Faculty of Engineering

Development of Blockchain-Based Secure Wide Area Measurement System for Smart Grid Integration

Md Abu Sayed

Master of Engineering
2026

Development of Blockchain-Based Secure Wide-Area Measurement System for Smart Grid Integration

Md Abu Sayed

A thesis submitted

In fulfillment of the requirements for the degree of Master of Engineering

(Electrical Engineering)

Faculty of Engineering
UNIVERSITI MALAYSIA SARAWAK
2026

DECLARATION

I declare that the work in this thesis was carried out in accordance with the regulations of Universiti Malaysia Sarawak. Except where due acknowledgements have been made, the work is that of the author alone. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

……

Signature

Name: Md Abu Sayed

Matric No.: 21020049

Faculty of Engineering

Universiti Malaysia Sarawak

Date: 20/02/2026

ACKNOWLEDGEMENT

I would like to take this opportunity to give full credit to my supervisor for direct contribution throughout my research. My sincere gratitude goes to my parents for their unconditional support throughout the thesis.

Also, my sincere acknowledgement to the Centre for Graduate Studies (CGS), for the advice and support given during period of my study in Universiti Malaysia Sarawak.

Finally, I would like to thank the management of the Universiti Malaysia Sarawak for making it possible for me to complete my study here in Sarawak. Thank you all.

ABSTRACT

The increasing penetration of inverter-based generation has made modern power grids highly dependent on synchrophasor based WAMS and two-way communication infrastructures. As a result, the deployment of Phasor Measurement Units (PMUs) at substation buses has grown significantly. This rapid deployment has also increased the volume of data transmission, thereby expanding the surface of unauthorized access. Blockchain (BC) technology has recently been proposed as a promising solution to preserved PMUs data integrity and confidentiality. In conventional IoT-based BC architectures, each sensor reading is often processed as an individual transaction resulting network congestion and processing overhead that negatively affect real-time data processing. To overcome the limitation, this thesis proposed a subdivision-based BC-integrated WAMS framework utilizing a distributed consensus algorithm and fast signature scheme. The primary objective of the thesis is to investigate data communication, automatic monitoring of electrical parameters and security aspects in the substation domain. This is achieved through the using of MATLAB-SCADA and Hyperledger Fabric based co-simulation test bed. Subsequently, the thesis demonstrates the implementation of proposed framework for secure phasor data sharing. Additionally, the thesis delves into discussing the performance metrics and transaction handling ability of the proposed scheme in comparison with existing state-of-the-art. Experimental results from quantitative analysis highlight the impact of significant reduction in transaction volume by 99.4–99.8 %. Therefore, queuing delay becomes negligible, and latency drops by 3-5s approximately that decrease network congestion issues and improve overall scalability.

Keywords: Smart grid, WAMS, synchro phasor measurement, cyber security, cryptography, blockchain.

Pembangunan Pengukuran Kawasan Luas Selamat Berasaskan Blockchain untuk Integrasi Grid Pintar

ABSTRAK

Penembusan penjanaan berasaskan inverter yang semakin meningkat telah menjadikan grid kuasa moden sangat bergantung pada WAMS berasaskan sinkrofasor dan infrastruktur komunikasi dua hala. Akibatnya, penggunaan Unit Pengukuran Fasor (PMU) di bas pencawang telah berkembang dengan ketara. Penggunaan pesat ini juga telah meningkatkan jumlah penghantaran data, sekali gus meluaskan permukaan akses tanpa kebenaran. Teknologi Rantaian Blok (BC) baru-baru ini telah dicadangkan sebagai penyelesaian yang menjanjikan untuk memelihara integriti dan kerahsiaan PMU. Dalam seni bina berasaskan BC konvensional, setiap bacaan sensor sering diproses sebagai transaksi individu yang mengakibatkan kesesakan rangkaian dan overhed pemprosesan yang memberi kesan negatif kepada pemprosesan data masa nyata. Untuk mengatasi batasan ini, tesis ini mencadangkan rangka kerja WAMS bersepadu BC berasaskan subbahagian menggunakan algoritma konsensus teragih dan skema tandatangan pantas.Objektif utama tesis ini adalah untuk menyiasat komunikasi data, pemantauan automatik parameter elektrik, dan aspek keselamatan dalam domain substation. Keputusan eksperimen dari analisis kuantitatif menunjukkan impak signifikan daripada pengurangan jumlah transaksi sebanyak 99.4–99.8%; dengan itu, kelewatan dalam antrian menjadi boleh diabaikan, dan latensi menurun sebanyak 3-5s secara kira-kira serta meningkatkan throughput dan latensi.

Kata kunci: *Grid pintar, WAMS, pengukuran fasor segerak, keselamatan siber, kriptografi, rantaian sekat.*

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AMI	Advance Metering Infrastructure
BC	Blockchain
DERs	Distributed Energy Resources
DIAM	Decentralized Identity and Access Management
DLT	Distributed Ledger Technology
DFT	Discrete Fourier Transform
ECDSA	Elliptic Curve Digital Signature Algorithm
EV	Electric Vehicle
EdDSA	Edwards-curve Digital Signature Algorithm
GPS	Global Positioning System
IDS	Intrusion Detection System
IED	Intelligent Electronic Devices
MQTT	MQ Telemetry Transport
OPC	Open Platform Communications
OPC UA	OPC Unified Architecture
PDC	Phasor Data Concentrator
PKI	Public Key Infrastructure
PMU	Phasor Measurement Unit
SCADA	Supervisory Control and Data Acquisition
TX	Transaction
UI	User Interface
VPN	Virtual Private Network
WAMS	Wide Area Measurement System

CHAPTER 1

INTRODUCTION

1.1 Study Background

The modern power grid has embraced wide area measurement system (WAMS) and heterogeneous communication architecture to enhance high-resolution grid monitoring and dynamic control. With the increasing reliance on data obtained by measurements and monitoring devices, protecting data integrity and confidentiality against potential cyber-threat in the smart grid is gradually becoming challenging. Hence, secure data sharing is crucial for efficient and safer power grids. A typical WAMS comprises Phasor Measurement Unit (PMU), Phasor Data Concentrator (PDC), and a two-way communication architecture following IEEE C37.118 protocols for real-time monitoring. However, the communication architecture of WAMS is centralized and lacks robust security mechanisms, making it vulnerable to a single point of failure (Sufyan et al., 2021). Therefore, phasor data exchanges between the PMU and PDC must be protected against malicious access and malfunction. Although increase PMU integration in the different parts of the power grid has revolutionized situational awareness and grid visibility. These PMUs are exposed to malicious attackers that expanding the surface of unauthorized access. As a result, PMUs are exposed to cyber threats such as unauthorized manipulation of phasor data because of the lack of robust device management and data authentication. Hence, verifying the devices and achieving trust before exchanging data is essential. Blockchain (BC) or Distributed Ledger Technology (DLT) has shown great potential to preserve energy data integrity and confidentiality using cryptographic properties (Thakkar et al., 2019; Zhao et al., 2020).

1.2 Problem Statement

With the increasing penetration of inverter base energy generation, the modern power grid, vastly relies on PMU based WAMS and two-way communication topologies. Hence, the installation of PMU devices has been rising exponentially at the substation buses. This integration enhances the real-time monitoring and analysis of the power grid's dynamic states that improves the situational awareness and grid visibility (Xu et al., 2022). However, the growing installation of PMU devices has increased the volume of data transmission, thereby expanding the surface of unauthorized access (Kateb et al., 2019; Ravikumar et al., 2020; Schweitzer Engineering Laboratories, 2020). Therefore, any malicious access such as data alteration (e.g., man-in the middle attack), stealthy modification (false data injection) could breach the utility data integrity and confidentiality (Zhuang et al., 2021a). This is mainly because of inadequate device management and data authentication protocols (Dehalwar et al., 2022a). Hence, it is crucial to verify the devices and establish trust before data exchange. Implementing robust access management, device verification, and data authentication can effectively safeguard the PMU data integrity and confidentiality (Dehalwar et al., 2022b). BC technology has shown great potential to protect data integrity and confidentiality. A wide range of research paper (Ahlund et al., n.d.; Shen et al., 2020; Zhuang et al., 2021b) showcased the incorporation of BC technology to enhance smart grid data management.

BC as a core technology efficiently preserves data integrity and confidentiality. This is achieved through incorporation with data authentication and source verification using asymmetric cryptography and hashing functions (Bhattacharjee et al., 2020a; Thakkar et al., 2019a). Recent studies highlight the usage of BC technology for securing data management (Guo et al., 2022; Kong et al., 2020) as well as ensuring the integrity and confidentiality of energy data (Mylrea & Gourisetti, 2017; Sikeridis et al., 2020; Vasukidevi & Sethukarasi,

2022; Yang et al., 2019). Thus, incorporating BC technology on top of the communication layer can significantly enhance secure data sharing.

In BC-based WAMS architecture, the PMU devices function as client nodes, capturing measurements and storing them in immutable databases. Each measurement from a PMU is treated as a BC transaction, encapsulating either phasor data or control instructions. Despite its potential benefits, the conventional blockchain framework faces significant challenges related to throughput and latency, particularly when applied to big data-driven WAMS applications (Fan et al., 2020; Ferrag & Shu, 2021). Considering the data recording rate of a PMU (30 to 60 samples/s) (Follum et al., 2021; Xu et al., 2021), if every PMU reading is treated as a separate transaction, the network is flooded with a high volume of small transactions that can cause network congestion in the system, leading to delays in the process of each transaction. Network segmentation and data compression techniques can effectively reduce data volume and size. For instance, a WAMS can be divided into subdivisions, with PMUs connected to the PDC through the clustered network

In contrast, the time it takes for each transaction to be confirmed and added to the BC increases, leading to higher overall latency. Therefore, data rate and the speed of receiving big data from PMU devices might be infeasible to process (Asefi et al., 2022), resulting in network congestion in the BC-enabled system. This is primarily due to computational complexity of cryptographic functions and consensus difficulties (Colaco et al., 2020) which are often incompatible with the stringent real-time data processing demands of WAMS. For instance, all participating peer nodes broadcast and verify every transaction and block in the traditional BC architecture. Thus, peer node data verification increases processing overhead and block confirmation time. However, permissioned BC with partially centralized network could reduce the data verification time.

1.3 Motivation and Research Problems

In the recent transformation of WAMS due to the massive RE integration into the grid, PMUs generate high-frequency data for real-time monitoring and control. A typical WAMS function through a collective technological effort relies on PMU, PDC, and centralized communication architecture. Whereas PMU is a logical device installed in power buses and provides precise time-synchronized measurement using a standard Global Positioning System (GPS) (Lee & Centeno, 2019). The collected measurements are sent to PDC through vulnerable communication network. However, data sharing via vulnerable communication network exposes to malicious intruders who can exploit the system parameters. Therefore, traditional data management approaches are insufficient to meet the stringent real-time, high-volume, and secure communication demands of WAMS. The illustration of WAMS architecture in Figure 1.1 indicates the traditional nature of data communication between the measurement devices and the control centre. Unauthorized access, data manipulation, and latency directly threaten the grid's stability and reliability.

BC technology provides excellent data management features such as data authentication, device identification, and access control mechanisms using a hashing function, digital signature, and consensus to address smart grid data integrity and confidentiality (Banoun & Diarra, 2021; Dehalwar et al., 2022; X. Fan et al., 2020). In BC-enabled WAMS architecture, every PMU integrated into the network undergoes prior verification, and the data provided by these devices is authenticated using cryptographic mechanisms. Hence, only verified PMUs recorded phasor data in a decentralized and immutable database that could inherently establish trust between the PMU devices and back-end servers. Each measurement is recorded as a transaction, organized chronologically in blocks, and linked through hashes to form an immutable ledger.

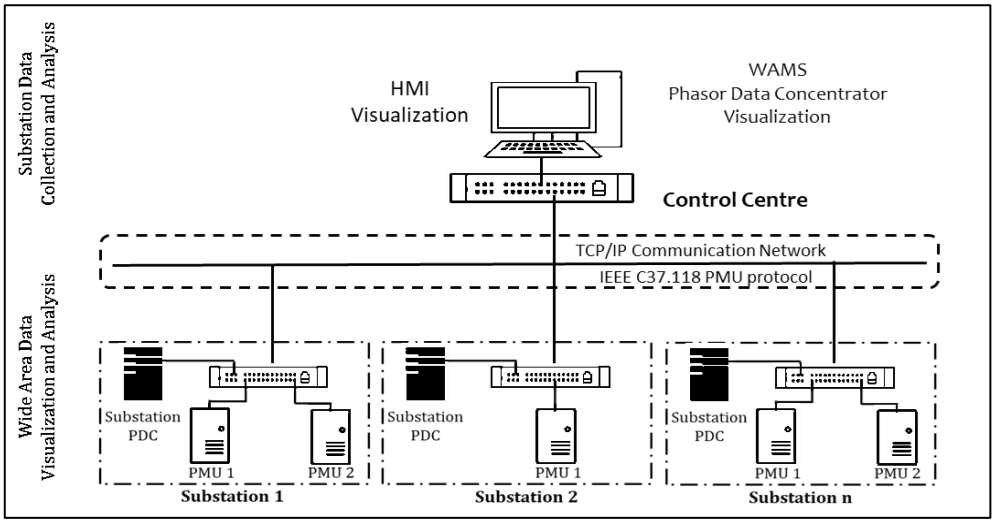


Figure 1.1: Traditional WAMS Architecture (Gore & Kande, 2015)

However, conventional BC systems are not optimized for high-frequency, big data applications like PMU-based WAMS due to their low throughput and high latency. The motivation for this research stems from the crucial need to design a scalable and lightweight blockchain framework that can maintain data integrity and confidentiality support real-time data exchange and adapt to the increasing number of PMUs without compromising performance. This research seeks to bridge the gap between secure communication and scalable blockchain infrastructure in smart grid environments, ensuring a reliable and future-proof WAMS ecosystem. Therefore, the thesis addresses the following research questions to address these issues.

i. What is the resilient WAMS architecture for two-way communication in smart grid?

ii. How does utility protect the phasor data integrity and confidentiality in the WAMS network?

iii. Is the BC-integrated WAMS framework scalable enough to handle real-time data recording?

iv. How to analyse the performance of BC integrated WAMS framework and its scalability?

1.4 Thesis Contribution and Novelties

To ensure secure and tamper-proof phasor data recording, a private, permissioned blockchain is proposed. This architecture offers data authentication, device identification, and access control mechanisms using a hashing function, digital signature effectively minimizing cybersecurity risks such as unauthorized access, data tampering, and message injection, even in a centralized setting. In this model, pre-authorized nodes such as control centers and substations participate in data recording and validation. The architecture limits external access and enhances security through strict access control, identity-based authentication, and cryptographically secured transactions.

To address network congestion challenges, a scalable BC framework adapted for WAMS is necessary. Such a framework must support high transaction throughput, low latency, and efficient data management while maintaining the security and integrity of the data. The architectural framework should ensure secure and efficient real-time data exchange while overcoming the limitations of conventional BC systems in terms of high transaction processing and network scalability. Therefore, specific challenges addressed in the proposed framework are network congestion issue while protecting phasor data integrity and confidentiality during transmission. Therefore, the framework can handle increasing number of transactions with increased nodes, reducing the transaction processing time and block

confirmation time to meet the real-time requirements. Nevertheless, a lightweight consensus algorithm efficiently supports to processing a high volume of data transaction.

This research introduces a novel framework of BC integrated sub-division based WAMS framework with a lightweight consensus algorithm for robust and resilient data exchanges. The proposed framework divides the WAMS into “n” sub-divisions, where PMU nodes are connected in a clustered network. In each sub-division, the measurements of all PMU nodes in the cluster have been accumulated for one second and packed into a single transaction (TX) instead of considering every measurement as a transaction. This in turns decreases the number of transactions and improves the throughput in the network. Then collected transactions are transferred to the PDC gateway node for verification. While local PDC verified the transactions, it is considered as valid instead of all peer node verification, resulting in less block confirmation time, which helps in higher throughput and lower latency. In this manner, the proposed approach secures data recording, sharing and addresses scalability issues in the WAMS network. The novelties and contributions of the thesis are highlighted in the following points:

i. Proposed BC designed sub-division-based WAMS architecture to address high-scale data transaction requirements in real-time

ii. Propose the use of data aggregation and compression at the PMU to improve the network congestion issue and transaction throughput

iii. Proposed a lightweight consensus algorithm for fast data verification and block confirmation and improve transaction latency

1.5 Research Objectives

This research proposes BC-integrated WAMS to protect phasor data integrity and confidentiality in smart grid. In this regard, the following objectives are to be achieved:

i. To investigate the resilient of the existing WAMS architecture, two-way communication system, and data security

ii. To develop a subdivision-based BC integrated WAMS framework for phasor data protection in a two-way communication environment

iii. To implement the BC-based WAMS framework with Hyperledger Fabric-MATLAB-based co-simulation test bed

iv. To analyse the performance of the proposed framework

1.6 Research Goal and Hypothesis

This research is focused on the design and implementation of a scalable BC-based framework for ensuring the integrity, and confidentiality of PMU data in WAMS. The primary goal is to investigate the WAMS and two-way phasor data communication in smart grid environment. Nevertheless, this study addresses the challenges of network congestion, high data rates, and latency that arise when BC is integrated into real-time smart grid communication infrastructures. This is achieved through a sub-division based WAMS where PMUs group in cluster. Data readings of all PMUs at the individual cluster are summed up at a specific time window as a data segment. Then every data segment considered as single transaction instead of every PMU reading as separate transaction. Meanwhile, A custom consensus protocol is implemented to reduce block confirmation time and computational

overhead. The proposed framework is designed to fit in the IoT-scale environment with lower computation requirements.

The framework is implemented by MATLAB-SCADA and Hyperledger Fabric based testbed in co-simulation environment. The PMU data is simulated using DERs integrated IEEE 9-bus, 39-bus and 118-bus hybrid systems, with data rate at 50 samples per second to reflect real-time operating conditions, aligning the study with real world deployment scenarios and testing the BCs data handling capabilities. The integration of DERs and sizes were intentionally chosen to create dynamic and realistic PMU data loads. Lossless time-series compression (e.g., Gorilla algorithm) (Iqbal & Keskar, 2021) is employed to reduce transaction size and minimize network load. All tests and performance evaluations are carried out in a controlled lab environment, using simulating tools (e.g., Node-RED, Python, Linux-based nodes) to validate the architecture under realistic data loads. Nevertheless, the research does not involve physical PMU device deployment or field testing in real substations. Particularly, the research hypothesis has been listed as follows to make justification of research objectives:

i. The investigation will demonstrate the data sharing of WAMS

ii. The proposed subdivision-based BC framework will achieve higher throughput and lower latency compared to conventional BC architectures

iii. The proposed BC framework will allow to handle real-time data streaming in an increasing number of PMU nodes

iv. The proposed BC framework will provide potential improvement in terms of efficiency, and scalability comparing existing solutions.

1.7 Thesis Structure

The thesis is organized by following sections as follows:

Chapter 1-Introduction: This chapter introduces the research background and identifies the key challenges. The problem statement is clearly formulated, followed by research questions, objectives, and hypotheses that shape the study. The chapter also outlines the thesis contributions.

Chapter 2- Literature Review: The chapter provides a detailed overview of WAMS, blockchain based architecture. Besides the theoretical foundation, chapter 2 explores the research gap and existing work relevant to proposed architecture.

Chapter 3- Methodology: This chapter presents the research methodology, beginning with the modelling of a DER-integrated hybrid power system and the simulation of synchrophasor-based monitoring. Meanwhile, two case studies—one is IEEE bus systems without BC, and another one is with BC—are designed to implement the proposed framework. However, case study 3 explain the performance evaluation of proposed framework with increased PMU nodes.

Chapter 4- Results and Discussion: Chapter 4 discusses the outcomes of each case study, with a comparative analysis of WAMS performance with and without BC integration. Performance metrics such as block size, latency, and transaction throughput confirm the feasibility and effectiveness of the proposed BC-enhanced WAMS.

Chapter 5-Conclusion and Recommendation: The final chapter summarizes the key findings and validates the proposed solution’s ability to address the identified research problem. Recommendations for future research work include exploring scalable consensus algorithms and deploying the proposed framework in real-world testbeds for further validation.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

The conventional power grid undergoes a rapid transition towards the smart grid that accommodate additional renewable energy (RE) and electric vehicle (EV) to address carbon footprint. Hence, power system today is becoming even more complex to monitor and control with the high penetration of RE integration. Therefore, utilities continuously adopt advanced sensing and measuring technologies at all levels of the network to provide real-time monitoring of the power grid across vast geographical areas. The consequences of US electrical power system blackout in 2004 (Appasani & Mohanta, 2018) and similar other blackout around the world (Huang et al., 2018) forces the power system to embrace WAMS that utilized synchro phasor measurement technology for high-resolution monitoring and real-time fault detection (Appasani & Mohanta, 2018). Regardless of the various potential aspects, phasor measurement has increased the volume of data transmission, thereby expanding the surface for unauthorized access. As a result, the cyber-security risk in smart grid infrastructure is gradually increasing, posing a challenge for utilities to protect data integrity and confidentiality (CISCO Systems, 2012). Hence, proper device identification and data authentication is necessary for robust and resilient data transfer. Blockchain (BC) or distributed ledger technology (DLT) is highly potential to address data integrity and confidentiality issues. Researchers are increasingly discussing the use of BC technology as a mitigation technique to address cybersecurity issues in smart grids (Hossain et al., 2020; Kishore et al., 2021; Marchesi, 2018).

2.2 Smart Grid

Smart Grid is a modernized electrical network that enables two-way data and energy flows and capable of self-healing and control capabilities against energy disturbance as stated by U.S. Energy Independence and Security Act of 2007 (EISA) (EISA, 2007). Hence it indicates to an evolutionary change of traditional power grid that's integrated with upgraded digital technology and two-way communication network infrastructure. In the conventional power grid, electricity flows from the power plant to consumers in a one-way direction. Utilities manage the grid by forecasting demand based on historical consumption trends, enabling them to plan and adjust the generation and distribution of electricity accordingly. With the integration of renewable energy (RE), power now flows in the opposite direction, as consumers generate energy through small-scale systems and send surplus power back to the grid, increasing grid complexity. This dynamic nature of generation and consumption is putting the new stress on the power grid requiring utilities to gain better visibility for ensuring grid stability by accurately monitoring energy generation and consumption.

This high penetration of inverter-based power generation has increased complexities on smart grid infrastructure to maintain reliable grid control. Therefore, Utilities are progressively integrating advanced sensing, metering, and innovative measurement technologies to monitor the state of the grid in real-time across wide geographical areas. In addition, sensing and measurement technologies include WAMS, Intelligent Electronic Devices (IEDs), Advanced Metering Infrastructure (AMI), smart meters, and others (Atmaja et al., 2019). Figure 2.1 illustrated the classification of measurements components and communication technologies in smart grid. This work only focused on WAMS and related measurement components considering the research scope and objectives.

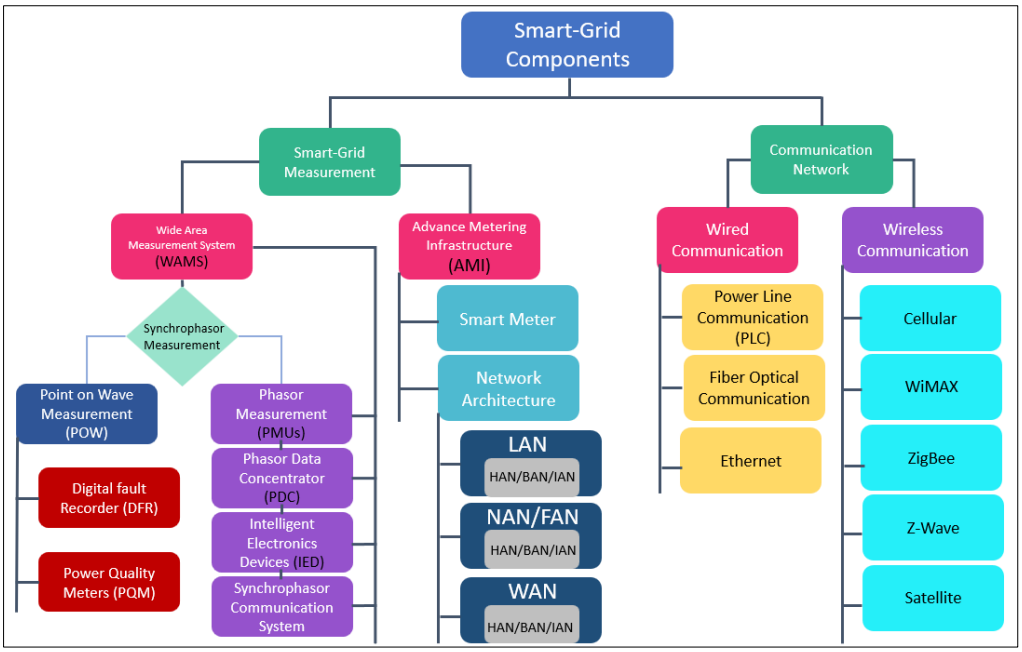


Figure 2.1: Classification of Smart Grid Components (Abrahamsen et al., 2021)

2.3 Wide Area Measurement System (WAMS)

WAMS is a collective technological effort based on synchronous measurement technology (SMT) that takes measurements of electrical parameters continuously for high-resolution snapshoot across the entire power system. This is considered an attractive technology nowadays because of synchronized data sampling capability and fastest transmission rate. Typically, SCADA based conventional monitoring systems reports data of power grid at every 4-6 seconds. Whereas the data reporting rate in synchrophasor measurement system is 30-60 records per second or higher which is a hundred times faster than traditional SCADA system. The comparison of SCADA versus WAMS monitoring in Figure 2.2 clearly indicates a high resolution visibility in real time (Follum et al., 2021; Xu et al., 2021). The synchronized data sampling ability allows WAMS to take measurements from different parts of the power grid simultaneously using a high-accuracy Global Positioning System (GPS), strengthening utility monitoring and operation by providing a clear snapshot of system stability under stressed operating conditions.

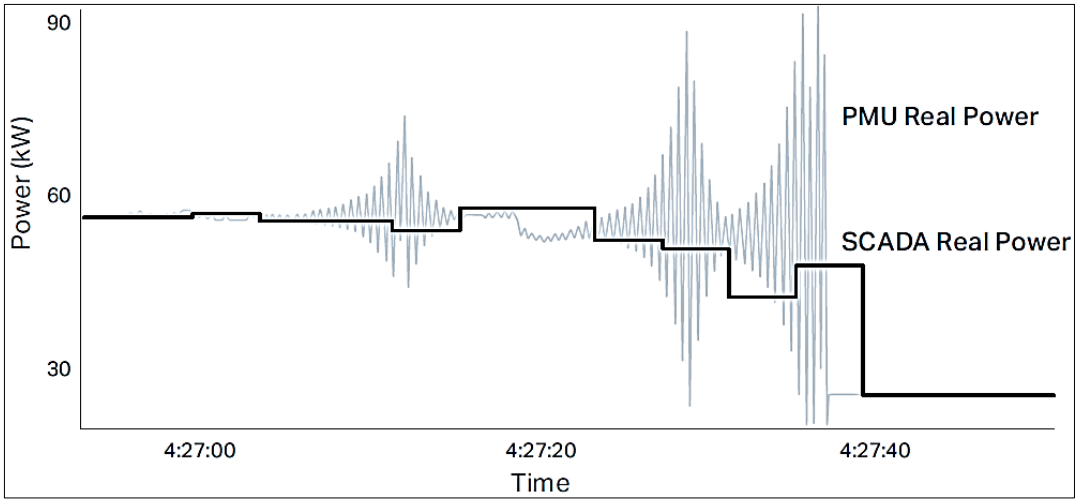


Figure 2.2: SCADA vs WAMS Monitoring (Usman & Faruque, 2019)

Additionally, typical WAMS architecture comprises PMUs, PDCs, and centralized two-way communication network to link the PMU, PDC and control centre for data streaming. The PMU is an electronic device installed in different parts of the transmission bus that provides precise time synchronized measured values of the voltage phasor, current phasor, frequency, rate of change of frequency (ROCOF) and phase angle using a common GPS (Lee & Centeno, 2019). Consequently, all the synchronized measurements then transmit to the PDC at a constant rate at 50–60 frames per second (fps) to guarantee the dynamic events monitoring (Phadke & Bi, 2018). Such a time synchronize measurement from different power node benefited in terms of better and high-resolution monitoring. The collected measurements are utilized for monitoring and identifying grid stability and related weaknesses, which helps implement countermeasures to protect the power grid. A PDC (regional PDC) collects data from approximately 50-60 PMUs (Kateb, 2019).

Since the evolution of the synchrophasor measurement system, researchers have widely discussed the increased integration of PMUs with heterogeneous communication architecture in a wide area network of the grid. Therefore, robust and resilient communication infrastructure is required with advanced information technologies (IT) to

enhance the full potential of synchrophasor technologies (Kateb et al., 2018). However, the integration of an enormous number of intelligent electronic devices in different parts of the power grid, such as PMUs and IEDs, has increased the possible cyber-attack surface among the attackers. Therefore, a cyber-attack on these devices could lead to severe cascading failures, potentially causing a total blackout of the power grid, similar to the 2015 Ukrainian cyber-attack (Alert, 2021). Likewise, this high installation of IoT enabled PMU devices at the edge of the substation has increased the volume of data streaming rate in the synchrophasor network which is cyber vulnerable to the attackers and security threats to the phasor data integrity, confidentiality, and availability (Yang et al., 2019). Hence, current centralized WAMS architecture is not sustainable enough to manage these huge volume of data streaming securely (Kateb et al., 2019). As a result, utilities around the world are looking for a secure data processing technique for manage this high volume of phasor data efficiently. Therefore, secure data processing over the cyber-resilient and scalable communication network is necessary in the WAMS architecture.

2.3.1 WAMS Security

The PMU-based WAMS has been widely used in the modern power grid due to its high data reporting capability. Although PMU integration in the different parts of the power grid has revolutionized the situational awareness and visibility of the power grid, it exposed to malicious attacker due to vulnerable communication architecture including PMU data modification, data interruption, data fabrication and interceptions. A cyber-attack on the power system, similar to the Ukrainian cyber-attack on Kyiv (Alert, 2021; Tatipatri & Arun, 2024), can lead to widespread outages, leaving millions without power. Attackers, often driven by financial motives, can compromise the integrity, confidentiality, and authenticity of communication channels.

The authors (Kateb et al., 2019; Schweitzer Engineering Laboratories, 2020) outlined the traditional architectures of WAMS. While typical WAMS embraced IEEE C37.118 that is centralized in nature. However, data sharing in centralized synchro phasor architecture lacks data protection mechanism which is vulnerable to malicious access (Bhattacharjee et al., 2020; Thakkar et al., 2019). As a result, any unauthorized access by malicious intruders in the synchro phasor network resulted in massive outages and destruction of power infrastructure. Therefore, data sharing between the PMU and PDC in the centralized architecture is not resilient to tolerate the failure of node in the network. Hence, a decentralized architecture with a strong security mechanism is quite essential to be developed (Музика, 2020), easing the cyber-attack and prevent blackout of the entire power grid. According to the ref. (Zhang et al., 2021), most of the data traffic transmitted by PMUs in synchrophasor communication network is not encrypted over the internet which endangered confidential utility data to the public.

Furthermore, synchrophasor measurement system exposed several types of cyber-attack because of its sophisticated and centralized nature of network. Gunduz & Das (2020) and Hossain & Peng (2020) demonstrated different types of cyber-attacks, including man-in the middle attack, packet analysis attack, malicious access, false data injection and data spoofing attack, among others. While researchers in (Ghiasi et al., 2021) classified multiple type of data modification attack in synchrophasor system. However, either type of malicious attack can manipulate critical electrical parameters and falsify the sensor measurement and configuration in the substation and consumer premises equally. Thus, the utility might be misled into making incorrect decisions that affect the grid's reliability and stability. Therefore, any unauthorized access to the synchrophasor network can lead to data

interruption, data fabrication, data modification and data interception attack (Bhattacharjee et al., 2020).

2.3.2 Security Objectives

Cyber security objectives is well known as "CIA" which are Confidentiality, Integrity, and Availability as demonstrated in (Cisco Networking Academy:Cybersecurity, 2021; Gunduz & Das, 2020; Kimani et al., 2019; Kumar et al., 2015). Confidentiality refers to data protection against exposer while integrity suggest protecting data against alteration or modification and availability describes as assuring data access in network when needed. The CIA-tired and standard countermeasures in smart grid synchrophasor network have been explained in the following subsection.

2.3.2.1 Data Integrity

Data integrity in WAMS perhaps described as any unauthorized alteration, stealthy modification, or destruction of sensor measurement from wide area grid network. As PMU providing sensitive measurements, hence it is important to transfer accurate data packets to PDC. Therefore, losing data integrity leads to wrong decision making related to the power measurements that may have catastrophic effect to the synchro phasor devices. False data injection (FDI) attack particularly categorized as common integrity attack in smart grid which capable to jeopardize the field measurement and state estimation that mislead the control centre to decision making. As a result, cascade grid failure could be taken place (Deng et al., 2019). However, Hash verifications, input/output checksums, and proper authentication systems are few efficient countermeasures used to achieved the data integrity in the WAMS network (Shahraeini & Kotzanikolaou, 2020; Thakkar et al., 2019).

2.3.2.2 Data Confidentiality

The confidentiality deals with privacy and protection of critical grid information and prevent the unauthorized access to the critical energy data and grid information. Data exchanged between the PMU-PDC in the synchrophasor network is essential to protect and secure confidential energy data. Hence, data encryption techniques and access control helps to maintain the confidentiality of information (Thakkar et al., 2019). However, in confidentiality attacks, unauthorized individuals or entities are targeted to access critical energy data and smart grid information. In addition, the violation of data confidentiality is mostly in AMI networks where intruders can gain access by using root password recovery or exploitation of system limitations (Asghar et al., 2017) and collect the consumer critical electricity data to violate the customer privacy. Therefore, data authentications and authorization processes to access data are vital to maintaining integrity and confidentiality.

