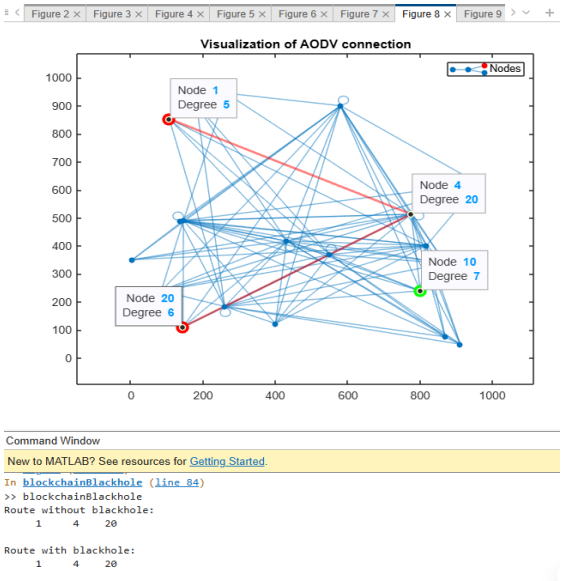


Figure 41: The lines "Route without blackhole" and "Route with blackhole" indicate the paths followed by data packets from the source node to the destination node in the simulated network (3 cases).

6.10 Detection of Uncertainties Using Extended Kalman Filter

The primary focus of our work is on the smart grid system, with the main objective being to protect it from hackers who compromise grid security by introducing false data. To address this issue, we have employed the Extended Kalman filter, which is utilized to identify uncertainties within the grid. This filter continuously compares incoming data with predefined or existing data to detect any uncertainties. If the comparison yields unsatisfactory results, it indicates a potential problem with the data, suggesting that external sources may be injecting information that could pose a threat to the grids. This is particularly crucial because grids play a vital role in the overall power system.

6.10.1 Extended Kalman Filter Simulation

In our MATLAB Simulation, we have implemented the Extended Kalman filter to address uncertainties in smart grid systems. This filter will be integrated with the smart grid simulation for uncertainty detection. The implementation process is illustrated in the figure provided below.

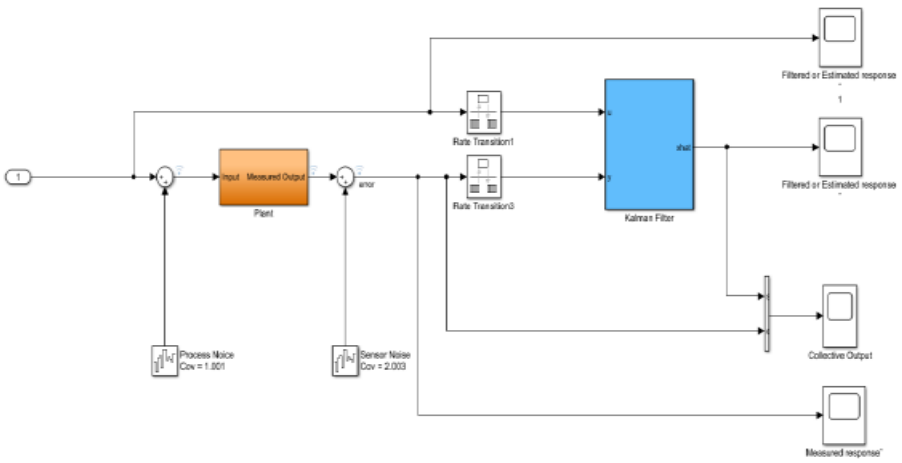


Figure 42: Simulation of Extended Kalman Filter

6.10.2 Smart Grid Simulation

The Smart Grid System has been incorporated into the MATLAB simulation, as illustrated in the figure below. Additionally, we have integrated the Extended Kalman Filter into the MATLAB Simulation, as depicted in figure 46. These two components have been combined to identify uncertainties within smart grid systems.

Our examination of an intricate Smart Grid control mechanism employs simulation to replicate both the communication network and the power system. This control mechanism utilizes a wireless communication network to engage distributed storage units within a portion of the electrical grid, compensating for temporary power loss from a solar photovoltaic (PV) array. Furthermore, it would be advantageous to connect communication system modeling with simulations of emerging Smart Grid applications on operational power systems. This co-simulation environment would enable engineers to evaluate the viability of employing specific network technologies to support communication-based Smart Grid control schemes.

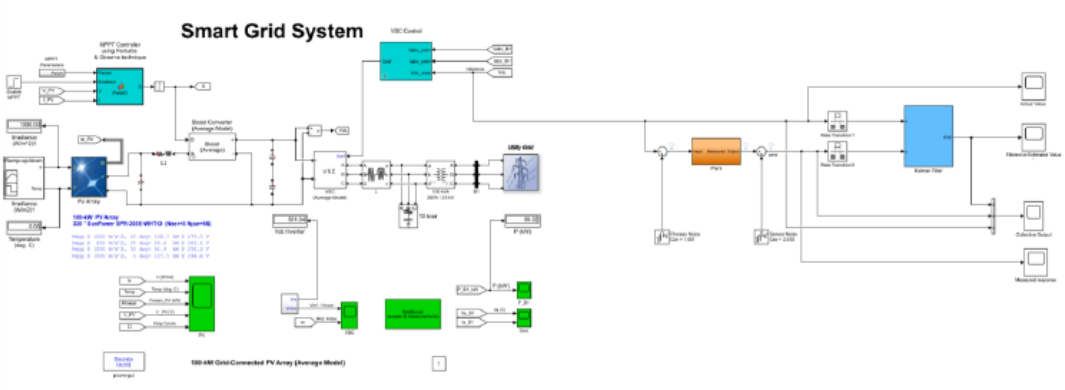


Figure 43: Smart Grid Implementation with Kalman Filter

6.10.3 Simulation Results of Smart Grid Uncertainties without EKF

Now we are trying to test the uncertainties in the Smart Grid by changing the value of the voltage at the controller. See table 8.

