IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 22 December 2023, accepted 29 January 2024, date of publication 2 February 2024, date of current version 8 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3361752

RESEARCH ARTICLE

Securing Smart Grid Data With Blockchain and Wireless Sensor Networks: A Collaborative Approach

SALEH ALMASABI[1], (Member, IEEE), AHMAD SHAF[2], TARIQ ALI[2], MARYAM ZAFAR[2], MUHAMMAD IRFAN[1], AND TURKI ALSUWIAN[1]

[1]Electrical Engineering Department, College of Engineering, Najran University, Najran 11001, Saudi Arabia
[2]Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus, Sahiwal 57000, Pakistan

Corresponding author: Saleh Almasabi (ssalmasabi@nu.edu.sa)

This work was supported by the Deanship of Scientific Research, Najran University, Saudi Arabia, under the Distinguished Funding Program under Grant NU/DRP/SERC/12/8.

ABSTRACT The rapid advancement of grid modernization and the proliferation of smart grids have engendered a critical need for cyber-physical security. Recent cyber-attacks targeting grid infrastructure, notably leading to substantial blackouts in Ukraine, underscore the vulnerabilities and potentially catastrophic consequences of such incursions. These attacks, whether stemming from cyber threats such as Denial of Service (DOS), False Data Injection Attacks (FDIA), or complex cyber-physical manipulations, emphasize the imperative of robust cybersecurity protocols in smart grid operations. This research investigates a pivotal approach to fortify and safeguard smart grid systems by integrating blockchain technology with wireless sensor nodes. By leveraging a Proof of Authority (PoA) Ethereum Blockchain framework, the study delves into the transformative capabilities of Blockchain within Supervisory Control and Data Acquisition (SCADA) networks. Specifically, it examines configurations across IEEE 14-bus, 30-bus, and 118-bus topologies. In addition to elucidating the inherent vulnerabilities in traditional SCADA systems, this study meticulously evaluates an array of performance matrices. Statistical analyses encompassing mean, standard deviation, skewness, kurtosis, and confidence levels provide nuanced insights into the efficacy of blockchain mechanisms in enhancing SCADA resilience against contemporary cyber threats. This research endeavors to bridge the gap in modern cybersecurity paradigms by fusing blockchain technology with wireless sensor nodes. By fortifying data integrity, elevating the reliability of data transmission, and augmenting trustworthiness within SCADA infrastructures, this study aims to present robust solutions to the escalating cybersecurity challenges faced by smart grid systems.

INDEX TERMS Blockchain technology, cyber-physical security, cyber threats, data integrity, data transmission reliability, FDIA, proof of authority (PoA), SCADA systems, smart grids security, trustworthiness, wireless sensor networks.

I. INTRODUCTION

The power grid is becoming a data-driven complex cyber-physical system, with the advancement of various technologies such as Phasor measurement units (PMUs) and the need for a robust operation to handle the intermittency of renewable energy resources (RERs). The operation of the power grid nowadays relies on the processing of measurements such as voltage magnitudes, power flows, and demand forecasts. This massive amount of data is collected throughout the network and processed using the Supervisory Control and Data Acquisition (SCADA) system.

The pivotal role of SCADA systems for smart grids stems from the importance of the safe and secure operation of the grid. As real-time data (measurements) are gathered throughout the grid from an array of sensors and Intelligent

The associate editor coordinating the review of this manuscript and approving it for publication was Usama Mir.

Electronic Devices (IEDs), SCADA systems facilitate the seamless transmission of this data to a centralized control center [1]. Comprising three fundamental elements [2], SCADA systems encompass:

1) Remote Terminal Units (RTUs): Positioned strategically within the substation, RTUs serve as data collection hubs, interfacing with sensors and IEDs, and formatting the acquired data for transmission to the control center. Phasor measurement Units (PMUs) which are replacing RTUs are also part of the SCADA system.
2) Communication Network: This network interconnects the RTUs with the central control center, utilizing diverse technologies like fiber optic cables, wireless radio, or satellite communication to ensure efficient data transmission.
3) Main Station: Serving as the nerve center of the SCADA system, the main station receives incoming data from RTUs, processes it, and presents a comprehensive view to operators. Furthermore, it dispatches vital control commands-such as circuit breaker operations-back to the RTUs, enabling active grid management.

Despite their crucial role in managing power grids, SCADA systems within smart grid stations present vulnerabilities due to their distributed nature, comprising various wired and wireless nodes. This structure elevates the risk of cyber threats, allowing intruders to exploit weaknesses and potentially disrupt SCADA operations [3], [4].

When considering attacks on cyber-physical systems, two main categories emerge [3], [5]: physical and cyber-attacks. Physical attacks require physical access, potentially involving actions like cable disconnection, component destruction, or unauthorized machinery access. Implementing preventive measures like surveillance, locks, and intrusion detection can mitigate these intrusions. On the other hand, cyber-attacks utilize networked electronic devices to exploit hardware or software vulnerabilities. Deception attacks manipulate sensor data or control messages, aiming to mislead CPS control systems [6]. Techniques such as False Data Injection, Topology Attacks, Load Redistribution, and Stealthy Attacks are examples of these strategies [7]. Network-based attacks [8] focus on vulnerabilities within network protocols, posing a threat to critical Industrial Control Systems (ICS) functionality. These attacks, including Man-in-the-Middle, Spoofing, Denial of Service, and Replay Attacks, exploit the stringent real-time requirements of ICSs, potentially causing data loss or communication delays.

Ukraine faced devastating cyberattacks causing widespread blackouts [9]. The 2015 assault, using BlackEnergy malware via spear-phishing, affected 225,000 people, manipulating grid equipment and taking hours to rectify. A more sophisticated 2016 attack, exploiting firmware vulnerabilities, hit 1.5 million, installing BlackEnergy to disable power distribution for days. The 2017 WannaCry ransomware attack [10] affected millions of computers globally, impacting critical infrastructure systems and demanding ransom payments, showcasing the widespread disruption. The 2021 Colonial Pipeline attack [11], executed using ransomware, disrupted fuel supplies along the US East Coast. Exploiting a VPN server vulnerability, attackers encrypted critical systems, demanding a hefty ransom for decryption. Moreover, in 2020-2021, attempted cyber infiltrations on many US economy sectors by hackers highlighted the persistent threat to critical infrastructure [12]. These incidents underscore the urgent need for robust cybersecurity measures within SCADA systems, emphasizing the imperative of preemptive measures to safeguard critical infrastructure against evolving cyber threats.

Machine Learning Techniques (MLTs) [13], [14], [15], [16], [17], [18], [19], [20] extensively deployed for SCADA network monitoring, intrusion prediction, detection, and classification comprise various categories. Supervised learning algorithms, including Support Vector Machines (SVM), K-Nearest Neighbor (KNN), Logistic Regression (LR), Neural Networks (such as CNN and RNN), Bayes, Decision Trees, Artificial Neural Networks, Rule Induction, and Discriminant Analysis, are commonly utilized. Unsupervised learning algorithms like Isolation Forest, One-Class Support Vector Machine (OCSVM), and Autoencoders (such as Sparse Autoencoders, Undercomplete Autoencoders, Variational Autoencoders, and Fair Clustering) are employed when labeled data is insufficient. Deep Learning algorithms such as Deep Neural Networks (DNN), Convolutional Neural Network (CNN), Deep Belief Network (DBN), Long Short-Term Memory (LSTM), Recurrent Neural Network (RNN, including Simple Recurrent Unit and Bi-directional Recurrent Unit), Stacked Autoencoder (StAE), and Gated Recurrent Units (GRU) offer enhanced representations and performance. Additionally, Ensemble Learning approaches like Random Forest (RF), Bagging, Boosting (Adaptive Boosting, Gradient Boosting), ensemble deep learning, and ensemble neural network models have been employed to improve accuracy and resilience in the face of sophisticated attacks. Datasets like CICIDS2017, CICIDS2019, IEC, ADFA-LD, KDD99, NSL-KDD, and KDD are commonly used for training and testing these models.

However, despite the efficacy of MLTs in fortifying SCADA systems, these algorithms exhibit certain limitations.

1) Supervised learning algorithms heavily relied on labeled data for training, a resource often scarce in the cybersecurity domain. The constantly evolving attack patterns and the emergence of novel threats not present in the training data posed challenges for supervised models to generalize and adapt effectively to new attack scenarios.
2) Unsupervised algorithms excelled in identifying anomalies, yet they faced the issue of generating false positives, causing unnecessary alarms and resource inefficiencies. Additionally, distinguishing between benign anomalies and actual attacks proved challenging for unsupervised methods.

3) Deep learning models, known for their prowess in representation learning, demanded significant computational resources and large datasets, rendering them impractical for resource-constrained SCADA environments. The process of training and deploying deep learning models consumed considerable time and resources, limiting their real-time applicability in SCADA security protocols.
4) Ensemble methods, while capable of enhancing accuracy, introduced complexities in deployment and maintenance. The intricate process of selecting, training, and coordinating multiple models posed challenges, particularly in dynamic SCADA environments.

These limitations pave the way for exploring innovative solutions like a Blockchain-enabled secure system architecture, which aims to augment existing defenses and address the shortcomings of conventional MLTs within SCADA systems.

Blockchain technology stands out as a pioneering solution for security and data storage in modern contexts. Functioning as a distributed database, it meticulously tracks every transaction occurring across network-connected devices. Operating as an electronic ledger, it meticulously records interactions and transactions in distinct blocks. What sets blockchain apart is its decentralized nature, where all users in the network maintain and authenticate messages. Only after successfully passing the authentication process are communications added to the blockchain. Multiple messages are amalgamated to form blocks and a transaction garners success only upon unanimous agreement from all participating network nodes. Notably, blockchain technology boasts an immutable characteristic, ensuring the steadfastness and security of transaction data [21].

Meanwhile, leveraging blockchain technology, other scholarly articles propose a data storage architecture tailored for wireless sensor networks. This architecture serves a dual purpose: managing data access and effectively storing information generated by the nodes [22]. Furthermore, the authors present a proficient routing technique that enhances routing performance in a separate study. This demonstrates the depth of blockchain's potential in augmenting network operations through its integration with Markov decision processes [23].