2.3.2.3 Data Availability

The availability refers to uninterrupted data communication and continuous data transmission between different entities in the grid. In addition, it ensures reliable and appropriate data accessibility in the synchrophasor network. Access to information will be disrupted if availability is lost, which could impact power delivery decisions (Kateb, 2019). In addition, availability guarantees the reliable data access on time, which is significant for the steady operation of the smart grid. However, cyber-attack could create an obstacle to delaying the availability by interrupting the data communication, block or corrupting the control signal, which make the bad impact on grid stability, grid operation, grid efficiency and security of smart grid (Beasley et al., 2015; Yan et al., 2012).

Cyber vulnerabilities and security challenges in smart grid are investigated in (Gunduz & Das, 2020). Similarly, the researchers demonstrated cyber threats in

synchrophasor networks (Shapsough et al., 2016; Tufail et al., 2021). Unlike IT networks, where security and privacy requirements focus on the centre of the network where data is stored, the smart grid network requires protection at both the network centre and edge, as it is inherently distributed in nature (Aloul et al., 2012; Garlapati, 2020). Ample research in this field have suggested different method to improve the security and privacy of smart grid using Intrusion Detection System (IDS), firewalls, and encryption method which consider as traditional approach for smart grid network security. Hence, the conventional smart grid security mechanisms suffer from limitations, such as centralized access control, which has become increasingly irrelevant due to the high penetration of electronic devices in the smart grid. Therefore, a partially centralized, permissioned blockchain offers significant potential in this regard, providing a controlled database management system, data immutability.

2.4 Traditional Countermeasures to Secure Network

To prevent security breaches in the network, several countermeasures and mitigation techniques has been proposed in the literature, such as Firewall, Intrusion Detection System (IDS), Virtual Private Network (VPN) etc. (Gunduz & Das, 2020; Waseem et al., 2023). The authors summarizes the best practices to deal with cyber vulnerabilities in smart grid (Hojabri et al., 2019). Meanwhile, Yang et al. (2019) conducted an experimental study of a malicious attack on PMU in smart grid and proposed a multilayer architecture protected by firewall and VPN-enabled security gateways which prevent access to external attackers to local power system networks. The VPN tunnel securely encapsulates IEEE C37.118 messages to mitigate potential cyber risks. Vulnerabilities in IEEE C37.118 have also been highlighted in (Hadi et al., 2020; R. Khan et al., 2016) through demonstration of SQL injection (Structured Query Language) attack.

Particularly, firewall utilized for network security alongside intrusion detection systems (IDS). While encryption and authentication are used for data security and host IDS for device security parallelly in the industry (Quincozes et al., 2021). From the vulnerability assessment in ref. (Niu et al., 2018), the author points out the causes of vulnerabilities: e.g., data encryption, lack of data and device verification, and data authentication. At the same time, attackers can easily track and analyse non-encrypted data. However, these technologies are not hundred percent suitable to secure data exchanges in the WAMS network due to the real-time data communication requirement (Gunduz & Das, 2020; Tufail et al., 2021). It is still necessary to develop a scalable decentralized architecture with data authentication and device verification for robust data transfer in smart grids. The distributed ledger or Blockchain (BC) is a promising technology for resilient data exchange in smart grid WAMS.

2.5 Blockchain Overview

BC is a decentralized, distributed digital ledger system that provides transparent data recording with authentication and source verification using public key cryptography (PKI) and a digital signature to prove ownership of data while the blocks linked together cryptographically creating chain of blocks with data integrity and immutability. Hence, it allows participating nodes to record the data in a decentralized manner; thus, the data entry is not stored on a central server (Asefi et al., 2022). The algorithm that defines the rules and helps to reach the decision is called the consensus algorithm. Recorded data is available to all participants nodes in the network. The recorded data on the node is immutable, tamper-proof, and traceable, enhancing the security and availability of the host organization. The participating nodes must agree on a set of rules (consensus) to add new data to the block. However, complete data replication in WAMS architecture might raise scalability and storage issues since the power grid deals with a large volume of measurements data. Instead

an extensive WAMS network can be divided into multiple sub-divisions and apply a hierarchical BC approach to address scalability issues (Asefi et al., 2022; Bhattacharjee et al., 2020). To verify transactions and appending block in the ledger, peer nodes perform a validity check called consensus mechanisms. However, transactions and block verification by a set of nodes increases processing overhead, affecting the network's scalability performance. Therefore, development of a practical consensus algorithm is essential for fast transactions verification in real-time. In this way, BC technology can efficiently address cyber concerns in smart grid, WAMS network. The author in (Sadu et al., 2021) proposed a BC-based resilient grid automation system against cyber-attack. Most of the research in the literature concentrates on BC applications in P2P energy trading and cybersecurity within smart grids. Nevertheless, a few studies have also explored substation automation and synchrophasor systems (Gayo et al., 2020; Zhou et al., 2022).

Recently, BC has been widely discussed in the industry due to its decentralized data storing and processing ability. The researchers in (Hossain et al., 2020; Kishore et al., 2021; Mollah et al., 2021a) showcased the incorporation of BC technology into smart grids to enhance secure data management. Similarly, the adoption of BC framework of WAMS for state estimation sharing has been addressed in (Asefi et al., 2022; Bhattacharjee et al., 2020). Most existing research work on BC-integrated architecture are based on public BC (Asefi et al., 2022; Sikeridis et al., 2020). Whereas permission BC architecture increases, transactions speed and block confirmation time, which can improve network scalability performance. Meanwhile, the researcher rated permissioned BC very high for non-financial applications comparing permissioned less public BC based on access control, transaction validation, and reading ledger (Oikonomou et al., 2021; Son et al., 2021; Swathi & Venkatesan, 2021). Different types of BC have been proposed in the literature to meet various industrial

requirements based on consensus mechanism and network openness. Therefore, this thesis mainly focused on the security features of BC with hashing function and digital signature for data resiliency. However, considering all the research directions including, restriction on node access, computational complexity, partially centralized framework based on permissioned-private BC can helps to restrict the network from unauthorized access to the BC enabled system (Hasankhani et al., 2021).

2.6 Blockchain Network

Classes of nodes, ledger type, consensus algorithm and smart contracts are considered as core components of BC, which are significantly contributed to form its architecture. Based on the permissions and ledger accessibility, a book chapter in (Rehmani et al., 2021), classified BC network as permissioned and permission less BC. Permissioned BC further classified as private and consortium BC. Where permission less BC categorized as public BC. In the permissioned-private BC, any nodes can join at any time, read the ledger data, and validate transactions in this category. Although nodes in public blockchain are trust less and anonymous, results in long transaction approval time and consumes large power. In contrast, only pre-approved nodes can participate in the network and validate the transaction in permissioned-private blockchain. As a result, the transaction approval rate in permissioned-private BC is quite fast that suited IoT application.

Though public, consortium, and private blockchains differ in many aspects, they still share several similar components that contribute to the development of their architecture (Shrimali & Patel, 2022). These components include cryptographic encryption, hashing function, Markel tree, timestamp, consensus, etc. A Markel tree is defined as a data structure applied for organizing and validating larger set of data into a block while every block has

unique timestamps which generate variation for the block. Hashing is a mathematical function that produces a fixed output for any given input, though hashing algorithms are used to generate hash keys. The mining is the process of recording the transaction (data entry) into the block while orderer service mechanism has been utilized in the private-permissioned blockchain to chain the block instead of mining (Agung & Handayani, 2020). Consensus algorithms are an agreement reached between all peers of BC networks to ensure the validity of changes in stored data. The transaction flow of BC has been demonstrated in the following sub-sections.

2.6.1 Blockchain Transaction

Depending upon the application and deployment area, transaction can be in the form of digital asset transfer, cryptocurrency transfer. Hence, a BC transaction is a digitally signed piece of data that represents a record of an action taken on a blockchain network. This action could involve the transfer of crypto currency, the recording of data. For instant, deploying BC based architecture in smart grid for secure data recording and management; transactions may contain energy consumption data, measurement data or control instructions to perform. Therefore, each measurement recorded by a PMU treated as a transaction. However, transaction volume has significant influence on processing of data verification time that affect the transaction throughput (data recording) in the WAMS network (Fan et al., 2020).

2.6.2 Transaction Signing and Hashing

Once the client node initiates the transaction, it is required to sign and attached digital signature. This process involves asymmetric cryptography using sender node private key that facilitates the authenticity and integrity of the transaction. Consequently, transaction data hashed into a fixed-length data string through a hashing algorithm. Nonetheless, the

output hash value uniquely represents the transaction data. It is to be noted that, the hashing algorithm and digital signature scheme significantly impact data verification time (Feng et al., 2023), thus affecting the throughput and latency in BC-designed architecture. Therefore, optimized IoT-friendly, suitable signature algorithm must be utilized by BC framework for fast data transaction in real-time.

2.6.3 Transaction Verification

Transaction verification involves checking the digital signature and ensuring that the data adheres to the network's rules and protocols according to consensus. In BC-integrated data recording environment, each measurement recorded by a sensor device is treated as a transaction. The transaction includes sensor ID, timestamp, and the measured data. The verification process checks whether data comes from a valid sensor device, and whether it has not been tampered with. Cryptographic techniques, such as digital signatures, are used to verify the authenticity of the transaction data. However, transaction verification depends on cryptographic and consensus overhead which might add significant latency in the network. Therefore, fast signature scheme with small key size and distributed consensus is necessary for fast transaction verification.

2.6.4 Transaction Broadcast

Transaction broadcast is the process of sharing the verified transaction across the network to all participating nodes (other sensors and devices in the network). Once a sensor records a measurement and the transaction is verified, it broadcasts this transaction to the network. The broadcasted transaction is sent to all nodes in the network so that they can receive the new data. Each node that receives the transaction can then verify it independently before including it in their own copy of the blockchain.

2.6.5 Transaction/Block Validation

Transaction/block validation is the process by which nodes in the network ensure that a new block (which contains a set of transactions) is legitimate and follows the consensus rules before adding it to their copy of the blockchain. After transactions are broadcasted and collected, they are grouped into a block. The block undergoes a validation process to ensure all contained transactions are verified and follow network protocols. Consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), or Proof of Authority (PoA), are used to agree on the validity of the block. Once validated, the block is added to the blockchain, and the updated blockchain is distributed to all nodes in the network. Particularly, the validator collects signed transactions into a transaction pool creates a new block at regular intervals.

2.6.6 Block Confirmation Time

Block confirmation time is the time a BC network takes for a new block to be accepted and confirmed. A higher number of confirmations increases the confidence that the block and its transactions are permanently recorded in the BC designed database and cannot be reversed.

2.6.7 Blockchain and Block Structure

Blockchain (BC) is simply a database system that shared with participating nodes in a distributed network. As the name suggests, it is a chain of blocks containing data or information that is structured sequentially, secured, and connected through a hash function with the previous block, as demonstrated in Figure 2.3 (a). The block in the chain is attached with timestamps; hence, it shall not be backdated. Three blocks in the ledger chain, demonstrated in the Figure 2.3 (b), which are cryptographically connected, such as, block-3

carrying the data, hash value and previous block hash value as well. Hence the communication has initiated based on validation, verification, and consensus; If all the requirements meet, the communication has been established, and transection will start from every block. The structure of BC can be defined with the combination of four key theories: (1) linked lists, (2) digital signature, (3) hash functions, and (4) peer-to-peer networks which are proven method in computer science for secure data communication (Dedeoglu et al., 2020).

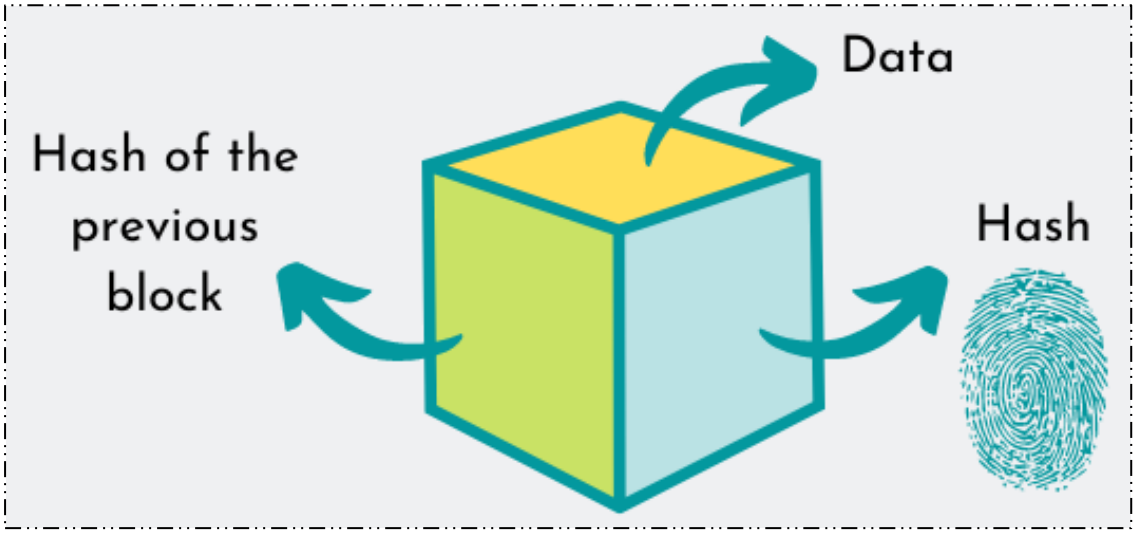
2.6.7.1 Linked List

The linked list is a data structure that chains the data elements into a list where latest data entry is linked to the last appended data in the list as pictured in Figure 2.3 (c).

2.6.7.2 Digital Signature

The second key element of a BC system is the digital signature, which is a part of the cryptographic encryption, and public key infrastructure (PKI) that ensures the data access only by an authorized entity. However, cryptographic encryption can be symmetric or asymmetric key cryptography. In symmetric key cryptography, a single common key used to encrypt and decrypt messages. While encryption and decryption are done using a pair of keys in asymmetric key cryptography. A public key uses for encryption, and a private key for decryption. However, BC technology embraces asymmetric key cryptography technique for encryption and decryption through public and private keys in every blockchain node. The sender uses recipient public key to encrypt the data while the receiver uses own private key to decrypt the data. Hence, the encrypted data can be verified and validated by all the nodes in the blockchain through public key that protects the data integrity and accountability. There are many asymmetric key encryptions algorithm used such as Rivest Shamir Adleman (RSA), Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm

(ECDSA), Edwards-curve Digital Signature Algorithm (EdDSA), Elgamal. However, ECDSA and EdDSA are two popular digital signature algorithms specifically to design IoT-oriented BC architecture due to its fast key generation capability and small key size. Elliptic curves are non-singular curves where a line between two points will intersect a third point. Elliptic curve cryptography uses ECDSA (Elliptic Curve Digital Signature Algorithm) based on the DSA algorithm with different mathematical expressions to generate public-private keys. Public-private key often referred to PKI.



(a)

(b)

(c)

Figure 2.3: Blockchain Representation (a) Block; (b) BC Structure and (c) Link List Data Structure (Rehmani et al., 2021)

2.6.7.3 Hash Functions

The third vital element of BC is hash function that makes BC network cryptographically secured. A hash function is a mathematical function that provides fixed output against any given input. However, a slight change in the input will significantly change the output. Hash is a one-way function that quickly calculates the result. BC utilized SHA-hashing, particularly, SHA-256 hashing function due to fixed-length output and faster cypher text output. Additionally, when the block is complete or in the time to create the new block in the chain, the block configures with the hash function, H(x), where x is the number of existing blocks in the chain, then the hash stored in the next block, consequently developing the 'chain'. The process continued at the last block, as a result any alternation to a block can be notified and hash will be shown as invalid. In a block of chain, each block contains two core components: a header and a body (Pal et al., 2021). The block header comprises with the block number, the hash value of the previous block, hash value of the current block, timestamp, the nonce and the address of the creator, while the body of the block contains transaction or record (Pal et al., 2021; Thukral, 2021).

2.6.7.4 Peer-to-Peer Network

The final element of a BC enabled system is peer-to-peer network where participating nodes share data packets among other node based on different BC architecture and eliminating central controller. Figure 2.4 represents the difference of centralized and BC-based decentralized and distributed P2P architectures.

2.6.8 Blockchain Architecture

Typically, a BC architecture refers to the structural design of a BC system that enables secure, decentralized, and transparent data management. Specifically, BC architecture in smart grid referred to the structural framework where data generated by sensors and monitoring devices are treated as transactions and securely recorded in immutable database. BC contains a chain of blocks that record different data or transactions while a single block in the chain is well capable of storing multiple transactions. However, each block in the chain referenced with the cryptographic hash of the previous data block. Hence, BC is simply a chain of blocks (data records) that are cryptographically connected with previous blocks (Garlapati, 2020). However, a block not only contains transaction data and cryptographic hash but also the last hash block and timestamp that makes it more resistant to any alternation and modification (Banks et al., 2019; Garlapati, 2020).

In conventional BC networks, each participant keeps a replica of the digital ledger and follows consensus protocol to update it; thus, the digital ledger then replicated on all nodes across the network, making the network more robust and freer of single point of failure. However, full node data replication in WAMS architecture raises the scalability and storage issues in wide area network where data volume is high. Recently, BC is widely discussed due to decentralized data storing and processing ability, which can eliminate unauthorized access in the synchro phasor network (Mollah et al., 2021).

Moreover, BC offers all necessary features such as decentralized identification, data authorization, and access control mechanisms to address unauthorized access. A network of nodes, distributed ledger, consensus algorithm and smart contracts is considered core components of BC architecture. Based on the permissions on the ledger, accessibility could

be divided into permissioned-private and permissionless-public and consortium. In the permissionless-public BC, any nodes can join at any time, read the ledger data, and validate transactions in this category. Although nodes in public BC are trust less and anonymous, results in long transaction approval time and consumes large power. In contrast, only pre-approved nodes can participate in the network and validate the transaction in the permissioned-private BC. As a result, the transaction approval rate in permissioned-private BC is quite fast which suited IoT application. Though public, consortium and private blockchain differ their attributes in many ways, still they have several similar components in BC architecture, these are cryptographic hash function, Markel tree, timestamp, consensus, etc. Markel tree defined as a data structure applied for organizing and validating larger set of data into a block while every block has unique timestamps which generate variation for the block. Cryptographic hashing algorithms are used to generate hash keys, while hashing is a mathematical function that provides fixed output against any given input. Mining is the process of recording the transaction into the block-chain while orderer service mechanism has been utilized in the private-permissioned blockchain to chain the block instead of mining. Consensus algorithms are an agreement reached between all peers of blockchain networks to ensure the validity of changes in stored data.

2.6.8.1 Centralized and Semi-Centralized Blockchain Architecture

While the initial concept of BC is rooted in decentralization, certain applications, particularly IoT based WAMS may benefit from partially centralized or semi-centralized distributed ledger technologies (DLTs). In such frameworks, a trusted authority or group of pre-approved nodes manages the network's operation, offering improved efficiency, control, and compliance compared to fully decentralized systems. Hyperledger Fabric, Corda for instance, is a permissioned BC framework designed for IoT-scale data management

application. Recent research has highlighted the benefits of such frameworks in energy and smart grid applications. For example, (Liu et al., 2023; Y. Wang et al., 2021) proposed a semi-centralized blockchain system with multi-chain technique for auditing communications of WAMS, emphasizing fast consensus and access control. In WAMS contexts, such frameworks could be tailored to allow central entity coordinates between distributed nodes, improving performance and scalability in grid monitoring tasks. Figure 2.4 clearly illustrated the comparison of centralized, decentralized and distributed P2P architecture

Although the private blockchain architecture is not fully decentralized, it is designed as a permissioned, partially centralized ledger system specifically to suit the operational and security needs of critical infrastructures like WAMS. Unlike public BCs, where any node can join and participate in consensus, the proposed framework only permits authenticated, pre-approved nodes (e.g., control centers, substations, and data aggregators) to record and verify transactions. From a cybersecurity perspective, this design significantly reduces the attack surface by limiting external access and enforcing strong identity management. Each transaction is cryptographically signed, immutably recorded, and traceable, thereby ensuring data integrity and non-repudiation.

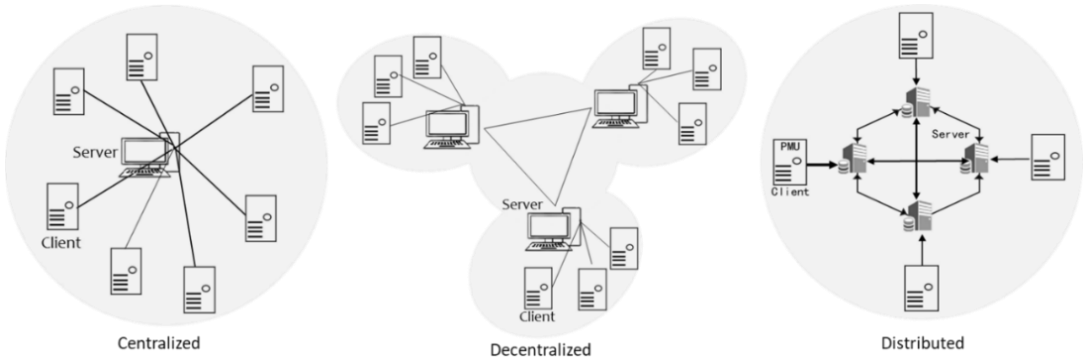


Figure 2.4: Comparison of Centralized, BC-based Decentralized and Distributed P2P Architectures (Mollah et al., 2021)

2.6.9 Blockchain Node

A BC node is suggesting to an entity, which links to a BC network and performs different duties (Agung & Handayani, 2020). Full node and light node are the two types of a node demonstrated in the literature (Petersen & Jansson, 2017). However, node has the privileges to join or leave the network at any time. The main function of a full node is to verify the transaction and store the copy of BC while light node used for light transection on a limited resource to validate transaction. Chronological data records benefit the formation of a ledger chain, whereas a single block in the ledger chain contains a set of data. However, once the block added in the chain it become nearly immutable, tamper-proof which cannot be altered by unauthorized entities (Kang et al., 2017).

The fundamental difference between consortium, private, and public blockchains lies in the types of nodes involved—specifically, the computers within the network that are responsible for data verification, validation, transfer, and storage. Moreover, the nodes in the public BC are thrust less and anonymous which is responsible for large power consumption and extensive transaction approval time. While nodes in private and consortium blockchains are trusted, and the consensus mechanism based on trusted nodes helps to reduce power consumption and increase the transaction approval rate. A blockchain network consists of several types of nodes, and each node hosts a copy of the ledger (Asefi et al., 2022). However, hosting copies on all the nodes in the network increases storage concerns, which is a significant issue in IoT-based applications.

2.7 Blockchain Performance

To determine the BC performance, it is essential to highlight the correlation between the throughput vs block size, block confirmation time vs throughput, and transaction size vs

throughput. According to book chapter in (Rehmani et al., 2021), the basic parameters such as number of transactions, transaction size, block size and block confirmation time significantly impact the throughput and latency in the proposed system, as illustrated in Figure 2.5. As transaction size (bytes) and block confirmation time (s) increase, the throughput (Tx/s) of the proposed blockchain network gradually decreases, as shown in Figure 2.5 (a & b). This decline is primarily because of a decrease in adding blocks to the BC ledger. In contrast, the throughput exhibits a linear increase with larger block sizes in Figure 2.5 (c) due to accommodating a higher number of transactions in a block.

In the context of WAMS, each PMU typically transmits data at a high frequency—commonly 30 to 60 samples per second—resulting in a continuous stream of time-sensitive measurements. When this high-frequency data is mapped directly into BC transactions without any aggregation or optimization, the network quickly becomes saturated with a large volume of small transactions. This leads to transaction backlog, increased block confirmation time, and ultimately, network congestion, making real-time data processing infeasible (Follum et al., 2021; Asefi et al., 2022b). As shown in Figure 2.5, the block confirmation time and transaction size have a direct opposite impact on blockchain throughput, which further exacerbates latency under high data rates. The problem becomes more critical when multiple PMU nodes are active, leading to a rapid increase in transaction generation that exceeds the BC's processing capacity (Fan et al., 2020; Colaco et al., 2020). Therefore, addressing network congestion is essential for ensuring the scalability and sensitivity of BC-enabled WAMS applications.

It is worth mentioning that transaction throughput can be managed by configuring block size, appropriate BC framework and lightweight consensus. Substantial block size can

store additional transactions, increasing the throughput; however, it extends the block proliferation time. Transaction throughput can be characterized as the total number of transactions per second a BC network can process, and it is calculated as (Tx/s). On the other hand, transaction latency refers to the time taken for a transaction to be processed and confirmed to be added to the ledger. It is another crucial metric of any BC network besides the transaction throughput in evaluating the scalability of a BC based system. Transaction latency is usually assessed as the average latency of the network.

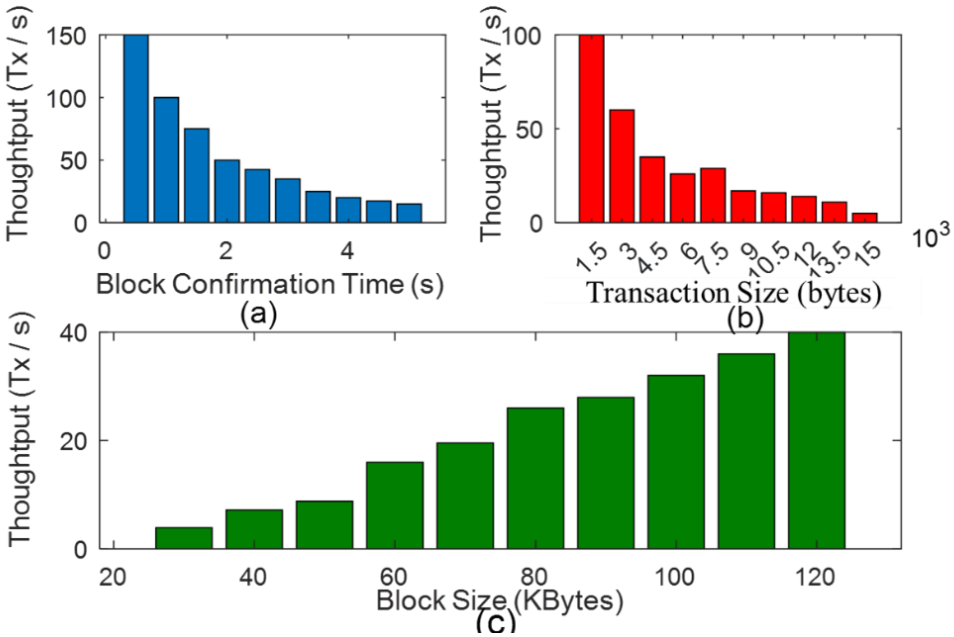


Figure 2.5: Impact of Throughput; (a) Block confirmation Time (b) Transaction Size, (c) Block Size (Rehmani et al., 2021)

2.8 Research Gap: Problem Formulation

This section demonstrates the key findings and related method based on the recent literature that has been collected on Tables 2.1 and 2.2. According to (Kateb et al., 2019), the increased installation of PMUs at the edge of the substation has increases the surface of unauthorized access. While any malicious access such as unauthorized alteration (e.g., man-

in the middle attack, false data injection) stealthy modification (false data injection) could breach the utility data integrity and confidentiality (Zhuang et al., 2021). BC as a core technology effectively defends data integrity and confidentiality, through the incorporation of authentication and source verification using asymmetric cryptography and hashing functions (Bhattacharjee et al., 2020; Thakkar et al., 2019). A number of studies (Ahlund et al., n.d.; Shen et al., 2020; Zhuang et al., 2021) showcased the integration of BC technology into smart grids to enhance data integrity and asset management, privacy preserving for smart grid data communication (Desai et al., 2019; Guan et al., 2018), privacy protection for smart meter and advanced metering infrastructures (AMI) or both (Houda et al., 2020; Tian et al., 2022; S. Zhang et al., 2020). However, only few works concentrate BC scalability and suitability on big data based, real-time and high throughput applications.

Nonetheless, the conventional BC framework has throughput and latency issues to be integrated into high volume of data recording or big data-based WAMS application (Fan et al., 2020; Ferrag & Shu, 2021). This is primarily due to computational complexity of cryptographic functions and consensus difficulties (Colaco et al., 2020); such as data verification, block creation, validation, and block confirmation time. For instance, all participating peer nodes broadcast and verify every transaction and block in the conventional BC architecture. Thus, peer node data verification increases processing overhead and block confirmation time. Given that the typical data recording rate of a PMU ranges from 30 to 60 samples per second (Follum et al., 2021; Xu et al., 2022), treating each individual PMU recording as a separate BC transaction significantly increases the transaction volume. This, in turn, adds processing delays that exacerbates throughput challenges in the WAMS network.

The performance of a BC-integrated network relies on its ability to process the number of transactions per second (TPS) according to performance analysis of a BC architecture demonstrated in (Bamakan et al., 2020). Hence, careful consideration of several parameters including transaction size, transaction-processing time, and number of transactions in the block, block size, cryptographic encryption, and consensus mechanism is necessary. The higher the transactions included in the block, the higher the throughput. Whereas the higher the transaction size and block confirmation time, the lower the throughput and lower latency (Fan et al., 2020). Additionally, increase in the number of participating PMU nodes increases the number of transactions and block size (Kbytes) exponentially, which may increase the transaction processing time and the block size in the ledger. Thus, the high transaction volume and block confirmation time are critical concerns related to the throughput and latency (Abdella et al., 2021). The authors (Bamakan et al., 2020; Fan et al., 2020), demonstrate the correlation between throughput and factors such as a high volume of transactions, limited block size, low transaction capacity per block, and extended transaction processing time.

Recently, various methods have been proposed in the literature to increase the number of transactions per block, such as lightweight, sharding, and hierarchical-based BC approaches (Al Ahmed et al., 2022; Mahmoudian Esfahani, 2022; Sahoo et al., 2019; Wang et al., 2019). However, these techniques introduce new challenges, such as data partitioning and synchronization, which are fundamental features of WAMS. Therefore, the necessity of network segmentation and sub-division-based architecture has been outlined in (Bhattacharjee et al., 2020; Asefi et al., 2022), to minimize throughput issues effectively.

Liang et al., (2019) proposed a distributed BC- framework for modern power systems to protect against cyber-attacks. However, optimizing computational efficiency of cryptographic functions and consensus mechanisms is necessary to handle real-time scale data transactions. Meanwhile, the work in (Bhattacharjee et al., 2020) proposed a bloom filter-based PMU device ID validation and ECDSA based PMU measurement authentication which suffers to handle real-time scale transactions due to the large volume of measurement. However, EdDSA-based authentication accelerate the signing procedure significantly as said by comprehensive studies in (Feng et al., 2023; Guruprakash & Koppu, 2022), thereby improving throughput issues. A Proof of Concept (PoC) based BC technique used in (Colaco et al., 2020), to secure sensors measurements for power system. Although, the proposed technique showed significant performance improvement over current methods while large-scale deployment in the electric grid needs further study on optimizing the parameters for better performance and scalability.

Moreover, a semi-centralized BC approach is proposed by (Wang et al., 2021) for wide area protection system (WAPS). This method employs a multi-chain structure that separates chains for different communication channels to reduce node load. Although this approach has reduced the number of nodes and the data stored in each node through full node and light node data replication, it still lacks the scalability needed to manage the growing volume of communication data in large-scale WAPS. In (Sadu et al., 2021), proposed BC designed substation automation system. Similarly, the adoption of BC framework for state estimation sharing has been addressed in (Asefi et al., 2022).

Furthermore, (Bhattacharya et al., 2022) proposed a two-layer BC framework using peer nodes consensus mechanism to ensure time synchronization and fault identification in WAMS. However, peer nodes consensus increases block confirmation time particularly in

the increased installation of PMUs thus limits throughput of the network. The author (Abdelsalam et al., 2024) introduces a weighted average consensus mechanism integrated with a BC framework for Cyber-Physical Power Systems (CPPS). However, implementing such framework and managing the consensus mechanism can be computationally intensive and may require significant resourceconstrain. This is primarily due to the difficulty level of consensus algorithm, which is hardly suitable for high throughput and big databased application.

In (Almasabi et al., 2024), a collaborative approach demonstrated combining BC technology with wireless sensor networks to secure data in smart grids. This is achieved through PoA based smart contracts for automated data validation and storage to secure smart grid data. However, the proposed technique shows significant latency associated with BC transactions (data recording in BC-enabled system) due to computational overhead. Future research could investigate ways to reduce the latency associated with BC transactions to improve real-time performance.

With summarizing the literature review, it is necessary for a scalable BC framework that can handle large volumes of transactions without compromising performance. In this regard, subdivision of the wide area network into smaller networks, PMU-data accumulation and segmentation utilizing lightweight cryptographic technique and resource constraint consensus algorithms effectively reduced latency, and improved throughput that helps to achieve required scalability of IoT based architecture.

Table 2.1: Recent Findings Issues in Existing WAMS Architecture

Authors	Area of Research	Findings
(Niu et al., 2018)	1) Vulnerability assessment for PMU communication networks.	✓ Another layer security mechanism is necessary on top of the communication layer
(Chenine et al., 2014; Gore & Kande, 2015; Thakkar et al., 2019b)	1) Analysis of Wide Area Monitoring System architecture. 2) Applicability of Blockchain for Synchrophasor Network	✓ Existing WAMS are centralized by default.
(Bhattacharjee et al., 2020b)	1. Block-Phasor: A Decentralized Blockchain Framework for secure synchrophasor system.	✓ Centralized WAMS architecture is cyber vulnerable to single point of failure
(Hossain & Peng, 2020; Waseem et al., 2023)	1) Cyber–physical security for on-going smart grid initiatives: A survey 2) Cybersecurity in smart grids, challenges and solutions	✓ Unauthorized and malicious access braces data integrity and confidentiality
(Silveira et al., 2021)	1) Cyber Vulnerability Assessment of a Digital Secondary System in an Electrical Substation System.	✓ Unauthorized alteration, stealthy modification could breach the utility data integrity and confidentiality.