Table 8:Values of different uncertainties

Uncertainties	Voltage Level (V)
Uncertainty 1	500
Uncertainty 2	1000
Uncertainty 3	1500

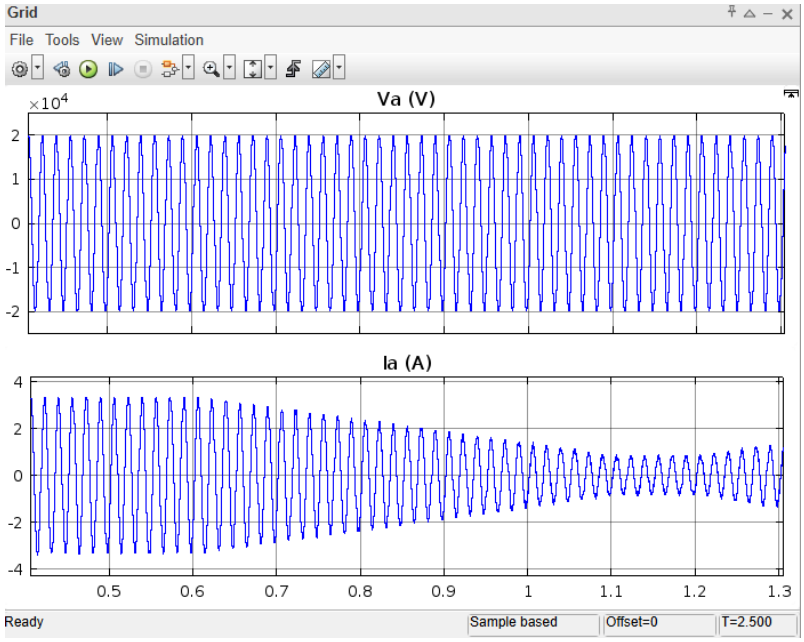


Figure 44: Simulation Results of Grid at the voltage of 500

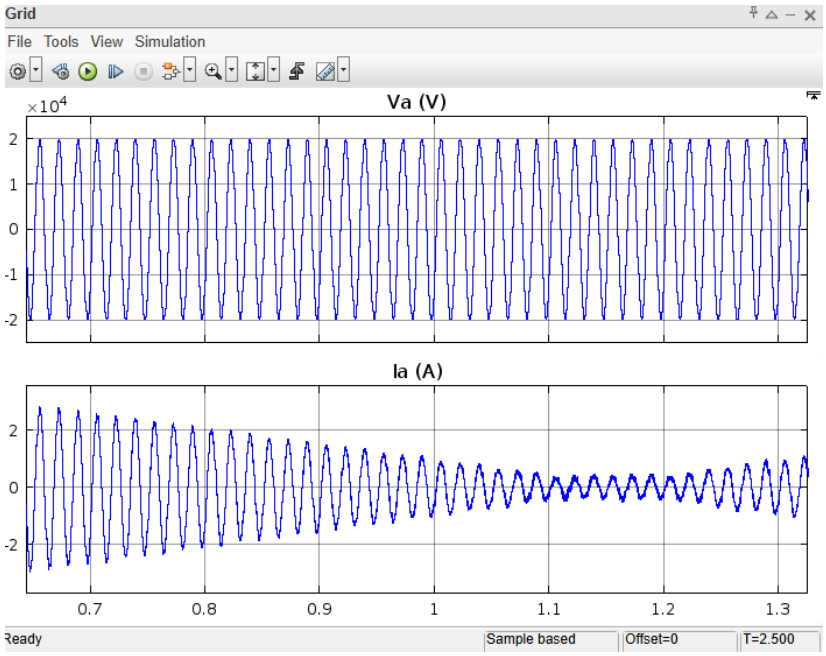


Figure 45: Simulation Results of Grid at the voltage of 1000

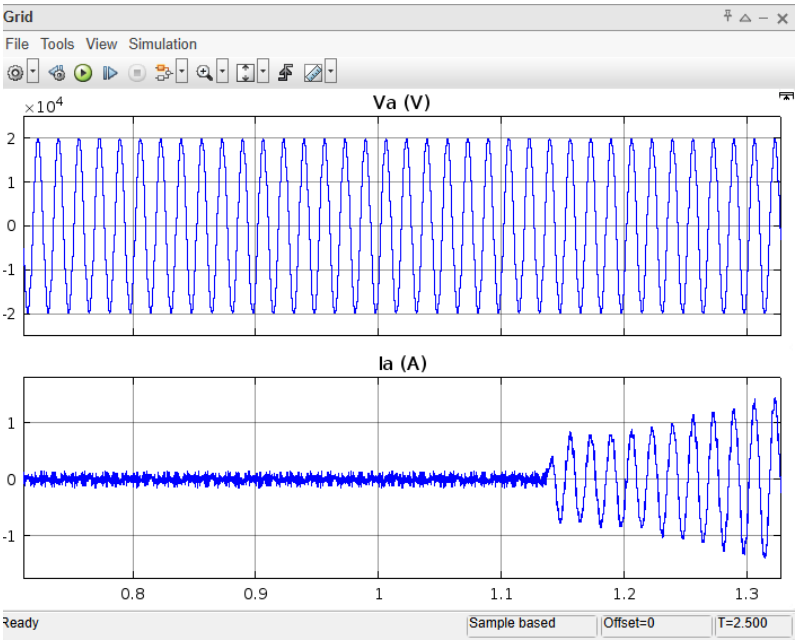


Figure 46: Simulation Results of Grid at the voltage of 1500

6.10.4 Simulation Results of Smart Grid Uncertainties with EKF

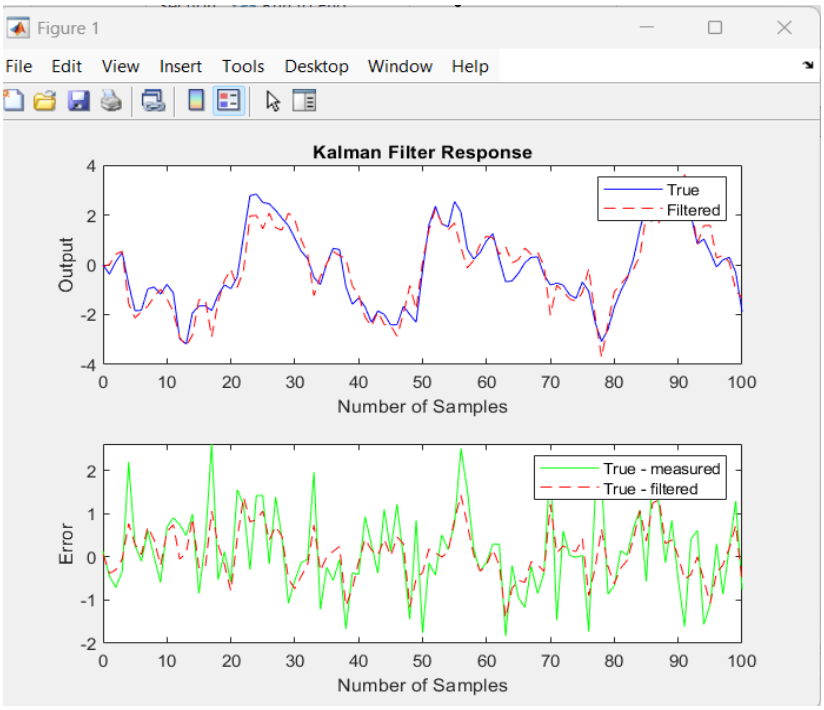


Figure 47: Extended Kalman Filter Normal Response

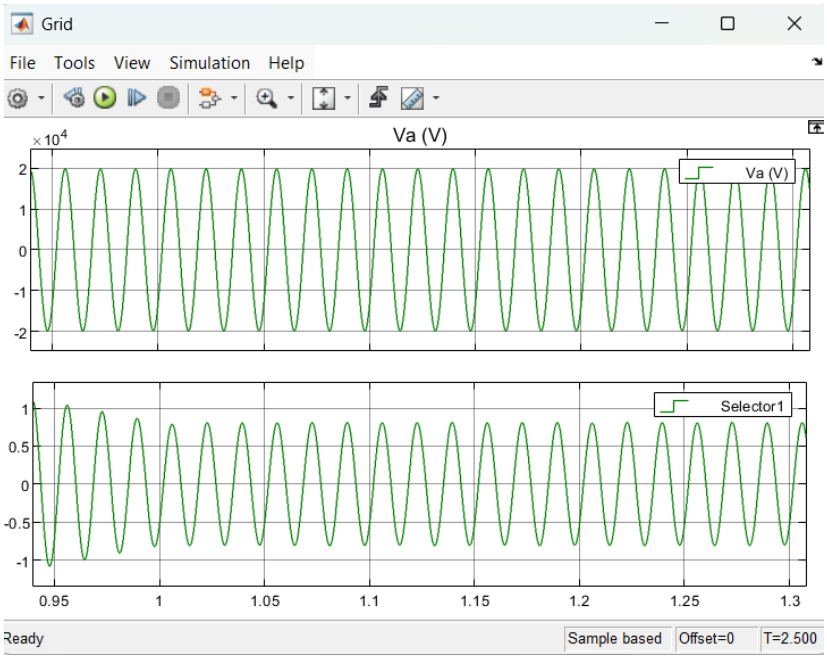


Figure 48: Simulation Results of Grid at the voltage of 500

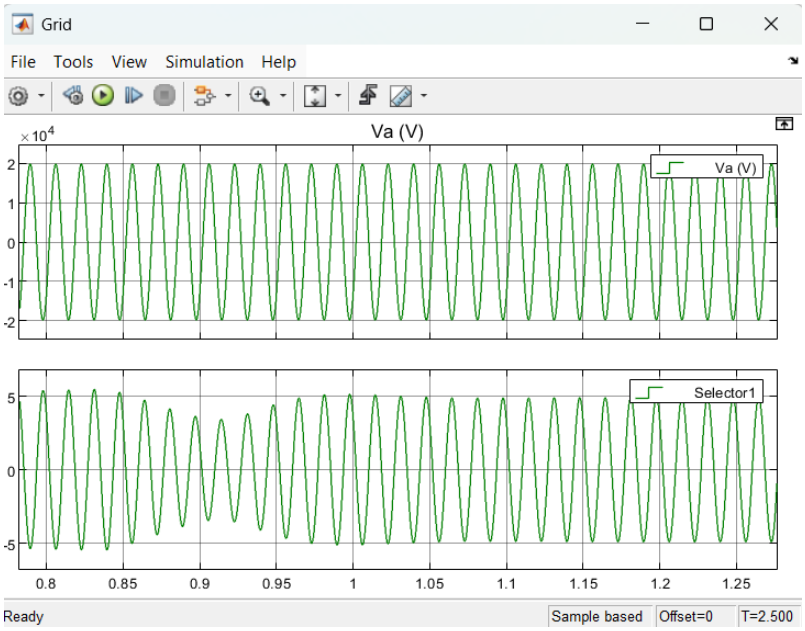


Figure 49: Simulation Results of Grid at the voltage of 1000