As technology progresses, WSNs are becoming increasingly used for controlling and monitoring various applications. These networks are known for their resilience, compact size, cost-effectiveness, and energy efficiency. WSNs deployed at various electrical line loading points record discrete electrical quantities (current, voltage, power). Real-time data is transmitted to the SCADA center via a wireless link using IEEE 802.15.4 security protocol [24]. Kantarci et al. [25] assessed the cost-effective approach to residential load management in smart grid systems using WSNs. The evaluation considered factors such as energy cost, reliance on consumers' maximum demand, energy conservation, and CO2 emission reduction. The study compared the in-home energy management technique with the optimization-based residential energy management technique. iHOM's performance was analyzed in terms of local resource capacity development, load prioritization, and online pricing of supplied energy. When discussing smart grids, it's important to recognize that potential attacks can originate from different elements of a power system. These may include SCADA, electric transportation infrastructure, PMUs, advanced metering infrastructure (AMI), energy storage subsystems, and other crucial components of the smart grid. To address challenges in distributed networks, it is crucial to log information for effective analyses of cybercrimes and prediction of system failures in Smart Grid management.

Cohen [26] recently explored a method for cyber investigators to de-anonymize a significant portion of Bitcoin clients, presenting new possibilities for blockchain forensics. Erol-Kantarci and Mouftah [27] emphasized the importance of smart grid science as a robust security element in power systems. They outlined applications, obstacles, and open issues in this field. Building on their research, the study has summarized challenges in Smart Grid related to Blockchain. Smart Grid faces another obstacle concerning data volume. Various power devices generate extensive data, transmitting them through the communication infrastructure. The data streams are considered infinite sequences of timestamped records. Each record comprises key-value pairs, with the keys representing reading attributes and the values containing the corresponding data [28]. Managing and processing this immense volume of data poses significant challenges, compounded by privacy concerns.

Batista et al. [29] conducted an analysis of the monitoring performance of Photovoltaic (PV) and wind energy systems in smart grids, employing ZigBee technology. Various tests were conducted to explore energy management solutions through ZigBee, and the utilization of a smart metering system for efficient bi-directional energy control and monitoring was examined, supported by experimental results. Tushar et al. [30] introduced an energy management solution for integrating distributed sources into smart grids, utilizing an algorithm based on Stackelberg equilibrium (SE). The conclusion drawn was that energy production becomes more cost-effective as SE approaches the energy demand of residential units (RUs) and the energy trend of the shared facility controller (SFC) for energy storage devices. Zhao et al. [31] conducted a study on energy management, addressing both the load and supply aspects through an optimization algorithm grounded in the convexity of power balance between supply and demand. Their research aimed to minimize transmission losses by transforming equality constraints into inequality constraints within an evolved objective function. To facilitate direct communication between distributed resources and loads, they employed a consensus-based distributed energy management approach known as CEMA (Consensus-Based Distributed Energy Management). This technique operated with the goal of maximizing social welfare, achieved by reducing tariffs

and ensuring a maintained power balance. The integration of blockchain technology could further enhance the security, transparency, and efficiency of such a decentralized energy management system.

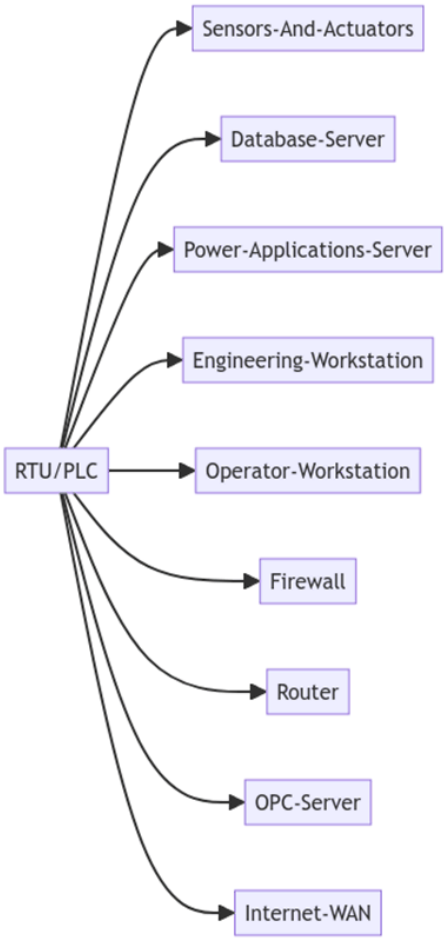


FIGURE 1. Architectural system of SCADA network in smart grid.

However, traditional security approaches often overlook the dynamic landscape of cyber threats and the intricate, distributed nature of smart grid infrastructures. This study aims to bridge these gaps by proposing a pioneering blockchain-based security framework tailored explicitly for wireless sensor networks within SCADA environments Fig. 1. Our model represents a holistic solution, strategically designed to not only address existing limitations but also proactively anticipate emerging cyber threats. The key components of this framework include:

- **Crafting a Cutting-Edge System Design for Enhanced Security:**
  - We've developed a sophisticated system design that blends blockchain tech, smart contracts, and encryption protocols. This setup ensures top-tier security for wireless sensor networks within SCADA systems, making sure our data stays integral and secure.
- **A Full-Spectrum Defense Against Cyber Threats:**
  - Our approach covers all bases when it comes to security. By understanding and countering evolving cyber threats, we're proactively defending against potential risks. We're not just closing existing loopholes but also preparing for future threats, making our smart grid systems more resilient.
- **Revolutionizing Smart Grid Integrity with Scalable Security:**
  - We've seamlessly woven blockchain into our wireless sensor networks. This maintains data integrity and keeps it confidential and accessible as our systems grow. Our goal is to manage energy securely while being flexible enough to adapt to changing needs.
- **Creating an Innovative Architecture for Secure and Scalable Energy Management:**
  - Our architecture isn't just about security; it's also designed to scale. We've built a framework for monitoring and controlling energy that's both secure and adaptable. This ensures data safety at every level and can grow to meet future demands and technological advancements.

In the subsequent sections, this paper delves into a detailed exploration of our methodology (Section II), outlining the material and methods employed in constructing our innovative security framework. Section III comprehensively presents our findings, analyzing the results derived from our proposed system. Finally, the Conclusion encapsulates the essence of our discoveries, drawing insightful conclusions from the synthesized findings.

II. MATERIALS AND METHODS

A. STRUCTURE OF BLOCKCHAIN NETWORK

Blockchain refers to a technology that involves a continually expanding series of data structures known as blocks. Cryptography is used to link and secure these blocks. These blocks are linked and safeguarded through cryptography. The technology enables secure data transmission, relying on a highly intricate encryption system. It functions similarly to a business ledger, documenting every transaction cautiously and detailed documentation of every peer-to-peer record. Every block contains details about its creation time and is linked to the previous block, complete with a timestamp and transaction data. The data is unchangeable once the network accepts it [32]. Blockchain is designed to combat fraud and alteration of data. Each transaction is stored in a block, which is then effectively connected to create a chain. Significant information is contained in each block, which includes the value of the current block, the transaction execution time, the address of the previous block, a random number (nonce), and the current block header as shown in Fig. 2. The quantity and particulars of the acquired data are primarily stored in the block structure. Additionally, information stored on the Blockchain is permanent and always accessible. The obtained data is kept private and non-duplicable by using digital

signatures in the form of a Merkle tree. The Mekle-root value is unique in blocks because the Merkle-tree hash function processes the received data. Here is the visual structure of Blockchain:

B. CATEGORIES OF BLOCKCHAIN

Blockchain systems can be divided into three primary categories based on ownership and the audience that may participate in the block addition and verification process. Public Blockchain: Anyone can participate in the agreement process on a public blockchain, where all records are accessible to the general public. Public blockchains, which include many participants, have the highest immutability. They are often less efficient than consortium and private blockchains, however. Private Blockchain: On the other hand, only nodes belonging to a particular organization can connect to the network and participate in the consensus process in a private blockchain. This suggests a consensus process based on permissions and is frequently regarded as a centralized network managed by a single entity [33]. Private blockchains are more efficient than public blockchains, but since they have fewer users, they are more vulnerable to manipulation. Consortium Blockchain: A permission-based consensus method is also used by consortium blockchains; however, participation is restricted to many organizations. As a result, the system becomes more decentralized. Consensus blockchains, like private ones, are very efficient but may be more prone to manipulation than public ones because of their small member base.

C. DATA IN EACH BLOCK

Each block has different information depending on the type of Blockchain. For example, transaction details, such as sender and recipient details and the number of bitcoins traded, may be found on the Blockchain of Bitcoin. In contrast, a blockchain for health insurance would store data about the covered person, including their medical history. Each block has its hash code, a distinguishing fingerprint to identify the block and its contents. If there is any modification to block material, this hash code is updated. Additionally, the hash of the preceding block, serving as its identifier, contributes to forming the entire chain. Any modification to a single block disrupts the consistency of subsequent blocks, illustrating the interconnected and tamper-resistant nature of the Blockchain [34].

D. HOW BLOCKCHAIN WORKS?

Consider Blockchain as a unique form of ledger technology. It functions similarly to a digital notepad that records transactional data. This notebook is set up as a chain of blocks, and when additional entries are made, it becomes longer. A fresh block is generated each time new data is added. Special codes link each newly inserted block to the one that came before it. In the Blockchain, this produces a safe and immutable record. Consider the initial block as the beginning of a chain, and the other blocks that contain information are like the links in the chain. Any attempts to alter the data in the second block will disrupt connections with the third and subsequent blocks. This occurs due to the hash, a unique code that links each block. A block's hash changes when its contents are modified, rendering it incompatible with subsequent blocks. Therefore, once data is written, the Blockchain's architecture helps ensure that nobody can readily change it. Blockchain technology makes use of an algorithm known as a consensus algorithm. Proof of Work (PoW) and Proof of Stake (PoS) are popular. Proof of Work is similar to a security measure; it causes the addition of additional blocks to be slowed down. For instance, adding a new block in Bitcoin takes around ten minutes. This makes tampering extremely difficult since it requires much time to perform the work for every following block if someone tries to modify the data in one block. Another technique to ensure that transactions are legitimate is Proof of Stake (PoS), which operates differently than Proof of Work (PoW). In Proof of Stake (PoS), individuals are randomly selected depending on their stake amount to confirm new blocks. The selected individual will declare whether or not a new block is acceptable. A stake is a sum of money a candidate must deposit to be selected; if they approve an illegal transaction, they risk losing their investment. Additionally, the amount of money they can attempt to manipulate the system with is limited. If they successfully declare a block to be good, they will be rewarded with a portion of the transaction fees from that block. If this person does not want to continue as a validator, after a certain period to authenticate this person does not make any fake claims, their shares and earnings will be refunded. Therefore, attempting to scam the system by verifying phony blocks costs a lot of time and money.