Table 2.2: Recent Blockchain-based Data Management in Smart-Grid Application

Authors	Area of Research	Method Applied		Strengths/Limitation
		Nature of Blockchain (BC)	Consensus Algorithm	
(Liang et al., 2019)	Power grid data protection	Private Blockchain	Distributed Consensus	1) Mining issues with computational overhead 2) Limitation with High-scale data transaction
(Kong et al., 2020)	Sensors Measurements for Power Systems	Private Blockchain / Multi-chain approach	Practical Byzantine Fault Tolerance (PBFT)	1) High Communication Overhead 2) Low throughput and high Latency issues 3) Limited Scalability
(Bhattacharjee et al., 2020)	Data security of Synchrophasor	1) Bloom filter-based identity validation 2) ECDSA based authentication	Practical Byzantine Fault Tolerance (PBFT)	1) Low throughput and high Latency issues 2) Lacks large volume of measurement transactions in real-time

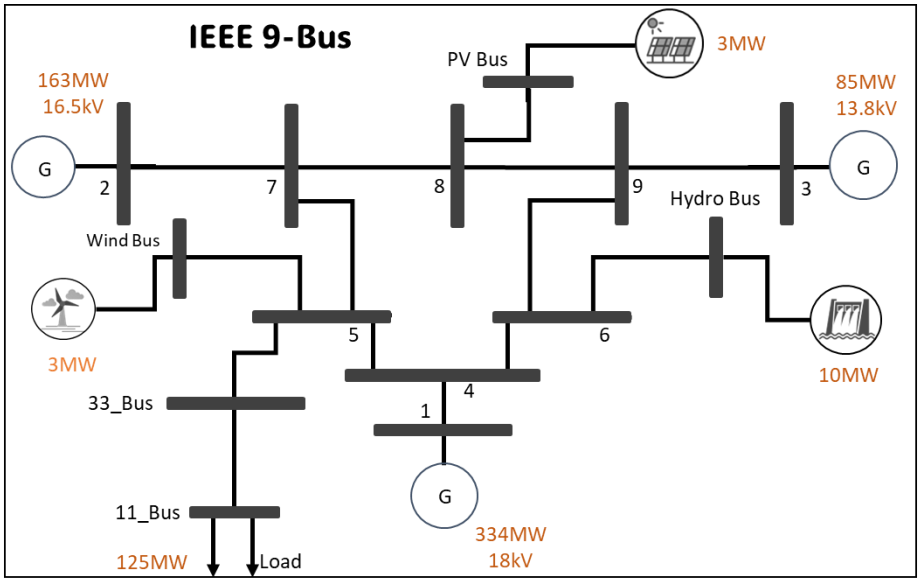
Table 2.2: continue

(Asefi et al., 2022; Sadu et al., 2021; Y. Wang et al., 2021b)	1) Substation automation system 2) A Multiple Attribute Decision Making based algorithm 3) Distributed state estimation in Smart grid	1) Semi-centralized architecture 2) Multi-chain structure 3) Deletable BC to reduce the storage burden of WAPS	1) Proof of stack 2) Proof of Concept (PoC) 3) Public BC/Ethereum	1) High latency with an increase in number of the transactions per block 2) Low throughput with increased number of nodes in the network 3) Multi-chain structure minimizes the number of nodes on a blockchain, and the amount of data stored in each node
(Bhattacharya et al., 2022)	Time synchronization and Fault Identification in WAMS	Two-layer Blockchain on top of the WAMS network	Private blockchain Proof of Authority (PoA)	1) Fully decentralized measurement sharing increases computational overhead in the network 2) Peer nodes consensus increases block confirmation time thus limits scalability of the network
(Almasabi et al., 2024)	Wireless Sensor Networks in Smart Grid	Ethereum Blockchain network	Proof of Authority (PoA)	1) Limited throughput with the increased number of nodes in the network 2) Consensus algorithm difficulty level is high-not suitable to handle real-time scale transaction

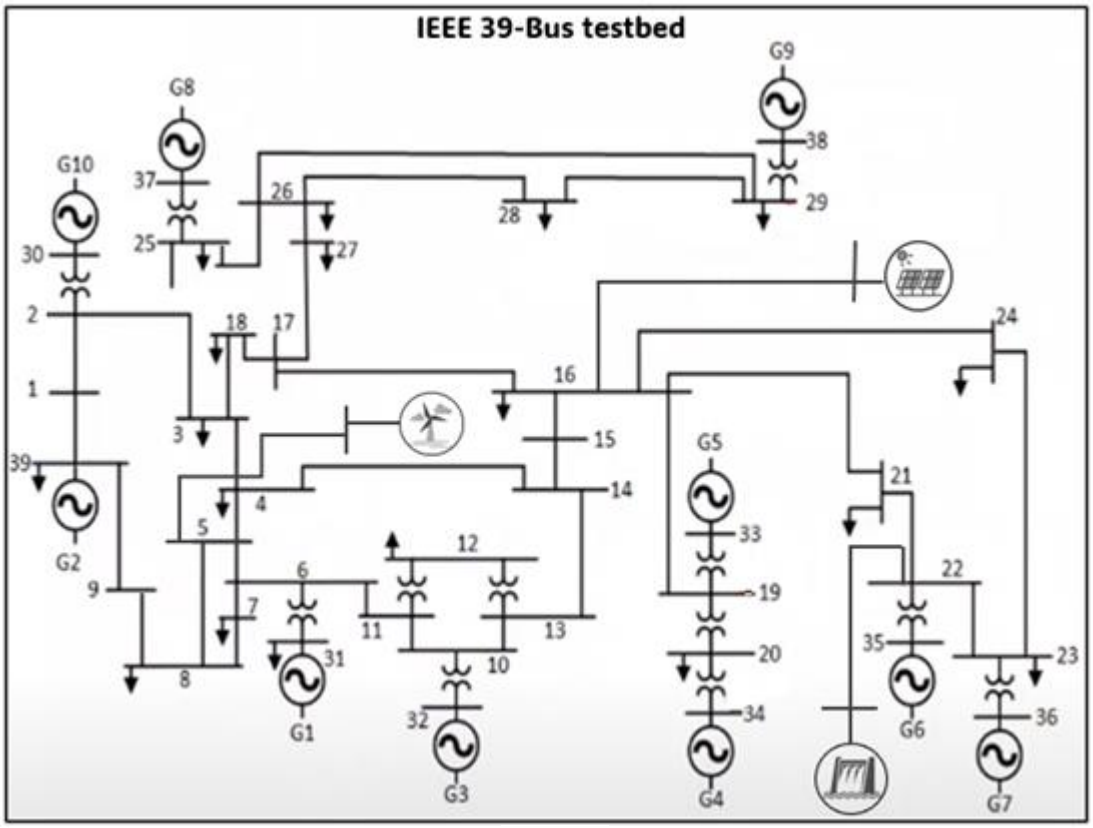
2.9 Modified IEEE Bus System

The IEEE test systems used in this work illustrate the range of operating conditions that a wide-area measurement system must support. The author in (Saha et al., 2024) studied behavior of IEEE 9 bus with different renewable energy integration. This is a part of the Western System Coordinating Council and contains only nine buses and three generators, making it easy to control because it has few voltage-control devices. Meanwhile, this research utilized MATLAB IEEE 9-bus system publicly available in (Pettikkattil, 2024). However, the system has modified with versatile renewable energy integration as shown in Figure 2.6 (a). As such, 2MW Solar PV plant integrated to bus-8 while 375MW hydro plant integrated to bus-6 and 10MW wind farm integrated to bus-5. However, 9-bus model has further extended with distributed substations bus to feed industrial and residential consumers. The substation comprises 33 and 11 kV bus bar, 225 km transmission line. The IEEE 39-bus network, also known as the New-England 10-machine system (Brunelle, 2024; Wang et al., 2018), represents a portion of the New-England grid with 10 generators and 46 lines. Consequently, a 5 MW PV plant is integrated to bus-16 while 10 MW wind farm is integrated to bus-5 and integrated to bus-22 as depicted in Figure 2.6 (b).

Considering the integration of BC into WAMS for PMU data, these RE sizes are selected intentionally to create dynamic and realistic PMU data loads. Small PV and wind units generate dynamic data rates as they depend on uncertain whether condition, while larger hydro units produce high volume phasor streams. This range allows us to evaluate the BC enabled WAMS across typical operational scenarios. Therefore, it demonstrates the capability of proposed architecture how it handles PMU data. Nevertheless, the thesis carried out IEEE 118-bus model (Peña et al., 2018) and conducted feasibility study of BC approach with extended buses.



(a)



(b)

Figure 2.6: Representation of schemetic diagram of IEEE bus system; (a) IEEE 9 Bus System (Pettikkattil, 2024), and (b) IEEE 39 Bus System (Brunelle, 2024)

2.10 Chapter Summary

This chapter has demonstrated a comprehensive review of the existing literature related to PMUs, WAMS, smart grid communication challenges, and the emerging role of blockchain (BC) technology in secure energy data management.

The literature demonstrates that with the increasing penetration of inverter-based generation, PMU devices have become a crucial component in enhancing real-time observability and dynamic state estimation in modern power grids. However, the exponential deployment of PMUs has resulted in a dramatic increase in data volume and communication frequency, thereby introducing vulnerabilities such as unauthorized access, data tampering, and false data injection attacks.

Several studies have highlighted the inadequacy of traditional communication systems in addressing the security and trust issues arising from two-way communication topologies. To address these concerns, researchers have explored the use of BC technology, particularly for its features such as immutability, distributed trust, cryptographic security, and data transparency. BC has shown strong potential in protecting data integrity and confidentiality in energy systems, particularly using asymmetric encryption, hashing algorithms, and consensus mechanisms.

Despite these advantages, the reviewed literature also reveals critical limitations when BC applied to high frequency, real-time data transmission systems like WAMS. The major challenges include low transaction throughput, high latency, and scalability issues, especially when every PMU reading treated as a separate transaction. These problems are primarily due to the computational cost of cryptographic operations.

To address these gaps, several studies have proposed architectural modifications, data aggregation, or improvise consensus mechanisms. However, most existing approaches fall short of achieving the real-time processing speed, and network scalability in PMU-based WAMS. Additionally, literature review conducted in this work highlights a significant research gap: the need for a lightweight, scalable BC framework that supports secure and real-time phasor data transmission in a high-throughput environment. This gap forms the basis and motivation for the proposed research, which aims to design and evaluate a BC-enabled WAMS architecture capable of meeting the demands of modern smart grid systems without compromising data integrity or system responsiveness.

CHAPTER 3

METHODOLOGY

3.1 Overview

The research methodology comprises three main phases aimed at achieving the research objectives, as illustrated in Figure 3.1. The primary goal of the thesis is to investigate the WAMS architecture, two-way communication system, and data security. To address the identified research gaps, the thesis proposes a framework for a subdivision-based blockchain-integrated WAMS to ensure the integrity and confidentiality of phasor data, thereby facilitating robust monitoring of electrical parameters. The research methodology structured with three case studies. Case Study 1 focuses on investigating the WAMS architecture through Distributed Energy Resources (DERs) integrated hybrid power system and a communication architecture design. This involves a laboratory experiment utilizing IEEE 9-bus and 39-bus systems and a two-way communication architecture within a co-simulation environment. Notably, the modified MATLAB IEEE 9-bus and 39-bus power networks are employed as power systems interfaced with a cloud server, an Open Platform Communications (OPC) web server helping as the communication channel, and SCADA Wonderware InTouch software as the Human-Machine Interface (HMI) for monitoring in Case Study 1. Furthermore, the experiment extended by applying proposed BC framework in Case Study 2 where PMU identity is verified, and PMU data is authenticated to protect data integrity and confidentiality. Furthermore, the performance of the proposed framework evaluated in Case Study 3 using parameters from the result achieved in Case Study 2. The expected outcome of the project is to achieve a secure WAMS framework.

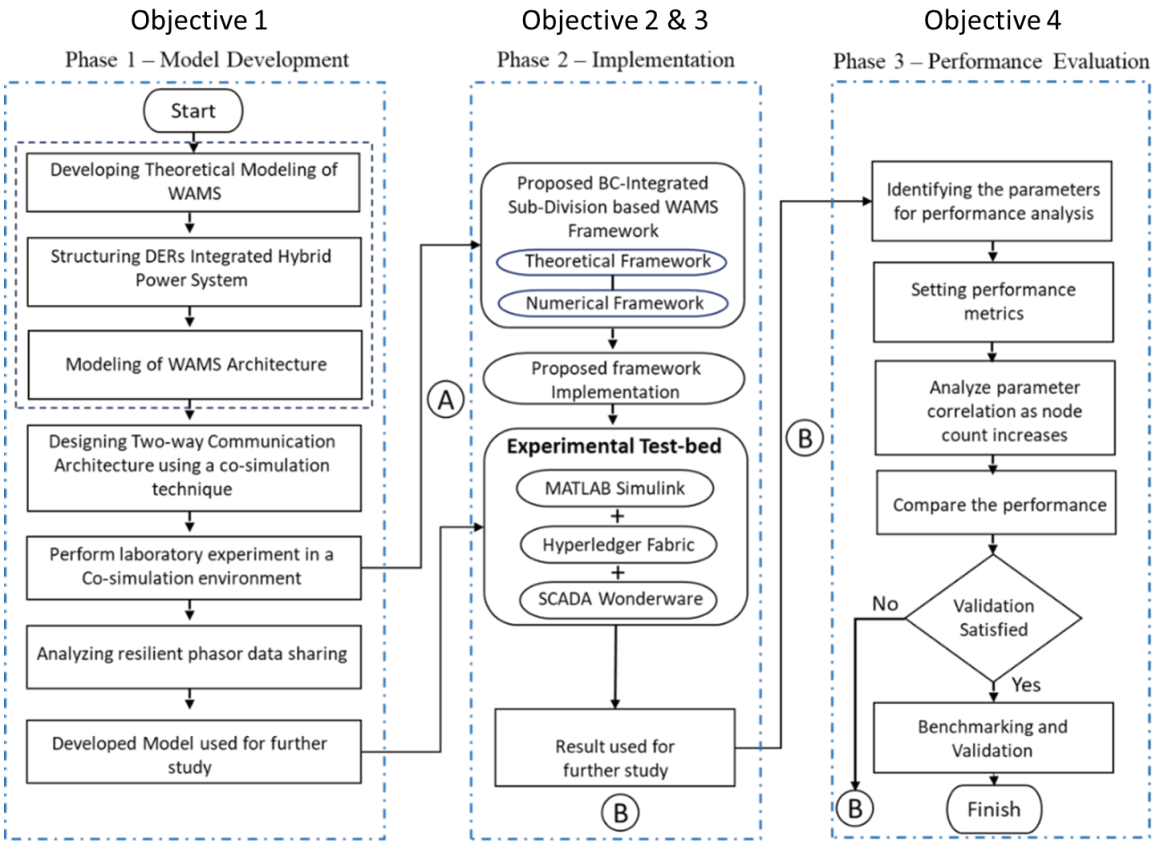


Figure 3.1: Research Methodology Flow Chart

3.2 Modelling of WAMS

The components of WAMS include PMU, PDC, and communication mediums (Bhonsle, 2018). Therefore, the modelling of WAMS architecture conducted by structuring a DERs integrated hybrid power system that involves the placement of PMUs in the transmission bus bar and establishing communication channels between the PMUs and PDC (SCADA machine) for real-time data monitoring. Initially, DERs integrated hybrid power system simulated using MATLAB Simulink. The developed hybrid power system incorporates with a utility-scale PV plant, a wind farm, Hydro and a battery storage system. Subsequently, a communication framework is designed to connect the MATLAB Simulink model with SCADA machine (PDC) using a cloud server, OPC web server (open platform communications) in co-simulation environments. Hence, the data sharing between the

simulated power network and SCADA monitoring has established for real-time monitoring and control. Finally, BC technology has integrated to share secure state estimations in the WAMS architecture.

3.2.1 Simulation of DERs Integrated Hybrid Power System

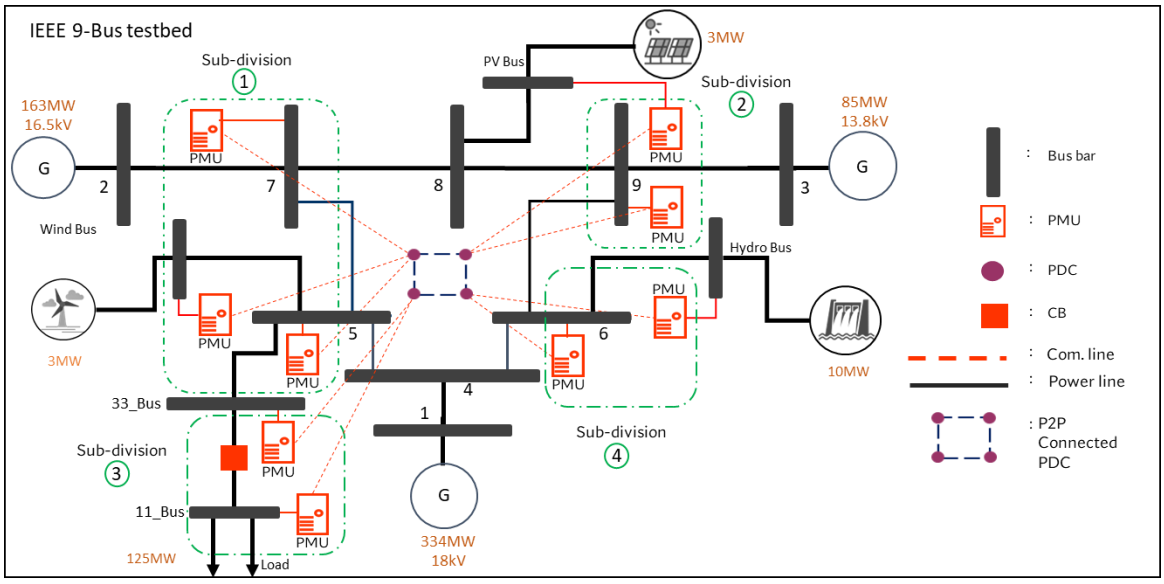
The simulation design of hybrid energy network relied on the P.M. Anderson 9-bus system and the revised New England 39-bus system, incorporating large-scale DER generation. Figures 3.2 (a) and 3.2 (b) illustrate the DER-integrated energy systems. These DER-integrated models were simulated using MATLAB/Simulink 2023b based on (Brunelle, 2024; Pettikkattil, 2024; Wang et al., 2018). To simplify the simulation, the 9-bus network consists of three generators with base voltage levels of 13.8 kV, 16.5 kV, 18 kV, and three loads specifically configured as follows: Bus 5 (125 MW, 50 MVAR), Bus 6 (90 MW, 30 MVAR), and Bus 8 (100 MW, 35 MVAR). Meanwhile, a 2MW Solar PV plant is integrated to bus-8 while 375MW hydro plant is integrated to bus-6 and 10MW wind farm is integrated to bus-5. However, 9-bus model has further extended with distributed substations bus to feed industrial and residential consumers. The substation comprises 33 and 11 kV bus bar, 225 km transmission line.

Likewise, 39-bus system comprises with 10 machines, and 20-load bus which is our second test bench study system in this thesis. The model has been further extended to DERs integration. A 5-MW PV plant integrated to bus-16 while 10 MW wind farm is integrated to bus-5. Table 3.1 illustrates the capacity of distributed energy generation with base voltage of DERs integrated bus. It is relevant to point out that, considering the current research scope; this work follows the general grid code in terms of mandatory voltage/frequency

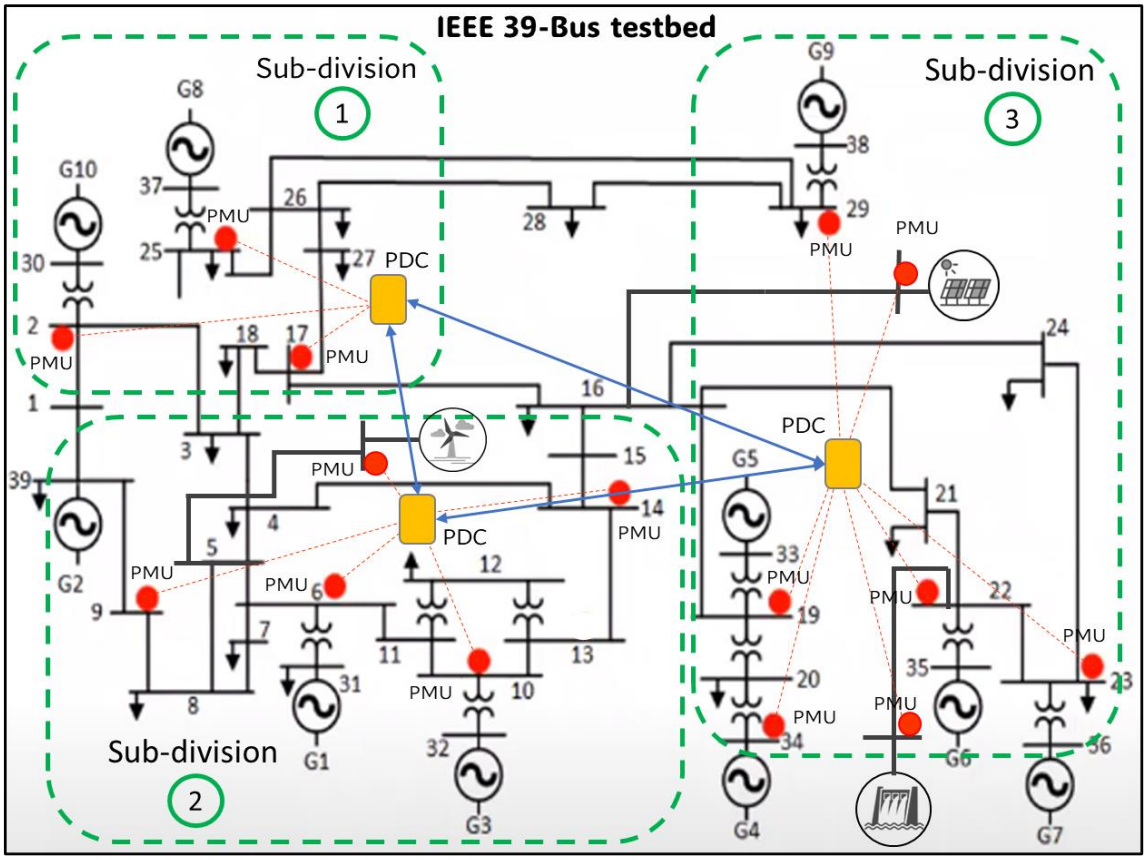
requirements to integrate different Renewable Energy (RE) sources. Ref. (Ropp, 2019) highlighted the IEEE 1547-2018 standard and explain briefly the impacts on cooperatives.

Table 3.1: Distributed Energy Network Parameters

Cases	DERs Integrated Bus	Type	Capacity
Case 1: DERs integrated 9 bus system	PV bus	Solar	2MW
	Wind bus	Wind	10MW
	Hydro bus	Hydro	375MW
Case 2: DERs integrated 39 bus system	PV bus	Solar	5MW
	Wind bus	Wind	10MW
	Hydro bus	Hydro	157MW



(a)



(b)

Figure 3.2: Sub-division based PMU Placement in WAMS Architecture (a) IEEE 9 Bus System, and (b) IEEE 39 Bus System

3.2.2 Integrating Synchrophasor Measurement System

Upon the simulation completion of the hybrid power system in the MATLAB Simulink, PMU module integrated into the transmission buses of the power system. This integration facilitates continuous measurement of electrical parameters, including magnitude (|u|), phase angle (**Φ**), and frequency ([f]) of voltage and current for the corresponding bus bar. The MATLAB PMU module enables to set the sampling rate (Nsr) in points per cycle, thereby allowing dynamic monitoring of the real-time behaviour of the DERs-integrated hybrid power system. While the project utilized 50 sampling rate Nsr (point/cycle) for better grid visibility based on IEEE C37.118.1 protocol.

For the 9-bus network, PMU modules (PMU1-PMU7) are connected to Bus 5, Bus 6, Bus 7, Bus 9, the Wind Bus, the PV Bus, and the Hydro Bus, respectively, through current transformers (CTs) and potential transformers (PTs). Moreover, PMU-A linked to the primary bus (11kV bus) in Substation A, along with CT/VT, while PMU-B connected to the secondary bus (33kV bus) at Substation B. Similarly, the phasor measurement system comprises PMUs 1-14, which connected to the following buses of 39-bus network: Bus 2, Bus 6, Bus 9, Bus 10, Bus 13, Bus 14, Bus 17, Bus 19, Bus 22, Bus 25, Bus 29, as well as the PV, Wind, and Hydro buses. The placement of PMU modules illustrated in Figures 3.2(a) and 3.2(b), which achieved through an optimal PMU placement technique in accordance with the PMU configuration in Table 3.2. The PMUs measure voltage and/or current phasors continuously at their respective nodes in the network and transmit the data to the PDC using the TCP/IP protocol, adhering to the parameters specified by the IEEE C37.118.1 and IEEE C37.118.2 standards.

Table 3.2: PMU Configuration of Simulated Power Model

	PMUs	**Bus Location**	**Corresponding Observable Bus**
DERs Integrated IEEE 9-Bus System	PMU_1	Bus 5	4, 1, 5
	PMU_2	Bus 6	6, 3, 7
	PMU_3	Bus 7	8, 2, 9
	PMU_4	Bus 9	3, 9
	PMU_5	PV Bus	8, PV Grid Bus
	PMU_6	Wind Bus	5, Wind Grid Bus
	PMU_7	Hydro Bus	6, Hydro Grid Bus

Table 3.2: continue

DERs Integrated IEEE 39-Bus System	PMU_2	Bus 6	11, 6, 7
	PMU_3	Bus 9	5, 8, 9, 39
	PMU_4	Bus 10	10, 11, 12
	PMU_5	Bus 13	12, 13
	PMU_6	Bus 14	4, 15, 16
	PMU_7	Bus 17	17, 18, 27
	PMU_8	Bus 19	19, 20
	PMU_9	Bus 22	21, 22, 35
	PMU_{10}	Bus 25	25, 26, 37
	PMU_{11}	Bus 29	28, 29, 38
	PMU_{12}	PV Bus	PV Grid Bus, PV G_bus
	PMU_{13}	Wind Bus	Wind Grid Bus, Wind G_bus
	PMU_{14}	Hydro Bus	Hydro Bus, Hydro G_bus

Additionally, in substation buses, the PMU has interfaced with relay and circuit breaker (CB) so that any fault occurs, CB contact open and isolated. Furthermore, the PMU takes the original time-domain signal as shown in equation 3.1. Then time-domain signal converted into frequency domain using DFT algorithm (Discrete Fourier transform) shown in equation 3.2 and extract phasor magnitude and phase. Whereas, X is the frequency domain representation of an individual sampled signal x_k of a PMU where $x_k\{k = 0,1 \ldots., N\}$, k

represents the sample index (e.g. k^{th}sample), and *N* is the total number of samples taken over a single time window. Therefore, estimated voltage and current phasor given by a PMU presented in equation 3.4 and 3.5. It is to be noted that, I_i^{est} represents magnitude of the estimated current phasor, V_i^{est} magnitude of the estimated voltage phasor, f_i^{est} estimated frequency that is same as for the current. Since generating frequency (f_{ss} , Hz) is same across the network, voltage in all points of the power network will have the same frequency in the steady state condition, which is measured by PMU as following equation (3.2).

$$e_i(t) = E_i \cos(2\pi f_{ss} t + \delta_i) \quad \text{Equation 3.1}$$

$$X = \frac{\sqrt{2}}{N} \sum_{K=0}^{K=N-1} x_k e^{-jk\frac{2\pi}{N}} \quad \text{Equation 3.2}$$

$$i_i^{est} = I_i^{est} \cos(2\pi f_i^{est} t + \theta_i^{est}) \quad \text{Equation 3.3}$$

$$v_i^{est} = V_i^{est} \cos(2\pi f_i^{est} t + \theta_i^{est}) \quad \text{Equation 3.4}$$

3.2.3 Design of Communication Architecture for Real-time Monitoring and Control

The design of communication architecture has carried out using co-simulation technique where the simulated power system is integrated with the communication framework that facilitates data pipelines between MATLAB Simulink model and SCADA for real-time monitoring and control. Therefore, the MATLAB-Simulink model has interfaced with OPC Unified Architecture (OPC UA) web server (KEPServerEX) and ThingSpeak cloud server, which allows aggregating phasor data and real-time data transfer for monitoring and control in the SCADA HMI. This work utilized AVEVA Wonderware InTouch which is a high-level supervisory control and data acquisition (SCADA) software. The data transfer between MATLAB Simulink power system and Wonderware InTouch

SCADA required OPC KEPServerEX as the intermediary server to facilitate, data transfer can occur bidirectionally, from MATLAB to SCADA or vice versa as shown in Figure 3.3.

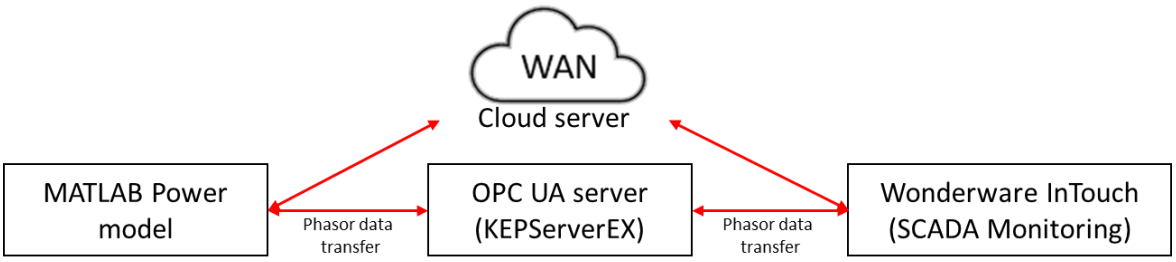
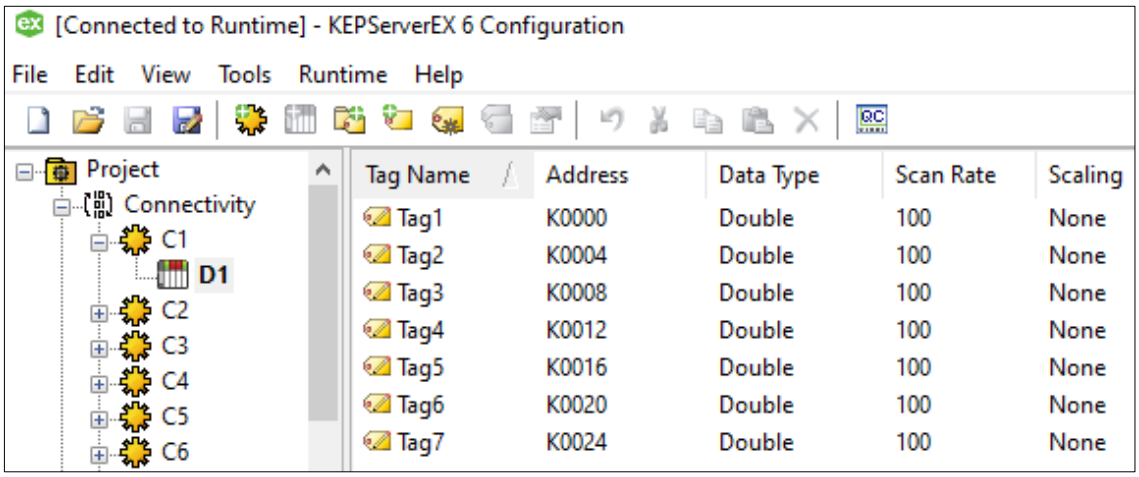


Figure 3.3: Bi-directional Data Transfer between Power Model and SCADA

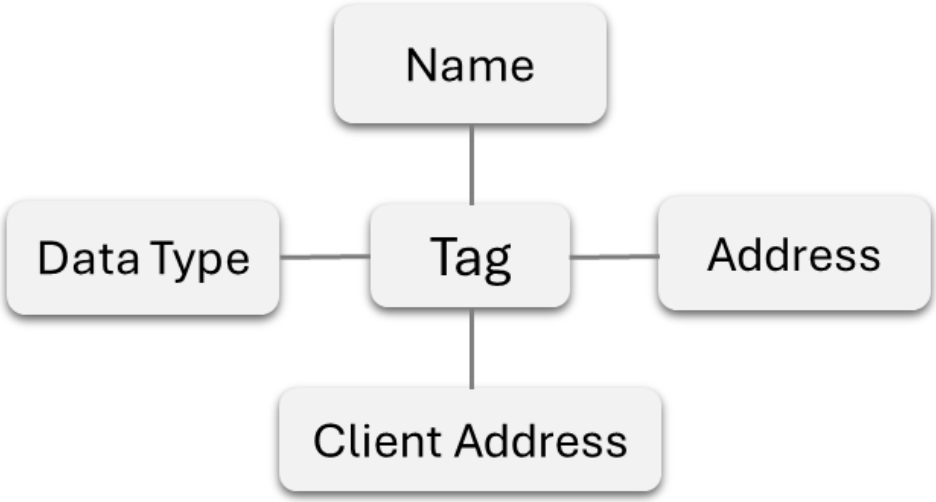
3.2.3.1 Server Configuration

In the initial setup, it is necessary to establish the communication channel. The channel type "Simulator" is assigned to "C1" when adding a channel in KEPServerEX. Subsequently, the device wizard is configured with the name "D1". While an alias "C1D1" is also declared to enable the client computer to connect to the server. Table 5 demonstrates the server settings utilized in KEPServerEX. Individual channel created in the KEPServer for every single PMU as shown in Figure 3.4 (a).

The foremost procedure involves adding tags to the server. Each tag represents a unique real-time monitoring, control, and automation parameter. Firstly, every tag must possess a distinct name for differentiation. Secondly, the data type options include string, boolean, char, bytes, short, word, long, float, double, and more, depending on the utilized data type. Furthermore, an address must be assigned to each tag, with formats varying depending on the data type. Lastly, the user selects the client access functionality, allowing the client computer to read or write data exclusively. Figure 3.4 (b) outlines the characteristics of the server tag.