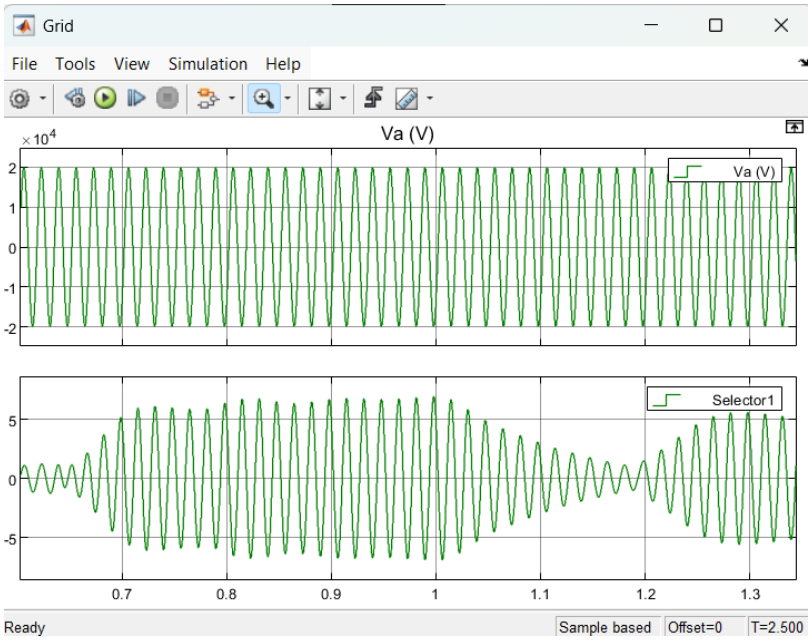


Figure 50: Simulation Results of Grid at the voltage of 1500

CHAPTER SEVEN

CONCLUSION AND FUTURE RECOMMENDATION

7.1 Conclusion

In conclusion, this research successfully designed and implemented a fault detection system for smart grids that integrates Fiber Bragg Grating (FBG) sensors, Blockchain technology, and uncertainty identification using the Extended Kalman Filter (EKF). The integration of these technologies has demonstrated significant improvements in the stability, reliability, and efficiency of power transmission and distribution systems. Key benefits include enhanced security, improved transparency, increased efficiency, greater fault detection reliability, and overall operational flexibility.