E. THE CRYPTOGRAPHY HASH FUNCTION SHA-256

A common cryptographic technique called SHA-256 (Secure Hash technique 256) generates a fixed-length, 256-bit (32-byte) hash result. The SHA-256 algorithm aims to produce a distinct digital fingerprint of a piece of data, such as a file or message. Creating a SHA-256 hash entails passing the input data through an advanced mathematical formula that yields a distinct output value [35]. This output value is the hash, a digital fingerprint of the input data. Applications for the SHA-256 algorithm include blockchain technology, digital signatures, and password authentication. Secure Hashing Technique A cryptographic hash algorithm called SHA-256, or 256-bit, may transform any text into an almost unique 256-bit alphanumeric string. The output is referred to as a hash or hash value. Collision resistance, or the infeasibility of finding two distinct inputs that result in the same hash output, is a key feature of hash functions. SHA-256 is designed to be collision-resistant.

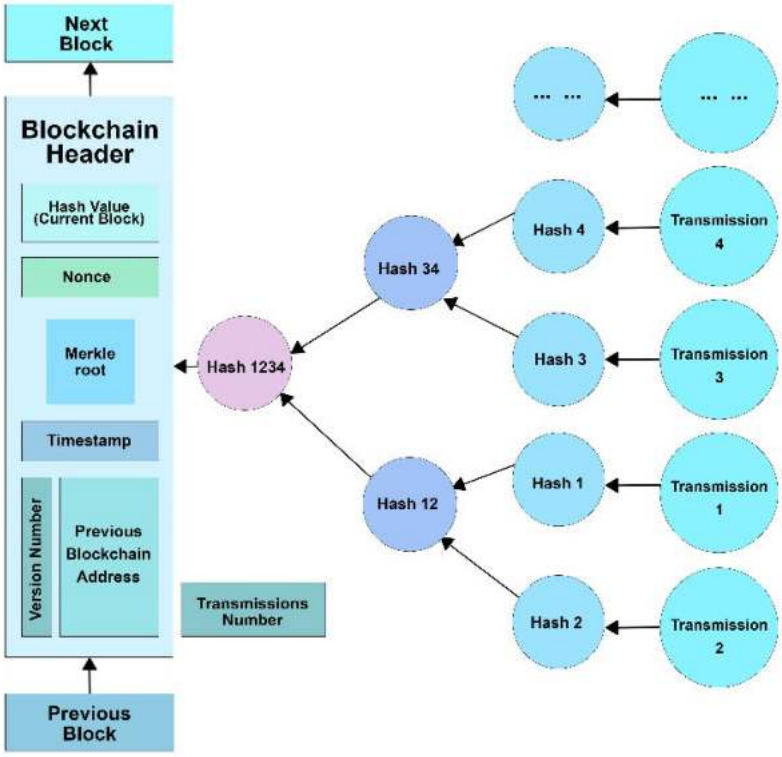


FIGURE 2. General Structure of Blockchain.

III. PROPOSED SYSTEM ARCHITECTURE

This paper suggests authentication procedures and security measures for the network. The sensor network structure includes sensor nodes (SNs), cluster heads (CHs), base stations (BSs), and end-users. The authentication process helps in verifying the identity of the user and ensures the legitimacy of the user and devices. Sensor nodes are equipped with sensors such as PMUs at the substations in order to gather information (measurement data). In a sensor network, cluster heads are nodes that serve as intermediaries between sensor nodes and base stations (Control Center). They help in organizing and managing data transmission within a cluster of sensor nodes. Base stations are central nodes in the network that collect and aggregate data from sensor nodes or cluster heads. They often act as the gateway for transmitting data to external systems or end-users. Fig. 3. Shows a visual representation of this framework and Fig. 4 represents the flow diagram of the proposed system:

Sensor nodes share common traits such as computing power and storage space. These nodes transmit data to designated cluster heads, typically those with superior computing power and storage capacity. The private blockchain is integrated into these cluster heads, while the public blockchain is implemented on base stations. The base station also manages the initialization process which provides an essential basis for the network's operation. In the duration of registration, nodes go through a careful setup process in order to determine their presence and function inside the network. The procedure then moves on to authentication, which makes sure that only nodes with permission may take part in network activities. The generation of public and private keys by the base station is a pivotal aspect of the security infrastructure. All nodes may access public keys, which enable secure communication, while only their respective entities can access private keys, which verify the integrity and provenance of the data being communicated. This cryptographic architecture provides an additional degree of security to the data-sharing process while also protecting against unauthorized access. Smart contracts play a pivotal role in the operational framework as they are deployed on public blockchains. In the context of the registration process, cluster heads utilize these smart contracts to verify the existence of clusters and execute the registration steps. These smart contracts effectively verify the accuracy and legitimacy of the MAC addresses linked to the cluster heads. The identification (ID) of the cluster heads is privately registered in the public blockchain on successful authentication. An error notice is sent out right away in the case of unsuccessful verification. Simultaneously, sensor node registration takes place on the private blockchain. Once the sensor nodes successfully complete the registration process, they gain authorization to actively participate in the network. The registration procedures for both sensor nodes and cluster heads follow a consistent methodology. In addition, when

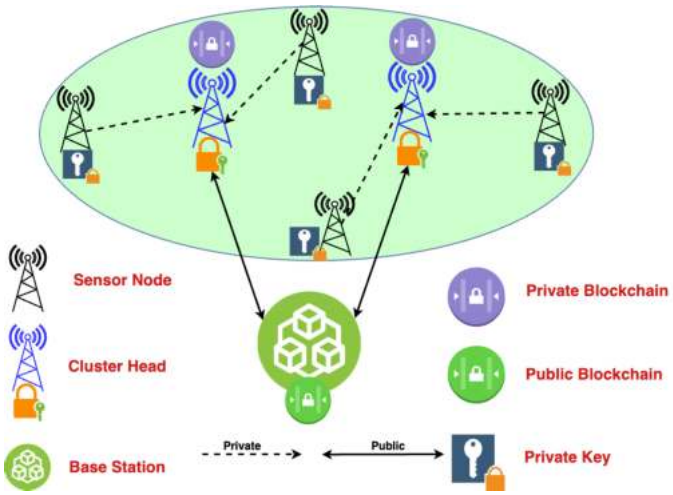


FIGURE 3. The proposed system model diagram.

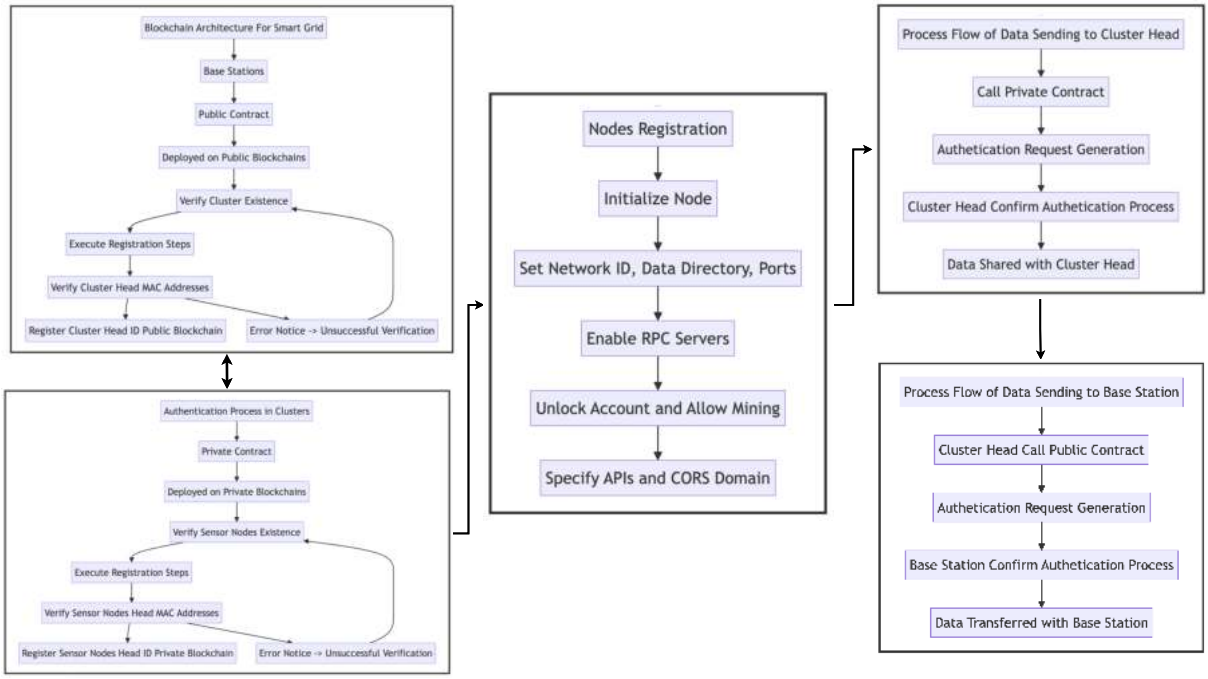


FIGURE 4. The proposed system flow diagram.

sensor nodes are deployed, they must be connected to their corresponding cluster heads. The network's collaborative structure is enhanced by this link, which enables smooth data interchange and communication between sensor nodes and their assigned cluster leaders. The interaction of public and private blockchains, smart contracts, and registration procedures creates a strong basis for the secure and efficient functioning of the network ecosystem. Wireless sensor networks face two prevalent types of attacks: external attacks and internal attacks. The registration and authentication processes of nodes significantly mitigate external attacks by preventing unauthorized entry, thus thwarting potential hackers from gaining access to the network.