(a)



(b)

Figure 3.4: Characteristics; (a) Characteristics of Server Tag; (b) Server Configuration

Table 3.3: Server Setting

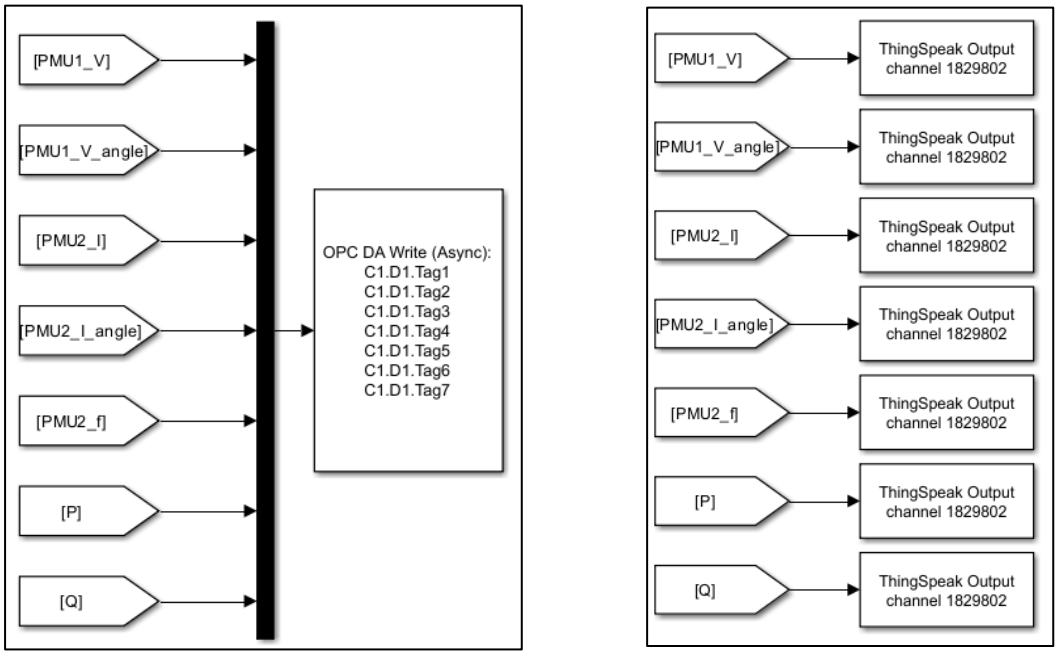
Item	Detail
Channel Name	C1
Device Name	D1

Table 3.3: continue

Alias Name	C1D1
Driver	Simulator
Model	16 Bit Device
Mapped to	C1.D1

3.2.3.2 MATLAB Simulink Configuration

Once the server configuration is established, a monitoring framework is developed to gather all PMU measurements. The subsequent step involves utilizing OPC to establish a connection with the server. The Channel, C1, and its corresponding Device, D1, store all the necessary tags for communication during the data transfer process within the server cloud. The “From Block” parameters readings in Figure 3.5 (a) are then transmitted to the OPC Write block with unique tags from Tag1 to Tag7. This facilitates data transfer to the SCADA system via the server for real-time monitoring. The data type used is “double”, which accurately represents the reading value. Meanwhile, the “From Block” parameters readings in Figure 3.5 (b) sent to ThingSpeak cloud server. This accomplished using the “Write Block” of the ThingSpeak input channel to stream the data. Prior to this, the channel ID, write API key, and field need to be set up.



(a) (b)

Figure 3.5: OPC Framework in MATLAB (a) PMU Measurement to Web Server, (b) and Cloud Server

3.2.3.3 SCADA Configuration

The SCADA interface is developed using Wonderware Intouch maker. Initially, the "Access Names" from the "Special" section are added to the settings as shown in Table 3.4. The topic name is set the same as the alias name (refer to Table 3.3) to ensure the SCADA platform recognizes the channel from the server. The SuiteLink protocol is utilized to support communication over the network. When connecting to KEPServerEX via SuiteLink, the application name must be set exactly as "server_runtime".

Following that, the tags (Tag1 to Tag150) from the server are defined in the "Tagname Dictionary" within the "Special" section. In the "Tagname Dictionary", each tag is assigned a unique tag name. The tag type is set to "I/O Real" for monitoring purposes, while the tag type is "I/O Real" for controlling purposes. All these tags must have the Access Name "C1D1". Figure 3.6 (a) demonstrates the definition of all the tags used in SCADA.

Meanwhile, the designs of user interface (UI) have developed using Wonderware InTouch. The SCADA dashboard of energy management system has been developed and encompasses three main sections: monitoring, manual control, and automation. The display colour, maximum value, minimum value, and tag number for each monitoring screen have configured, where the tag number must exactly follow the OPC configuration. The tags containing crucial parameters have added to the dashboard panel of SCADA energy management system, as illustrated in Figure 3.6 (b).

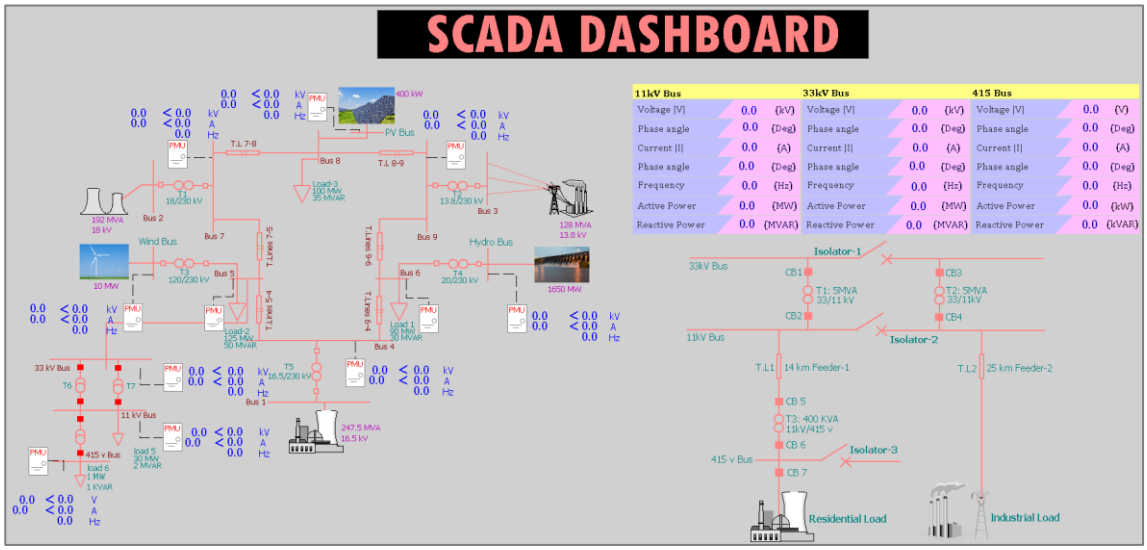
AVEVA Wonderware InTouch is a high-level supervisory control and data acquisition (SCADA) software utilized as a PDC in this work that allows synchrophasor specific protocol and configuration running in a dedicated computer. Initially, PMUs collect the electrical parameters and broadcast them to the OPC UA web server and ThingSpeak cloud server simultaneously. Then, the substation extracts those electrical parameters and visualizes them in the SCADA HMI (SCADA-UI) following IEEE C37.118 protocol. Therefore, collected parameters have been stored in the SCADA Historian database for offline data analysis in various file formats.

Table 3.4: Access Setting

Item	Detail
Access Name	C1D1
Application Name	server_runtime
Topic Name	C1D1
Protocol	SuitLink

Tagname	Tag Type	Access Name	Alarm Group
Tag19	I/O Real	C3D3	$System
Tag2	I/O Real	C1D1	$System
Tag20	I/O Real	C3D3	$System
Tag21	I/O Real	C3D3	$System
Tag22	I/O Real	C4D4	$System
Tag23	I/O Real	C4D4	$System
Tag24	I/O Real	C4D4	$System
Tag25	I/O Real	C4D4	$System
Tag26	I/O Real	C4D4	$System
Tag27	I/O Real	C4D4	$System
Tag28	I/O Real	C4D4	$System
Tag29	I/O Real	C5D5	$System
Tag3	I/O Real	C1D1	$System
Tag30	I/O Real	C5D5	$System
Tag31	I/O Real	C5D5	$System
Tag32	I/O Real	C5D5	$System
Tag33	I/O Real	C5D5	$System
Tag34	I/O Real	C5D5	$System
Tag35	I/O Real	C5D5	$System
Tag36	I/O Real	C6D6	$System
Tag37	I/O Real	C6D6	$System
Tag38	I/O Real	C6D6	$System
Tag39	I/O Real	C6D6	$System
Tag4	I/O Real	C1D1	$System
Tag40	I/O Real	C6D6	$System
Tag41	I/O Real	C6D6	$System
Tag42	I/O Real	C6D6	$System

(a)



(b)

Figure 3.6: SCADA Configuration (a) Definition of Tags, (b) SCADA Energy Management System Dashboard

3.3 Proposed Sub-Division based WAMS Architecture

In conventional IoT based BC architectures, every sensor measurement logged as a separate transaction (Wang et al., 2025). For instance, a cluster consist of m PMU sensor produces $50 \times m$ transactions per second with 50 samples/s, which promptly overwhelms the throughput of most existing ledgers. The most recognized and widely available public BC such as Bitcoin are restricted by a 1 MB block size and a 10-minute block interval (Koech & Alae, 2025), so their on-chain throughput is estimated at only 7 transactions per second (TPS) (Yadav & Shevkar, 2021). While Ethereum BC provides bit faster TPS which is 20 transactions per second (Yadav & Shevkar, 2021). Even permissioned BC like Hyperledger Fabric is limited to only 100-160 of transactions per second (Ajwalia & Shah, 2025) and specialized optimizations push its throughput to around 1000 transactions per second (Bandara et al., 2021). Though, Hyperledger is unable to process real-time transactions (Bandara et al., 2021).

In response to the research gap identified in the literature review—specifically, the limitations of the conventional BC framework shown in Figure 3.7 in integrating with high-throughput WAMS applications—this thesis proposes a BC-designed, subdivision-based WAMS framework illustrated in Figure 3.8 which briefly explained in subsequent section. The PMUs act as client nodes, capturing phasor measurements and storing them in a distributed ledger while measurement recorded by a PMU is treated as a transaction, thus BC transactions contain phasor measurements or control instructions. As PMU data recording is automatically stored their measurement in the historical data base typically in the PDC. Hence, when BC integrated, measurement data will be stored BC data base in PDC as well. Therefore, data will be stored in the immutable local and offline data base in the proposed BC system. Furthermore, proposed framework employs a fast signature scheme

with small key size and lightweight consensus mechanisms. Specifically, it utilizes Decentralized Identity and Access Management, DIAM-based PMU identity validation and Edwards-Curve Digital Signature Algorithm (EdDSA) with SHA-256 for PMU data authentication, both of which enhance transaction verification time and improve transaction throughput.

3.3.1 DIAM based PMU Identity Validation

The proposed framework utilized DIAM technique for managing PMU device ID validation by creating a decentralized identity system. By using DIAM, the necessities of central authorities eliminated. In this regard, every PMU device configures with a unique cryptographic key pair express as $PK_i^{pmu+} and\ SK_i^{pmu+}$ which used to create self-sovereign identity (SSI). While the secret key injected by the manufacturer. Hence, SSI of PMU devices denoted as $identity(PK_i^{pmu+}, SK_i^{pmu+})$ which is store as unique ID to registered in the database using a decentralized identity provider (DID) that ensures the PMUs identity. After all, the data structure can be constructed for PMU device identity which is stored on the BC network as mentioned in Eq-3.7 It is assumed that any PMU identity specified as $ID_i^{pmu+} where\ i = 1,2 \ldots n$, n is the total number of PMUs for given sub-division cluster. While PMUs transmit their reading, it uses SSI to authenticate and request permission to submit the reading to the PDC blockchain. Access control policies specify the terms of the access agreement in the network. The following equation can determine the respective PMU identity with proper ID number.

$$PMU_i^{iden} = \mathbb{PK}_i^{pmu}\left(PMU_i^{ser.num} \left|\left| \text{gate}_{ID_i^{pmu}} \right|\right| \text{deploy}_{\text{date}}\right) \quad \text{Equation 3.5}$$

where $PMU_i^{ser.num}$ is the serial number of the device; $\text{gate}_{ID_i^{pmu}}$ is the identifier of the

unique gateway in the geographical zone where the device is deployed; and $\text{deploy}_{\text{date}}$ is the date of deployment of the device.

3.3.2 EdDSA-with-SHA256 based PMU Data Authentication

The proposed approach utilizes Edward curve digital signature, EdDSA which is incorporates with SHA256 hashing function to verify PMU measurements. This signature scheme is deterministic and generating fast signatures with a compact key size, 256 bits (Feng et al., 2023) while maintaining a high level of security. It also reduces computational complexity and communication overhead in the WAMS network. Therefore, the EdDSA signature algorithm is well-suited to meet fast digital signature requirements for IoT-scale applications (Feng et al., 2023; Shi et al., 2022). Data authentication is achieved through three functions in the proposed approach such as $KeyGen(EdParams)$, $Sign(Sk^+, Pk^+, phasor)$ and $Varify(Sk^+, Pk^+, \tau)$. Where $EdParams$ parameters defined by $EdParams$ *(*$\mathbb{E}_p$*,*$\boldsymbol{b}$*,*$\boldsymbol{G}$*,*$\mathfrak{H}$*)*. In the *KeyGen* phase, each PMU derives a private key and generates a corresponding public key using cryptographic hashing following the eq. 3.6-3.8. During the *Sign* phase, the PMUs computes digital signature $\mathcal{R}$, $\mathcal{S}$ (see eq.3.9-3.11) that is attached to the measurement data before transmission. Finally, in the *Verify* phase, the blockchain network validates the received signature using the public key as explained the steps in eq.12-13.

- KeyGen( ):

1) Set a private key, $\text{Sk}^+ \leftarrow \{0, 1\}^b$, and generate a hash value $\text{H}(\text{Sk}^+) = (\text{h}_0, \text{h}_1, \ldots \ldots \text{h}_{2b-1})$ Equation 3.6

2) Define $(\text{h}_0 = \text{h}_1 = \text{h}_{b-1} = 0)$ & $\text{h}_{b-2} = 1$, to determine an integer, $\mathcal{S} = \sum_{i=0}^{b-1} 2^i . \text{h}_i \; ; \; \mathcal{S} \in \mathbb{R}_q$ Equation 3.7

3) Compute the public key, $\mathrm{Pk}^{+} = \mathrm{Sk}^{+}.\mathrm{G}$ Equation 3.8

- $\mathrm{Sign}(\mathrm{Sk}^{+}, \mathrm{Pk}^{+}, \mathrm{phasor}) \rightarrow \{\mathcal{R}, \mathcal{S}\}$:

1) Define $\mathrm{H_R}(\mathrm{Sk}^{+}) = (\mathrm{h_b}, \ldots \mathrm{h_{2b-1}})$ to compute a random nonce $\mathrm{r} = \mathrm{H_R}(\mathrm{Sk}^{+}, \mathrm{phasor}) \bmod \mathrm{q}$ Equation 3.9

2) Compute $\mathcal{R} = \mathrm{r}[\mathrm{G}], \text{ and } \mathcal{S} = \mathrm{r} + \mathrm{H}(\mathcal{R}, \mathrm{Pk}^{+}, \mathrm{phasor}) \bmod \mathrm{q}$ Equation 3.10

3) Signature output $\tau = \mathcal{R}, \mathcal{S}$ Equation 3.11

- $\mathrm{Varify}(\mathrm{Sk}^{+}, \mathrm{phasor}, \tau)$:

1) Compute, $\forall := \mathrm{H}(\mathcal{R}, \mathrm{Pk}^{+}, \mathrm{phasor})$. Equation 3.12

2) Compare, if output holds $[2^3.\mathrm{S}]\mathrm{G} = [2^3]\mathcal{R} + [2^3.\forall]\ \mathrm{Pk}^{+}$ [Output (1) accept], otherwise [Output (0) reject]. Equation 3.13

3.3.3 Data Recording in Proposed BC Framework

Unlike existing works, proposed framework is designed to handle a high volume of real-time transaction (data storing) in BC system with increased number of PMU nodes. To achieve this scalability, the proposed framework uses sub-division-based network topology (Figure 3.8) and data compression techniques at the gateway level. Hence, the architecture of WAMS divided into “n” sub-divisions in the proposed approach where “m” number of PMU nodes are connected in a clustered network in each sub-division. With data accumulation and compression, the measurement of all PMU nodes for one second in each sub-division consolidated into a single compressed data segment. Consequently, every data segment recorded by a PMUs is treated as a transaction instead of considering every measurement as a transaction. Hence compressed data segment then processes as a BC transaction.

In this manner, proposed approach reduces the transaction volume and increases transactions number in the block, thus enhancing the throughput in the network. Subsequently, collected transactions are transferred to the PDC gateway node for verification. While local PDC verified the transactions, it is considered as valid instead of all peer node verification, resulting in less block confirmation time, which helps in lower latency. In this way, the proposed approach secures data recording and addresses scalability issues to handle large volume of transactions (data recording) in the WAMS network.

The data recording operation started with PMU device registration in the proposed framework. Every PMUs in the cluster registering their own IDs with the utility via web-based user interface (UI) by using private key while utility verified the identity of PMUs using public key. During PMU registration, the identity of each device is recorded in the BC network by storing its unique ID, serial number, device address, and communication port. Once approved the devices only can record the measurement in the system.

3.3.3.1 Data Segmentation and Compression

This section represents the data queuing and demonstrated mathematical model as shown in eq-3.8. Assume to divide the WAMS into n sub-division, where each sub-division s contains of N_s number of PMUs connected to a local gateway device (PDC) and storing the data in the BC integrated system. The PMUs report phasor measurement at rate of μ_s samples per second hence all the PMU readings within a cluster are accumulated over a fixed interval $\tau = 1$s instead of transmitting every PMU reading individually. Therefore, every PMU reading accumulated in the cluster given by $k_t = N_s \cdot \mu_s \cdot \tau$. Let $\Phi_{i,j}$ denote the j-th measurement from PMU i and encapsulates k_t consecutive reading into a single compressed data segment (d) which expressed as eq-3.18. Meanwhile, b symbolized the average size (in bytes) of a single PMU reading and γ is compression ratio. Hence, raw data

size generated by cluster s is $D_s^{\text{raw}} = k_t \cdot b$ and the compressed data size is $D_s^{\text{comp}} = (1 - \gamma)\, D_s^{\text{raw}}$. Thus, each cluster generates one compressed data segment per second which consider as transaction in proposed approach.

$$d_s = \text{Comp}\{\Phi_{i,j}\}\, i = 1 \ldots\ldots N_s, j = 1 \ldots\ldots \mu_s \tau \qquad \text{Equation 3.14}$$

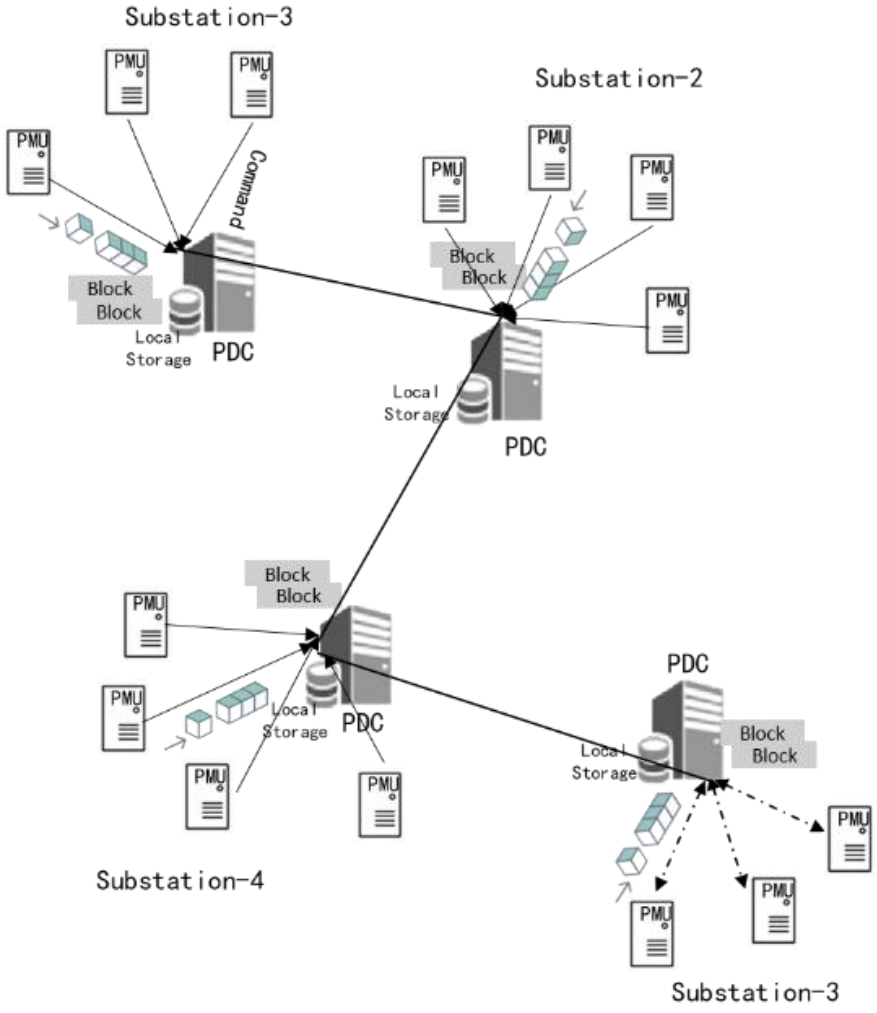


Figure 3.7: Conventional BC-based WAMS Architecture

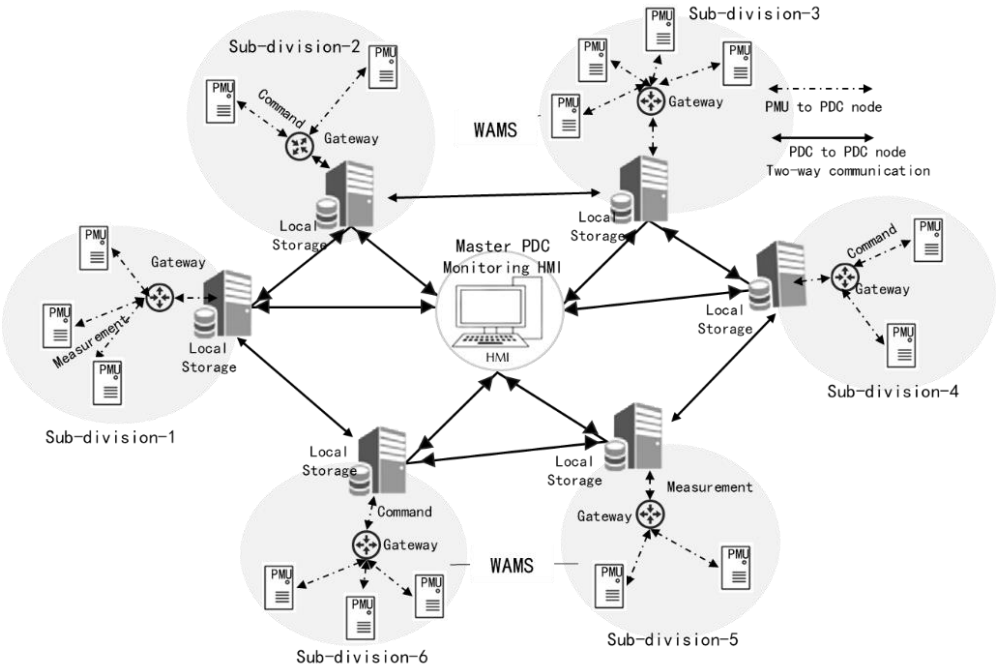


Figure 3.8: Proposed BC integrated sub-division-based WAMS Architecture

3.3.3.2 PDC Data Queueing Model

The PMU reading comprises time stamps and data segment accumulated since the last reading thus PMUs of each cluster sends its compressed data segment to the corresponding local PDC, which acts as a gateway node. Since each cluster generates one data segment every $\tau = 1$s, inter-arrival time of PMU reading in the gateway nodes follows a Poisson process with a rate with $\lambda_s = \frac{1}{\tau} = 1\text{segment/s}$. Hence, each data segments reflect as a single transaction which in turn reduces the transaction frequency in the BC enabled system. The service time is assumed to follow an exponential distribution with mean service rate μ_p segments per second. As the gateway PDC is follows M/M/1 queue model, the stability condition of the gateway queue is defined by $\lambda_s < \mu_p$. Therefore, the average time spent by a data segment at the gateway are expressed as eq 3.6.

$$\lambda_s = \frac{1}{\tau} \qquad \text{Equation 3.15}$$

$$\mathbb{E}[T_s] = \frac{1}{\mu_p - \lambda_s} = \frac{1}{\mu_p - \frac{1}{\tau}}$$ Equation 3.16

3.3.3.3 Blockchain Queueing Model

As PMU reading within the cluster accumulated and generates one compressed data segment, the PMUs initiate the transaction along with that data segment thus it becomes one transaction for $\tau = 1\text{s}$ time intervals. The blockchain creates a block with the transaction received from gateway device in each sub-division after performing the consensus process Since each cluster creates one transaction per second, the transaction arrival rate at the blockchain network is $\frac{n}{\tau}$. Thus, arriving transaction per second defined by eq 3.20 in the block that also depends on the number of clusters in the network. Let μ_b refer to the block generation rate per second which assumed to be exponentially distributed while every block can contain a variable number of transactions limited by $p \leq T_b \leq q$. Hence, proposed BC follows policy stated to generate new block every time. It is to be noted that, p represent the minimum number of transactions while q is maximum per block. The average number of transactions per block can be defined by eq 3.21 and effective blockchain transaction service rate is therefore expressed as eq 3.22 respectively. Thus, a transactions waits on average half of the block generation time denoted as block time as eq 3.23. Nevertheless, transaction processing system is modeled as an M/M/1 queue with transation arrival rate or transaction rate λ_{BC} and service rate μ_{BC}. The stability condition of the blockchain queue is denoted as $\lambda_{BC} < \mu_{BC}$ where the average transaction confirmation delay is stated as eq 3.24. Nevertheless, the representation of data queuing and segmentation model for single sub-division is shown in Figure 3.9.

$$\lambda_{BC} = \frac{n}{\tau}$$ Equation 3.17

$$\mathbb{E}[T_b] = \frac{p+q}{2}$$ Equation 3.18

$$\mu_{BC} = \frac{\mu_b}{\mathbb{E}[T_b]}$$ Equation 3.19

$$T_b = \frac{T_{blk}}{2}$$ Equation 3.20

$$\mathbb{E}[T_{BC}] = \frac{1}{\mu_{BC} - \lambda_{BC}}$$ Equation 3.21

Furthermore, the recording and data latency has determined from the theoratical model explained in previos section. The average BC recording latency, T_r is the time taken to record the transaction in the BC that referes to the post-aggregation latency determined as eq 3.25. This includes gateway queueing time T_s , transaction queueing time T_{BC}, plus block formation time, $\frac{T_{blk}}{2}$ and consensus time, T_c. Whereas, average data latency is the time taken to accumolate the PMU measurement into segments plus average BC recording latency mensioned earlier. As PMU reading are accumulated over a fixed interval, the avearage accumulation time expressed as $\frac{\tau}{2}$. Therefore, the data latency of proposed BC framework is represented as eq 3.26.

$$T_r = T_s + T_{BC} + \frac{T_{blk}}{2} + T_c$$ Equation 3.22

$$\mathrm{T} = T_r + \frac{\tau}{2}$$ Equation 3.23

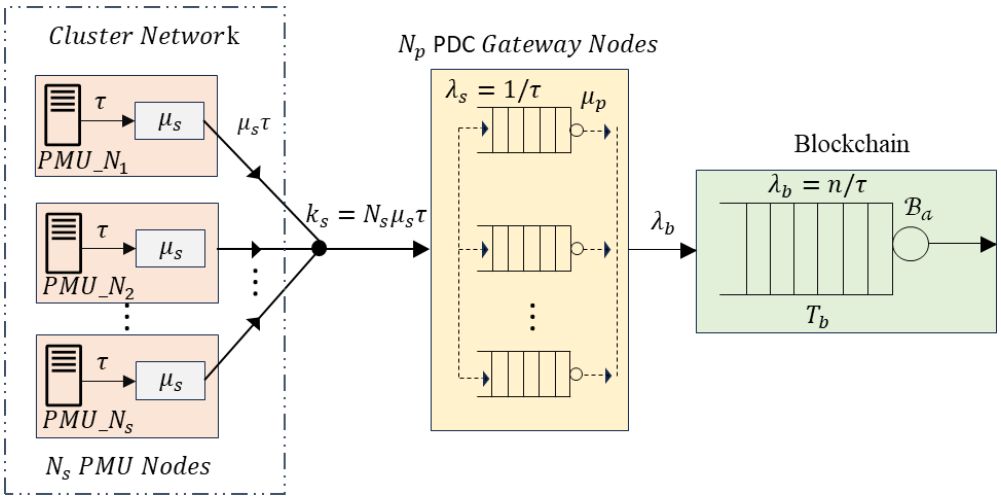


Figure 3.9: Representation of Data Queuing and Segmentation Model

3.3.4 Transaction Flow in the Proposed Approach

As transaction flow of proposed approach presented in Figure 3.9, PMUs registered with valid ID represented as PMU_{ID_i}.While PMU transmit the phasor data to gateway device (PDC), PMUs generate key pairs which denoted as $PK_i^{pmu+}$and SK_i^{pmu+} shown in (Eq 3.9-3.10). Consequently, every PMU reading is fed into SHA256 hashing algorithm and reform as hash value denoted as $H(phasor_i^{pmu})$. Therefore, the hash value has encrypted and attach digital signature using PMUs private key represented as $Sign(SK_i^{pmu+}, H(phasor_i^{pmu}))$. However, $Sign()$ indicates the function of digital signature while $H(phasor_i^{pmu})$ refer to the hash value of measurement data sent by validated PMU correspond to PMU_{ID_i} which is registered and authenticated. The digital signature of PMU measurement is mentioned in Equation 3.11-3.13. Therefore, phasor measurement transmitted by a PMU denoted as $\{PK_i^{pmu+},\ Sign(SK_i^{pmu+}, H(phasor_i^{pmu})\}$ which is used to authenticate the identity of the sender PMU and secure immutability of the phasor data. On the other hand, PDC uses the PMUs public key, PK_i^{pmu+} to retrieve the transaction TX hash and compare the hash value of the received file with the original transaction TX hash as shown in (Eq 3.15-3.16) and

verify PMU measurement representing $varify\{PK_i^{pmu+},\ Sign(SK_i^{pmu+}, H(phasor_i^{pmu})\}$ by validate function $varify$ ( ).