The research introduced FBG sensing technology as a superior alternative to conventional sensors in Microgrids (MGs). Through simulations, it was established that electromagnetic interference (EMI) and high voltage (HV) adversely impact the accuracy of conventional sensors, whereas FBG sensors exhibit high immunity to such disturbances. Furthermore, the measurement data were applied to critical points in the Simulink model of a smart grid to evaluate the effects of replacing conventional sensors with FBG sensors on performance, reliability, and security. The findings clearly indicated that FBG sensors provided superior accuracy and robustness against EMI and HV, resulting in enhanced MG performance.

Another crucial aspect of this research was the adoption of blockchain technology for energy trading among energy users. A decentralized energy trading platform was developed using Python within the Anaconda, Jupyter Notebook, and Visual Studio Code environments. Various energy trading scenarios were simulated, wherein energy was either bought or sold among nodes representing solar-powered homes connected to a blockchain network. The results from decentralized solar renewable generation in MATLAB/Simulink were exported and integrated into the Python environment via Jupyter Notebook. This blockchain-based trading platform enabled secure monitoring and management of energy transactions, ensuring reliability and transparency in peer-to-peer energy trading.

Furthermore, the implementation of the Extended Kalman Filter in MATLAB was instrumental in identifying uncertainties within smart grids. Initially, manual data testing was conducted on the smart grid by varying voltage values to observe system behavior without EKF. Subsequently, the Smart Grid System was integrated with EKF, achieving the objective of detecting uncertainties effectively. The cascading of the Smart Grid System with EKF resulted in improved fault detection, thereby increasing the reliability and security of smart grid operations.

Despite the numerous advantages demonstrated, certain challenges remain, including the need for substantial infrastructure investment and the development of standardized protocols for broader adoption. Nonetheless, the promising outcomes of this study highlight the transformative potential of integrating blockchain technology and

optical fiber sensors into smart grids. As technological advancements continue, the widespread adoption of this approach is expected to further enhance the efficiency, security, and reliability of power grids, paving the way for a more resilient and intelligent energy infrastructure. By the end we achieved the following:

1. **Security and Transparency:**

Blockchain technology provides a secure and transparent platform for the smart grid system, protecting it against cyber threats, faults, and unauthorized access. This contributes to the overall security of the smart grid system.

2. Reliable Improved Communication:

The integration of blockchain technology and Fiber Bragg Grating (FBG) sensors enables real-time monitoring and control of energy generation, distribution, and consumption. This contributes to the overall efficiency of the smart grid system.

3. Real-time Fault Detection:

Fiber Bragg Grating (FBG) sensors provide real-time monitoring and control of electrical energy flow, enabling the efficiency and accuracy of the fault detection process. The integration of these sensors contributes to the overall reliability of the smart grid system.

4. Robustness and Resilience:

Smart grid systems need to be robust and resilient to uncertainties and disturbances to ensure uninterrupted power supply and grid resilience. By

effectively managing uncertainties through the EKF, smart grid operators can enhance the robustness of the system, mitigate potential risks, and improve the overall performance and stability of the grid under varying operating conditions.

7.2 Future Recommendations

To build upon the findings of this research, several areas for future work are recommended:

1. **Scalability and Performance Optimization** – Future studies should explore the scalability of the proposed system by testing its performance in larger and more complex smart grid environments. Performance optimization techniques, including advanced data compression and network efficiency improvements, should be investigated to enhance real-time processing capabilities.
2. **Development of Standardized Protocols** – Standardized communication and security protocols must be developed to ensure seamless interoperability between blockchain networks, smart grid components, and optical fiber sensors.
3. **Integration with Artificial Intelligence (AI) and Machine Learning (ML)** – Incorporating AI and ML techniques can further improve fault detection and anomaly prediction in smart grids. Future research should explore how predictive analytics can enhance system reliability.
4. **Energy Efficiency and Sustainability** – The energy consumption of blockchain technology remains a concern. Research should focus on energy-efficient

consensus mechanisms and sustainable blockchain solutions tailored for smart grid applications.

5. **Real-World Implementation and Testing** – Pilot projects and real-world implementation of the proposed system should be conducted to validate the theoretical and simulation-based findings. Collaboration with energy providers and regulatory bodies will be essential to facilitate practical deployment.
6. **Enhanced Security Measures** – Further research should investigate additional cybersecurity measures to strengthen blockchain-based smart grid systems against evolving threats, including quantum computing vulnerabilities.
7. **Economic and Policy Considerations** – The financial viability and regulatory implications of integrating blockchain and optical fiber sensor technology into smart grids should be explored. Cost-benefit analyses and policy recommendations can help drive adoption in the energy sector.

By addressing these future research directions, the effectiveness and adoption of blockchain-integrated smart grids can be further enhanced, leading to more sustainable and resilient energy infrastructures.

REFERENCES

[1] H. Farhangis, IEEE Power and Energy Magazine, 8, 18 (2010)

[2] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati and G. P. Hanckes, IEEE Transactions on Industrial Informatics, 7, 529 (2011)

[3] M. Swans, Blockchain: Blueprint for a new economy, (2015)

[4] C. Burger, A. Kuhlmann, P. Richard and J. Weinmanns, DENA German Energy Agency, (2016)

[5] J. Berst, "Electronomics: Why we need smart grid technology and infrastructure today," Xconomy, February 2009.

[6] B. Chameides, "The new smart grid: 21st century tech for the 21st century," Popular Science, February 2009.

[7] D. Coalition, "Smart meters, demand response, & lowincome customers," Demand Response and Smart Grid Coalition, August 2007.

[8] D. Coalition, "Demand response, smart grid, & renewable energy," Demand Response and Smart Grid Coalition, August 2007.

[9] E. Miller, "Smart grid overview," Trilliant, Inc., February 2009.

[10] Y. Mo, T. H. J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig and B. Sinopolis, Proceedings of the IEEE, 100, 195 (2012)

[11] R. K. Pandey and M. Misras, IEEE, 1 (2016)

[12] H. GHARAVI and R. GHAFURIANs, Proceedings of the IEEE, 99, (2011)

1911.03298

[13] H. Farhangi, \The path of the smart grid," Power and Energy Magazine, IEEE, vol. 8, no. 1, pp. 18{28, Jan.-Feb. 2010.

[14] R. R. Mohassel, A. S. Fung, F. Mohammadi, and K. Raahemifar, “A survey on advanced metering infrastructure and its application in smart grids,” in 2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 1–8, IEEE, 2014.

[15] Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli. Cyber–physical security of a smart grid infrastructure. Proceedings of the IEEE, 100(1):195–209, Jan 2012.