IV. SYSTEM SETUP

Fig. 5 depicts the development process of the proposed system.

A. CREATING NODES

Nodes are the building blocks of the system, storing and managing data. To create a node, we have taken these steps:

1) Select a node type (e.g., miner, non-miner)
2) Configure the hardware (e.g., CPU, RAM, storage)
3) Install the necessary software (e.g., Geth, Metamask)
4) Ensure communication capabilities (e.g., network connectivity)

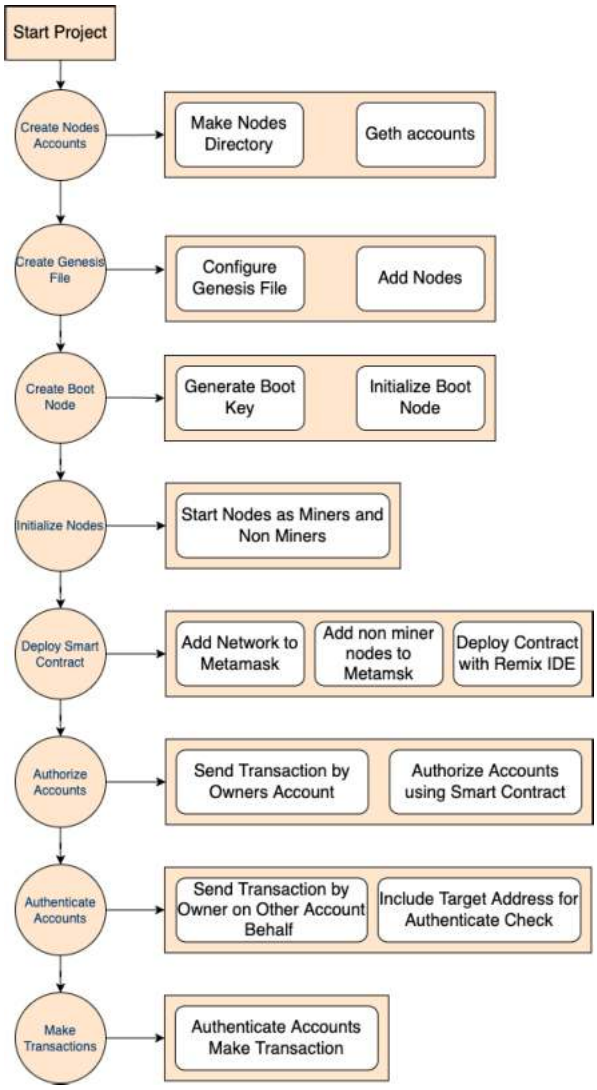


FIGURE 5. The proposed system development Diagram.

B. NODE CONFIGURATION

Once nodes are created, they must be configured to work together. This includes:

1) Defining node accounts
2) Setting roles and permissions for each account
3) Configuring network settings (e.g., IP address, port number)

C. GETH ACCOUNTS

Geth accounts to manage the system's cryptocurrency and access. Each node requires a Geth account, which would be securely stored.

D. GENESIS FILE CREATION

The Genesis file contains the initial configuration of the system, such as:

1) Network ID
2) Initial accounts and balances
3) Consensus mechanism
4) Block size
5) Difficulty

This file is created using a text editor and specific information is included.

E. CONFIGURING GENESIS FILE

After creating the Genesis file, we configured it to match the specific requirements of the system.

F. ADDING NODES TO GENESIS FILE

Nodes are added to the Genesis file to enable communication and data sharing. This includes adding the IP address and port number for each node.

G. CREATING THE BOOT NODE

The Boot Node is a special node that initiates the system and creates the initial blockchain. It requires a securely stored key.

H. GENERATING BOOT KEY

The Boot Key is a cryptographic key that is used to secure the Boot Node. It should be generated and stored securely.

I. BOOT NODE INITIALIZATION

The Boot Node needs to be initialized using the Geth command-line tool. The Boot Key is required for this process.

V. SYSTEM DEPLOYMENT

A. STARTING NODES

Nodes can be started as miners or non-miners using the Geth command-line tool.

B. METAMASK INTEGRATION

Metamask is a wallet that is integrated into the system. This allows users to manage their accounts and interact with the system.

C. DEPLOYING CONTRACTS

Smart contracts can be deployed to the system using the Remix IDE. This allows for the creation of custom applications and functionalities.

D. ACCOUNT AUTHORIZATION

The contract owner can authorize accounts for system usage and authenticate accounts for data access and modification.

E. TRANSACTION HANDLING

Once authorized and authenticated, accounts can send transactions to store data permanently on the blockchain. The contract owner manages access and can retrieve stored data.

VI. RESULTS

This simulation environment evaluates the feasibility and performance of a novel blockchain-based system for collecting and managing sensor data within a private network.

The system seeks to offer a secure, efficient, and transparent approach to data storage, retrieval, and analysis by leveraging a combination of public and private blockchain contracts, cluster heads, and sensor nodes. Table 1 Employed various libraries to simulate a robust blockchain system for managing sensor data effectively.

The simulation setup will be built upon the following key components:

1. Public Blockchain Contracts:
- Purpose: Defines the logic and rules for storing and managing data on the Blockchain.
- Key functions:
  - `storeData`: Allows authorized nodes to submit sensor readings.
  - `getData`: Retrieves specific data entries based on index or public access methods.
  - `Authenticate/deauthenticate`: Manages node access permissions.
  - `getDataCountPublic`: Publicly accessible function to get total data entries.
- Additional features include access control mechanisms, event logging for data storage, and potential tokenization for data ownership.

2. Private Blockchain Contracts (Clique Consensus):
- Purpose: Enables efficient and secure data sharing within a limited group of authorized nodes (cluster heads and sensor nodes).
- Key features:
  - Clique consensus: Block validation based on a pre-defined validator set (cluster heads) for faster transaction processing.
  - Configurable parameters: Block time, epoch duration, gas limit, and initial allocations.
  - Extra data: Includes addresses of participants for transparency and potential manipulation detection.

3. Cluster Head Code:
- Purpose: Manages sensor nodes, validates and aggregates their data before relaying to the public Blockchain.
- Key functionalities:
  - Communicates with sensor nodes and collects data.
  - Verifies sensor node authorization and data integrity.
  - Aggregates received data into meaningful formats for public chain submission.
  - It might implement additional logic like data filtering, anomaly detection, or pre-processing.

4. Sensor Node Code:
- Purpose: Generates and submits sensor readings to the cluster head.
- Key functionalities:
  - Connects to the Ethereum node and the specific cluster head contract.
  - Generates sensor data (replace with actual readings in your simulation).
  - Builds and signs transactions to call the `storeData` function on the cluster head contract.
  - Handles transaction confirmation and potential errors.
  - It might include data encryption, logging, and scheduling data transmissions.

5. Genesis File Code:
- Purpose: Defines the initial state of the blockchain network.
- Key elements:
  - Chain ID and network parameters for specific block configurations (homesteadBlock, eip150Block, etc.).
  - Clique consensus settings: block time, epoch duration, and validator set.
  - Block parameters: difficulty, gas limit, and extra data.
  - Initial token allocations for participating addresses.

A. PERFORMANCE METRICS AND SIGNIFICANCE

In evaluating the efficacy and functionality of blockchain networks, various performance metrics serve as crucial benchmarks, offering insights into the network's security, efficiency, scalability, and reliability. Each metric plays a distinct role in assessing different facets of blockchain operation, providing invaluable information for analysis and improvement. Equations 1-6 are used to monitor the performance of the proposed system.

Security Metrics:
- Hash Power: Reflects the computational power dedicated to securing the network, impacting its attack resistance.
- 51% Attack Resistance: Measures the network's ability to withstand a malicious majority control, ensuring stability.
- Double-Spend Resistance: Indicates the network's capability to prevent unauthorized spending of digital assets.

Consensus Mechanism Metrics:
- Consensus Algorithm: Defines the protocol governing how transactions are validated and added to the Blockchain, impacting security and decentralization.
- Throughput: This represents the rate of successful transaction processing within the network, influencing its speed and capacity.

Decentralization Metrics:
- Node Distribution: Determines the spread of network nodes, influencing resilience against central points of failure.
- Node Count: Reflects the number and role of nodes within the network, contributing to its decentralization.

Performance Metrics:
- Latency: Measures the delay in transaction confirmation, affecting the network's responsiveness.
- Scalability: Assesses the network's ability to handle increased transaction loads without compromising performance.

TABLE 1. Utilized Libraries in Simulating a Blockchain System for Sensor Data.

Component	Library	Description
Public Blockchain Contracts	web3.py	It connects to the Ethereum node, sends transactions, and interacts with contracts.
	JSON	Parses and handles contract ABI (Application Binary Interface) data.
	py-solc-x	Compiles Solidity contracts for deployment on the private network.
Private Blockchain Contracts (Clique Consensus)	web3.py	Connects to the private Ethereum node and interacts with contracts.
	geth_poa_middleware	Enables Clique consensus for block validation in the private network.
	web3.py	Connects to both public and private Ethereum nodes.
Cluster Head Code	JSON	Parses and processes sensor data received from nodes.
	time	Tracks the time it is taken for data aggregation and other operations.
	web3.py	Connects to the private Ethereum node and the cluster head contract.
Sensor Node Code	random	Generates random data to simulate sensor readings.
	time	Tracks time they are taken for transaction signing and confirmation.
Genesis File Code	JSON	Parses and loads the configuration file for the private network.

[]

Consistency and Finality Metrics:

- Finality Time: Indicates the time required for transactions to be considered immutable, impacting transaction reliability.
- Fork Rate: The frequency of divergent chains within the network influences data consistency.

Immutability Metrics:

- Immutability: Reflects the robustness of the Blockchain's permanence and resistance to unauthorized modifications.