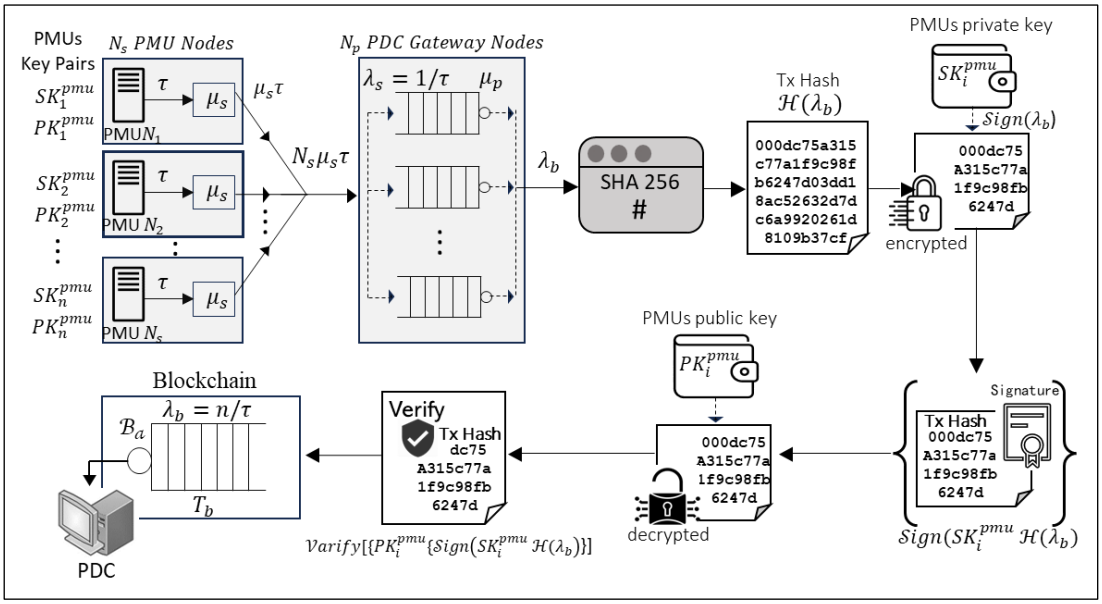


Figure 3.10: Transaction Flow of Proposed Approach

3.3.5 Lightweight Consensus Algorithm for WAMS

According to the proposed consensus algorithm in Figure 3.11, the PMUs act as a client node and creates a transaction proposal as $(PROPOSE, Tx, [anchor]$. Hence every transaction has the following arguments $T_b(\ \mathbb{Sk}^+, \mathbb{Pk}^+,\ Sign, metadata)$, where $\mathbb{Sk}^+$ is the PMUs secrete key, $\mathbb{Pk}^+$ is the PMUs public key, $Sign$ is representing signature given by the PMU and endorsing node and $metadata$ is represented the hash value of PMU measurement. The transaction is then transmitted to the gateway device validating and endorsing measurement as $< T_b - \text{ENDORSED}, Sign >$. Verified data is then broadcast to the PDC node in the peer. The PDC verifies the signature of endorsing node and added in the block defined as B_{i+1}. It is essential to highlight that the proposed framework adopted with participants consensus instead of group consensus. Therefore, the transaction is verified only by the endorsing node instead of verifying by every node, improving the transaction

processing time shown in Figure 3.12 (a). A transactions (TX) flow diagram in Figure 3.12 (b) indicates the steps from transactions proposal, endorsement and append the block in the ledger. The structure of a block in the proposed approach can be expressed as Eq-3.12:

$$|\mathrm{T}_b|\mathcal{H}|\mathrm{Key}(\mathbb{Sk}^+, \mathbb{Pk}^+)\big|\mathrm{Timestamp}|\mathrm{Validator}_{\mathcal{S}\mathrm{ig}}\big| \qquad \text{Equation 3.24}$$

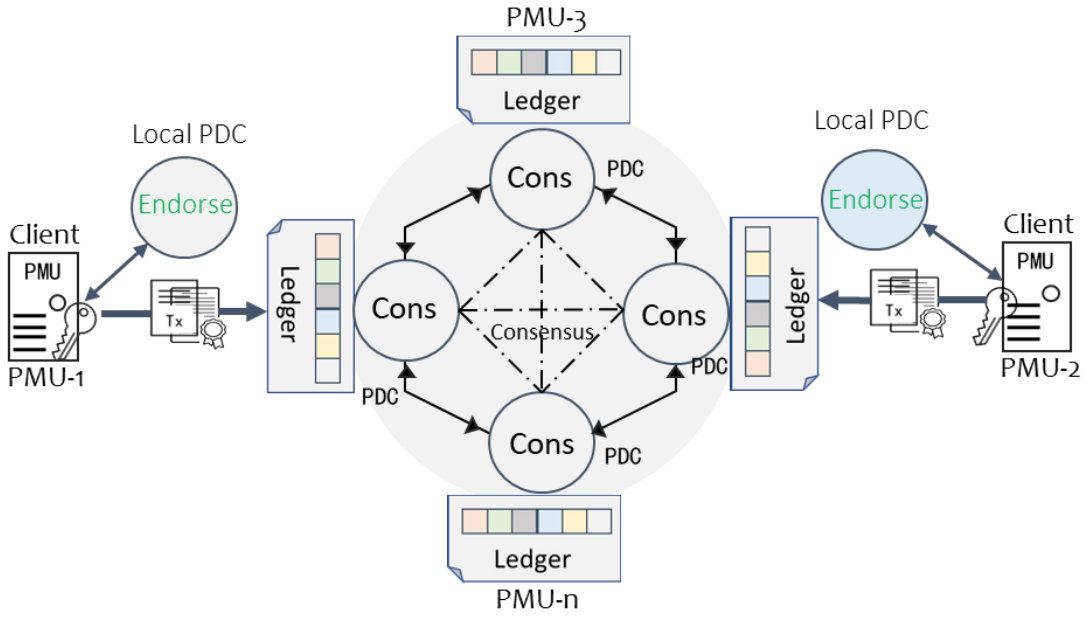
Algorithm: Distributed Consensus for WAMS

Input: $\forall T_k \in Tx$, $Sign \in (\mathbb{Sk}^+, \mathbb{Pk}^+)$, $metadata$, $\forall B_i \in B$

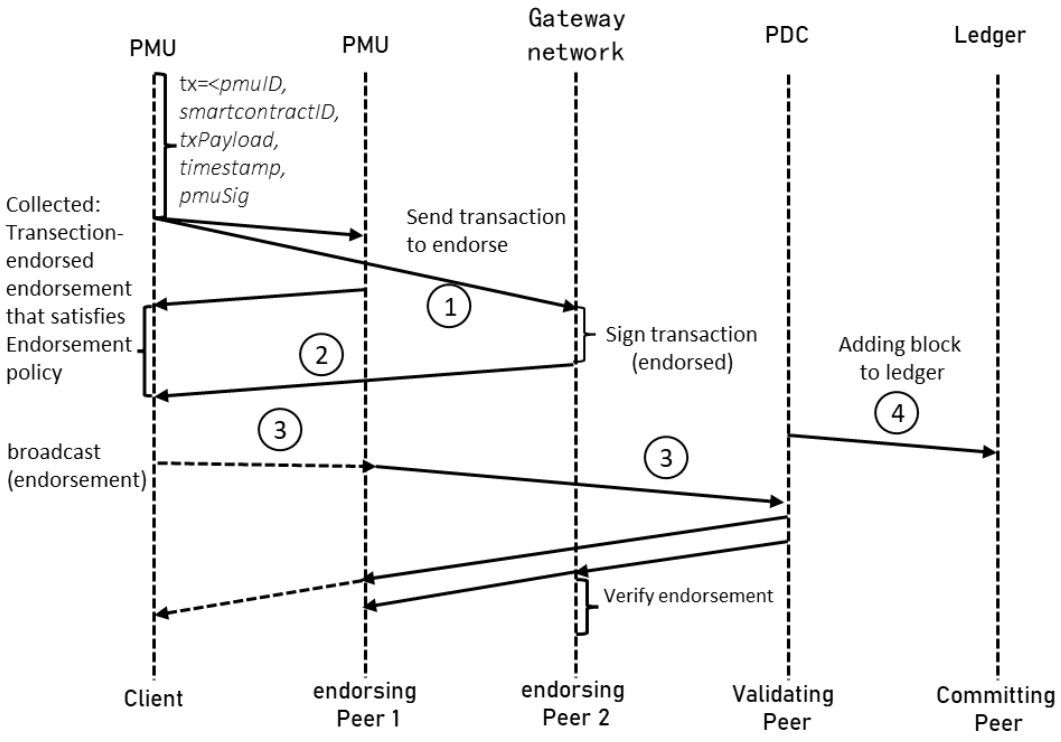
Output: B_{i+1} ..... B_{i+n}

1. *Initialize:*
2. T_b : *PMU initialize the Tx*
3. P_i : *PDC*
4. m *: number of PDC in the network*
5. $\boldsymbol{B}_{byte}$: *Block Size*
6. *j = 0*
7. $\boldsymbol{B}_i$ *: last appended block in ledger*
8. $Sign\ (T_b)$*: PMU* $Sign$ *the Tx*
9. $varify\{(Sign\ (T_k)\}$*: PDC verify the PMU signature*
10. ***if*** *valid* ← *Tx endorsed <* T_b*-ENDORSED,* $Sign$ *>*
11. ***else*** *Tx invalid <* T_b*-INVALID, Rejected>*
12. *<ENDORSED-* T_b*,* $Sign$ *>: broadcast to the peer PDC*
13. *Peer PDC verify* $(ENDORCED - T_b)$
14. ***while*** $j \leq m || T_b, Sign$
15. j ← *j+1 (update transaction pool)*
16. ***if*** $B_{byte} = 0$ T_b ← *Genesis Transaction (* T_S *)*
17. ***else*** B_{i+1} ← B_i $[Sign\ \{\mathcal{H}(T_b)\}, T_b]$ *appended block*
18. ***end while***

Figure 3.11: Distributed Consensus Algorithm



(a)



(b)

Figure 3.12: (a) TX Endorsement (b) and TX flow in Proposed Approach

3.4 Case Study 1: Experiment of WAMS without Blockchain Integration

The experiment of WAMS has conducted in Case Study 1 using laboratory test bed shown in first partial part of Figure 3.12. The implementation test bed follows co-simulation technique using MATLAB IEEE 9-bus system, cloud server, OPC web server and SCADA Wonderware InTouch, that briefly discussed in previous section. A simulated DERs integrated hybrid power system consolidated with a two-way communication system in the experiment. The PMUs in the simulated model continuously measure phasor measurement through current transformer (CTs) and voltage transformer (VTs) interfacing different bus bars and standardize into standard values (SV) by following IEEE C37.118 protocol. Then measured values transmitted to the ThinkSpeak cloud server and OPC UA KEPserver simultaneously. Hence, SCADA machine from substation extracts those SV for monitoring. As a result, it expands the communication between the devices in different substations.

3.5 Case Study 2: Experiment with Blockchain Integration

The implementation of proposed BC approach has been demonstrated in Case Study 2 corresponding to second part of Figure 3.12. This is achieved through MATLAB-SCADA co-simulation design testbed integrates with Hyperledger Fabric BC to records PMU measurement. For the performance validation, Hyperledger BC setup is prepared and installed with a Linux machine (64-bit Ubuntu operating system with eight GB RAM) and configured with organizations representing validator peer which are org_1 ------ org_n. For each organization have a certificate authority which are CA_1 ------ CA_n and one Membership Service Provider (MSP) for validating the transection proposal.

The proposed framework in section 3.3 has been tested and evaluated with different bus configuration and cluster sizes that includes IEEE bus systems as illustrated Table 3.5.

Initially, the experiment of BC integration for secure phasor data sharing has conducted with IEEE 9-bus system. In this regard, IEEE 9-bus network divided into 2 sub-divisions with 3 and 4 PMUs for each sub-division respectively. Furthermore, proposed framework is tested with increased number of PMU nodes with large number of network (IEEE 39-bus, and 118-bus network) to analyze in high volume of data recording ability in WAMS application. Therefore, IEEE 39-bus, and 118-bus network has been divided into 3, and 4 sub-divisions with different number of PMU nodes in accordance with configuration Table 3.5. Hence, the PMU reading in the cluster consolidated into cluster gateways as far proposed approach. Then, a set of PMUs interface with lossless time series data compression technique to compress the phasor data into data segment (Dahunsi et al., 2021; Kaur & Kaur, 2015).

This technique uses Gorilla algorithm (Iqbal & Keskar, 2021), which is based on delta-delta encoding to compress time stamp point and XOR-based compression for floating point values. The experiment utilized Python's panda library to compress the PMU data and converted into data segment at 1's interval while each segment contains ***N*** reading from multiple PMUs depending on the number of PMUs in the cluster. At the same time, Node-RED is a graphical flow utilize in this work to integrate different PMU nodes to receive, transform, and output data from OPC server sent by the virtual PMU in the MATLAB model. PMUs measure current and voltage phasors and are published to Node-RED MQTT massage broker through OPC UA protocol. On the other hand, Linux machines subscribe to the same topic and receive the payload that generates the transaction proposal by node.js. Then transaction proposal endorsed by at least one peer, attached digital signature, and submitted to the blockchain network. Subsequently smart contact (chaincode) is called appropriate function and validate the transaction. Finally, the transaction was recorded in the BC ledger successfully.

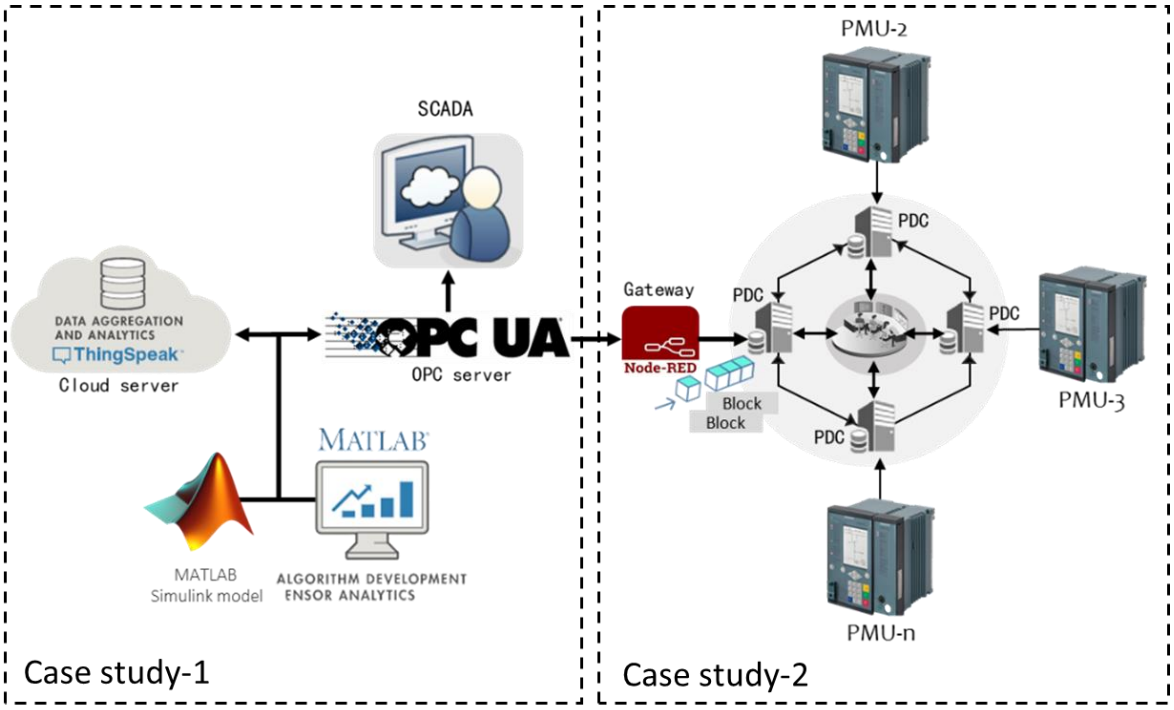


Figure 3.13: Implementation of proposed approach in Co-Simulation Environment

3.6 Case Study 3: Experiment with Increased PMU Nodes

The experiment has extended with IEEE 39 and118 bus systems in Case study 3, to evaluate the scalability performance of proposed scheme with quantitative analysis. The proposed framework demonstrated in Section 3.3 has been analysed using increased bus numbers and cluster sizes. Therefore, a quantitative analysis and comparison in terms of scalability have been conducted with increased number of PMU nodes according to the sub-division cluster size and number of PMUs shown in Table 3.5. Nevertheless, the cluster sizes and number of PMUs defined by IEEE 39 and 118 bus systems as shown in Table 3.5.

It is important to note that, number of PMU measurements per second, commonly referred to the sampling rate or sample values of a PMU. A typical PMU provides between 30 to 60 samples per second. However, in this research, the sampling rate is set to 50 samples

per second in the simulation model. Therefore, the number of PMU readings was selected accordingly for each cluster for the purpose of quantitative analysis.

Table 3.5: PMU Clusters in IEEE Buses

System	Number of PMUs in Cluster $(n \times m = N_s)$	Number of PMU readings in the cluster per second (k_t)
IEEE 9 Bus	3 PMUs Cluster	150
	4 PMUs Cluster	200
IEEE 39 Bus	3 PMUs Cluster	150
	5 PMUs Cluster	250
	7 PMUs Cluster	350
IEEE 118 Bus	3 PMUs Cluster	150
	7 PMUs Cluster	350
	10 PMUs Cluster	500
	23 PMUs Cluster	1150

3.7 Chapter Summary

This chapter outlines the research methodology adopted to design, implement, and evaluate the proposed blockchain-integrated sub-division-based WAMS framework. The methodology is structured systematically to provide clarity on the experimental procedures and system architecture. The proposed framework incorporates following key components: DIAM-based PMU device verification, EdDSA-based PMU data authentication, and A lightweight consensus mechanism for efficient transaction validation. These components collectively aim to enhance data security, reduce processing delays, and ensure the trustworthiness of PMU data across the network. The chapter is divided into multiple sections detailing the security mechanisms used. It briefly describes how DIAM enables secure and decentralized device identification, while EdDSA ensures cryptographic integrity and authenticity of phasor data during transmission.

To evaluate the framework, three experimental case studies were conducted: Case Study 1 presents the development of a testbed environment for simulating a WAMS scenario. Case Study 2 focuses on integrating blockchain into the testbed to measure its performance in securing PMU data. Case Study 3 extends the experiment by increasing the number of nodes and transaction volume to assess scalability and latency under high data rates. These case studies demonstrate the practical feasibility of the proposed architecture in maintaining data integrity, confidentiality, and trust during real-time PMU communication.

Overall, the methodology is designed to validate that the proposed framework can effectively mitigate unauthorized access, ensure secure, real-time data exchange, contributing to a more resilient, and secure smart grid infrastructure.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Overview

In this section, the thesis result including proposed approach has demonstrated using the experimental test case outlined in Section 4.2. Consequently, the implementation and performance analysis of the proposed framework are presented accordingly. The first case study demonstrates the simulation results of DERs integrated WAMS, two-way phasor data communication, and SCADA monitoring without BC integration using IEEE 9-bus system. Meanwhile, the thesis emphasizes the implantation result of the proposed blockchain (BC) framework in the second case study. Additionally, we extend the implementation experiment of proposed framework with IEEE 39 and 118-bus system in case study 3 to evaluate the performance. In the experiment, PMUs recording phasor data in immutable database after authentication which in turn inherently establish trust between the PMU devices and back-end servers. Hence, data measurement (transactions) is stored and organized by time stamps in groups called blocks. These blocks are linked together and form a chain of blocks, or a BC which is immutable. All phasor data stored in the BC enabled WAMS system has been monitored in SCADA UI. Furthermore, the performance analysis of proposed framework is presented in the final phase of the thesis using some critical parameters e.g., transaction throughput, transaction latency, and corresponding scalability of the network. The evaluation of scalability improvement has been shown after implementation of proposed sub-division based WAMS architecture. This work considers phasor measurement including voltage and current magnitudes, phase angles and frequency for each bus bar.

4.2 Case Study 1: Real-time Dynamic Monitoring in WAMS Architecture

The experimental result from the simulation of WAMS is demonstrated by observing the DERs-integrated hybrid power system under normal operating conditions. Meanwhile, the simulation results also documented during extreme fault conditions including relay operations and related circuit breaker tripping to assess the performance of dynamic grid operation. The laboratory experimental test bed set up shown in Figure 2 (Appendix).

4.2.1 Monitoring Results in MATLAB Simulink

The PMU measurement in Figure 4.2 (a) through 4.2 (g) analysed using same parameters and same unit, for instance, voltage magnitude (v), current magnitude (A) and phase angle (deg) and frequency (Hz). It is observed that, the PMUs at bus 5,6,7,9 (IEEE 9-bus network) shows stable voltage reading within the reference and stable line voltage in normal operating conditions, which is $v_{ab} = 230kV$; average amplitude starts from $t = 0$ initially and after $t = 0.02s$ gradually steady into rated bus voltage as illustrated in Figure 5.2 (a), (b), (c) and (d). Similarly, phase angle and frequency also settled into constant output after a while, stabilizing the system. Hence, all these parameters reflect state of the grid in real-time, which helps the utility for high-resolution monitoring.

On the other hand, PMU in PV bus has shown large phase shift, and associated voltage drops in the magnitude shown in Figure 4.2 (e). This fluctuation of bus voltage results in fluctuated current due to the intermittent nature of irradiation and switching condition. Therefore, this larger phase angle in the PV bus indicates system instability, whereas voltage amplitude drops, specifying the grid stress. Additionally, a sudden de-escalation is noticed for a few moments in the initial terminal voltage of the wind turbine as shown Figure 4.2 (f). As a result, fluctuation of inrush current has been noticed that again

decreases gradually. This is attributed to the intermittent characteristics of wind speed. After t = 0.02s, voltage, current and frequency gradually returned to the normal operating condition and stabilized the system (see Figure 4.2 (f). Although PMU measurement of hydro bus in Figure 4.2 (g) shows, a stable voltage reading within the reference range and maintains stable line voltage under normal operating conditions. It is worth mentioning that the initial frequency fluctuation has observed which occurs because of transient instability caused by a temporary mismatch between load and generation as shown Figure 4.2. As the system reaches power balance, the frequency gradually stabilizes. In the meantime, the same transient behaviour is also visible in the ThingSpeak cloud since the measured data is transmitted in real time as shown in Figure 4.4. This dynamic behaviour of the buses has successfully captured by phasor measurement devices installed in the specific buses and sent to the phasor data concentrator for aggregate.

Furthermore, the three lines to ground fault (3L-G-F) are applied in the load side of 33kV bus for 0.14s; however, it is removed after 0.15s while the simulation starts. The fault configuration for B1 is set for 125% threshold limit of CT in the inherent time delay. In this context, PMU reading has been displayed in Figure 4.1 while a 3-line to ground fault (3L-G-F) applied at substation bus. The system behaves stable for 0.1s until the fault occurs for 0.13s, the relay sends command signal to CB to trip and cleared the fault while current cross the relay threshold setting. In this point, PMUs in the 33kV bus reads larger phase angle that indicates system instability whereas voltage amplitude drops into lower magnitude that indicate fault located outside the bus. Moreover, PMU in 11kV bus has shown extreme phase difference and associated voltage drop in the magnitude as shown in Figure 4.1 after fault occurs in the substation area. The relays in the network trigger and isolate upon receiving the fault signal and return to normal operation after 0.13 seconds.

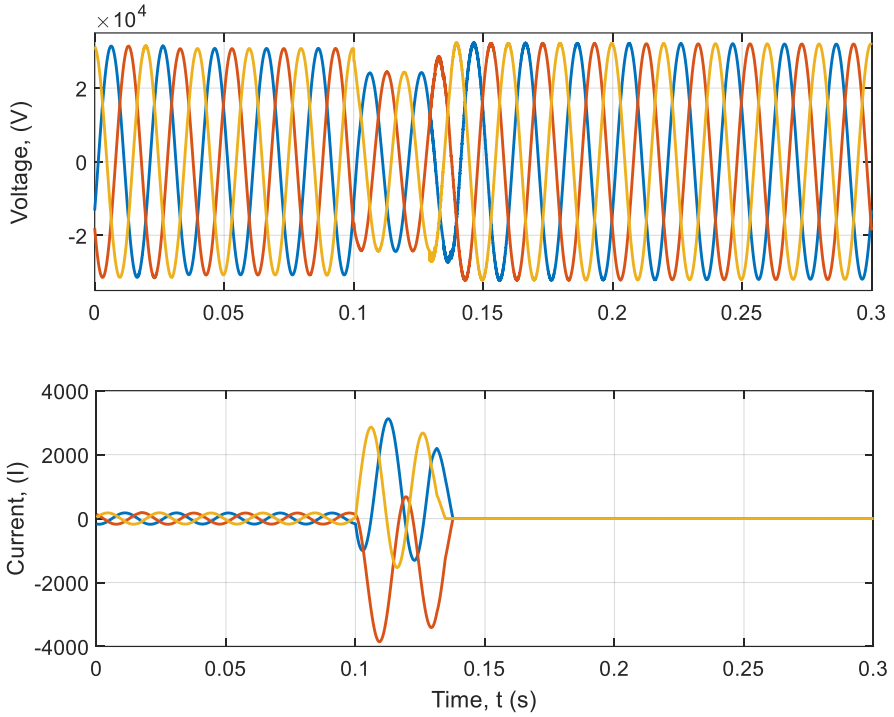
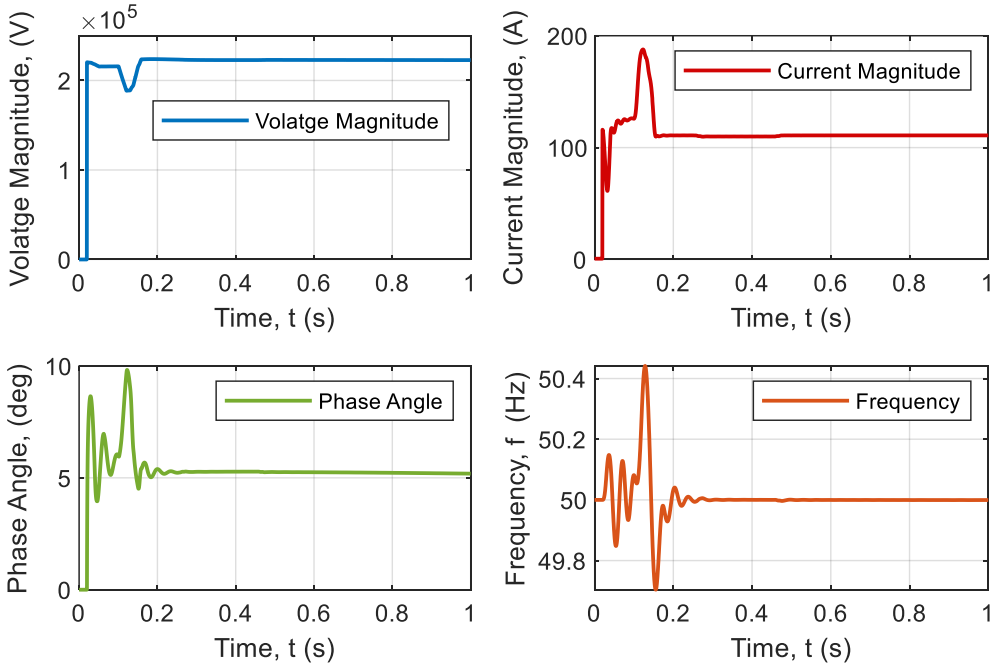
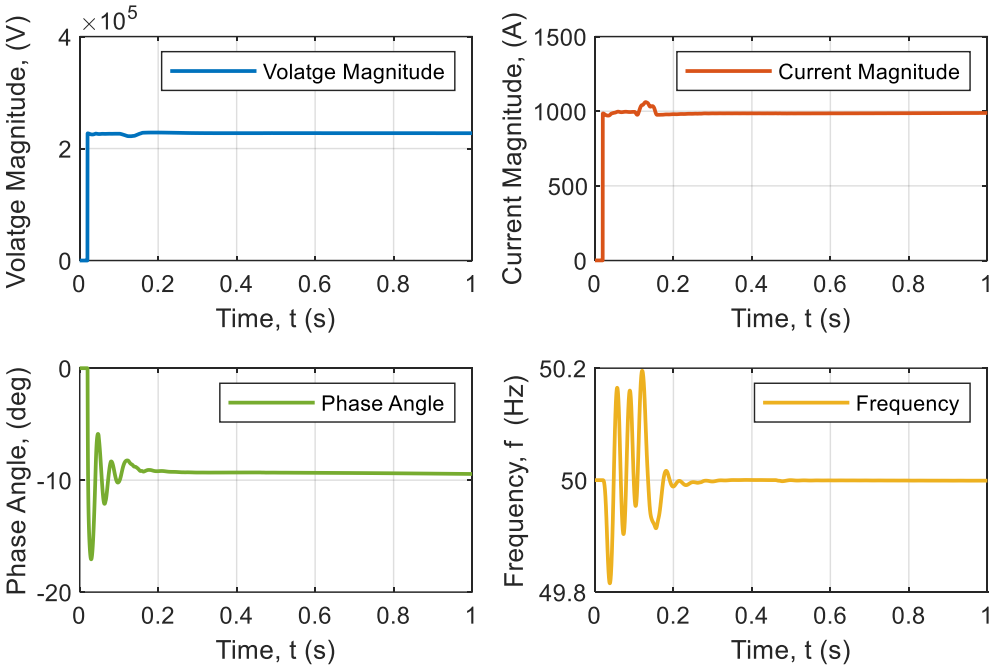


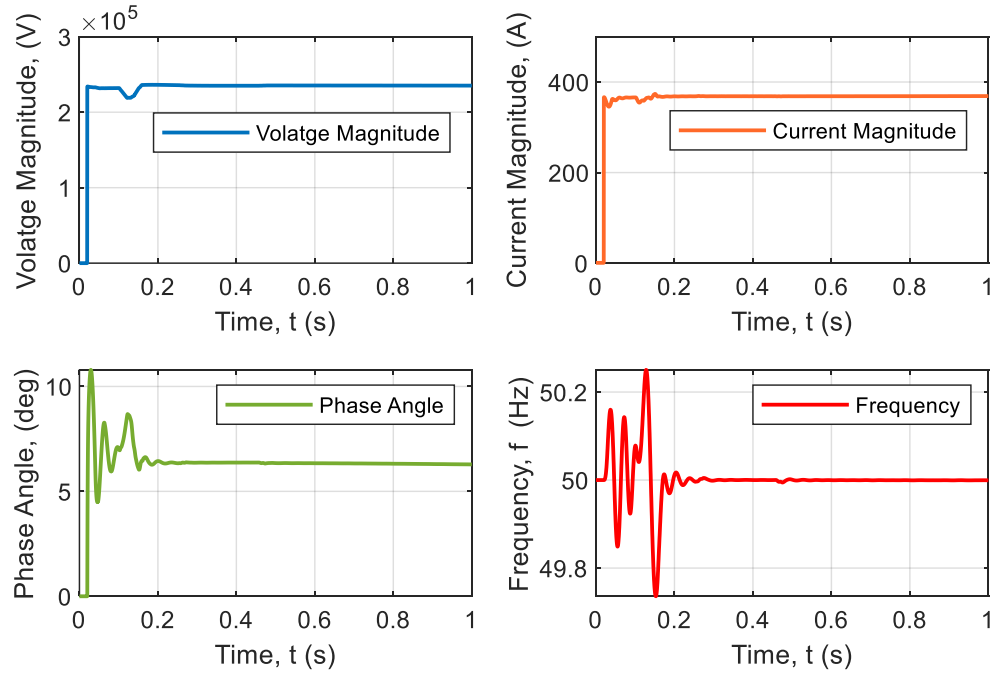
Figure 4.1: Fault Bus at 11kV-Bus



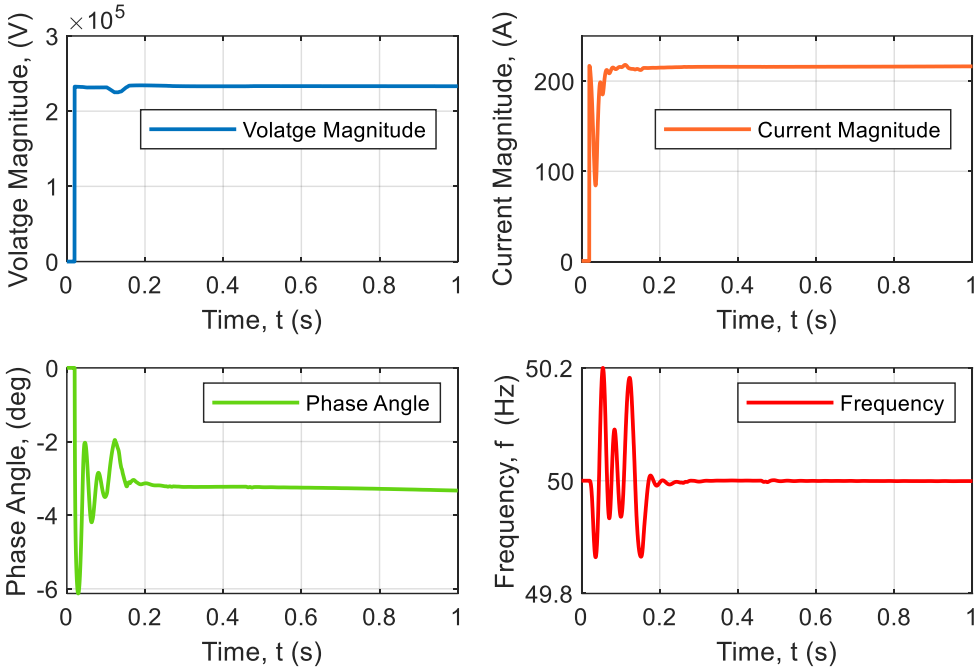
(a) Bus 5


×10^5
Volatge Magnitude, (V)
Volatge Magnitude
Time, t (s)
Current Magnitude, (A)
Current Magnitude
Phase Angle, (deg)
Phase Angle
Frequency, f (Hz)
Frequency

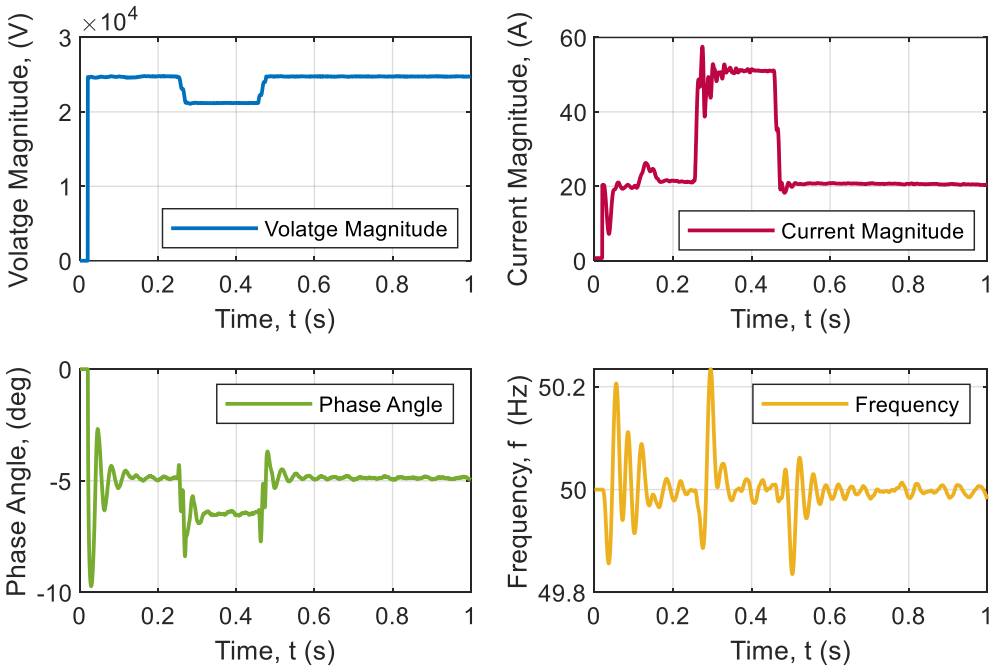
(b) Bus 6


×10^5
Volatge Magnitude, (V)
Volatge Magnitude
Time, t (s)
Current Magnitude, (A)
Current Magnitude
Phase Angle, (deg)
Phase Angle
Frequency, f (Hz)
Frequency

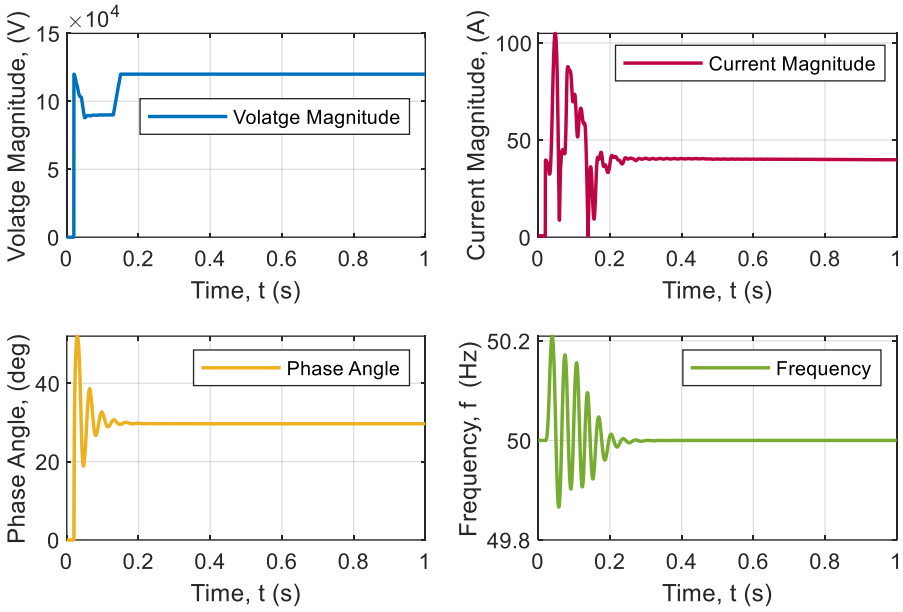
(c) Bus 7



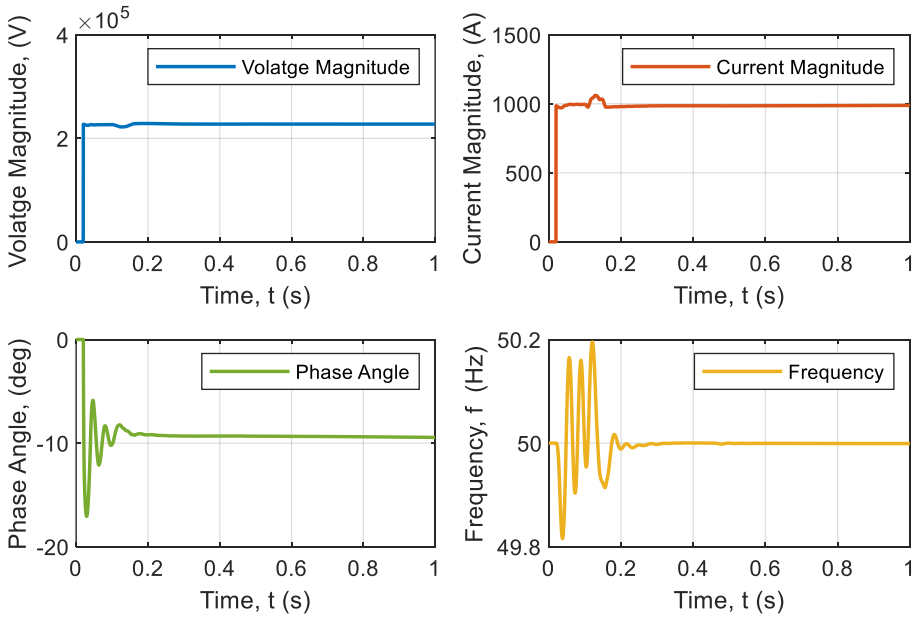
(d) Bus 9



(e) PV Bus



(f) Wind Bus



(g) Hydro Bus

Figure 4.2: Phasor Estimation at Transmission Buses (Bus 5, 6, 7, 9), Wind Bus, PV Bus, and Hydro Bus

4.2.2 Monitoring Results in Web Server

Referred to the WAMS architecture outlined in section 3.2, the measurements of all grid events and command signals transmitted to OPC and the ThingSpeak cloud server to establish connectivity with SCADA monitoring. Therefore, monitoring data of every individual PMU are visible in the server OPC quick client, as illustrated in Figure 4.3 (for PMU1). The data type used is double, representing the actual monitoring values. Timestamps indicate when data is streamed through the server, while the "good" quality reflects that the data have been retrieved successfully. The update count represents the number of data changes during the streaming process. Every channel holding individual PMU reading in the KEPServer shown in Figure 4.3. This validates the data readings from power system busbar have successfully streamed to the server.