[16] Ekram Hossain, Zhu Han, and H Vincent Poor. Smart grid communications and networking. Cambridge University Press, 2012.

[17] Saida Elyengui, Riadh Bouhouchi, and Tahar Ezzedine. The Enhancement of Communication Technologies and Networks for Smart Grid Applications. International Journal of Emerging Trends & Technology in Computer Science, 2(6):107–115, 2013.

[18] Wenye Wang and Zhuo Lu. Cyber security in the Smart Grid: Survey and challenges. Computer Networks, 57(5):1344–1371, 2013.

[19] S. Chren, B. Rossi, B. Bühnova, and T. Pitner. Reliability data for smart grids: Where the real data can be found. In 2018 Smart City Symposium Prague (SCSP), pages 1–6, May 2018.

[20] Tanya L. Brewer Victoria Y. Pillitteri. Guidelines for smart grid cybersecurity. National Institute of Standards and Technology, 1:668, 2014.

[21] NIST Special Publication. NIST Special Publication 1108R2 NIST Framework and Roadmap for Smart Grid Interoperability Standards , NIST Special Publication 1108R2 NIST Framework and Roadmap for Smart Grid Interoperability Standards. NIST Special Publication, 0:1–90, 2012.

[22] P D Ray, R Harnoor, and M Hentea. Smart power grid security: A unified risk management approach. 44th Annual 2010 IEEE International Carnahan Conference on Security Technology, pages 276–285, 2010.

[23] Paria Jokar, Nasim Arianpoo, and Victor C. M. Leung. A survey on security issues in smart grids. Security and Communication Networks, 9(3):262–273, 2012.

[24] Rajendra Kumar Pandey and Mohit Misra. Cyber security threats — Smart grid infrastructure. 2016 National Power Systems Conference (NPSC), pages 1–6, 2016.

[25] Dharmendra Yadav and Anjali R Mahajan. Smart Grid Cyber Security and Risk Assessment : An Overview. International Journal of Science, Engineering and Technology Research (IJSETR), 4(9):3078–3085, 2015.

[26] Lindah Kotut and Luay A Wahsheh. Survey of cyber security challenges and solutions in smart grids. In Cybersecurity Symposium (CYBERSEC), 2016, pages 32–37. IEEE, 2016.

[27] Y. Yan, Y. Qian, H. Sharif, and D. Tipper. A survey on cyber security for smart grid communications. IEEE Communications Surveys Tutorials, 14(4):998–1010, Fourth 2012.

[28] Sanjay Goel, Yuan Hong, Vagelis Papakonstantinou, and Dariusz Kloza. Smart grid security. Springer, 2015.

[29] Nikos Komninos, Eleni Philippou, Andreas Pitsillides, and Senior Member. Survey in Smart Grid and Smart Home Security : Issues , Challenges and Countermeasures. IEEE Communications Surveys Tutorials, 16(4):1933–1954, 2014.

[30] M. M. Werneck, R. Allil, B. Ribeiro, and F. de Nazaré, "A guide to fiber bragg grating sensors," Current Trends in Short-and Long-Period Fibre Gratings; InTech: Rijeka, Croatia, pp. 1-24, 2013.

[31] K. Hill, Y. Fujii, D. C. Johnson, and B. Kawasaki, "Photosensitivity in optical fiber waveguides: Application to reflection filter fabrication," Applied physics letters, vol. 32, pp. 647-649, 1978.

[32] G. Meltz, W. W. Morey, and W. Glenn, "Formation of Bragg gratings in optical fibers by a transverse holographic method," Optics letters, vol. 14, pp. 823-825, 1989.

[33] M. Kreuzer, "Strain measurement with fiber Bragg grating sensors," HBM, Darmstadt, S2338-1.0 e, 2006.

[34] A. D. Kersey, M. A. Davis, H. J. Patrick, M. LeBlanc, K. P. Koo, C. G. Askins, et al., "Fiber grating sensors," Journal of Lightwave Technology, vol. 15, pp. 1442-1463, Aug 1997.

[35] G. R. Store, "Global Fiber Bragg Grating Sensors Sales Market Report 2018," 2018.

[36] Y. J. Rao, "In-fibre Bragg grating sensors," Measurement Science and Technology, vol. 8, pp. 355-375, Apr 1997.

[37] D. Arora, J. Prakash, H. Singh, and A. Wason, "Reflectivity and Braggs wavelength in FBG," International Journal of Engineering, vol. 5, pp. 341-9, 2011.

[38] A. Othonos and K. Kalli, Fiber Bragg gratings: fundamentals and applications in telecommunications and sensing: Artech House, 1999.

[39] Mohammed, A.; Melecio, J.I.; Djurovic, S. Electrical Machine Permanent Magnets Health Monitoring and Diagnosis Using an Air-gap Magnetic Sensor. IEEE Sens. J. 2020, 20, 5251–5259.

[40] Mohammed, A.; Djurovi´c, S. A study of distributed embedded thermal monitoring in electric coils based on FBG sensor multiplexing. Microprocess. Microsyst. 2018, 62, 102–109.

[41] Mohammed, A.; Djurovic, S. FBG Thermal Sensing Features for Hot Spot Monitoring in Random Wound Electric Machine Coils. IEEE Sens. J. 2017, 17, 3058–3067.

[42] Mohammed, A.; Hu, B.; Hu, Z.; Djurovi´c, S.; Ran, L.; Barnes, M.; Mawby, P.A. Distributed Thermal Monitoring ofWind Turbine Power Electronic Modules Using FBG Sensing Technology. IEEE Sens. J. 2020, 20, 9886–9894.

[43] K. O. Hill and G. Meltz, "Fiber Bragg grating technology fundamentals and overview," Journal of lightwave technology, vol. 15, pp. 1263-1276, 1997.

[44] K. O. Hill, B. Malo, F. Bilodeau, D. Johnson, and J. Albert, "Bragg gratings fabricated in monomode photosensitive optical fiber by UV exposure through a phase mask," Applied Physics Letters, vol. 62, pp. 1035-1037, 1993.

[45] HBM. (2018). Optical sensors based on Fiber Bragg Gratings (FBG). Available: https://www.hbm.com/en/1629/fiber-bragg-grating-technology-explained/

[46] W. W. Morey, G. Meltz, and W. H. Glenn, "Fiber optic Bragg grating sensors," in OE/FIBERS'89, 1990, pp. 98-107.