Economic Metrics:

- Token Value: Represents the stability and utility of the native token within the network.
- Incentive Structure: Reflects the mechanisms encouraging network participants to maintain its integrity.

Interoperability Metrics:

- Cross-Chain Compatibility: Evaluates the network's ability to interact and share data with other blockchain networks.

$$\text{Hash Power} = \frac{\sum_{\mathbf{i=1}}^{\mathbf{n}} \mathrm{H_i}}{\sum_{\mathbf{j=1}}^{\mathbf{m}} \mathrm{T_j}} \tag{1}$$

H_i: Individual hash rates of n miners and T_j: Individual mining times of m blocks.

$$51\%\ \text{Attack Resistance} = \frac{\sum_{\mathbf{i=1}}^{n} \mathrm{HN_i}}{\sum_{\mathbf{j=1}}^{n} \mathrm{TN_j}} \times 100 \tag{2}$$

HN_i: Number of honest nodes in each subset i and TN_j: Total number of nodes in each subset j.

$$\textbf{Throughput} = \frac{\sum_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{TT_i}}{\sum_{\mathbf{j=1}}^{\mathbf{m}} \mathbf{TiT_j}} \tag{3}$$

$\mathbf{TT}_i$: Total transactions processed in a time segment i and $\mathbf{TiT}_j$: Time taken to process transactions in segment j.

$$\textbf{Node Distribution} = \frac{\sum_{\mathbf{i=1}}^{n} NC_{\mathbf{i}}}{\sum_{\mathbf{j=1}}^{m} TN_{\mathbf{j}}} \times 100 \tag{4}$$

NC_i: Number of nodes clustered in region i and TN_j: Total number of nodes in segment j.

$$\textbf{Latency} = \frac{\sum_{\mathbf{i=1}}^{\mathbf{n}} \mathrm{TD_i}}{\sum_{\mathbf{j=1}}^{\mathbf{m}} \mathrm{TS_j}} \tag{5}$$

D_i: Time delay in transaction confirmation in subset i and S_i: Total transactions sent in subset j.

$$\textbf{Finality Time} = \frac{\text{Blocks}}{\text{Consensus}} \times \textbf{Block Time} \tag{6}$$

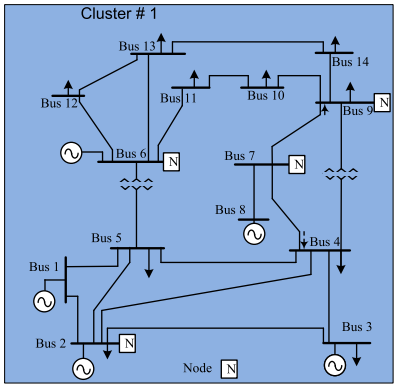
Blocks: Number of confirmed blocks. Consensus: Number of nodes agreeing on consensus. Block Time: Average time to generate a block.

B. NETWORK ARCHITECTURE

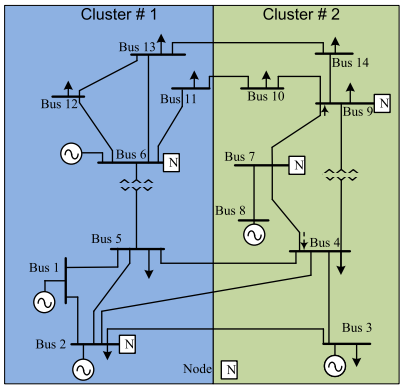
The network architecture was tested across various test systems to evaluate its performance in diverse scenarios. Test cases were conducted on the IEEE 14-bus, IEEE 30-bus, and IEEE 118-bus networks, each representing different complexities and node-cluster configurations:

1. IEEE 14-bus:
   - Test Case 1: Utilizing four nodes (PMUs/RTUs) and 1 cluster.
   - Test Case 2: Employing four nodes (PMUs/RTUs) with 2 clusters (two nodes per cluster).
2. IEEE 30-bus:
   - Test Case: Hybrid configuration engaging four nodes (PMUs/RTUs) within 1 cluster and operating five nodes in a second cluster configuration.
3. IEEE 118-bus: Hybrid Combination by deploying a total of 4 clusters and 30 nodes as follows:
   - Cluster I: Deploying eleven nodes (PMUs/RTUs) within 1 cluster.
   - Cluster II: Utilizing nine nodes (PMUs/RTUs) with 1 cluster.
   - Cluster III: Implementing eight nodes (PMUs/RTUs) within 1 cluster.
   - Cluster IV: Employing two nodes (PMUs/RTUs) in 1 cluster configuration.

The number of nodes is chosen such that the network is guaranteed to have full observability. These diverse test cases aimed to assess the scalability, performance, and efficiency of the network architecture across different bus networks and node-cluster arrangements. In the proposed system, there are four networks with nine cluster heads organized as follows: N1CH (Network 1 Cluster Head 1), N2CH1 (Network 2 Cluster Head 1), N2CH2 (Network 2 Cluster Head 2), N3CH1



(a) IEEE 14-bus system with One cluster and four nodes



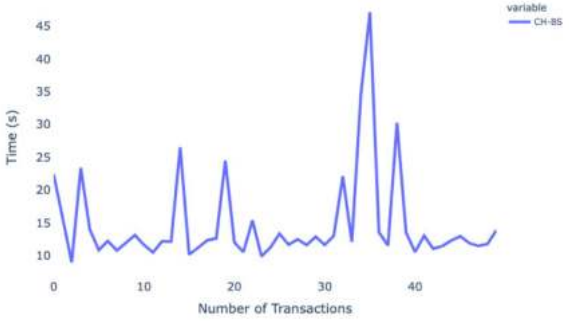
(b) IEEE 14-bus system with two clusters and four nodes

FIGURE 6. IEEE 14-bus test system with two possible configurations.

(Network 3 Cluster Head 1), N3CH2 (Network 3 Cluster Head 2), N4CH1 (Network 4 Cluster Head 1), N4CH2 (Network 4 Cluster Head 2), N4CH3 (Network 4 Cluster Head 3), and N4CH4 (Network 4 Cluster Head 4).

Each sensor node transmits 50 transactions to the cluster head, and the individual transaction details, including time, are illustrated in the respective figures. Similarly, the cluster head forwards the received information to the base station, and the time taken for their transmission is also evaluated. In each graph, the x-axis represents the number of transactions, while the y-axis denotes the time required for the completion and storage of transactions on the blockchain network.

Fig. 6 shows the two test cases for the IEEE 14-bus test system. In the first case, the whole network is combined into one cluster with four nodes. The other case shows the network with two clusters and two nodes per cluster. The graphical representation showing data sharing of both cluster-to-base data and node-to-cluster for the first test case is depicted in Fig. 7, and its performance evaluation is presented in Table 4. Similarly, the graphical representation for data sharing of the IEEE 14-bus network with two clusters and four nodes is shown in Fig. 8.



(a) Cluster to base station data sharing

(b) Nodes to cluster data sharing

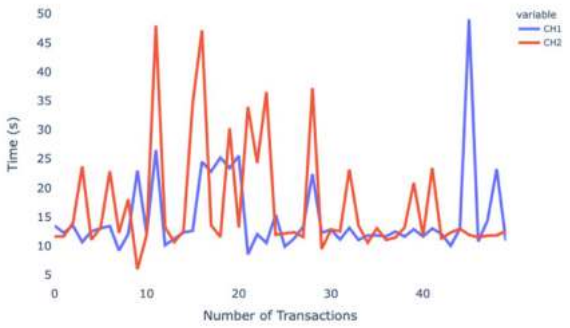
FIGURE 7. Graphical representation of IEEE 14-bus with 1 cluster and four nodes.

Network 1 in Fig. 7, consisting of four sensor nodes, the average time for each sensor node to transmit 50 transactions to the cluster head was approximately 9.95 units. Additionally, the average time for Cluster 1 to relay these transactions to the base station was about 14.77 units.

On the other hand, in network 2 in Fig. 8 the IEEE 14-bus system was divided into two clusters, each comprising two sensor nodes. The average time for the sensor nodes in the first subnetwork was approximately 9.92 units, while for the second subnetwork, it was approximately 9.95 units. When these clusters forwarded 50 transactions per node to the base station, Cluster 1 took about 14.88 units on average, whereas Cluster 2 took notably longer at around 17.08 units. However, the collective average time for both clusters in Network 2 to transmit data to the base station was around 15.98 units.

Comparatively, Network 1 demonstrated slightly lower individual node transmission times than Network 2's subnetworks. However, when considering the transmission from clusters to the base station, Network 2 showcased varying times between its clusters, with Cluster 1 closely aligning with the performance of Cluster 1 in Network 1, while Cluster 2 lagged notably behind in transmission efficiency. The performance of both configurations for the IEEE 14-bus is similar security-wise with a higher number of transactions for the two clusters configuration.

For the IEEE-30-bus system, Fig. 9 illustrates the graphical representation of the network with two clusters and nine nodes, with performance evaluation presented in Table 5.



(a) Clusters to base station data sharing

(b) Four Nodes sharing data with cluster 1 and 2

FIGURE 8. Graphical representation of IEEE 14-bus with 2 clusters and four nodes.

(a) Clusters to base station data sharing

(b) Five Nodes sharing data with cluster 1

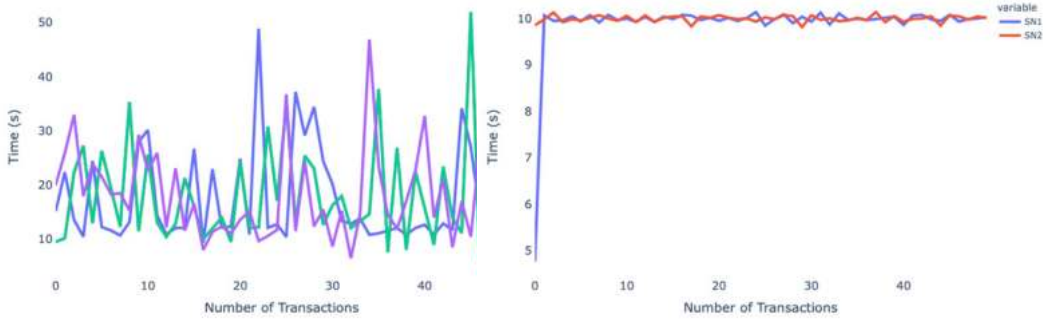
(c) Four Nodes sharing data with cluster 2

FIGURE 9. Graphical representation of IEEE 30-bus with 2 clusters and nine nodes.