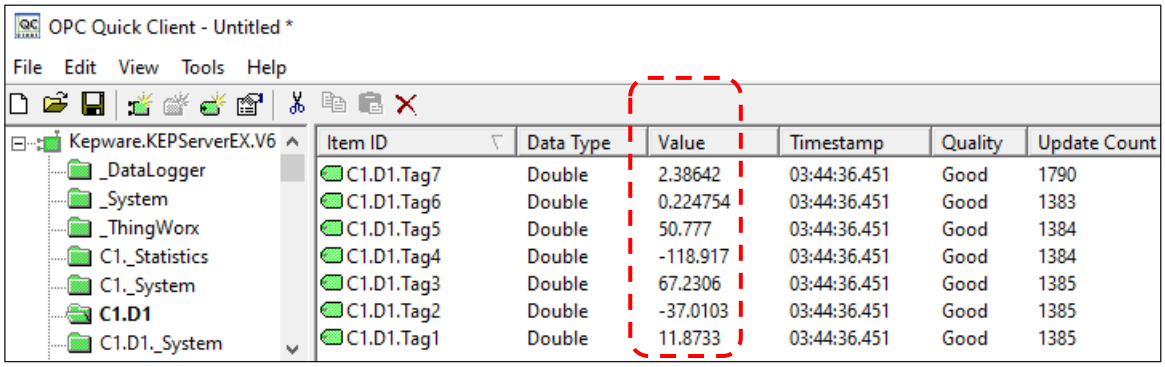


Figure 4.3: Monitoring Data in Web Server (KEPServer)

4.2.3 Monitoring Results in Cloud Server

As far as WAMS architecture outlined in section 3.2, the PMUs transmitting electrical parameters simultaneously to the cloud server and OPC server. Figure 4.4 represented the bus voltage and system frequency accurately that validated data transfer between MATLAB power model and ThinksSpeak cloud server. This facilitates the substation SCADA HMI to extract and stored the measurement in the SCADA Historian

database for offline event analysis. However, the small frequency deviation in last subfigure 4.4 which is quickly converges to steady-state conditions. This temporary frequency oscillations occurs due to load–generation imbalance and synchronization processes.

Figure 4.4: Monitoring Data in Thingspeak Cloud Server

4.2.4 Monitoring Results in SCADA

The SCADA energy management system dashboard, shown in Figure 4.5, displays all the essential real-time dynamic readings from each PMUs in the bus bar of the hybrid energy model. However, the full window of the SCADA HMI is depicted in Figure 1 (Appendix). These readings are successfully streamed from the utility network, modelled in Simulink, to the SCADA dashboard via the OPC server. The behaviour of the power parameters has been thoroughly analyzed in the monitoring results from MATLAB Simulink. It's important to note that the data streaming from the server to the SCADA system experiences minimal delays. Additionally, the laboratory experiment on phasor data sharing within the WAMS architecture is illustrated in Figure 2 (Appendix).

G1: Bus 4			G2: Bus 7			G3: Bus 9		
Voltage |V|	223.6	(kV)	Voltage |V|	232.4	(kV)	Voltage |V|	231.9	(kV)
Phase angle	8.4	(Deg)	Phase angle	4.6	(Deg)	Phase angle	-2.1	(Deg)
Current |I|	483.5	(A)	Current |I|	361.9	(A)	Current |I|	257.9	(A)
Phase angle	-22.4	(Deg)	Phase angle	-18.1	(Deg)	Phase angle	182.4	(Deg)
Frequency	49.8	(Hz)	Frequency	50.1	(Hz)	Frequency	50.0	(Hz)
Active Power	131.4	(MW)	Active Power	77.6	(MW)	Active Power	-59.6	(MW)
Reactive Power	134.9	(MVAR)	Reactive Power	131.4	(MVAR)	Reactive Power	-105.4	(MVAR)
Bus 5			**Bus 6**			**Bus 8**		
Voltage |V|	216.9	(kV)	Voltage |V|	226.3	(kV)	Voltage |V|	228.1	(kV)
Phase angle	4.0	(Deg)	Phase angle	-6.2	(Deg)	Phase angle	15.8	(Deg)
Current |I|	117.3	(A)	Current |I|	986.4	(A)	Current |I|	2.7	(A)
Phase angle	69.1	(Deg)	Phase angle	-5.9	(Deg)	Phase angle	-35.9	(Deg)
Frequency	50.3	(Hz)	Frequency	49.9	(Hz)	Frequency	50.1	(Hz)
Active Power	17.1	(MW)	Active Power	-0.1	(MW)	Active Power	1.0	(MW)
Reactive Power	-77.1	(MVAR)	Reactive Power	12.9	(MVAR)	Reactive Power	0.7	(MVAR)
PV Bus			**Wind Bus**			**Hydro Bus**		
Voltage |V|	24.6	(kV)	Voltage |V|	96.6	(kV)	Voltage |V|	226.3	(kV)
Phase angle	-2.8	(Deg)	Phase angle	20.1	(Deg)	Phase angle	-6.2	(Deg)
Current |I|	15.8	(A)	Current |I|	99.3	(A)	Current |I|	986.4	(A)
Phase angle	-178.2	(Deg)	Phase angle	102.4	(Deg)	Phase angle	-5.9	(Deg)
Frequency	50.0	(Hz)	Frequency	50.1	(Hz)	Frequency	49.9	(Hz)
Active Power	-0.4	(MW)	Active Power	1.3	(MW)	Active Power	223.2	(MW)
Reactive Power	-0.5	(MVAR)	Reactive Power	-16.1	(MVAR)	Reactive Power	12.9	(MVAR)

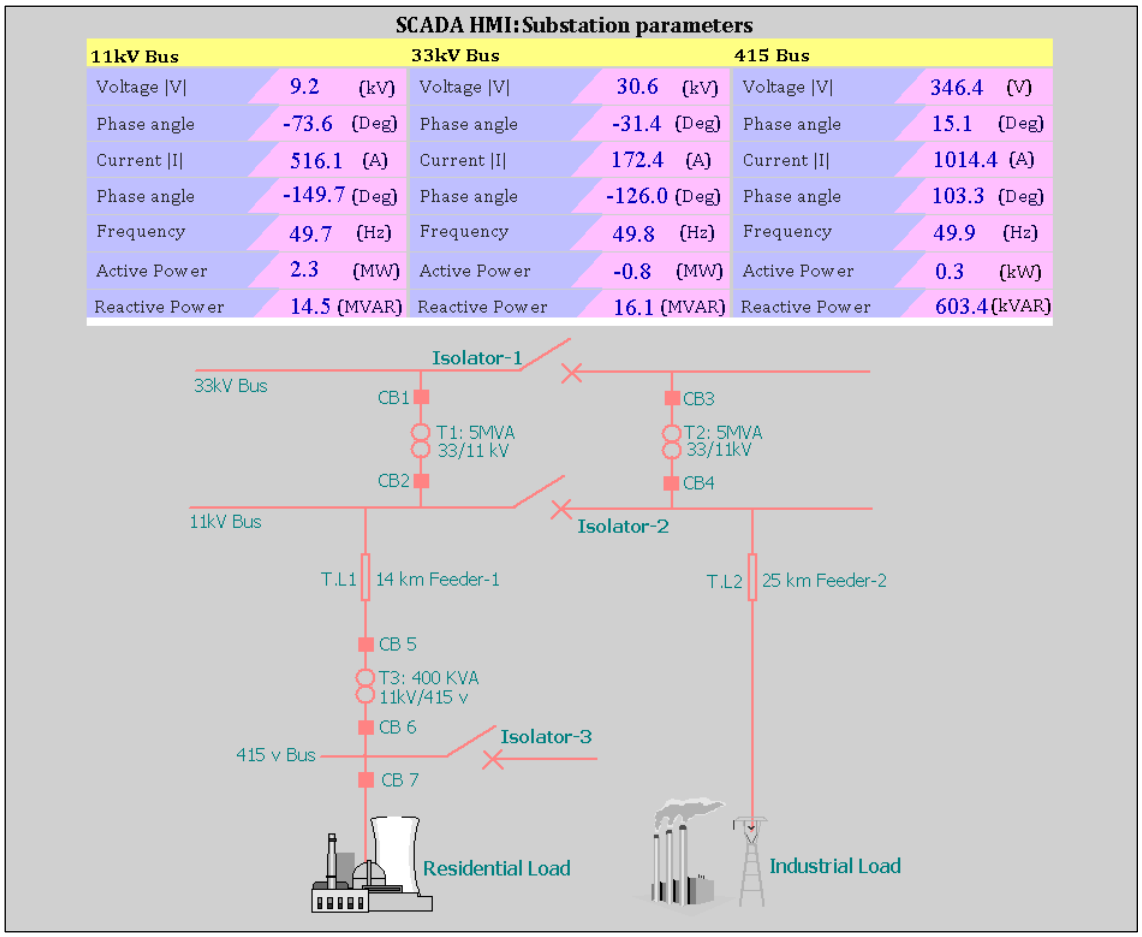


Figure 4.5: Monitoring of Electrical Parameters in SCADA UI

4.3 Case Study 2: Blockchain to Share Phasor Data in IEEE 9 Bus System

As far as the method explained in section 3.5, Node-RED is employed in this project as a graphical interface to facilitate the data recording of PMU nodes in BC-enabled system. It serves to receive, transform, and output data from an OPC server, which is transmitted by the PMU within the MATLAB model. Figure 4.6 clearly explains the graphical flow of data that fed to BC. The PMUs transmit current and voltage phasors in real-time, which was published to the Node-RED MQTT message broker via the OPC UA protocol as shown in Figure 4.6. On the other hand, Linux machines subscribe to the same topic, receiving the payload that initiates the transaction proposal through node.js. Subsequently, the transaction proposal endorsed by at least one peer, attached with a digital signature, and submitted to

the blockchain network. Following this, the appropriate function is invoked by a smart contract, which validates the transaction. Finally, the transaction is recorded in the ledger.

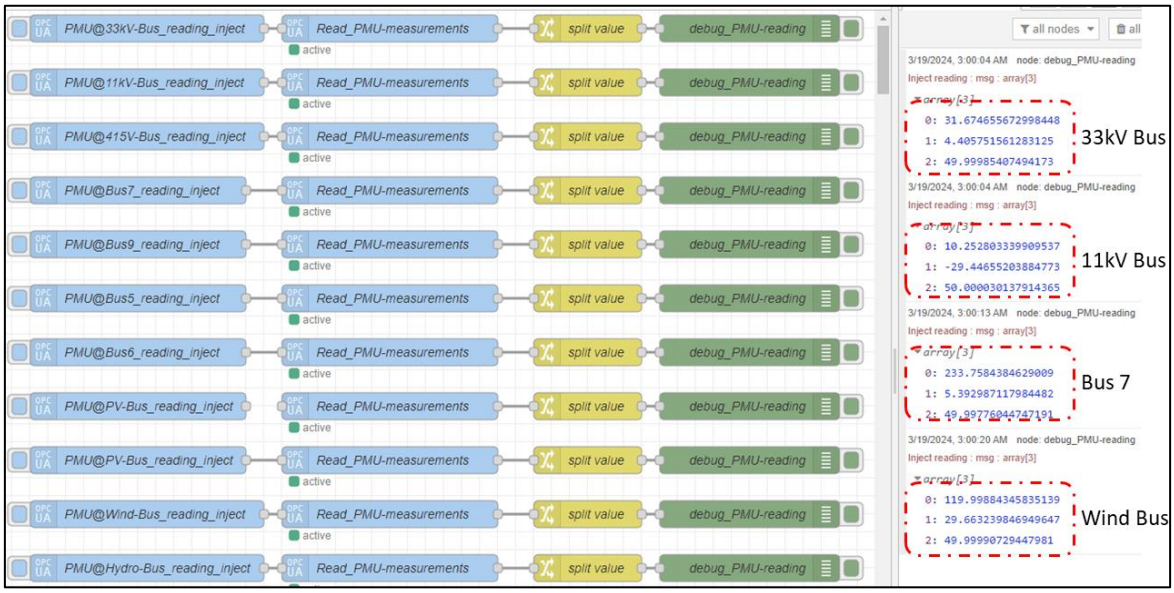
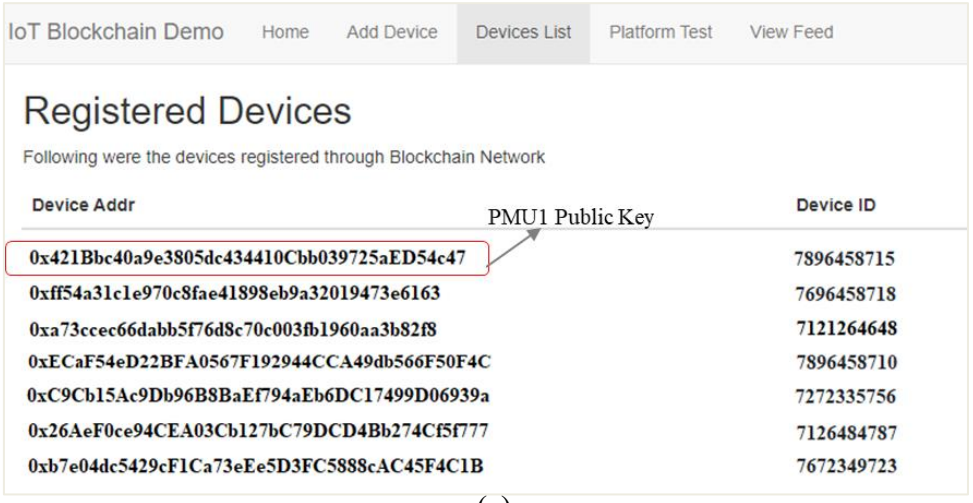
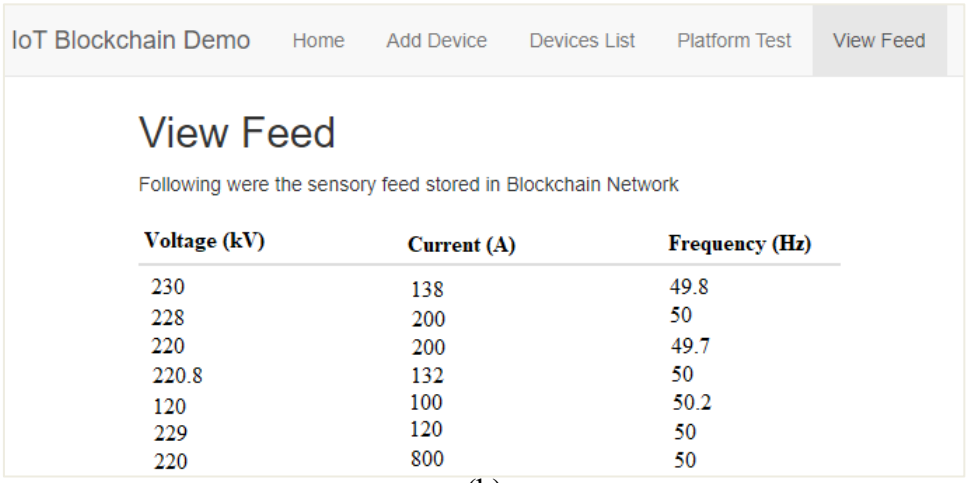


Figure 4.6: PMU Measurements Published in Node-RED Interface

Initially, the PMU devices undergo verification, and data authentication process to ensure resilient data sharing as illustrated in Figure 4.7, a web-based device registration user interface (UI). Hence, all PMUs deployed in experimental network registered via a web-based administrative UI using *Add Device* button. The Figure 4.7 (a) clearly shows the PMU device registration using their own ID number. During PMU registration, the identity of each device is recorded on the BC network by storing its unique ID, serial number, device address, and communication port information. Nevertheless, list of registered devices has confirmed using *Devices List* button with their address. The address often calls public key of a particular device which is assign while a PMU registered in the BC-integrated architecture. All registered device identities have been authenticated, ensuring that only verified PMUs can submit transactions (transmit data) to the PDC. Hence, authenticated PMU share state variables and recorded in the BC based data base system.



(a)



(b)

Figure 4.7: PMU Measurement Sharing with BC; (a) Device Registration UI, (b) PMU Feeding in Web Interface

Furthermore, the registered PMUs then sharing data with their secret key (SK^+). The admin machine authenticated the PMU device using verifying key (PK^+) which confirms that the data originates from a legitimate and authorized device within the network. Table 4.3 listed the first transaction of all the registered PMUs shared their reading to PDC. The transaction data in the table represents the device ID, public and private keys of sender and block number in which the transaction includes. Nevertheless, the PMU recording in the BC as shown in Figure 4.7 (b), section *View Feed*. For the registering devices, admin UI refers to the createPMU function on PMU smart contract and executed the function to authenticate.

While device identity verification establishes the source of the data, data authentication ensures the integrity and authenticity of the data. After all, the PDC machine run database querying for data visualization and then transfer to SCADA UI for monitoring. Therefore, all the measurement recorded by PMUs in the BC system monitored in the SCADA UI as illustrated in Figure 4.8.

Table 4.1: Blockchain Transaction in WAMS Network

	Block Information				
Block Index	1				
Transaction Data	Sender	Receiver	Registered Device	Phasor Measurement	
				(kV)	(A)
Bus 7	PMU	PDC	7896458715	230	138
Private Key	0x84e390a740662e78c804cca488d4b32a24e385f4d502b				
Public Key	0x421Bbc40a9e3805dc434410Cbb039725aED54c47				
	Block Information				
Block Index	2				
Transaction Data	Sender	Receiver	Registered Device	Phasor Measurement	
				(kV)	(A)
Bus 9	PMU	PDC	7696458718	228	200
Private Key	0xf22571633f06ef4fdffed9d10252ed89b40129c78c38ef5				
Public Key	0xff54a31c1e970c8fae41898eb9a32019473e6163				
	Block Information				
Block Index	3				
Transaction Data	Sender	Receiver	Registered Device	Phasor Measurement	
				(kV)	(A)
PV Bus	PMU	PDC	7121264648	220	200
Private Key	0xb755b5702e867bdeaccb48f2bc3b3b0ade8dce38aab9bc				
Public Key	0xa73ccec66dabb5f76d8c70c003fb1960aa3b82f8				

Table 4.1: continue

	Block Information				
Block Index	4				
Transaction Data	Sender	Receiver	Registered Device	Phasor Measurement	
				(kV)	(A)
Bus 5	PMU	PDC	7896458710	220.8	132
Private Key	0x267bf588b59a0821598cb9b7e6bb4fd9bf0ffa5203b6c8				
Public Key	0xECaF54eD22BFA0567F192944CCA49db566F50F4C				
	Block Information				
Block Index	5				
Transaction Data	Sender	Receiver	Registered Device	Phasor Measurement	
				(kV)	(A)
Wind Bus	PMU	PDC	7272335756	120	100
Private Key	0x0d5412c07075D61c86d416b98E2040411E68c02F				
Public Key	0xC9Cb15Ac9Db96B8BaEf794aEb6DC17499D06939a				
	Block Information				
Block Index	6				
Transaction Data	Sender	Receiver	Registered Device	Phasor Measurement	
				(kV)	(A)
Bus 6	PMU	PDC	7126484787	229	120
Private Key	0xb74ddc20bd11a9fff148f04cc4188fb8c08d32ca2dea799				
Public Key	0x26AeF0ce94CEA03Cb127bC79DCD4Bb274Cf5f777				
	Block Information				
Block Index	7				
Transaction Data	Sender	Receiver	Registered Device	Phasor Measurement	
				(kV)	(A)
Hydro Bus	PMU	PDC	7672349723	220	800
Private Key	0xb3F48D1F0e496d83548D3D334B578454B3cec569				
Public Key	0xb7e04dc5429cF1Ca73eEe5D3FC5888cAC45F4C1B				

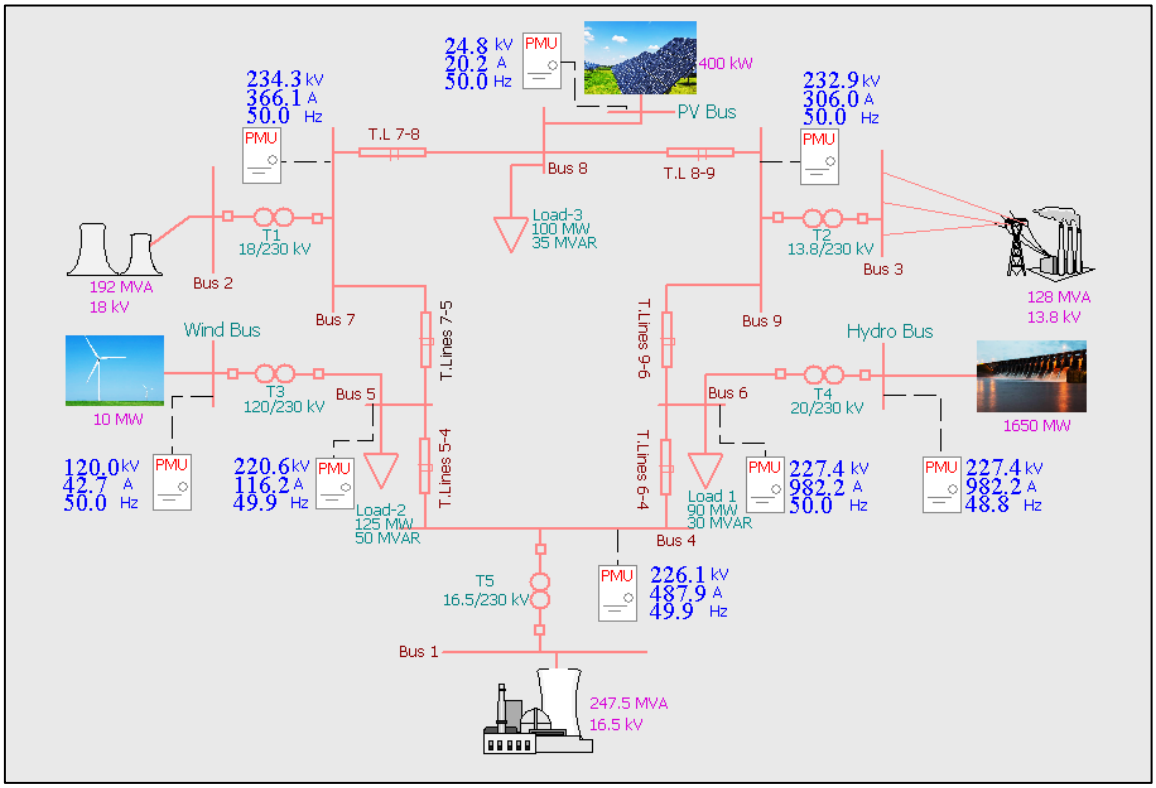


Figure 4.8: Monitoring Data in SCADA UI

4.4 Case Study 3: Blockchain to Share Phasor Data in Increased PMU Nodes

The implementation result of proposed framework demonstrated with different sizes of PMU clusters, ranging from 3 to 25 PMUs. Table 4.3 illustrated the variation of PMU readings (per/sec) in the different cluster. Nevertheless, the time series PMU measurement of 39-bus system to PDC gateway demonstrated in Figure 3 (Section Appendix).

4.4.1 Data Accumulation in Sub-Divisions

As the data segmentation strategy in the proposed framework, PMU readings accumulated over a 1-second interval and compressing these readings into a single data segment before initiating transaction. Following the configuration in Table 5.3 for different cluster, the recording from these PMUs in each cluster is accumulated over 1s then compressed and reduce the size of collected data before it is submitted to the BC.

Table 4.2: Comparison of Data Segment Size with Different Configuration

Systems	Number of PMUs in Cluster ($n \times m = N_s$)	Number of PMU readings in the cluster per/sec (k_t)	Original Data Size (kB/sec)	Compressed Data Size (kB/sec)	Compression Ratio (%)
IEEE 9 Bus	3 PMUs Cluster	150	16.11	4.95	70%
	4 PMUs Cluster	200	21.48	6.6	
IEEE 39 Bus	3 PMUs Cluster	150	16.11	4.95	70%
	5 PMUs Cluster	250	26.84	8.25	
	7 PMUs Cluster	350	37.57	11.55	
IEEE 118 Bus	3 PMUs Cluster	150	16.11	4.95	70%
	7 PMUs Cluster	350	37.57	11.55	
	10 PMUs Cluster	500	53.71	16.5	
	23 PMUs Cluster	1,150	123.69	37.95	

4.4.2 Data Compression and Reduction in Transaction Volume

Referred to Table 4.4, the original data size for each cluster varies significantly depending on the number of PMUs and their readings. The IEEE 9-bus and 39-bus system is segmented into several clusters, each containing 3 to 7 PMUs. The data accumulation results indicate a significant data size reduction in post-compression. The data size decreasing as the number of PMUs in the cluster increases. This reduction is evident in the

Figure 4.9 that showing the relationship between the numbers of PMU readings, the number of PMUs in the cluster, and the data size (both original and compressed). The graph highlights that, as the cluster size grows, benefits of compression is more pronounced, further reducing the strain on the BC network. Meanwhile, the larger system IEEE 118-bus, with clusters containing up to 25 PMUs, further validates the framework's capability to handle extensive data volumes. The visual representation in Figure 4.9 also illustrates a clear trend where larger clusters result in more significant data size reductions, thereby optimizing the transaction process within the BC.

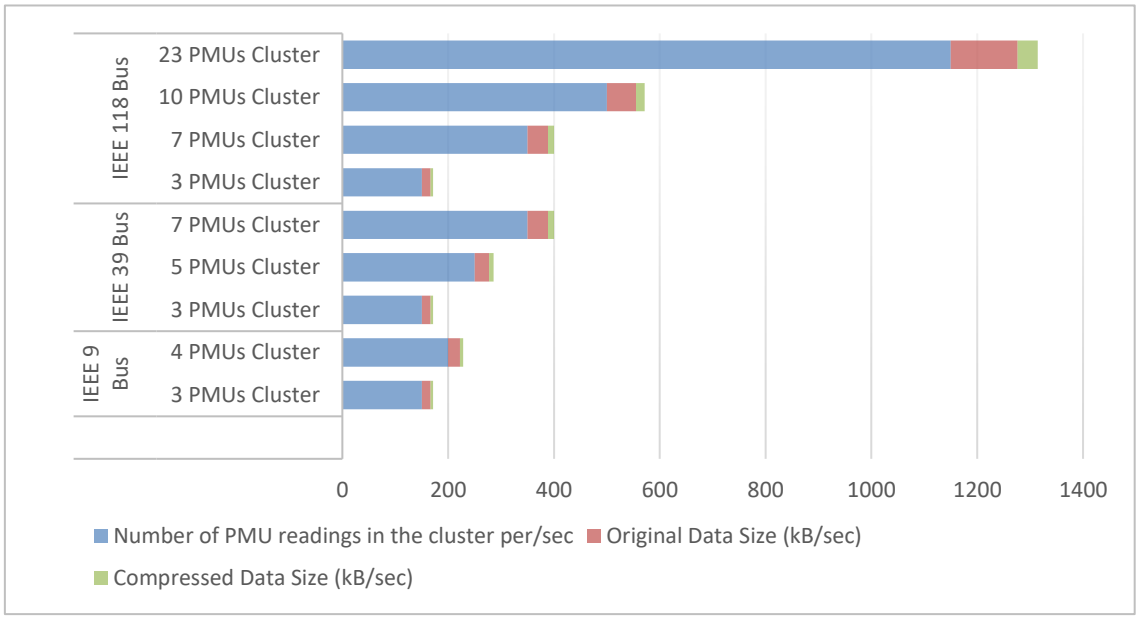


Figure 4.9: Data Reading with Original and Compressed Data Sizes in Clusters

Specifically, the original data sizes varied significantly with the smaller clusters (ranging from 3 to 7 PMUs per cluster) as Figure 4.9 suggest. While largest clusters generating upwards of 16.5 kB per second. However, data compression further reduced this data size by approximately 65% to 70% effectively, ensuring that the BC could handle the data without bottlenecks. In more complex system (118-bus system), with larger clusters (up to 25 PMUs per cluster), the original data size before compression could reach over 126 kB

per second. Here, compression reduced the data size to around 37.95 kB, achieving a similar reduction percentage. This demonstrates the scalability of proposed architecture and its ability to maintain high throughput even in larger grid configurations. The original data sizes for clusters with different numbers of PMUs (ranging from 3 to 25) were compared to their corresponding compressed sizes in Figure 4.10. The area plot comparison in Figure 4.10 indicates a significance reduction of data sizes after compression, which directly correlates with the reduction in transaction volume within the BC framework. Hence, the reduction in the number of transactions allows the BC to process more data per second, thus improving throughput. By compressing the PMU readings into a single data segment and aggregating these segments before initiating transactions, the proposed framework considerably reduces the transaction volume. This reduction is crucial for enhancing the throughput of the BC network, especially when dealing with large-scale systems. In such cases, the transaction volume minimized, leading to more efficient BC operation and lower network congestion.

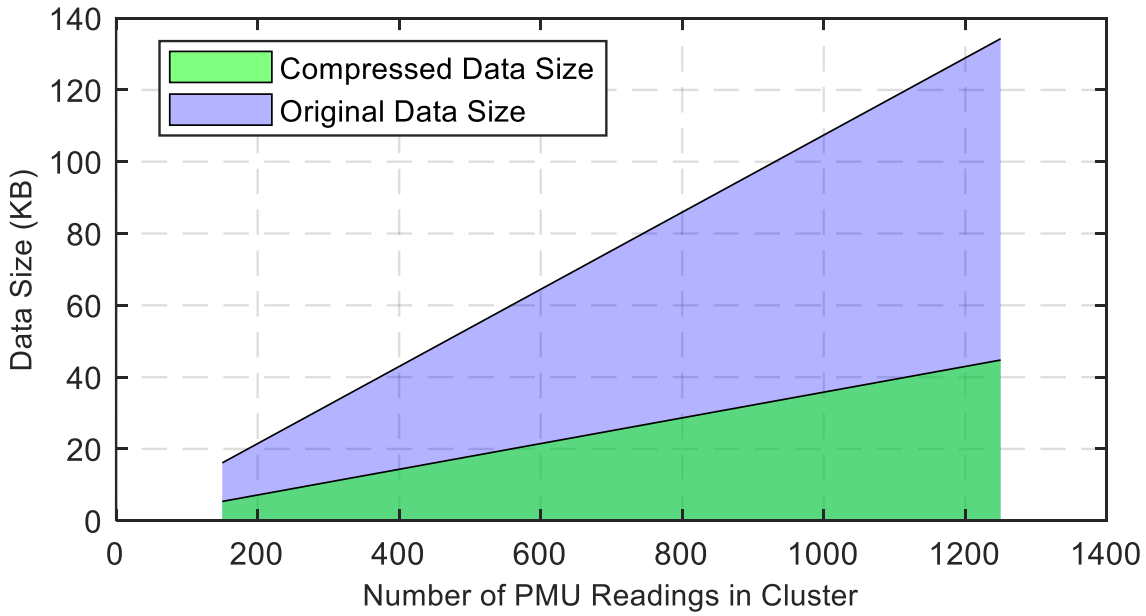


Figure 4.10: Data Size Comparison in Cluster

4.5 Performance Analysis of Proposed Framework

The performance analysis of proposed framework demonstrates in this section using some critical parameters, such as transaction throughput, latency, and corresponding scalability. Meanwhile, the thesis analysed the following metrics and associated impact that defined the overall performance and scalability of the proposed framework:

i. The Impact of the increased number of PMU nodes on transaction size and corresponding throughput

ii. The Impact of increased number of PMU nodes on block confirmation time and transaction latency

iii. The scalability of the proposed BC system with the increased number of PMU nodes

4.5.1 Analysis of Transaction Size and Throughput

The throughput of the proposed framework analyses in terms of transaction handling capacity per second (Tx/s). As the transaction throughput varies with the increased number of PMU nodes and the corresponding transaction size, it affects block sizes significantly. Therefore, bigger number of PMU nodes has escalated the transaction load and associated throughput in the network. The proposed framework enhances the BC throughput by minimizing the number of transactions per second as far transaction comparison in Figure 4.11. By encapsulating multiple PMU readings into a single transaction, the system reduces transaction load on the BC network, allowing it to process PMU data more efficiently. Without accumulation, the number of transactions/s for 3 PMU cluster in IEEE 9-bus is 150Tx/s while it is reduced to 1Tx/s with accumulation in the proposed framework.