[47] A. Mohammed and S. Djurović, "FBG array sensor use for distributed internal thermal monitoring in low voltage random wound coils," in 2017 6th Mediterranean Conference on Embedded Computing (MECO), 2017, pp. 1-4.

[48] S. Ugale and V. Mishra, "Fiber Bragg grating modeling, characterization and optimization with different index profiles," International Journal of Engineering Science and Technology, vol. 2, pp. 4463-4468, 2010.

[49] A. Mohammed, S. Djurović, A. Smith, and K. Tshiloz, "FBG sensing for hot spot thermal monitoring in electric machinery random wound components," in Electrical Machines (ICEM), 2016 XXII International Conference on, 2016, pp. 2266-2272.

[50] W. Li, Y.-W. Li, X.-D. Han, and G.-Q. Yu, "The study of enhancing temperature sensitivity for FBG temperature sensor," in Machine Learning and Cybernetics, 2009 International Conference on, 2009, pp. 2746-2749.

[51] Z. Zhou and J. Ou, "Techniques of temperature compensation for FBG strain sensors used in long-term structural monitoring," in Microtechnologies for the New Millennium 2005, 2005, pp. 167-172.

[52] SmartFibres. (2018). Our Technology. Available: https://www.smartfibres.com/technology

[53] D. Barrera, V. Finazzi, J. Villatoro, S. Sales, and V. Pruneri, "Packaged optical sensors based on regenerated fiber Bragg gratings for high temperature applications," IEEE Sensors Journal, vol. 12, pp. 107-112, 2012.

[54] A. Azhari, R. Liang, and E. Toyserkani, "A novel fibre Bragg grating sensor packaging design for ultra-high temperature sensing in harsh environments," Measurement Science and Technology, vol. 25, p. 075104, 2014.

[55] Y. Zhang, L. Zhu, F. Luo, M. Dong, R. Yang, W. He, et al., "Comparison of metal-packaged and adhesive-packaged fiber Bragg grating sensors," IEEE Sensors Journal, vol. 16, pp. 5958-5963, 2016.

[56] M. Fabian, D. M. Hind, C. Gerada, T. Sun, and K. T. Grattan, "Comprehensive monitoring of electrical machine parameters using an integrated fibre Bragg grating-based sensor system," Journal of Lightwave Technology, 2017.

[57] Y. Zhang, D. Feng, Z. Liu, Z. Guo, X. Dong, K. Chiang, et al., "High-sensitivity pressure sensor using a shielded polymer-coated fiber Bragg grating," IEEE Photonics Technology Letters, vol. 13, pp. 618-619, 2001.

[58] F.-f. Tian, J.-w. Cong, B.-f. Yun, and Y.-p. Cui, "A fiber Bragg grating current sensor with temperature compensation," Optoelectronics Letters, vol. 5, pp. 347-351, 2009.

[59] M. L. Filograno, M. Pisco, A. Catalano, E. Forte, M. Aiello, C. Cavaliere, et al., "Triaxial Fiber Optic Magnetic Field Sensor for Magnetic Resonance Imaging," Journal of Lightwave Technology, vol. 35, pp. 3924-3933, 2017.

[60] C. Doyle, "Fibre Bragg Grating Sensors-An Introduction to Bragg gratings and interrogation techniques," Smart Fibres Ltd, pp. 1-5, 2003.

[61] L. Hoffmann, M. S. Müller, S. Krämer, M. Giebel, G. Schwotzer, and T. Wieduwilt, "Applications of fibre optic temperature measurement," Proc. Estonian Acad. Sci. Eng, vol. 13, pp. 363-378, 2007.

[62] J.-H. Lee, S.-G. Kim, H.-J. Park, and M. Song, "Investigation of Fiber Bragg Grating temperature sensor for applications in electric power systems," in Properties and applications of Dielectric Materials, 2006. 8th International Conference on, 2006, pp. 431-434.

[63] C. Hudon, C. Guddemi, S. Gingras, R. Leite, and L. Mydlarski, "Rotor temperature monitoring using fiber Bragg gratings," in IEEE Electrical Insulation Conference (EIC), 2016, 2016, pp. 456-459.

[64] Y.-J. Rao, "Recent progress in applications of in-fibre Bragg grating sensors," Optics and lasers in Engineering, vol. 31, pp. 297-324, 1999.

[65] Y. Wang, L. Liang, Y. Yuan, G. Xu, and F. Liu, "A two fiber bragg gratings sensing system to monitor the torque of rotating shaft," Sensors, vol. 16, p. 138, 2016.

[66] C. Hudon, M. Lévesque, M. Essalihi, and C. Millet, "Investigation of rotor hotspot temperature using Fiber Bragg Gratings," in Electrical Insulation Conference (EIC), 2017 IEEE, 2017, pp. 313-316.

[67] A. Singh, S. Berggren, Y. Zhu, M. Han, and H. Huang, "Simultaneous strain and temperature measurement using a single fiber Bragg grating embedded in a composite laminate," Smart Materials and Structures, vol. 26, p. 115025, 2017.

[68] P. Wang, J. Liu, F. Song, and H. Zhao, "Quasi-distributed temperature measurement for stator bars in large generator via use of Fiber Bragg Gratings," in Strategic Technology (IFOST), 2011 6th International Forum on, 2011, pp. 810-813.

[69] Z. Gao, X. Zhu, Y. Fang, and H. Zhang, "Active monitoring and vibration control of smart structure aircraft based on FBG sensors and PZT actuators," Aerospace Science and Technology, vol. 63, pp. 101-109, 2017.

[70] W. Ecke and K. Schröder, "Fiber Bragg grating sensor system for operational load monitoring of wind turbine blades," in Smart Sensor Phenomena, Technology, Networks, and Systems 2008, 2008, p. 69330I.

[71] M. Optics, "Sensing Solutions."

[72] FBGS. FIBER BRAGG GRATING (FBG) SENSOR PRINCIPLE. Available: https://www.fbgs.com/technology/fbg-principle/

[73] N. INSTRUMENTS. (2018). PXI Universal Input Module. Available: http://www.ni.com/en-gb/support/model.pxie-4844.html

[74] Kucuksari, S.; Karady, G. Experimental comparison of conventional and optical current transformers. IEEE Trans. Power Delivery 2010, 25, 2455-2463.

[75] Gang, Z.; Shaohui, L.; Zhipeng, Z.; Wei, C. A novel electro-optic hybrid current measurement instrument for high-voltage power lines. IEEE Trans. Instru. Meas. 2001, 50, 1, 59–62.