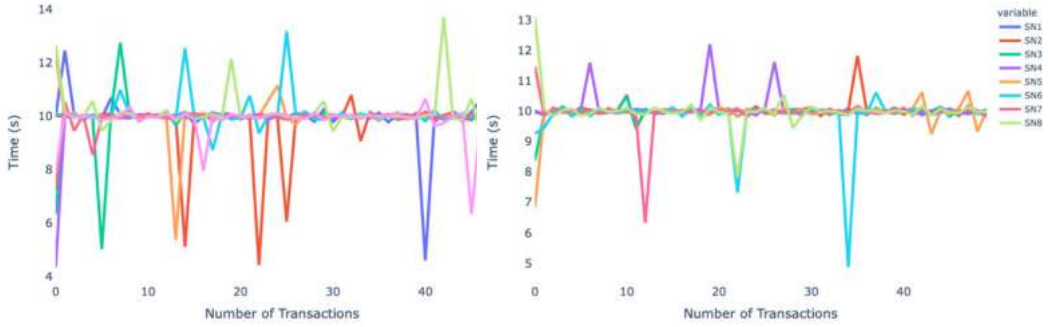
The IEEE 118-bus test system, the grid is divided into 4 clusters where each cluster has different number of nodes. The grid needs a minimum of 30 nodes for complete observability. These 30 nodes are organized into 4 clusters, where the number of nodes per cluster is different to mimic a realistic scenario. The nodes per cluster can differ depending on several factors such as the distance between substations and the cost. Fig. 10 showcases the graphical representation of the network performance for the IEEE 118-bus system, while Table 6 presents the parametric performance of the system. As can be seen, changing the network configuration by increasing/decreasing the cluster-to-node ratio has little effect on the overall security of the network. Therefore, the utility has the flexibility to choose the better configuration for its specific grid due to other factors such as distance and overall cost.

Figure 11 compiled the performance metrics of every cluster head into a singular visual representation, offering a comprehensive overview of their individual performances within a unified image. The mean represents the arithmetic average of all values in a dataset, serving as a central measure indicative of the dataset's general value. Standard error estimates the variability between sample means and population means, offering insight into how much the sample mean might deviate from the true population mean. The median is the middle value within a dataset, effectively dividing the data into two halves, illustrating the central tendency without being influenced by extreme values.

Standard deviation measures the dispersion of values around the mean, conveying how much individual data points deviate from the average. Sample variance assesses the spread of data points from the mean, providing a quantifiable measure of data distribution width. Kurtosis gauges the "tailedness" of a dataset's distribution, indicating whether the data has heavy or light tails compared to a normal distribution. Skewness measures the asymmetry of the data distribution, revealing whether the data is skewed



(a) Clusters to base station data sharing (b) Two Nodes sharing data with cluster 1



(c) Nine Nodes sharing data with cluster 2 (d) Eight Nodes sharing data with Cluster 3

(e) Eleven Nodes sharing data with Cluster 4

FIGURE 10. **Graphical representation of IEEE 118-bus with 4 clusters and thirty nodes.**

to the left or right. The range signifies the span between the smallest and largest values within the dataset, offering an overview of the data's scope. Minimum represents the smallest observed value within the dataset, while maximum denotes the largest value. Sum reflects the total sum of all values within the dataset, providing the combined value of all observations. Count specifies the number of observations in the dataset, showing the sample size. Largest(1) and Smallest(1) refer to the single largest and smallest values observed in the dataset, respectively, mirroring the maximum and minimum values. Based on statistical calculations and the provided sample statistics, the confidence level signifies the range within which the true population parameter will likely fall.

Table 2 presents an array of statistical metrics encompassing various networks N1C1, N2C1, N2C2, N3C1, N3C2, N4C1, N4C2, N4C3, and N4C4. Each matrix is analyzed across measures such as mean, standard error, median, standard deviation, sample variance, kurtosis, skewness, range, minimum, maximum, sum, count, largest, smallest, and confidence level. Across these matrices, key findings emerge: The mean values range approximately from 14.76 to 18.48, demonstrating variations across different network configurations. The standard error varies between 0.98 and 1.37 within distinct networks. Median values fluctuate from 12.22 to 16.8, indicating central tendencies. The standard deviation ranges from approximately 6.94 to 9.74, depicting data dispersion. Sample variance values span from 48.18 to

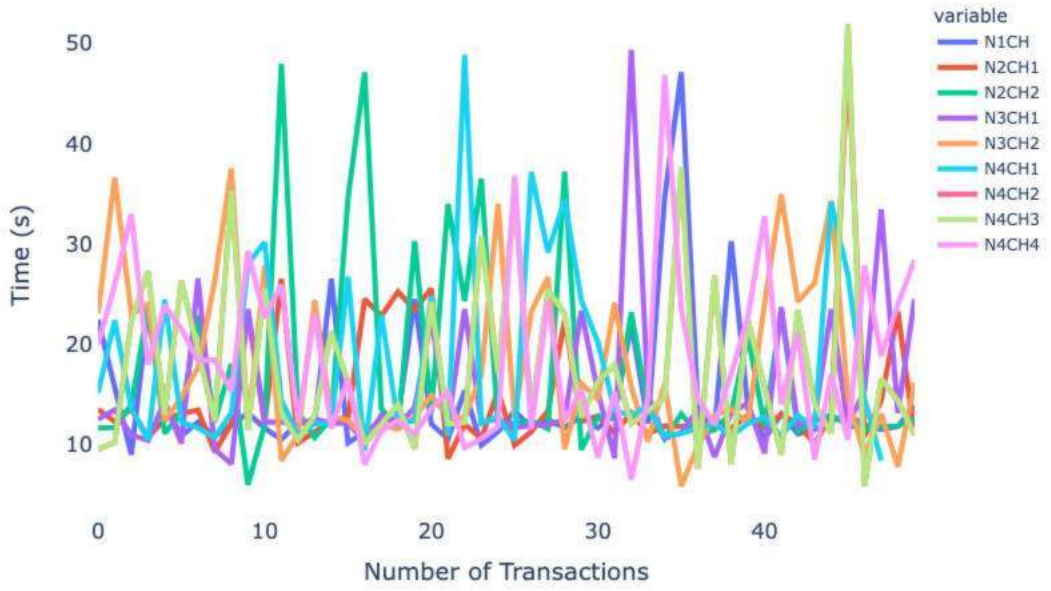


FIGURE 11. All cluster heads performance in proposed system.

TABLE 2. Performance matrices of each cluster in different networks.

Matrices	N1C1	N2C1	N2C2	N3C1	N3C2	N4C1	N4C2	N4C3	N4C4
Mean	14.77	14.88	17.08	15.08	17.78	17.31	17.75	17.75	18.48
Standard Error	1.01	0.98	1.38	1.04	1.17	1.30	1.29	1.29	1.17
Median	12.22	12.41	12.57	12.50	14.70	12.82	14.19	14.19	16.80
Standard Deviation	7.11	6.94	9.74	7.34	8.24	8.98	9.12	9.12	8.26
Sample Variance	50.59	48.18	94.81	53.93	67.92	80.70	83.16	83.16	68.17
Kurtosis	9.02	11.17	2.68	9.21	-0.10	2.15	2.97	2.97	1.64
Skewness	2.84	2.91	1.84	2.68	0.92	1.57	1.55	1.55	1.13
Range	38.16	40.49	41.99	41.33	31.69	40.48	46.06	46.06	40.34
Minimum	8.97	8.57	5.97	8.05	5.82	8.39	5.88	5.88	6.51
Maximum	47.13	49.06	47.96	49.38	37.51	48.87	51.94	51.94	46.86
Sum	738.2	743.9	854.0	753.8	888.8	830.8	887.3	887.3	924.2
Count	50.00	50.00	50.00	50.00	50.00	50.00	50.00	50.00	50.00
Largest(1)	47.13	49.06	47.96	49.38	37.51	48.87	51.94	51.94	46.86
Smallest(1)	8.97	8.57	5.97	8.05	5.82	8.39	5.88	5.88	6.51
Confidence Level(95.0%)	2.02	1.97	2.77	2.09	2.34	2.61	2.59	2.59	2.35

[]

TABLE 3. Cluster Nodes Transactions Average Time.

Clusters	Nodes	Transactions	Processing Time
1	4	200	9.9470
2	2	100	9.9204
3	2	100	9.9727
4	5	250	9.9280
5	4	200	10.0122
6	11	550	9.9250
7	9	450	9.9414
8	8	400	9.9769
9	2	100	9.9446

94.81, indicating data variability. Kurtosis values vary between -0.096 and 11.17, indicating differing degrees of tailedness in the distributions. Skewness ranges from 0.92 to 2.90, demonstrating the asymmetry of the data. The range spans approximately 31.69 to 46.05, showing the spread between minimum and maximum values. Minimum values oscillate between 5.87 and 8.97, while maximum values range from 37.51 to 51.94 across the datasets. Sum totals of values across different matrices range from approximately 738.28 to 924.24, signifying overall aggregated values. The confidence level (95.0%) fluctuates between approximately 1.97 and 2.77, indicating the range within which the true population parameter might fall based on sample statistics.

As shown in Table 3, the processing time for clusters 2, 4, 6, 7, 8, and 9 have relatively similar average times. Cluster 5 stands out with a slightly higher time of 10.0122. As for node ratio, clusters 6 and 7 have higher node counts but

TABLE 4. Simulation environment in IEEE 14-bus with 1 cluster and four nodes.