Similarly, the transactions have been decreased in different PMU clusters as well for IEEE 39-bus and IEEE 118-bus consecutively. The accumulation and compression in proposed framework lowering the frequency of transactions in 90-95%, regardless of the number of PMUs in the clusters. This approach significantly reduces the transaction load on the BC network, making the system more efficient and scalable. The comparison in Figure 4.11, illustrates the substantial benefits of using accumulation and compression techniques in terms of reducing the transaction volume in a BC-enabled PMU network.

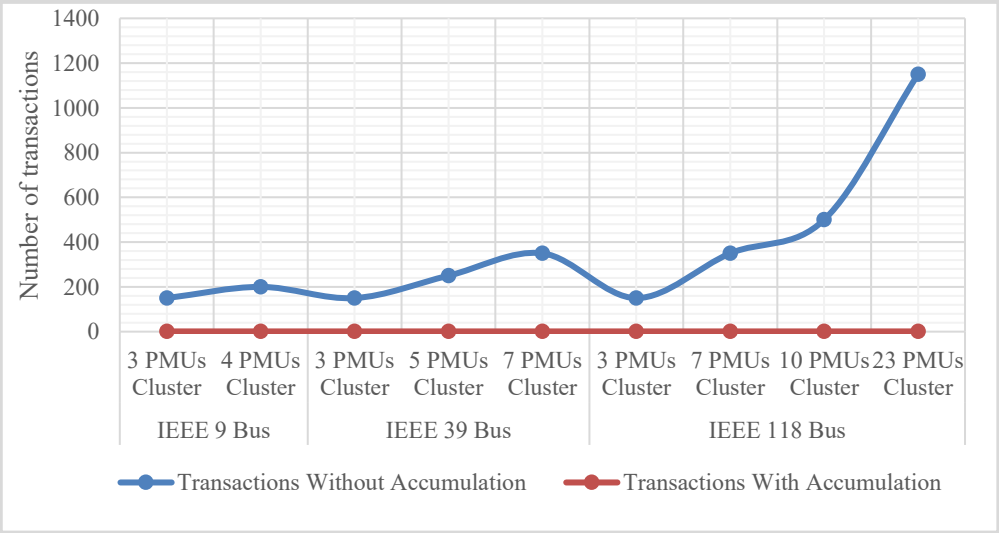


Figure 4.11: Transaction Frequency with/without Accumulation

Data segment as a function of accumulated numbers of PMU readings and data compression decreases transaction size in the proposed framework as shown in Figure 4.12 (a) compared to the conventional BC. This, reduction of transaction size has increased the block size even in the bigger number of PMU nodes in the cluster. Figure 4.12 (a) illustrates the reduction in transaction size as the number of PMU nodes increases. Therefore, an increase in the transaction size and larger block size improves the throughput in the network even in the increased number of PMU nodes as shown in Figure 4.12 (b). As our proposed

method directive, the sub-division based WAMS network maintains the workload and balanced block size with the marginal consensus algorithm.

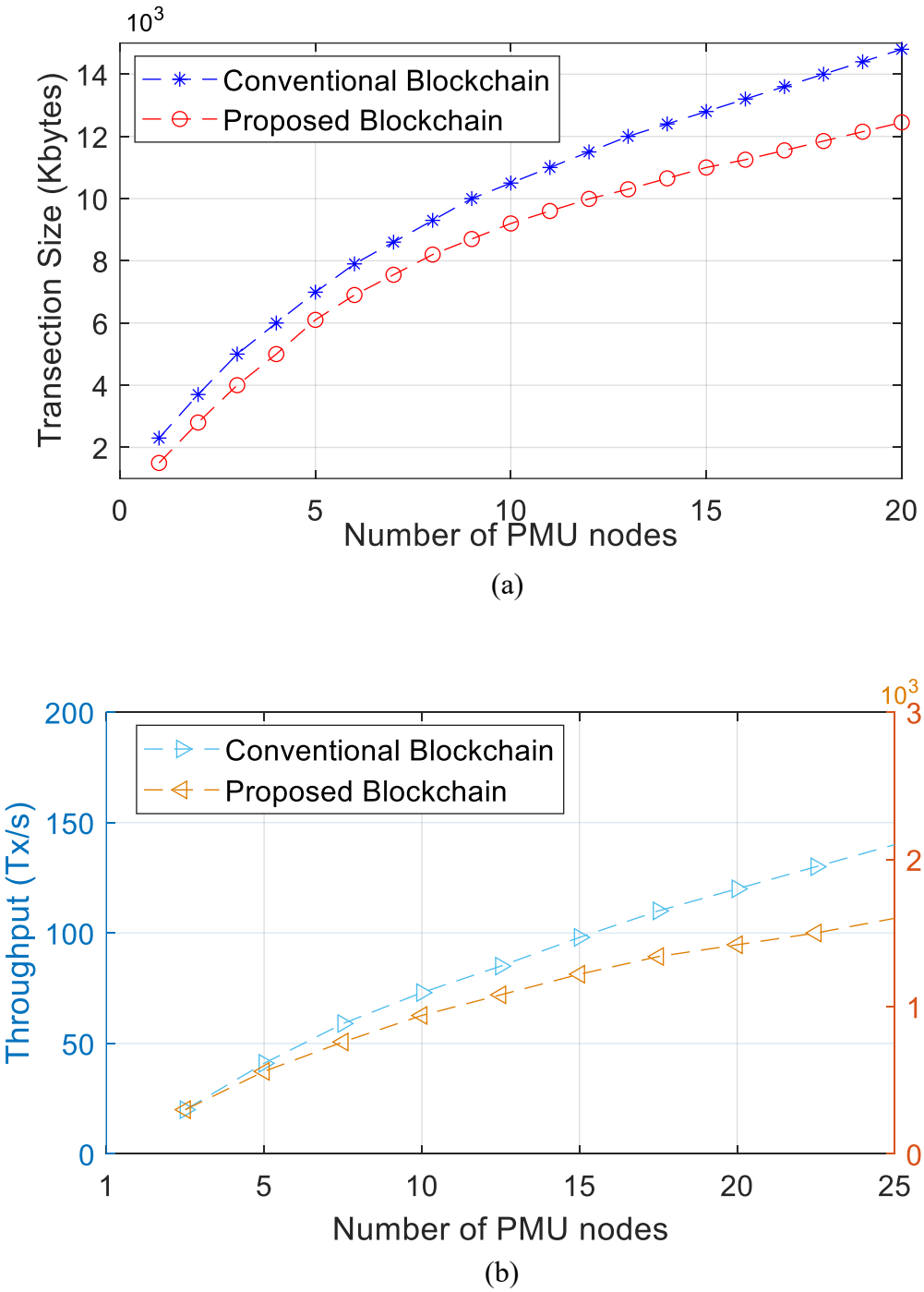


Figure 4.12: (a) Number of PMU Nodes against TX Size; (a) Throughtput against number of PMU nodes against number of TX

4.5.1.1 Transaction Throughput Before and After Compression

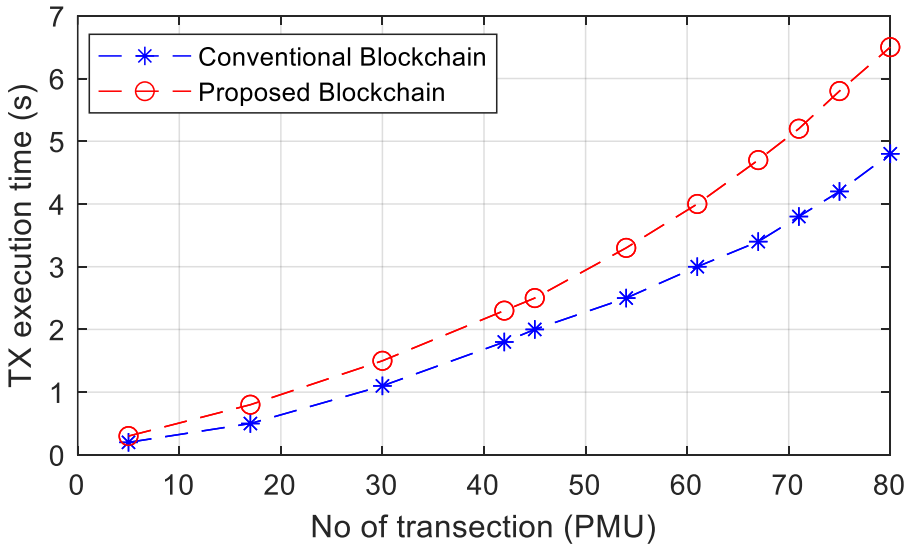
Table 4.5 clearly demonstrate the TPS before and after compression in the quantitative analysis. The experiment considers groups of PMUs into clusters for the IEEE 9-bus, 39-bus and 118-bus systems. Each PMU produces 50 samples per second. The table below uses the cluster sizes inferred from the dataset names (3–25 PMUs per cluster) and calculates the transaction load before and after applying one-second aggregation and compression. The throughput reduction factor is the ratio of transactions per second before compression and the transactions per second after compression. By aggregating one-second readings, the proposed framework reduces transaction load by 2-3 orders of magnitude. The compressed throughput (2–5 tx/s is comfortably below the throughput of typical permissioned BC (75 tx/s and up to 3000 tx/s in optimized setups), whereas the uncompressed load (350–2900 tx/s) would saturate or exceed the network.

Table 4.5: TPS Before and after Compression

Power system	PMUs per cluster	Total PMUs	TPS before compression	TPS after compression	Throughput reduction factor
IEEE 9-bus	Cluster 1: 3 PMUs Cluster 2: 4 PMUs	7	350 tx/s	2 tx/s	175×
IEEE 39-bus	Cluster 1: 3 PMUs Cluster 2: 5 PMUs Cluster 3: 7 PMUs	15	750 tx/s	3 tx/s	250×
IEEE 118-bus	Cluster 1: 3 PMUs Cluster 2: 7 PMUs Cluster 3: 10 PMUs Cluster 4: 15 PMUs Cluster 5: 23 PMUs	58	2900 tx/s	5 tx/s	580×

4.5.2 Analysis the Number of Transactions and Latency

The time delay caused by validating the transaction has a direct impact on the latency of the network. As the variation of cluster sizes in terms of PMU nodes in Figure 4.12, the number of transactions significantly reduced by accumulating PMU readings over a period (e.g., 1 second) and compressing the data. As a result, the network gets less congested with limited transactions, thus the system can handle incoming data more efficiently. With fewer transactions to process, the transaction confirmed more quickly, leading to lower latency in the proposed framework. Faster transaction confirmation time has guaranteed a lower latency in the network. The number of transactions significantly reduced by compressing all PMU measurements within the cluster into a single transaction segment. The comparison of several transactions against execution time presents in Figure 4.13 (a) by configuring the network with the proposed approach that suggested improvement of transaction execution time in the proposed BC versus conventional BC. This is achieved with reduced number of transactions by compressing all PMU measurements within the cluster into a single transaction segment in the proposed BC.



(a)

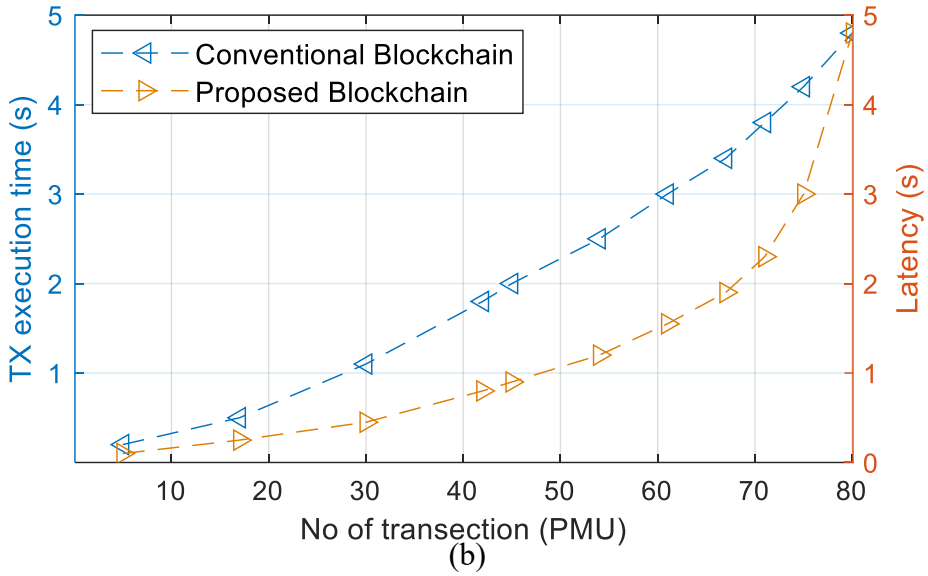


Figure 4.13: (a) Transaction against Number of PMU Nodes; (b) Number of Transactions against Execution Time

In Figure 4.13 (b), the significant improvement shown in the proposed method in terms of reduction number of transactions which is substantially improves the latency in the network. In contrast, the rise in the transaction loads on the system has increased the transaction execution time, raising network latency, as seen in Figure 4.13. Likewise, the transaction execution time has gradually increased with the increased number of PMU nodes in the network. However, marginal improvement in latency has been noticed in the proposed sub-division based WAMS, even in the increased PMU nodes as shown in Figure 4.13 (b).

4.5.2.1 Transaction Latency Before and after Compression

Because uncompressed PMU data would generate hundreds to thousands of transactions per second, it would overwhelm typical BC capacity, leading to large backlogs and indefinite delays. For example, the 118-bus system would require the ledger to handle 2900 tx/s. Even the optimized Hyperledger offline setup with a peak of ~3000 tx/s would be running at full capacity. Thus, any additional overhead such as cryptographic verification, consensus across multiple organizations could intensify the latency into tens or hundreds of

seconds. In contrast, after compression, the transaction arrival rate for the largest system is only 5 tx/s which is <7% of a 75 tx/s network and <0.2% of a 3000 tx/s network shown in Table 4.6.

The table highlights that the uncompressed systems would require BC system to process transactions at rates well above typical capacity, leading to high or unbounded latencies. After compression, the transaction arrival rates are so low that even a modest BC network can process them almost instantly. The use of EdDSA signatures further reduces cryptographic overhead because EdDSA is the fastest performing algorithm with smaller key sizes. Combined with local validation at the sub-division PDC, the proposed framework delivers near real-time performance suitable for WAMS.

Table 4.6: Estimated Latency Comparison

System	Arrival rate without compression (tx/s)	Latency under 75 tx/s service rate	Arrival rate with compression (tx/s)	Estimated latency (s)
IEEE 9-bus	350	Unstable/very high network would queue indefinitely.	2	1-2.5s
IEEE 39-bus	750	Unstable Would require high-performance setups (3000 tx/s)	3	3.5s
IEEE 118-bus	2900	Saturates even high-performance (3k tx/s) networks queueing would lead to additional time	5	5s

4.5.3 Analysis of Scalability

The PMU data in IEEE 9 bus system comprises with 2 clusters, 7 PMUs mentioned in Table 4.5 and 4.6, would need to process 350 tx/s which is far beyond the ~75 tx/s range queueing delays would be extremely high. While after compression, the arrival rate drops to 2 tx/s which is roughly 175× drop implies a $\approx$ 99.4 % reduction in latency. On the other hand, in IEEE 39 bus system consist of 3 clusters, 15 PMUs, the baseline arrival rate (750 tx/s) greatly exceeds typical Fabric throughput; compression reduces this to 3 tx/s. By lowering the load by 250×, the network moves from a congested regime to an under-utilized regime where latencies are on the order 3-3.5s. This translates to a $\approx$ 99.6 % latency reduction. For the IEEE 118 bus system (5 clusters, 58 PMUs), compressing to 5 tx/s reduces the load by 580×, bringing latency down to 5s which is a similar factor—over 99.8 %.

The performance analysis from IEEE 39 and 118 bus systems suggest that the proposed framework can maintain high throughput and low latency, even with larger and more complex WAMS networks. It is evident from the experimental quantitative analysis; the subdivision-based architecture enables the system to scale efficiently as the number of PMUs increases. As number of transactions increased, the transaction size has increased exponentially while the number of PMU nodes has increased. Likewise, transaction execution time rises with the increase in number of transactions. However, block and transaction sizes managed with the proposed method. Meanwhile, the proposed approach has minimized transaction load by data accumulation and compression technique. A decrease in the number of transactions enhances the transaction execution time, thus improving the scalability of the network. The reduction of transaction size with balance block size also indicates the improvement of scalability. The experimental assessment in this

study encourages the utility to embrace permissioned-private BC for robust utility data management.

4.5.4 Performance Comparison with Existing Methods

Conventional BC-based WAMS processed tens or hundreds of transactions per second and suffered from significant delays as described in performance comparison with existing methods. For example, Colaco et al. (2020) used Algorand's proof-of-stake and achieved roughly 8.6 transactions per second with confirmation times near 50 seconds. Bhattacharjee et al. (2020) and Bandara et al. (2021) delivered about 100 TPS and 365 TPS respectively, but only in off-line scenarios and without real-time scalability. Hyperledger Fabric testbeds and private Ethereum networks topped out around 75–100 TPS, with latency increasing sharply once they approached those limits, where permissioned BCs rarely exceed a few hundred TPS and often take seconds to finalise transactions. Aggarwal & Kaddoum's, 2024 QKD-enabled approach likewise to saw off-line throughput in the 50–100 TPS range with latencies of 2.3–2.9 seconds. By dividing the network into clusters, compressing PMU data into one-second windows, and locally validating with DIAM identities and EdDSA signatures, the proposed aggregated WAMS achieves approximately one aggregated transaction per second (≈10 aggregated TPS). This results in a 99.4–99.8% reduction in transaction volume, making queuing delays negligible. As a result, latency reduced by approximately 3–5 seconds, significantly improving both throughput and latency. This indication clearly proves constant transaction frequency even PMU count increases (refer to Figure 11) without increasing BC load which empirically validates the model.

Table 4.6: Scalability Comparison with Existing Methods

Ref.	Method/Work	Core design/Consensus	Throughput (approx.)	Latency performance	Real-Time Scalability
(Colaco et al., 2020)	Blockchain-based Sensor Data Validation	Uses Algorand's Pure Proof-of-Stake	Real-time throughput ≈8.6 TPS	with ≈50 s confirmation time.	Yes
(Bhattacharjee et al., 2020)	A Decentralized Blockchain Framework	Permissioned blockchain to secure synchrophasor measurements	Off-line throughput around 100 TPS	Latency under 1 s and latency increases as the number of PMUs/miners grows.	No
(Bandara et al., 2021)	Tikiri—a lightweight blockchain for IoT	Minimal IoT-oriented blockchain	≈365 TPS off-line throughput on resource-constrained devices.	Low latency on resource-constrained devices.	No
(Pajooh et al., 2022)	Hyperledger Fabric IoT testbed	Multi-org IoT network; various consensus policies	Off-line ≈100 TPS (saturates)	Latency remains <1 s up to ≈100 TPS; increases rapidly afterwards	No
(M. M. Khan et al., 2025)	Private Ethereum	16 peers (proof-of-authority)	Off-line ≈79 TPS	Low TPS compared to Hyperledger Fabric	No

Table 4.6: continue

(Melo et al., 2024)	Hyperledger Fabric SPN model	Simulation using stochastic Petri nets	Off-line ≈75 TPS (commit step saturates)	Throughput stagnates and delays grow rapidly beyond ≈75 TPS	No
(Aggarwal & Kaddoum, 2024)	Combines quantum key distribution (QKD) with blockchain for SCADA authentication	QKD hardware limits throughput, and blockchain consensus introduces additional latency.	Off-line throughput ~50-100 TPS	~2.3 - 2.9s	No
Proposed aggregated WAMS (this thesis)	Sub-division based WAMS	Subdivides WAMS into clusters; PMU data are compressed into 1-s windows and validated locally using DIAM-based identity and EdDSA signatures.	Real-time throughput ≈10 aggregated TPS (1 transaction/s Invoke transactions ≈2900 TPS	~1-5s	Yes

4.6 Chapter Summary

This chapter presents the investigation of WAMS and its two-way data exchange capabilities within a co-simulation environment. It details the design and implementation of the proposed BC-integrated data sharing and recording framework tailored for real-time WAMS applications.

The chapter outlines how the framework guarantees secure communication and data integrity across distributed PMU nodes. It also demonstrates the integration of BC components, including device verification, data authentication, and transaction management, into the simulated WAMS environment.

Furthermore, performance evaluation carried out using a series of experiments that analyses the key metrics such as transaction size, latency, throughput, and block confirmation time. The benchmarking results highlight the effectiveness of the proposed architecture in addressing network congestion, data security, and scalability challenges associated with high-frequency PMU data transmission.

Overall, the findings validate the proposed framework's potential to support resilient, secure, and real-time data sharing in modern power grid environments.

CHAPTER 5

CONCLUSION AND RECCOMENDATION

5.1 Conclusion

In conclusion, each research objective has been comprehensively addressed. First, the investigation of existing WAMS architectures, data communication, automatic monitoring of electrical parameters. The study also exposed the vulnerabilities of data integrity and confidentiality that existing security mechanisms struggled to protect in high-frequency substation domain.

Building on these insights, the second objective focused on developing a subdivision-based BC-integrated WAMS framework for phasor data protection. By partitioning the WAMS into smaller clusters and employing a permissioned BC layer to aggregate and authenticate phasor measurements, the proposed design distributes trust across the network. Leveraging DIAM-based identities and EdDSA signatures ensured that each cluster could verify its own data before adding it to the shared ledger, greatly enhancing confidentiality, integrity and availability.

The third objective was realised by implementing this framework on a Hyperledger Fabric–MATLAB co-simulation test bed. MATLAB provided a realistic power-system environment to generate synchrophasor data, while Hyperledger Fabric simulated the BC network. This integrated platform allowed rigorous testing of data aggregation, consensus processes and cluster interactions under realistic operating conditions.

The final objective achieved through the performance analysis demonstrated that the proposed approach delivers significant improvements. While many existing solutions achieve only tens or low hundreds of transactions per second and suffer from rising latency under load, the proposed WAMS achieved around one aggregated transaction per second ($\approx$10 aggregated TPS) and roughly 2900 invocation TPS, maintaining latencies of about 1–5 seconds. These results show that the subdivision-based BC framework not only meets real-time requirements but also scales gracefully, providing a secure, resilient and efficient foundation for future WAMS deployments.

5.2 Limitation

This thesis conducts the performance evaluation using linear PMU readings under stable grid conditions. However, the performance of the proposed framework may vary under non-linear, unstable grid conditions, which considered a limitation of the work. Since PMU data contains higher entropy during electrical grid events such as faults, load changes, or other disturbances, the data size can increase due to the richer content in each frame, leading to less effective compression and, consequently, larger sizes. Additionally, the increased deployment of PMU nodes leads to a significant rise in data storage volume, which poses another concern.

5.3 Recommendations

Future research should focus on optimization of BC framework and developing efficient methods to process dynamic and real-time data within BC-designed backend systems. A practical consensus algorithm is necessary to manage the high volume of data transactions generated by the increased number of PMU nodes. Additionally, integrating off-chain data storage could alleviate storage issues by storing only transaction metadata.

REFERENCES

Abdella, J., Tari, Z., Anwar, A., Mahmood, A., & Han, F. (2021). An architecture and performance evaluation of blockchain-based peer-to-peer energy trading. *IEEE Transactions on Smart Grid*, *12*(4), 3364-3378.

Abdelsalam, H. A., Eldosouky, A., ElGebaly, A. E., Khalaf, M., Zaki Diab, A. A., Rangarajan, S. S., Alghamdi, S., & Albalawi, H. (2024). A cyber-layer based on weighted average consensus in blockchain environment for accurate sharing of power systems' dynamic states. *International Journal of Electrical Power and Energy Systems*, *155*. https://doi.org/10.1016/j.ijepes.2023.109558

Abrahamsen, F. E., Ai, Y., & Cheffena, M. (2021). Communication technologies for smart grid: A comprehensive survey. Sensors, 21(23), 8087. http://arxiv.org/abs/2103.11657

Aggarwal, S., & Kaddoum, G. (2024). Authentication of Smart Grid by Integrating QKD and Blockchain in SCADA Systems. *IEEE Transactions on Network and Service Management*, *21*(5), 5768–5780. https://doi.org/10.1109/TNSM.2024.3423762

Agung, A. A. G., & Handayani, R. (2022). Blockchain for smart grid. Journal of King Saud University-Computer and Information Sciences, 34(3), 666–675. https://doi.org/10.1016/j.jksuci.2020.01.002

Al Ahmed, M. T., Hashim, F., Jahari Hashim, S., & Abdullah, A. (2022). Hierarchical blockchain structure for node authentication in IoT networks. *Egyptian Informatics Journal*, *23*(2). https://doi.org/10.1016/j.eij.2022.02.005

Alert, D. (2021). Cyber-attack against Ukrainian critical infrastructure (ICS-ALERT-H-16-056-01). Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

Almasabi, S., Shaf, A., Ali, T., Zafar, M., Irfan, M., & Alsuwian, T. (2024). Securing smart grid data with blockchain and wireless sensor networks: A collaborative approach. IEEE Access, 12, 19181-19198.

Aloul, F., Al-Ali, A. R., Al-Dalky, R., Al-Mardini, M., & El-Hajj, W. (2012). Smart Grid Security: Threats, Vulnerabilities and Solutions. *International Journal of Smart Grid and Clean Energy*. https://doi.org/10.12720/sgce.1.1.1-6

Appasani, B., & Mohanta, D. K. (2018). A review on synchrophasor communication system: communication technologies, standards and applications. In *Protection and Control of Modern Power Systems* (Vol. 3, Issue 1). https://doi.org/10.1186/s41601-018-0110-4

Asefi, S., Madhwal, Y., Yanovich, Y., & Gryazina, E. (2021). Application of blockchain for secure data transmission in distributed state estimation. IEEE Transactions on Control of Network Systems, 9(4), 1611-1621.

Asghar, M. R., Dán, G., Miorandi, D., & Chlamtac, I. (2017). Smart meter data privacy: A survey. IEEE Communications Surveys & Tutorials, 19(4), 2820-2835. https://doi.org/10.1109/COMST.2017.2720195

Atmaja, T. D., Andriani, D., & Darussalam, R. (2019). Smart Grid communication applications: measurement equipment and networks architecture for data and energy

flow. *Journal of Mechatronics, Electrical Power, and Vehicular Technology*, *10*(2), 73–84. https://doi.org/10.14203/j.mev.2019.v10.73-84

Dedeoglu, V., Dorri, A., Jurdak, R., Michelin, R. A., Lunardi, R. C., Kanhere, S. S., & Zorzo, A. F. (2020). A Journey in Applying Blockchain for Cyberphysical Systems. 2020 International Conference on Communication Systems and Networks, (COMSNETS 2020), Bengaluru, India. https://doi.org/10.1109/COMSNETS48256.2020.9027487

Ajwalia, M., & Shah, P. (2025). Performance comparison of permissioned and permissionless blockchain by varying workload transaction. BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 5(4). https://doi.org/10.1016/j.tbench.2025.100251

Bamakan, S. M. H., Motavali, A., & Babaei Bondarti, A. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. In *Expert Systems with Applications* (Vol. 154). https://doi.org/10.1016/j.eswa.2020.113385

Bandara, E., Tosh, D., Foytik, P., Shetty, S., Ranasinghe, N., & De Zoysa, K. (2021). Tikiri—Towards a lightweight blockchain for IoT. *Future Generation Computer Systems*, *119*. https://doi.org/10.1016/j.future.2021.02.006

Banks, C., Kim, S., Neposchlan, M., Velez, N., Duncan, K. J., James, J., ... & Hawthorne, D. (2019, April). Blockchain for power grids. In 2019 Southeastcon (pp. 1-5). IEEE *SOUTHEASTCON*

Banoun, N., & Diarra, N. (2021, May –). IoT-BDMS: Securing IoT devices with

Hyperledger Fabric blockchain [Paper presentation]. CS & IT Conference Proceedings (Vol. 11, No. 6), Paris, France. https://aircconline.com/csit/abstract/v11n6/csit110604.html

Beasley, C., Zhong, X., Deng, J., Brooks, R., & Venayagamoorthy, G. K. (2014, October). A survey of electric power synchrophasor network cyber security. In IEEE PES Innovative Smart Grid Technologies, Europe (pp. 1-5). IEEE. https://doi.org/10.1109/ISGTEurope.2014.7028738

Bhattacharjee, A., Badsha, S., Shahid, A. R., Livani, H., & Sengupta, S. (2020, July 13–14). *Block-Phasor: A decentralized blockchain framework to enhance security of synchrophasor*. *2020 IEEE Kansas Power and Energy Conference (KPEC 2020)*, Manhattan, Kansas, USA. https://doi.org/10.1109/KPEC47870.2020.9167676

Bhattacharya, P., Ghafouri, M., Soeanu, A., Kassouf, M., & Debbabi, M. (2022). Security enhancement of time synchronization and fault identification in WAMS using a two-layer blockchain framework. Applied Energy, 315, 118955.

Bhonsle, J. S. (2018). *A Review on Development of Wide Area Measurement System*. 2914–2918. https://doi.org/10.15662/IJAREEIE.2018.0706017

Brunelle, P. *10-Machine New-England Power System IEEE Benchmark", MATLAB Central File Exchange, 2023*.

Cisco Networking Academy:Cybersecurity. (2021). https://skillsforall.com/career-path/cybersecurity

CISCO Systems. (2012). *Improve Wide Area Monitoring*. 2–12. https://www.cisco.com/c/dam/en_us/solutions/industries/docs/energy/services_cs_wan_monitoring.pdf

Colaco, A. G., Nagananda, K. G., Blum, R. S., & Korth, H. F. (2020, February 17–20). *Blockchain-based sensor data validation for security in the future electric grid* [Paper presentation]. *2020 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference (ISGT 2020)*, Washington, DC, USA. https://doi.org/10.1109/ISGT45199.2020.9087676

Dahunsi, F. M., Somefun, O. A., Ponnle, A. A., & Adedeji, K. B. (2021). Compression techniques of electrical energy data for load monitoring: A review. Nigerian Journal of Technological Development, 18(3), 194-208. https://doi.org/10.4314/njtd.v18i3.4

Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R. C., Michelin, R. A., Zorzo, A. F., & Kanhere, S. S. (2019). Blockchain technologies for iot. In Advanced applications of blockchain technology (pp. 55-89). Singapore: Springer Singapore

Dehalwar, V., Kolhe, M. L., Deoli, S., & Jhariya, M. K. (2022). Blockchain-based trust management and authentication of devices in smart grid. Cleaner Engineering and Technology, 8, 100481. https://doi.org/10.1016/j.clet.2022.100481

Deng, R., Zhuang, P., & Liang, H. (2019). False Data Injection Attacks Against State Estimation in Power Distribution Systems. *IEEE Transactions on Smart Grid*, *10*(3). https://doi.org/10.1109/TSG.2018.2813280

Desai, S., Alhadad, R., Chilamkurti, N., & Mahmood, A. (2019). A survey of privacy preserving schemes in IoE enabled Smart Grid Advanced Metering Infrastructure. *Cluster Computing*, *22*(1), 43–69. https://doi.org/10.1007/s10586-018-2820-9

Sissine, F. (2007). Energy Independence and Security Act of 2007: A summary of major provisions (No. CRSRL34294).

Fan, C., Ghaemi, S., Khazaei, H., & Musilek, P. (2020). Performance Evaluation of Blockchain Systems: A Systematic Survey. In *IEEE Access* (Vol. 8). https://doi.org/10.1109/ACCESS.2020.3006078

Fan, X., Chai, Q., Xu, L., & Guo, D. (2020, November 9–13). *DIAM-IoT: A decentralized identity and access management framework for internet of things*. *BSCI 2020 – Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure (co-located with AsiaCCS 2020)*, Doha, Qatar. https://doi.org/10.1145/3384943.3409436

Feng, Q., Yang, K., Ma, M., & He, D. (2023). Efficient Multi-Party EdDSA Signature with Identifiable Aborts and its Applications to Blockchain. *IEEE Transactions on Information Forensics and Security*. https://doi.org/10.1109/tifs.2023.3256710

Ferrag, M. A., & Shu, L. (2021). The Performance Evaluation of Blockchain-Based Security and Privacy Systems for the Internet of Things: A Tutorial. In *IEEE Internet of Things Journal* (Vol. 8, Issue 24). https://doi.org/10.1109/JIOT.2021.3078072

Follum, J., Miller, L., Etingov, P., Kirkham, H., Riepnieks, A., Fan, X., & Ellwein, E. (2021).