[76] Bohnert, K.; Gabus, P.; Nehring, J.; Brandle, H. Temperature and Vibration Insensitive Fiber-Optic Current Sensor. J. Lightwave Tech. 2002, 20, 267-276.

[77] Rochford, K.B.; Rose, A.H.; Day, G.W. Magneto-optic sensors based on iron garnets. IEEE Trans. Mag. 1996, 32, 4113-4117.

[78] Law, C.T.; Bhattarai, K.; Yu, D.C. Fiber-optics-based fault detection in power systems. IEEE Trans. Power Delivery 2008, 23, 1271-1279. 6. Li, Y.; Li, W.; Han, X.; Li, J. Application of multi-sensor information fusion technology in the power transformer fault diagnosis. In Proceedings of International Conference on Machine Learning and Cybernetics, Boading, China, July 2009; pp. 29-33. 7. Orr, P.; Niewczas, P.; Dysko, A.; Booth, C. FBG-based fiber-optic current sensors for power systems protection: Laboratory evaluation. In the Proceedings of the 44th International Universities Power Engineering Conference (UPEC), Leuven, Belgium, May 2009; pp. 1-5.

[79] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2009, http://www.bitcoin.org/bitcoin.pdf.

[80] Brandon T. McDaniel, Samreen Mahmood, Mehmood Chadhar, Selena Firmin. Undecided. Human Behavior and Emerging Technologies, 2022:7384000, 2022.

[81] Hao Liang Peng Zhuang, Talha Zamir. Blockchain for cybersecurity in smart grid: A comprehensive survey. IEEE Transactions on Industrial Informatics, 17(1):3–19, 2021.

[82] Arshdeep Bahga, Vijay K. Madisetti. Blockchain platform for industrial internet of things. Journal of Software Engineering and Applications, 9(10):[36]533–546, 2016.

[83] Muhammad Baqer Mollah, Jun Zhao, Dusit Niyato, Kwok-Yan Lam, Xin Zhang, Amer M.Y.M. Ghias, Leong Hai Koh, Lei Yang. Blockchain for future smart grid: A comprehensive survey. IEEE Internet of Things Journal, pages 1–1, 2020.

[84] Li, Yun and Teng, Yun and Cao, Rongrong and Li, Ningfeng. Research on coordination control system of virtual power plant based on blockchain. 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP), pages 1377–1383, 2019.

[85] Ralph C. Merkle. A digital signature based on a conventional encryption function. Conference on the theory and application of cryptographic techniques, 293:369–378, 1987.

[86] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151:1–32, 2014.

[87] Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, Mubashir Husain Rehmani. Applications of blockchains in the internet of things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 21(2):1676–1717, 2019.

[89] Julija Golosova, Andrejs Romanovs. The advantages and disadvantages of the blockchain technology. 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), pages 1–6, 2018.

[90] Zhaoyang Dong, Fengji Luo, Gaoqi Liang. Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. Journal of Modern Power Systems and Clean Energy, 6:958—-967, Jul. 2018.

[91] Markus Jakobsson, Ari Juels. Proofs of Work and Bread Pudding Protocols(Extended Abstract), pages 258–272. Springer US, Boston, MA, 1999.

[92] Jason Spasovski, Peter Eklund. Proof of stake blockchain: Performance and scalability for groupware communications. Conference paper, November 2017.

[93] Proof of stack. Accessed: November 2022, https://en. bitcoin.it/wiki/Proof of Stake.

[94] Cong T. Nguyen, Dinh Thai Hoang, Diep N. Nguyen, Dusit Niyato, Huynh Tuong Nguyen, Eryk Dutkiewicz. Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications, and opportunities. IEEE Access, 7:85727–85745, 2019.

[95] Nick Szabo. Smart contracts : Building blocks for digital markets. 2018.

[96] DPoS. Accessed: October 2022. https://en.bitcoinwiki.org/wiki/DPoS.

[97] LPoS. Leasing proof of stake (pos/lpos). Accessed: October 2022, https://tokens-economy.gitbook.io/consensus/chain-based-proof-ofstake/leasing-proof-of-stake-pos-lpos.

[98] Iddo Bentov, Char-Tung Lee, Alex Mizrahi, Meni Rosenfeld. Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]y. SIGMETRICS Perform. Evaluation Rev., 42:34–37, 2014.

[99] Tuyet Duong, Lei Fan, Jonathan Katz, Phuc Thai, Hong-Sheng Zhou. 2-hop blockchain: Combining proof-of-work and proof-of-stake securely. European Symposium on Research in Computer Security, 2020.

[100] Alexander Chepurnoy, Tuyet Duong, Lei Fan, Hong-Sheng Zhou. Twinscoin: A cryptocurrency via proof-of-work and proof-of-stake. Cryptology ePrint Archive, page 232, 2017.

[101] Proof of Burn. Accessed: October 2022, https: //en.bitcoin.it/wiki/Proof of burn.

[102] Slimcoin a peer-to-peer crypto-currency with proof-of-burn. Accessed: October 2022, https://slimcoin.info/whitepaperSLM.pdf.

[103] Lin Chen, Lei Xu, Nolan Shah, Zhimin Gao, Yang Lu, Weidong Shi. On security analysis of proof-of-elapsed-time (poet). International Symposium on Stabilization, Safety, and Security of Distributed Systems, pages 282– 297, 2017.

[104] Sawtooth hyperledger. Accessed: November 2023, https://sawtooth.hyperledger.org/.

[105] Stefano De Angelis, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, Vladimiro Sassone. Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain. University of Southampton Institutional Repository, 2018.

[106] Parity Ethereum. Accessed: November 2022, https://wiki.parity.io/parity-ethereum.

[107] Proof of reputation (por). Accessed: November 2022, https://tokenseconomy.gitbook.io/consensus/chain-based-proof-of-capacityspace/proof-of-reputation-por.

[108] Consensus. Accessed: November 2022, https://tokenseconomy.gitbook.io/consensus/chain-based-proof-of-capacityspace/proof-of-reputation-por.

[109] Sidharth Shyamsukha, Pronaya Bhattacharya, Farnazbanu Patel, Sudeep Tanwar, Rajesh Gupta, Emil Pricop. Porf: Proof-of-reputation-based consensus scheme for fair transaction ordering. pages 1–6, 2021.

[110] Types of blockchains–decide which one is better for your investment needs. Data Flair, Accessed: November, 2022, https://dataflair.training/blogs/types-of-blockchain/.

[111] Yohannes T. Aklilu, Jianguo Ding. Survey on blockchain for smart grid management, control, and operation. Energies, 15(1), 2022.