Network 1	IEEE 14-bus Test Case 1
Blockchain Type	PoA Ethereum Blockchain network in each cluster, with an Ethereum test net (Goerli) for the public Blockchain.
Consensus Mechanism	Proof of Authority (PoA)
Security Metrics	
Hash Power	Close to 0 due to deterministic block creation by validators.
51% Attack Resistance	Strong resistance due to the presence of 5 mining nodes and low difficulty.
Double-Spend Resistance	N/A
Consensus Mechanism Metrics	
Consensus Algorithm	PoA ensures strong security and finality but limited decentralization.
Throughput	One transaction per 10 seconds per node, with four sensor nodes sending data to the cluster head.
Decentralization Metrics	
Node Distribution	Currently centralized on a local machine; intended distribution in the final deployment.
Node Count	Five nodes with 1 Cluster Head and 4 Sensor Nodes.
Performance Metrics	
Latency	Average of 10s.
Scalability	Highly scalable with five actively mining nodes.
Throughput	Four transactions every 10 seconds in total.
Consistency and Finality Metrics	
Finality Time	Customizable for desired security level.
Fork Rate	Negligible
Immutability Metrics	
Immutability	Robust and secure due to trusted validators ensuring blockchain integrity.
Economic Metrics	
Token Value	Stable unit of value for transactions and smart contracts.
Incentive Structure	Inherently incentivized validators ensure network integrity.
Interoperability Metrics	
Cross-Chain Compatibility	Independent blockchain setup with no direct connection between public and private networks.

[]

TABLE 5. Simulation environment in IEEE 30-bus with 2 clusters and nine nodes.

Network 3	IEEE 30-bus
Blockchain Type	PoA Ethereum Blockchain network in each cluster, with an Ethereum test net (Goerli) for the public Blockchain.
Consensus Mechanism	Proof of Authority (PoA)
Security Metrics	
Hash Power	Close to 0 due to deterministic block creation by validators.
51% Attack Resistance	There is strong resistance due to 6 mining nodes in the first cluster, five in the second cluster, and a low difficulty level.
Double-Spend Resistance	N/A
Consensus Mechanism Metrics	
Consensus Algorithm	PoA ensures strong security and finality but limited decentralization.
Throughput	One transaction per 10 seconds per sensor node with four sensor nodes sending data to cluster head 1 and 5 sensor nodes to cluster head 2.
Decentralization Metrics	
Node Distribution	Currently centralized on one local machine; intended distribution in the final deployment.
Node Count	Eleven nodes: 2 Cluster Heads and 9 Sensor Nodes.
Performance Metrics	
Latency	Average of 10s.
Scalability	Highly scalable with 11 actively mining nodes.
Throughput	Nine transactions every 10 seconds across the network from 9 sensor nodes to cluster heads.
Consistency and Finality Metrics	
Finality Time	Adjustable for desired security level.
Fork Rate	Negligible
Immutability Metrics	
Immutability	Robust and secure due to trusted validators ensuring blockchain integrity.
Economic Metrics	
Token Value	Stable unit of value for transactions and smart contracts.
Incentive Structure	Inherently incentivized validators ensure network integrity.
Interoperability Metrics	
Cross-Chain Compatibility	Independent blockchain setup with no direct connection between public and private networks.

relatively lower average times compared to their transaction volumes, indicating potential efficiency in processing. Based on this data, clusters 6 and 7 seem promising for a balance between security, time, and processing, considering their lower average times despite having a higher number of nodes and transactions. Therefore, the grid can be divided into sub-regions and managed by clusters, and increasing the number of clusters will have a minor effect on the processing time while maintaining the advantages of enhanced security.

C. ROCK-SOLID SECURITY ARCHITECTURE

1) BLOCKCHAIN-BASED IMMUTABILITY

The system leverages blockchain technology, ensuring data remains permanently recorded and tamper-proof. This immutable ledger guarantees data integrity and prevents unauthorized modifications, creating a robust foundation for secure data storage.

2) MULTI-LAYERED ENCRYPTION

Data is encrypted with private keys, accessible only by authorized entities. This safeguards sensitive information and ensures secure communication within the network.

3) SMART CONTRACT-ENABLED SECURITY

Smart contracts automate data validation and access control, further enhancing security and eliminating manual intervention vulnerabilities.

4) IMPENETRABLE GATEKEEPING

Only validated nodes can gain network access, significantly reducing the risk of unauthorized infiltration and malicious

TABLE 6. Simulation environment in IEEE 118-bus with 4 clusters and 30 nodes.

Network 4	IEEE 118-bus
Blockchain Type	PoA Ethereum Blockchain network in each cluster, with an Ethereum test net (Goerli) for the public Blockchain.
Consensus Mechanism	Proof of Authority (PoA)
Security Metrics	
Hash Power	Close to 0 due to deterministic block creation by validators.
51% Attack Resistance	Strong resistance due to 34 mining nodes and a low difficulty level of 1.
Double-Spend Resistance	N/A
Consensus Mechanism Metrics	
Consensus Algorithm	PoA ensures strong security and finality but limited decentralization.
Throughput	One transaction per 10 seconds per sensor node.
Decentralization Metrics	
Node Distribution	Currently centralized on one local machine; intended distribution in the final deployment.
Node Count	Thirty-four nodes: 4 Cluster Heads and 30 Sensor Nodes distributed across 4 clusters.
Performance Metrics	
Latency	Average of 10s.
Scalability	Highly scalable with 34 actively mining nodes.
Throughput	30 transactions every 10 seconds across all clusters.
Consistency and Finality Metrics	
Finality Time	Adjustable for desired security level.
Fork Rate	Zero
Immutability Metrics	
Immutability	Robust and secure due to trusted validators ensuring blockchain integrity.
Economic Metrics	
Token Value	Stable unit of value for transactions and smart contracts.
Incentive Structure	Inherently incentivized validators ensure network integrity.
Interoperability Metrics	
Cross-chain compatibility	Independent blockchain setup with no direct connection between public and private networks.

activity. This stringent approach bolsters the network's resilience against potential threats.

5) ENHANCED NETWORK RESILIENCE

The system incorporates data redundancy mechanisms to ensure data availability even if individual nodes fail. Additionally, error correction algorithms identify and rectify corrupted data, further safeguarding data integrity.

6) ROBUST COMMUNICATION PROTOCOLS

Reliable communication protocols minimize data loss due to network disruptions, ensuring smooth and secure data transmission.

7) PROACTIVE THREAT MITIGATION

These systems actively monitor the network for suspicious activity, identifying and preventing potential attacks before they can inflict damage.

8) DATA INTEGRITY CHECKS

Cryptographic hashing and digital signatures verify data authenticity and ensure it remains untampered with, upholding data integrity and preventing malicious manipulation.

9) CONTINUOUS MONITORING AND IMPROVEMENT

The system is constantly monitored for vulnerabilities and potential issues, enabling prompt identification and resolution.

10) DATA LOGGING AND ANALYSIS

Data logging facilitates forensic analysis in case of security incidents, allowing for thorough investigations and improvements to the system's security posture.

By combining blockchain technology, robust encryption methods, and meticulous access control procedures, the system's multi-layered security architecture prioritizes data security and ensures a highly resilient and trustworthy network. This comprehensive approach effectively mitigates the risks of data failure, duplication, or compromise, creating a secure environment for data storage and transmission.

VII. CONCLUSION

In conclusion, this research investigated the pivotal role of blockchain-integrated wireless sensor nodes in fortifying cyber-physical security within smart grid infrastructures. The escalating cyber threats targeting modern grid systems underscore the imperative of robust cybersecurity frameworks. The integration of blockchain technology, specifically leveraging a Proof of Authority (PoA) Ethereum Blockchain network, exhibited promising capabilities in bolstering data integrity, fortifying data transmission reliability, and amplifying trust within Supervisory Control and Data Acquisition (SCADA) networks. The empirical evaluation across IEEE 14-bus, 30-bus, and 118-bus topologies unveiled the transformative potential of Blockchain in mitigating vulnerabilities inherent in traditional SCADA systems. Statistical analyses, encompassing mean, standard deviation, skewness, kurtosis, and confidence levels, provided nuanced insights into the efficacy and resilience of blockchain-based solutions against contemporary cyber threats. The findings underscore the significance of blockchain technology as a viable mechanism to enhance cyber-physical security in smart grid operations. By addressing the complexities of cyber threats, such as DOS attacks, FDIA vulnerabilities, and potential cyber-physical manipulations, this study lays the groundwork for robust and resilient smart grid ecosystems. The outcomes of this research pave the way for future endeavors in

advancing cyber-physical security paradigms within smart grid infrastructures. As the landscape of cyber threats continues to evolve, further research and implementations are essential to fortify and safeguard critical infrastructure against emerging challenges.

APPENDIX
SIMULATION ENVIRONMENT

The section presents the simulation environments for the two test cases of the IEEE 14-bus, the test case for the IEEE 30-bus, and the hybrid case for the IEEE 118-bus test system.

REFERENCES

[1] K. Sayed and H. A. Gabbar, "SCADA and smart energy grid control automation," in *Smart Energy Grid Engineering*. Amsterdam, The Netherlands: Elsevier, 2017, pp. 481–514.

[2] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on SCADA systems: Secure protocols, incidents, threats and tactics," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1942–1976, 3rd Quart., 2020.

[3] Y. Wan and J. Cao, "A brief survey of recent advances and methodologies for the security control of complex cyber-physical networks," *Sensors*, vol. 23, no. 8, p. 4013, Apr. 2023.

[4] L. C. R. Salvador, N. H. P. Dai, and R. Zoltán, "SCADA systems: Security concerns and countermeasures," in *Proc. IEEE 21st World Symp. Appl. Mach. Intell. Inform. (SAMI)*, Herl'any, Slovakia, Feb. 2023, pp. 000251–000254, doi: 10.1109/SAMI58000.2023.10044495.

[5] M. Shrestha, C. Johansen, J. Noll, and D. Roverso, "A methodology for security classification applied to smart grid infrastructures," *Int. J. Crit. Infrastruct. Protection*, vol. 28, Mar. 2020, Art. no. 100342.

[6] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annu. Rev. Control*, vol. 47, pp. 394–411, Jan. 2019.

[7] S. Aoufi, A. Derhab, and M. Guerroumi, "Survey of false data injection in smart power grid: Attacks, countermeasures and challenges," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102518.