Phasors or waveforms: Considerations for choosing measurements to match your application (PNNL-31215). Pacific Northwest National Laboratory Richland, Washington 99354. https://www.naspi.org/documents/phasors-or-waveforms-considerations-choosing-measurements-match-your-application

Garlapati, S. (2020). Blockchain for IOT-based NANs and HANs in Smart Grid. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3512477

Gayo, M., Rodriguez, F. J., Santos, C., Martin, P., & Jimenez, J. A. (2020). Integration of Blockchain with IEC 61850 for Internal Management of Microgrids. *IEEE International Symposium on Industrial Electronics*, *2020-June*, 892–897. https://doi.org/10.1109/ISIE45063.2020.9152542

Gayo, M., Rodriguez, F. J., Santos, C., Martin, P., & Jimenez, J. A. (2020). *Integration of blockchain with IEC 61850 for internal management of microgrids*. *IEEE International Symposium on Industrial Electronics (ISIE 2020-June)*, Delft, Netherlands. https://doi.org/10.1109/ISIE45063.2020.9152542

Ghiasi, M., Dehghani, M., Niknam, T., Kavousi-Fard, A., Siano, P., & Alhelou, H. H. (2021). Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform. Ieee Access, 9, 29429-29440. https://doi.org/10.1109/ACCESS.2021.3059042

Gore, R., & Kande, M. (2015, February 16–19). *Analysis of wide area monitoring system architectures*. *IEEE International Conference on Industrial Technology (ICIT 2015)*, Seville, Spain. https://doi.org/10.1109/ICIT.2015.7125272

Guan, Z., Si, G., Zhang, X., Wu, L., Guizani, N., Du, X., & Ma, Y. (2018). Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities. *IEEE Communications Magazine*, *56*(7). https://doi.org/10.1109/MCOM.2018.1700401

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169, 107094

Guruprakash, J., & Koppu, S. (2022). An Empirical Study to Demonstrate that EdDSA can be used as a Performance Improvement Alternative to ECDSA in Blockchain and IoT. *Informatica (Slovenia)*, *46*(2). https://doi.org/10.31449/inf.v46i2.3807

Hadi, A. A., Bere, G., Kim, T., Ochoa, J. J., Zeng, J., & Seo, G. S. (2020, March 15–19). *Secure and cost-effective micro phasor measurement unit (PMU)-like metering for behind-the-meter (BTM) solar systems using blockchain-assisted smart inverters*. *IEEE Applied Power Electronics Conference and Exposition (APEC 2020)*, New Orleans, LA, USA. https://doi.org/10.1109/APEC39645.2020.9124385

Hasankhani, A., Mehdi Hakimi, S., Shafie-khah, M., & Asadolahi, H. (2021). Blockchain technology in the future smart grids: A comprehensive review and frameworks. *International Journal of Electrical Power and Energy Systems*, *129* (October 2020), 106811. https://doi.org/10.1016/j.ijepes.2021.106811

Honar Pajooh, H., Rashid, M. A., Alam, F., & Demidenko, S. (2022). Experimental performance analysis of a scalable distributed hyperledger fabric for a large-scale IoT testbed. *Sensors*, *22*(13), 4868.

Hojabri, M., Dersch, U., Papaemmanouil, A., & Bosshart, P. (2019). A comprehensive survey on phasor measurement unit applications in distribution systems. *Energies*, *12*(23), 1–23. https://doi.org/10.3390/en12234552

Hossain, M. M., & Peng, C. (2020). Cyber–physical security for on-going smart grid initiatives: A survey. *IET Cyber-Physical Systems: Theory and Applications*, *5*(3), 233–244. https://doi.org/10.1049/iet-cps.2019.0039

Hossain, S., Waheed, S., Rahman, Z., Shezan, S. K. A., & Hossain, M. (2020). Blockchain for the Security of Internet of Things: A Smart Home use Case using Ethereum. *International Journal of Recent Technology and Engineering*, *8*(5), 4601–4608. https://doi.org/10.35940/ijrte.e6861.018520

Houda, Z. A., Hafid, A., & Khoukhi, L. (2020, June 7–11). Blockchain meets AMI: Towards secure advanced metering infrastructures. *IEEE International Conference on Communications (ICC 2020)*, Dublin, Ireland. https://doi.org/10.1109/ICC40277.2020.9148963

Huang, B., Majidi, M., & Baldick, R. (2018). Case Study of Power System Cyber Attack Using Cascading Outage Analysis Model. *IEEE Power and Energy Society General Meeting*, *2018-August*. https://doi.org/10.1109/PESGM.2018.8585921

Iqbal, O., & Keskar, R. B. (2021, December 13–15). *Techniques to compress time-series data*. *2021 10th International Conference on Power Science and Engineering (ICPSE 2021)*, Istanbul, Turkey. https://doi.org/10.1109/ICPSE53473.2021.9656860

Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., & Hossain, E. (2017). Enabling Localized Peer-to-Peer Electricity Trading among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains. *IEEE Transactions on Industrial Informatics*, *13*(6). https://doi.org/10.1109/TII.2017.2709784

Wang, W., Sun, K., Zeng, C., Chen, C., Qiu, W., You, S., & Liu, Y. (2020). Information and communication infrastructures in modern wide-area systems. Wide Area Power Systems Stability, Protection, and Security, 71-104.

Kateb, R., Akaber, P., Tushar, M. H., Albarakati, A., Debbabi, M., & Assi, C. (2018). Enhancing WAMS communication network against delay attacks. IEEE Transactions on Smart Grid, 10(3), 2738-2751. https://doi.org/10.1109/TSG.2018.2809958

Kateb, R., Akaber, P., Tushar, M. H. K., Debbabi, M., & Assi, C. (2018, January 8–10). *Delay aware measurements gathering in WAMS communication network*. *2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP 2017)*, Montreal, QC, Canada. https://doi.org/10.1109/GlobalSIP.2017.8309129

Kaur, S., & Kaur, A. (2015). A review on Data Compression Techniques in Cloud Computing. *INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS*, *351*(5).

Khan, M. M., Khan, F. S., Nadeem, M., Khan, T. H., Haider, S., & Daas, D. (2025). Scalability and Efficiency Analysis of Hyperledger Fabric and Private Ethereum in Smart Contract Execution. Computers, 14(4), 132. https://doi.org/10.3390/computers14040132

Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2016, February 23–25). *IEEE C37.118-2 synchrophasor communication framework: Overview, cyber vulnerabilities analysis and performance evaluation*. *2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, Rome, Italy. https://doi.org/10.5220/0005745001670178

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36–49. https://doi.org/10.1016/j.ijcip.2019.01.001

Khan, M. M., Khan, F. S., Nadeem, M., Khan, T. H., Haider, S., & Daas, D. (2025). Scalability and Efficiency Analysis of Hyperledger Fabric and Private Ethereum in Smart Contract Execution. *Computers*, *14*(4), 132.

Kishore, S., Chan, J., Muthupoltotage, U. P., Young, N., & Sundaram, D. (2021, January 5–8). *Blockchain-based micro-credentials: Design, implementation, evaluation and adoption*. *Annual Hawaii International Conference on System Sciences (HICSS 2021)*, Honolulu, Hawaii, USA. https://doi.org/10.24251/hicss.2021.821

Kong, X., Zhang, J., Wang, H., & Shu, J. (2020). Framework of decentralized multi-chain data management for power systems. CSEE journal of power and energy systems, 6(2), 458-468. https://doi.org/10.17775/CSEEJPES.2018.00820

Koech, K. (2025). Blockchain Scaling: Analyzing the Relationship Between Block Size, Throughput, and Latency in Permissionless Blockchains [Electronic thesis or dissertation, Ohio Dominican University]. OhioLINK Electronic Thesis and

Dissertations Center. http://rave.ohiolink.edu/etdc/view?acc_num=oduhonors1746837229776809

Kumar, S., K Soni, M., & K Jain, D. (2015). Cyber Security Threats in Synchrophasor System in Wams. *International Journal of Computer Applications*, *115*(8), 17–22. https://doi.org/10.5120/20172-2355

Lee, L. A., & Centeno, V. (2019, April 22–24). *Comparison of μPMU and PMU*. *Clemson University Power Systems Conference (PSC 2018)*, Clemson, South Carolina, USA. https://doi.org/10.1109/PSC.2018.8664037

Liang, G., Weller, S. R., Luo, F., Zhao, J., & Dong, Z. Y. (2019). Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks. *IEEE Transactions on Smart Grid*, *10*(3), 3162-3173. https://doi.org/10.1109/TSG.2018.2819663

Liu, Y., Zhang, C., Yan, Y., Zhou, X., Tian, Z., & Zhang, J. (2022). A semi-centralized trust management model based on blockchain for data exchange in IoT system. IEEE Transactions on Services Computing, 16(2), 858-871.

Музика, В. В. (2020). ANALYSIS OF CYBER-ATTACKS ON UKRAINIAN POWER GRID SYSTEMS IN THE CONTEXT OF ARMED CONFLICT IN DONBAS. *Constitutional State*, *0*(39). https://doi.org/10.18524/2411-2054.2020.39.212983

Mahmoudian Esfahani, M. (2022). A hierarchical blockchain-based electricity market framework for energy transactions in a security-constrained cluster of microgrids.

International Journal of Electrical Power and Energy Systems, *139*. https://doi.org/10.1016/j.ijepes.2022.108011

Melo, C., Gonçalves, G., Silva, F. A., & Soares, A. (2024, June). Performance modeling and evaluation of hyperledger fabric: An analysis based on transaction flow and endorsement policies. In 2024 IEEE Symposium on Computers and Communications (ISCC) (pp. 1-6). IEEE.

Marchesi, M. (2018, March). Why blockchain is important for software developers, and why software engineering is important for blockchain software (Keynote). In 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE) (pp. 1-1). IEEE. https://doi.org/10.1109/iwbose.2018.8327564

Mollah, M. B., Zhao, J., Niyato, D., Lam, K. Y., Zhang, X., Ghias, A. M., ... & Yang, L. (2020). Blockchain for future smart grid: A comprehensive survey. IEEE Internet of Things journal, 8(1), 18-43.

Niu, X., Tong, Y., & Sun, J. (2018). Vulnerability assessment for PMU communication networks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11344 LNCS*. https://doi.org/10.1007/978-3-030-05755-8_4

Oikonomou, F. P., Ribeiro, J., Mantas, G., Bastos, J. M. C., & Rodriguez, J. (2021, September 7–10). *A Hyperledger Fabric-based blockchain architecture to secure IoT-based health monitoring systems*. *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom 2021)*, Athens, Greece.

https://doi.org/10.1109/MeditCom49071.2021.9647521

Pajooh, H. H., Rashid, M. A., Alam, F., & Demidenko, S. (2022). Experimental Performance Analysis of a Scalable Distributed Hyperledger Fabric for a Large-Scale IoT Testbed. *Sensors*, *22*(13). https://doi.org/10.3390/s22134868

Pal, O., Alam, B., Thakur, V., & Singh, S. (2021). Key management for blockchain technology. *ICT Express*, *7*(1). https://doi.org/10.1016/j.icte.2019.08.002

Peña, I., Martinez-Anido, C. B., & Hodge, B. M. (2018). An Extended IEEE 118-Bus Test System With High Renewable Penetration. *IEEE Transactions on Power Systems*, *33*(1). https://doi.org/10.1109/TPWRS.2017.2695963

Petersen, O., & Jansson, F. (2017). Blockchain Technology in Supply Chain Traceability Systems: Developing a Framework for Evaluating the Applicability. *Blockchain Technology in Supply Chain Traceability Systems: Developing a Framework for Evaluating the Applicability*.

Pettikkattil, J. (2024). *IEEE 9 Bus Transient Stability Analysis*. MATLAB Central File Exchange. https://www.mathworks.com/matlabcentral/fileexchange/66018-ieee-9-bus-transient-stability-analysis

Phadke, A. G., & Bi, T. (2018). Phasor measurement units, WAMS, and their applications in protection and control of power systems. *Journal of Modern Power Systems and Clean Energy*, *6*(4), 619–629. https://doi.org/10.1007/s40565-018-0423-3

Quincozes, S. E., Albuquerque, C., Passos, D., & Mossé, D. (2021). A survey on intrusion

detection and prevention systems in digital substations. Computer Networks, 184, 107679. https://doi.org/10.1016/j.comnet.2020.107679

Rehmani, M. H. (n.d.). *Textbooks in Telecommunication Engineering Blockchain Systems and Communication Networks : From Concepts to Implementation*. http://www.springer.com/series/13835%0Ahttps://www.springer.com/book/9783030717872%0AISSN

Ropp, M. (2019). Guide to the IEEE 1547-2018 standard and its impacts on cooperatives. In *National Rural Electric Cooperative Association* (Issue March)

Sadu, A., Jindal, A., Lipari, G., Ponci, F., & Monti, A. (2021). Resilient design of distribution grid automation system against cyber-physical attacks using blockchain and smart contract. *Blockchain: Research and Applications*, *2*(1), 100010. https://doi.org/10.1016/j.bcra.2021.100010

Sahoo, Swagatika, Akshay M. Fajge, Raju Halder, and Agostino Cortesi. "A hierarchical and abstraction-based blockchain model." Applied Sciences 9, no. 11 (2019): 2343. https://doi.org/10.3390/app9112343

Saha, S., Alam, F., Sayada, R., Rahman, R. M., & Hasan, A. S. M. J. (2024, ***December 3–6***). *Advanced load flow & fault analysis of renewable energy integration in IEEE 9 bus power system*. *IEEE Global Energy Conference (GEC 2024)*, *Batman, Turkiye*. https://doi.org/10.1109/GEC61857.2024.10882070

Schweitzer Engineering Laboratories. (2020). High-performance, versatile PDC software

designed and tested for reliable operation (SEL-5073). *SEL Application Guide*. https://selinc.com/products/5073/docs/

Shahraeini, M., & Kotzanikolaou, P. (2020). A dependency analysis model for resilient wide area measurement systems in smart grid. *IEEE Journal on Selected Areas in Communications*, *38*(1), 156–168. https://doi.org/10.1109/JSAC.2019.2952228

Shapsough, S., Qatan, F., Aburukba, R., Aloul, F., & Al Ali, A. R. (2015, October 20–23). *Smart grid cyber security: Challenges and solutions*. *2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE 2015)*, Offenburg, Germany. https://doi.org/10.1109/ICSGCE.2015.7454291

Shen, L., Hao, B., Li, Y., Yu, H., Zhang, S., Men, H., & Fan, J. (2020, November 18–20). *Blockchain-based power grid data asset management architecture*. *2020 International Conference on Computer Science and Management Technology (ICCSMT 2020)*, Shanghai, China. https://doi.org/10.1109/ICCSMT51754.2020.00049

Shi, Y., Liang, J., Li, M., Ma, T., Ye, G., Li, J., & Zhao, Q. (2022, October 26–28). *Threshold EDDSA signature for blockchain-based decentralized finance applications*. 25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2022), Limassol, Cyprus. https://doi.org/10.1145/3545948.3545977

Shrimali, B., & Patel, H. B. (2022). Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. In *Journal of King Saud University - Computer and Information Sciences* (Vol. 34, Issue 9). https://doi.org/10.1016/j.jksuci.2021.08.005

Sikeridis, D., Bidram, A., Devetsikiotis, M., & Reno, M. J. (2020). A blockchain-based mechanism for secure data exchange in smart grid protection systems. *2020 IEEE 17th Annual Consumer Communications and Networking Conference, CCNC 2020*. https://doi.org/10.1109/CCNC46108.2020.9045368

Son, D. H., Quynh, T. T. T., Khoa, T. V., Hoang, D. T., Trung, N. L., Ha, N. V., Niyato, D., Nguyen, D. N., & Dutkiewicz, E. (2021, October 14–16). *An effective framework of private Ethereum blockchain networks for smart grid*. 2021 International Conference on Advanced Technologies for Communications (ATC 2021), Ho Chi Minh City, Vietnam. https://doi.org/10.1109/ATC52653.2021.9598199

Sufyan, M. A. A., Zuhaib, M., Anees, M. A., Khair, A., & Rihan, M. (2021). Implementation of PMU-Based Distributed Wide Area Monitoring in Smart Grid. *IEEE Access*, *9*. https://doi.org/10.1109/ACCESS.2021.3119583

Swathi, P., & Venkatesan, M. (2021). Scalability improvement and analysis of permissioned-blockchain. *ICT Express*, *7*(3), 283–289. https://doi.org/10.1016/j.icte.2021.08.015

Tatipatri, N., & Arun, S. L. (2024). A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security. *IEEE Access*, *12*. https://doi.org/10.1109/ACCESS.2024.3361039

Thakkar, S., Dalvi, A., Siddavatam, I., & Kazi, F. (2019). Applicability of Blockchain for Synchrophasor Network. *SSRN Electronic Journal*, 1–4. https://doi.org/10.2139/ssrn.3367740

Thukral, M. K. (2021). Emergence of blockchain-technology application in peer-to-peer electrical-energy trading: A review. *Clean Energy*, *5*(1), 104–123. https://doi.org/10.1093/ce/zkaa033

Tian, H., Jian, Y., & Ge, X. (2022). Blockchain-based AMI framework for data security and privacy protection. *Sustainable Energy, Grids and Networks*, *32*. https://doi.org/10.1016/j.segan.2022.100807

Tufail, S., Parvez, I., Batool, S., & Sarwat, A. (2021). A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. *Energies*, *14*(18), 1–22. https://doi.org/10.3390/en14185894

Usman, M. U., & Faruque, M. O. (2019). Applications of synchrophasor technologies in power systems. *Journal of Modern Power Systems and Clean Energy*, *7*(2), 211–226. https://doi.org/10.1007/s40565-018-0455-8

Wang, G., Shi, Z. J., Nixon, M., & Han, S. (2019, October 21–23). *SoK: Sharding on blockchain*. 1st ACM Conference on Advances in Financial Technologies (AFT 2019), Zurich, Switzerland. https://doi.org/10.1145/3318041.3355457

Wang, L., Vo, Q. S., & Prokhorov, A. V. (2018). Stability Improvement of a Multimachine Power System Connected With a Large-Scale Hybrid Wind-Photovoltaic Farm Using a Supercapacitor. *IEEE Transactions on Industry Applications*, *54*(1). https://doi.org/10.1109/TIA.2017.2751004

Wang, Q., & Wang, Z. (2025). Blockchain-Enhanced IoT Sensor Data Management for

Engineering Monitoring. IEEE Sensors Journal, 25(4). https://doi.org/10.1109/JSEN.2024.3519542

Wang, Y., Li, J., Yan, Y., Chen, X., Yu, F., Zhao, S., Yu, T., & Feng, K. (2021a). A semi-centralized blockchain system with multi-chain for auditing communications of Wide Area Protection System. *PLoS ONE*, *16*(1 January), 1–20. https://doi.org/10.1371/journal.pone.0245560

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, *169*, 107094.

Waseem, M., Adnan Khan, M., Goudarzi, A., Fahad, S., Sajjad, I. A., & Siano, P. (2023). Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges. *Energies*, *16*(2). https://doi.org/10.3390/en16020820

Xu, W., Huang, Z., Xie, X., & Li, C. (2021). Synchronized waveforms–a frontier of data-based power system and apparatus monitoring, protection, and control. IEEE Transactions on Power Delivery, 37(1), 3-17.

Yadav, J., & Shevkar, R. (2021). Performance-Based Analysis of Blockchain Scalability Metric. Tehnicki Glasnik, 15(1), 133–142. https://doi.org/10.31803/tg-20210205103310

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. IEEE communications surveys & tutorials, 14(4), 998-1010.

https://doi.org/10.1109/SURV.2012.010912.00035

Yang, Y., Ju, J. Q., Li, Q. H., & Wang, Q. (2018, November 6–8). An experimental research on impacts of malicious attacks on PMU in smart grids [Paper presentation]. 2018 International Conference on Power System Technology (POWERCON 2018), Guangzhou, China. https://doi.org/10.1109/POWERCON.2018.8602008

Zhang, H., Liu, B., & Wu, H. (2021). Smart grid cyber-physical attack and defense: A review. IEEE Access, 9, 29641-29659.

Zhang, S., Rong, J., & Wang, B. (2020). A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain. International Journal of Electrical Power & Energy Systems, 121, 106140.

Zhao, Q., Chen, S., Liu, Z., Baker, T., & Zhang, Y. (2020). Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. *Information Processing & Management*, *57*(6), 102355.

Zhou, X., Sun, Y., Tu, F., & Su, H. (2022, August 7–10). Intelligent substation online monitoring system based on blockchain technology. 2022 IEEE International Conference on Mechatronics and Automation (ICMA 2022), Guilin, Guangxi, China. https://doi.org/10.1109/ICMA54519.2022.9856232

Zhou, X., Sun, Y., Tu, F., & Su, H. (2022, August 7–10). *Intelligent substation online monitoring system based on blockchain technology*. 2022 IEEE International Conference on Mechatronics and Automation (ICMA 2022), Guilin, China.

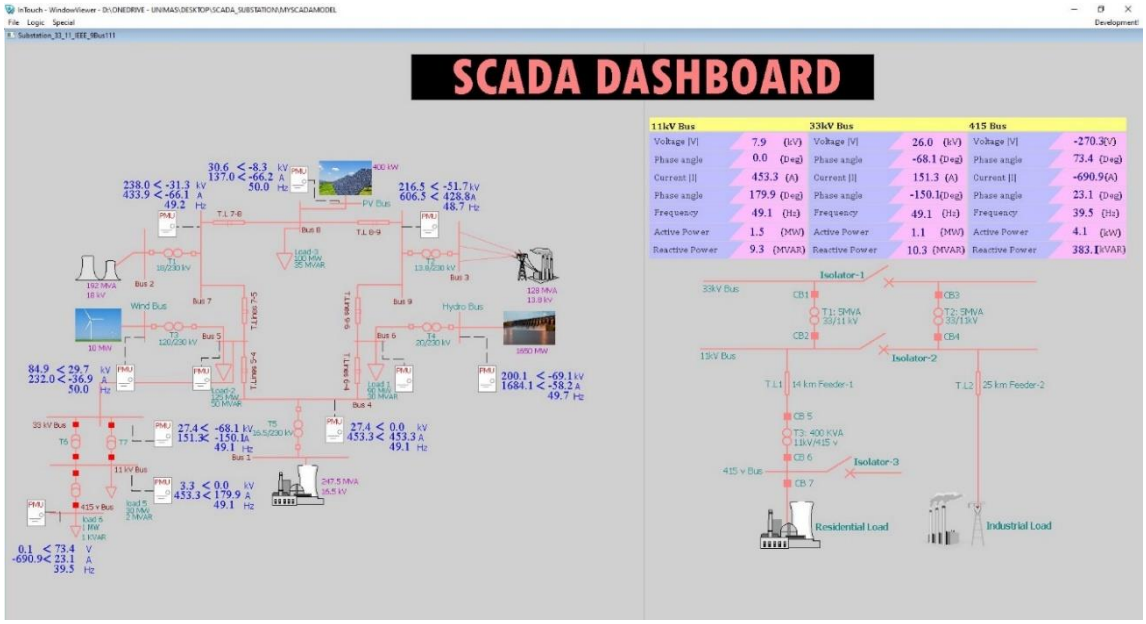
https://doi.org/10.1109/ICMA54519.2022.9856232

Zhuang, P., Zamir, T., & Liang, H. (2021a). Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey. *IEEE Transactions on Industrial Informatics*, *17*(1). https://doi.org/10.1109/TII.2020.2998479

Zhuang, P., Zamir, T., & Liang, H. (2021b). Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey. *IEEE Transactions on Industrial Informatics*, *17*(1), 3–19. https://doi.org/10.1109/TII.2020.2998479

APPENDICES

Appendix A: Laboratory Experiment



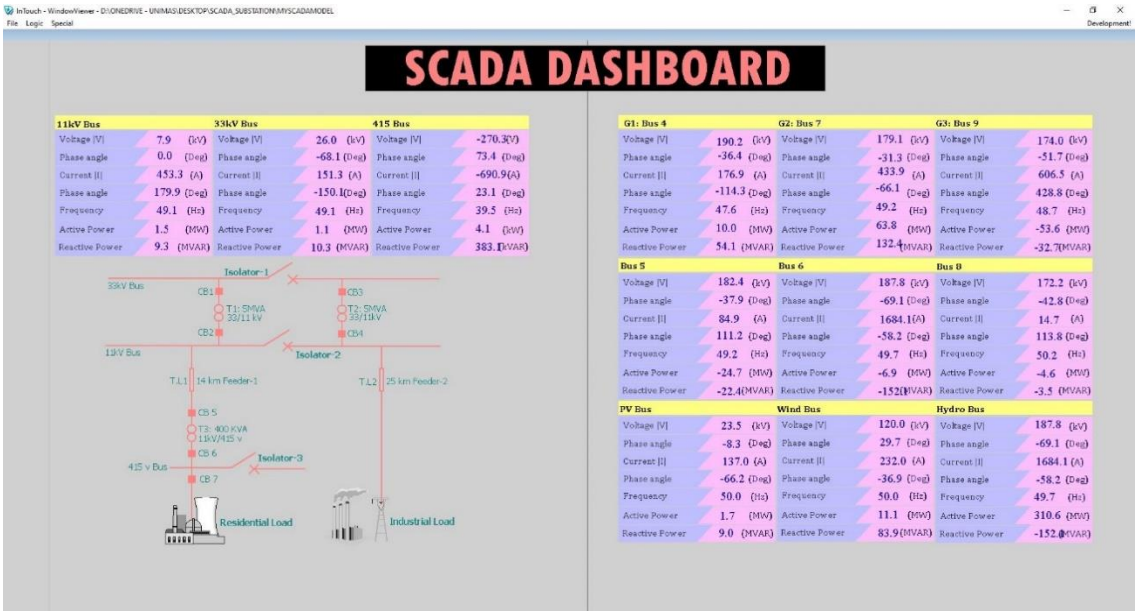


Figure 1: Complete Window of SCADA HMI

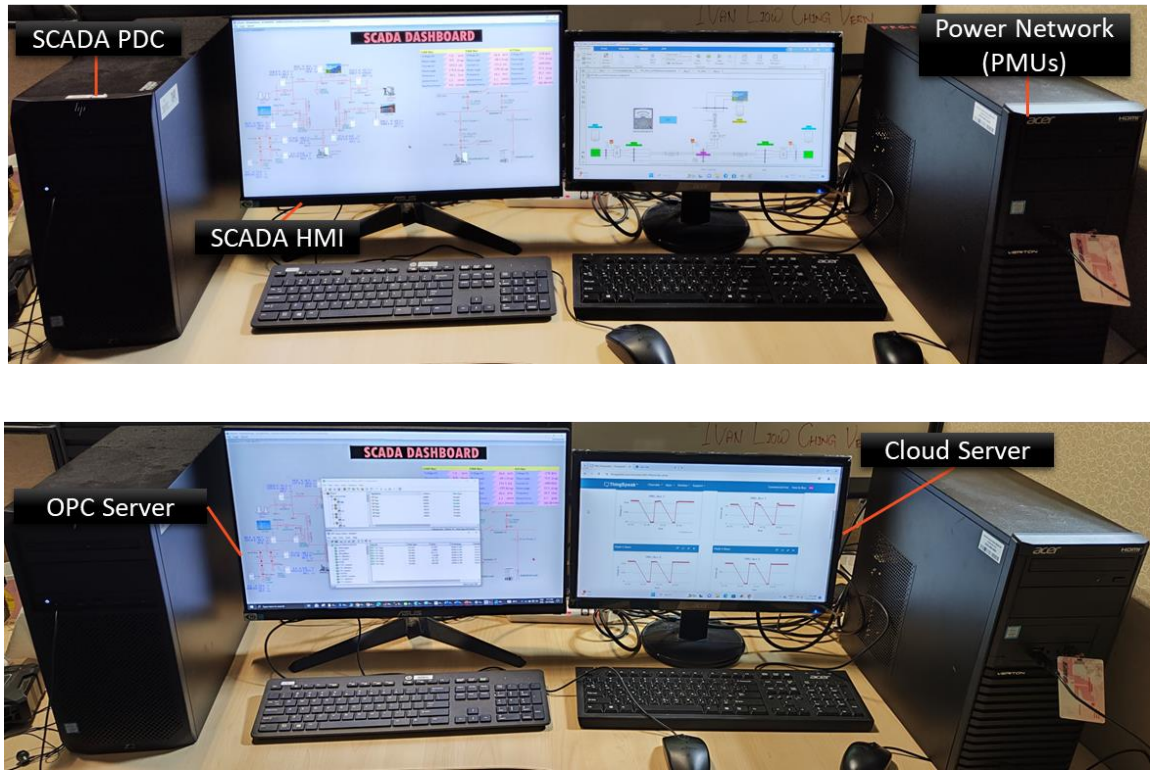
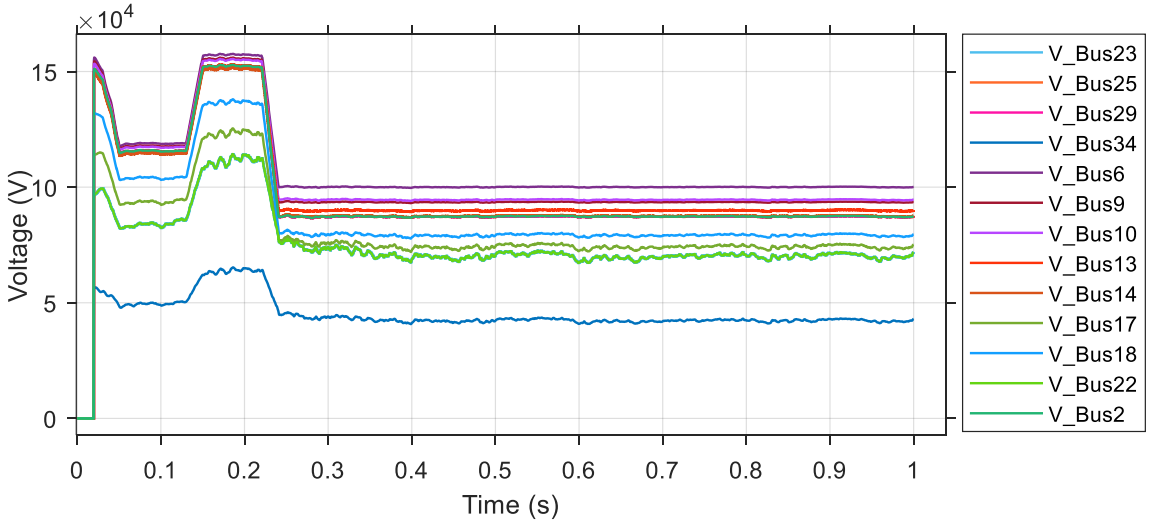
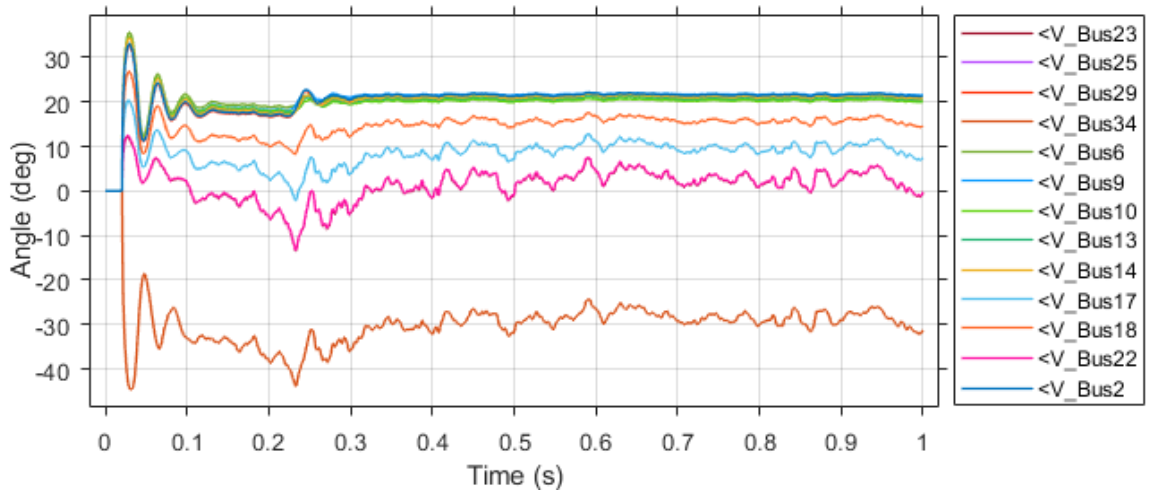


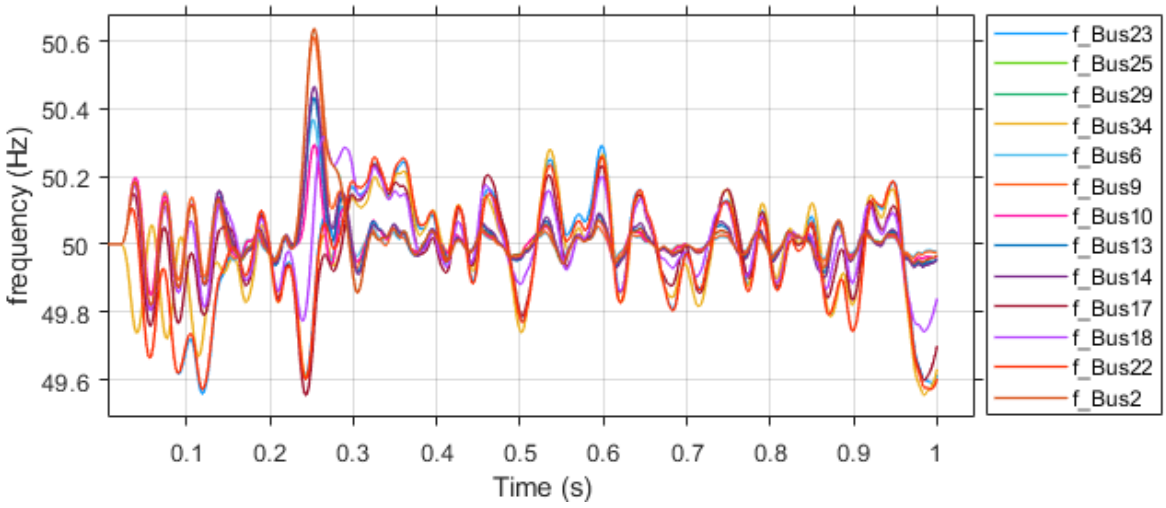
Figure 2: Laboratory Experiment of Phasor Data Sharing in WAMS



(a)



(b)



(c)

Figure 3: PMU Measurement Sharing of 39-Bus Sytem to PDC Gateway (a) Voltage Megnitude, (b) Phase Angle and (c) Frequency

Appendix B: Journal Publications

1. Sayed, M. A., Ahmed, M. M., Azlan, W., & Kin, L. W. (2024). Peer to peer solar energy sharing system for rural communities. *Cleaner Energy Systems*, *7*, 100102.