[112] Blockchain for hospitality. Accessed: November 15, 2022, https://www.hospitalitynet.org/file/152008497.pdf.

[113] Omar Dib, Kei-Leo Brousmiche, Antoine Durand, Eric Thea, Elyes Ben Hamida. Consortium blockchains: Overview, applications, and challenges. Int. J. Adv. Telecommun, 11:51–64, 2018.

[114] Seyed Mojtaba Hosseini Bamakan, Amirhossein Motavali, Alireza Babaei Bondarti. A survey of blockchain consensus algorithms performance evaluation criteria. Expert Systems with Applications, 154:113385, 2020.

[115] Hamid Malik, Ahsan Manzoor, Mika Ylianttila, Madhusanka Liyanage. Performance analysis of blockchain based smart grids with ethereum and hyperledger implementations.
2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pages 1– 5, 2019.

[116] K. Kim and J. M. Justl, "Potential Antitrust Risks in the Development and Use of Blockchain," Journal of Taxation & Regulation of Financial Institutions, Article vol. 31, no. 3, pp. 5-16, Spring2018 2018.

[117] A. Rosic. What is hashing? [step-by-step guide-under hood of blockchain] [Online]. Available: https://blockgeeks.com/guides/what-is-hashing/

[118] F. Glaser, "Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis," 2017.

[119] J. W. Moein Sabounchi, "Towards resilient networked microgrids: Blockchain-enabled peer-to-peer electricity trading mechanism," ed: IEEE, 2017, p. 1.

[120] F. Al-Turjman and M. Abujubbeh, “Iot-enabled smart grid via SM: An overview,” Future Generation Computer Systems, vol. 96, pp. 579–590, 2019.

[121] Y. Saleem, N. Crespi, M. H. Rehmani, and R. Copeland, “Internet of things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions,” IEEE Access, vol. 7, pp. 62 962–63 003, 2019.

[122] Y. Kabalci, E. Kabalci, S. Padmanaban, J. B. Holm-Nielsen, and F. Blaabjerg, “Internet of things applications as energy internet in smart grids and smart environments,” Electronics, vol. 8, no. 9, p. 972, 2019.

[123] K. Wang, J. Yu, Y. Yu, Y. Qian, D. Zeng, S. Guo, Y. Xiang, and J. Wu, “A survey on energy internet: Architecture, approach, and emerging technologies,” IEEE Systems Journal, vol. 12, no. 3, pp. 2403–2416, 2017.

[124] C. Yijia, L. Qiang, T. Yi, L. Yong, C. Yuanyang, S. Xia, and Z. Yao, “A comprehensive review of energy internet: basic concept, operation and planning methods, and research prospects,” Journal of Modern Power Systems and Clean Energy, vol. 6, no. 3, pp. 399–411, 2018.

[125] Z. Dong, J. Zhao, F. Wen, and Y. Xue, “From smart grid to energy internet: basic concept and research framework,” Automation of electric power systems, vol. 38, no. 15, pp. 1–11, 2014.

[126] S. Chen, H. Wen, J. Wu, W. Lei, W. Hou, W. Liu, A. Xu, and Y. Jiang, "Internet of things based smart grids supported by intelligent edge computing," IEEE Access, vol. 7, pp. 74 089–74 102, 2019.

[127] S. Hussain, F. Nadeem, M. A. Aftab, I. Ali, and T. S. Ustun, "The emerging energy internet: Architecture, benefits, challenges, and future prospects," Electronics, vol. 8, no. 9, p. 1037, 2019.

[128] S. Nakamoto et al., "Bitcoin: A peer-to-peer electronic cash system," 2008.

[129] Chen, Sijie, et al. "Blockchain for Decentralized Optimization of Energy Sources: EV Charging Coordination via Blockchain-Based Charging Power Quota Trading." Blockchain-Based Smart Grids, (2020)

[130] Amini, M. Hadi. "Decentralized Operation of Interdependent Power and Energy Networks: Blockchain and Security." Blockchain-Based Smart Grids, (2020).

[131] Bayati, Navid, et al. "Blockchain-Based Protection Schemes of DC Microgrids." Blockchain-Based Smart Grids, (2020).

[132] Kouveliotis-Lysikatos, Iasonas, et al. "Blockchain-Powered Applications for Smart Transactive Grids." 2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), (2019).

[133] Wang, Shen, et al. "Energy Crowdsourcing and Peer-to-Peer Energy Trading in Blockchain-Enabled Smart Grids." IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 8, (2019)

[134] Sikeridis, Dimitrios, et al. “A Blockchain-Based Mechanism for Secure Data Exchange in Smart Grid Protection Systems.” 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), (2020)

[135] R. Tourani, S. Misra, T. Mick, and G. Panwar. Security, privacy, and access control in information-centric networking: A survey. EEE Communications Surveys and Tutorials, 20(1):566–600, 2018.

[136] John M. Lewis and S.Lakshmivarahan. Dynamic Data Assimilation, a Least Squares Approach. 2006.

[137] A. Q. Al-Shetwi and S. Muhamad Zahim, "Sizing and design of PV array for photovoltaic power plant connected grid inverter," in The National Conference for Postgraduate Research (NCON-PGR), Pekan, Pahang, Sept, 2016, pp. 24-25.

[138] N. Femia, G. Petrone, G. Spagnuolo, and M. Vitelli, "Optimizing duty-cycle perturbation of P&O MPPT technique," vol. 3, S. U. DIIIE, Italy, Ed., ed. Piscataway, NJ, USA, USA: IEEE, 2004, pp. 1939-1944

[139] C. Kalpana, C. S. Babu, and J. S. Kumari, "Design and implementation of different MPPT algorithms for PV system," International Journal of Science, Engineering and Technology Research (IJSETR) Volume, vol. 2, no. 10, pp. 1926-1933, 2013.

[140] S. K. Kollimalla and M. K. Mishra, "A novel adaptive P&O MPPT algorithm considering sudden changes in the irradiance," IEEE Transactions on Energy conversion, vol. 29, no. 3, pp. 602-610, 2014.

[141] S. K. Kollimalla and M. K. Mishra, "Variable perturbation size adaptive P&O MPPT algorithm for sudden changes in irradiance," IEEE Transactions on Sustainable Energy, vol. 5, no. 3, pp. 718-728, 2014.

[142] B. Subudhi and R. Pradhan, "A comparative study on maximum power point tracking techniques for photovoltaic power systems," IEEE Transactions on sustainable energy, vol. 4, no. 1, pp. 89-98, 2013.