[8] A. J. G. de Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, "Artificial intelligence-based cyber security in the context of Indusstry 4.0—A survey," *Electronics*, vol. 12, no. 8, p. 1920, Apr. 2023.

[9] Y. Xiang, L. Wang, and N. Liu, "Coordinated attacks on electric power systems in a cyber-physical environment," *Electr. Power Syst. Res.*, vol. 149, pp. 156–168, Aug. 2017.

[10] E. Kalita, "WannaCry ransomware attack: Protect yourself from WannaCry ransomware cyber risk and cyber war," in *Proc. 34th Annu. Comput. Secur. Appl. Conf.*, ACM Digital Library, 2018, pp. 124–136.

[11] J. Beerman, D. Berent, Z. Falter, and S. Bhunia, "A review of colonial pipeline ransomware attack," in *Proc. IEEE/ACM 23rd Int. Symp. Cluster, Cloud Internet Comput. Workshops (CCGridW)*, May 2023, pp. 8–15.

[12] M. Alawida, A. E. Omolara, O. I. Abiodun, and M. Al-Rajab, "A deeper look into cybersecurity issues in the wake of COVID-19: A survey," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8176–8206, Nov. 2022.

[13] A. M. Y. Koay, R. K. L. Ko, H. Hettema, and K. Radke, "Machine learning in industrial control system (ICS) security: Current landscape, opportunities and challenges," *J. Intell. Inf. Syst.*, vol. 60, no. 2, pp. 377–405, Apr. 2023.

[14] L. Cui, Y. Qu, L. Gao, G. Xie, and S. Yu, "Detecting false data attacks using machine learning techniques in smart grid: A survey," *J. Netw. Comput. Appl.*, vol. 170, Nov. 2020, Art. no. 102808.

[15] S. Almasabi, T. Alsuwian, M. Awais, M. Irfan, M. Jalalah, B. Aljafari, and F. A. Harraz, "False data injection detection for phasor measurement units," *Sensors*, vol. 22, no. 9, p. 3146, Apr. 2022.

[16] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems," *IEEE Access*, vol. 7, pp. 46595–46620, 2019.

[17] S. Almasabi, T. Alsuwian, E. Javed, M. Irfan, M. Jalalah, B. Aljafari, and F. A. Harraz, "A novel technique to detect false data injection attacks on phasor measurement units," *Sensors*, vol. 21, no. 17, p. 5791, Aug. 2021.

[18] O. A. Alimi, K. Ouahada, and A. M. Abu-Mahfouz, "A review of machine learning approaches to power system security and stability," *IEEE Access*, vol. 8, pp. 113512–113531, 2020.

[19] O. A. Alimi, K. Ouahada, A. M. Abu-Mahfouz, S. Rimer, and K. O. A. Alimi, "A review of research works on supervised learning algorithms for SCADA intrusion detection and classification," *Sustainability*, vol. 13, no. 17, p. 9597, Aug. 2021.

[20] A. Chehri, I. Fofana, and X. Yang, "Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence," *Sustainability*, vol. 13, no. 6, p. 3196, Mar. 2021.

[21] T.-H. Kim, R. Goyat, M. K. Rai, G. Kumar, W. J. Buchanan, R. Saha, and R. Thomas, "A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks," *IEEE Access*, vol. 7, pp. 184133–184144, 2019.

[22] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, and J. Wang, "Incentive mechanism of data storage based on blockchain for wireless sensor networks," *Mobile Inf. Syst.*, vol. 2018, pp. 1–10, Aug. 2018.

[23] O. I. Khalaf and G. M. Abdulsahib, "Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2858–2873, Sep. 2021.

[24] S. Katyara, M. A. Shah, B. S. Chowdhary, F. Akhtar, and G. A. Lashari, "Monitoring, control and energy management of smart grid system via WSN technology through SCADA applications," *Wireless Pers. Commun.*, vol. 106, no. 4, pp. 1951–1968, Jun. 2019.

[25] M. Erol-Kantarci and H. T. Mouftah, "Wireless sensor networks for cost-efficient residential energy management in the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 314–325, Jun. 2011.

[26] D. Neilson, S. Hara, and I. Mitchell, "Bitcoin forensics: A tutorial," in *Global Security, Safety and Sustainability—The Security Challenges of the Connected World*. Cham, Switzerland: Springer, 2016, pp. 12–26.

[27] M. Erol-Kantarci and H. T. Mouftah, "Smart grid forensic science: Applications, challenges, and open issues," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 68–74, Jan. 2013.

[28] C. Stöcker and R. Abe. (2018). Software Defined Digital Grid on a P2P Network—On Systems of Autonomous Energy Cells. Medium. Accessed: Nov. 20, 2023. [Online]. Available: https://cstoecker.medium.com/software-defined-digital-grid-on-a-p2p-network-cdd17c9017e4

[29] N. C. Batista, R. Melício, J. C. O. Matias, and J. P. S. Catalão, "Photovoltaic and wind energy systems monitoring and building/home energy management using ZigBee devices within a smart grid," *Energy*, vol. 49, pp. 306–315, Jan. 2013.

[30] W. Tushar, B. Chai, C. Yuen, D. B. Smith, K. L. Wood, Z. Yang, and H. V. Poor, "Three-party energy management with distributed energy resources in smart grid," *IEEE Trans. Ind. Electron.*, vol. 62, no. 4, pp. 2487–2498, Apr. 2015.

[31] C. Zhao, J. He, P. Cheng, and J. Chen, "Consensus-based energy management in smart grid with transmission losses and directed communication," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2049–2061, Sep. 2017.

[32] B. Jo, R. Khan, and Y.-S. Lee, "Hybrid blockchain and Internet-of-Things network for underground structure health monitoring," *Sensors*, vol. 18, no. 12, p. 4268, Dec. 2018.

[33] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain, Res. Appl.*, vol. 3, no. 2, Jun. 2022, Art. no. 100067.

[34] C. G. Akcora, Y. R. Gel, and M. Kantarcioglu, "Blockchain networks: Data structures of Bitcoin, Monero, Zcash, Ethereum, Ripple, and IOTA," *WIREs Data Mining Knowl. Discovery*, vol. 12, no. 1, p. e1436, Jan. 2022.

[35] S. B. Suhaili and T. Watanabe, "Design of high-throughput SHA-256 hash function based on FPGA," in *Proc. 6th Int. Conf. Electr. Eng. Informat. (ICEEI)*, Nov. 2017, pp. 1–6.

SALEH ALMASABI (Member, IEEE) received the B.S. degree in electrical and electronics engineering from the King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia, in 2008, the M.S. degree from Wayne State University, Detroit, MI, USA, in 2014, and the Ph.D. degree from Michigan State University, East Lansing, MI. He is currently an Assistant Professor with the Electrical Engineering Department, Najran University Saudi Arabia. His research interests include power systems, smart grids, reliability, PMU applications, and cyber-physical security.

AHMAD SHAF received the B.S. and M.S. degrees in computer science from COMSATS University Islamabad (CUI), Sahiwal Campus, Sahiwal, Pakistan, in 2016 and 2018, respectively. He has a strong educational background in computer science. Currently, he is a Lecturer with the Department of Computer Science, CUI. In this role, he imparts his knowledge and expertise to students, contributing to their academic and professional development. He is a prolific Researcher, having authored more than 30 research articles in reputed journals, books, and conference proceedings. His research work has been recognized and cited by his peers, with 206 citations on Google Scholar and an H-index of ten. His current research interests include computer vision, data science, big data, machine learning, deep learning, the Internet of Things (IoT), and underwater wireless sensor networks (UWSNs). These diverse interests reflect his curiosity and involvement in cutting-edge technologies and their applications.

TARIQ ALI received the M.S. degree in computer science from SZABIST, Islamabad, Pakistan, in 2006, and the Ph.D. degree in information technology from University Teknologi PETRONAS, Malaysia, in 2015. During the M.S. degree, his specialization was networks and communication. He was a Lecturer with the Computer Science Department, Gordon College, Rawalpindi, Pakistan, from 2007 to 2009. He has served for more than two years as an IT Manager with the IT Department of the Government of Pakistan. He is currently an Assistant Professor with the Computer Science Department, COMSATS University Islamabad, Sahiwal Campus. He is on EoL leave and also doing a Postdoctoral Fellowship with Najran University, Saudi Arabia. He has published a good number of journal articles, conference papers, and book chapters on well-known publishing platforms. During the Ph.D. degree, his specialization was underwater wireless sensor networks. His current research interests include mobile and sensor networks, routing protocols, the Internet of Things, digital communication, and underwater acoustic sensor and actor networks.

MARYAM ZAFAR received the B.S. degree in computer science from COMSATS University Islamabad. Her academic journey was marked by a relentless pursuit of knowledge and a passion for computer science. Her enthusiasm for research has propelled her into the world of academia at a young age. She has actively engaged in research projects, contributing to the advancement of knowledge in her chosen field. She is a young and promising Researcher with a solid educational foundation in computer science. Her current research interests include emerging technologies and their potential impact on society.

MUHAMMAD IRFAN received the Ph.D. degree in electrical and electronic engineering from Universiti Teknologi PETRONAS, Malaysia, in 2016. He has two years of industry experience, from October 2009 to October 2011, and seven years of academic experience in teaching and research. Currently, he is an Associate Professor with the Electrical Engineering Department, Najran University, Saudi Arabia. He has authored several research articles in reputed journals, books, and conference proceedings (Google Scholar Citations 3100, H-index 25). His main research interests include automation and process control, condition monitoring, vibration analysis, artificial intelligence, the Internet of Things (IoT), big data analytics, smart cities, and smart healthcare.

TURKI ALSUWIAN received the B.S. degree in electrical and electronics engineering from King Saud University, Riyadh, Saudi Arabia, in 2004, the M.S. degree from WGannon University, USA, in 2011, and the Ph.D. degree from the University of Dayton, OH, USA. He is currently an Assistant Professor with the Electrical Engineering Department, Najran University Saudi Arabia. His research interests include control systems, automation and process control, and smart grids.