Cyber Threat Defense in Power Grids: Introducing the Grid-Lock Secure-Chain Consensus Framework

Rashi Saxena
Department of Computer science and Engineering, Koneru Lakshmaiah Education Foundation (KLEF), India
scholar.rashisaxena213@gmail.com

Lalitha Kumari
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (KLEF), India
plalithasuryakumari12@gmail.com

Abstract: *Blockchain technology has attracted the curiosity of experts in a variety of sectors, including its potential for Smart Grid (SG) cybersecurity. The study investigates vulnerabilities in smart Direct Current-MicroGrid (DC-MG) systems, particularly community identity servers, which pose a threat to the grid due to the increasing sophistication of existing cybersecurity frameworks, causing delays in real-time activities. The research proposes a novel, grid-lock secure-chain consensus framework to address these issues and improve contemporary power systems' capacity to defend themselves against cyberattacks. This design makes use of Proof of Vote (PoV), a consensus technique that enables decentralized voting across the network's meter nodes to reach consensus. For safe identification and transaction validation, every meter node has public and private keys. All information is encrypted before being transmitted to other nodes. The information is kept on a distributed ledger, where the Secure Hash Algorithm (SHA-256) hash technique is used to cryptographically connect each block. Only legitimate blocks are added to the blockchain due to the PoV process, which also maintains separate voting and accounting rights for security. The proposed design increases encryption techniques and decentralizes permission to lessen the possibility of cyberattacks without compromising system performance. The proposed framework achieves a significant improvement, with throughput increased by 53% and latency reduced by 19% compared to conventional consensus mechanisms such as Practical Byzantine Fault Tolerance (PBFT) and Proof of Work (PoW). Specifically, the framework demonstrates a throughput of 150 Transactions per second (Tx/s) and a latency of 0.89 seconds, outperforming PBFT's throughput of 98 Tx/s and latency of 11 seconds, and PoW's throughput of 120 Tx/s and latency of 1 second. This method represents a major leap in employing blockchain technology for current power system security as it not only strengthens the grid against assaults but also maximizes its resilience and operational efficiency. In particular, results obtained from testing on 118-bus topology setups demonstrate high throughput and low latency, confirming the framework's suitability for SG networks under high transaction volumes and potential cyber threats.*

Keywords: *Blockchain, cyber threats, proof of vote, smart grid, security, consensus mechanism.*

Received September 11, 2024; accepted April 15, 2025
https://doi.org/10.34028/iajit/22/4/1

1. Introduction

Modern technologies were combined with traditional electrical structures to produce a Smart Grid (SG). There are several methods by which an SG can control power and activities [13]. A selection of operational and energy measures include Smart Meters (SM) and appliances deployed at the client's site, a production meter, renewable energy generators, smart inverters, and energy-efficient resources positioned at the grid's location [26]. When gathering information about the production, transmission, and distribution of electricity, SG typically makes use of the Supervisory Control and Data Acquisition (SCADA) system [33]. SM installed on the user's side gather real-time power consumption data, which is then sent over the Wireless Sensor Network (WSN). The SCADA system assists in enhancing the SG's dependability and promptly troubleshooting power outages to prevent severe disruptions in power [10]. Though these technologies have made life easier, their use has also increased the risk of compromising safety. On the one hand, a lot of SG components like SM must communicate with the network often because they are deployed in unsupervised environments [30]. For data exchange, they typically use open WSNs, which make them susceptible to cyberattacks and malicious hardware damage. Common cyberattacks include attacks that cause a denial of service or false information injection [31]. The latter attempts to fabricate data to avoid detection by the electric power departments to commit power theft, while the former attempts to block or even interrupt the regular communication of the SG [37].

Furthermore, in the event of extensive failures or shortages of electricity, SGs powered by IoT technology adopt backup strategies like solar-powered SG control. Energy consumers have benefited greatly from IoT-enabled SGs, but they also come with several security and privacy risks [27]. An IoT-enabled SG, comprising both homogeneous and heterogeneous smart devices,

networks, and applications, exposes information from sensors conveyed across an unsecured communication channel to various privacy and security risks [7]. In such an environment, data exchanged amongst legitimate entities is vulnerable to Man-in-the-Middle (MitM) assaults, compromising its transparency and secrecy [21]. The protection of security features from cyberattacks also depends on the SG's availability. The Distributed Denial of Service (DDoS) attack is a well-known cyberattack that jeopardizes the availability of SG services [2]. Since an IoT-enabled SG necessitates all smart things to confirm their legitimacy and make sure that smart devices can be trusted for transmitting and receiving information among such entities, confirming the legitimacy of devices that sense is crucial to preventing cyberattacks in such associated surroundings [4]. Therefore, adequate security measures are essential to ensure the safe and dependable functioning of a SG in addition to the security of such private information. Any attempt at hacking a SG network has to be prohibited by a system of defense [5].

Security and privacy-protection systems are among the many fields that now make extensive use of machine-learning algorithms. In machine learning, a model is trained by feeding it features data that has predetermined labels [18]. Based on the feature data it is given, a model that has been constructed and trained can forecast labels. While there are many machine learning techniques, the most recent method is called "deep learning," or the use of neural networks. Decision trees, support vector machines, and reinforcement learning are some more [3]. During the past several years, businesses using SG systems have started analyzing electricity data using machine learning and deep learning models, fuzzy logic, Artificial Neural Networks (ANN), and genetic algorithms to improve the accuracy of determining the precise demand for electricity [9]. These algorithms are also used by industries for energy consumption forecasts and energy efficiency planning. Nonetheless, concerns about privacy and security in the SG have received less attention [11]. To fully benefit from SG technology, numerous concerns need to be explored. A SG's vulnerability to different risks, including several more like malicious data injection, denial-of-service attacks, and data theft, makes it difficult to ensure security and privacy [12, 17]. However, guarantees must be made that appropriate measures are put in place to preserve the enormous amount of data that flows via a SG. The power network can be made more resistant to cyberattacks by utilizing efficient approaches based on artificial intelligence, signal processing, neural networks, deep learning, and blockchain-based techniques for cyberattack detection. This will also increase the stability of Cyber-Physical Systems (CPS) [34].

The evolution of blockchain technology has recently aided in the advancement of research across several fields and offers encouraging responses to the issues mentioned above [6]. Peers can interact and transact on the blockchain without the requirement for a centralized authority because it is a Peer-to-Peer (P2P) network. Any attempt to alter or manipulate data will be discovered because blockchain transactions are traceable and immutable [40]. It has also been utilized to build power trading mechanisms due to its capacity to greatly increase trading security [35]. For monitoring and controlling DERs in SG, blockchain technology provides a dependable, robust, and secure information exchange architecture [14]. Furthermore, a variety of cryptographic techniques, including hash functions and symmetric and asymmetric encryption techniques, guarantee data integrity and confidentiality by preventing unwanted access to IoT-enabled SG data [19]. Blockchain can significantly improve interoperability and dependability in such networked systems while also enhancing the privacy and security of data exchange in IoT-enabled SGs. Since smart objects in IoT-enabled SG systems communicate with one another over open and unsecured channels, an adversary may take advantage of weaknesses and breach data privacy in such a networked environment [29]. In IoT-enabled SG networks, sharing of information security and privacy are provided via blockchain-based authentication and key agreements, mitigating these grave risks. Authorized devices must establish key agreements to generate secret keys, but linked devices may authenticate each other using their unique secret credentials due to blockchain-based authentication [22].

Smart contracts in more modern blockchain implementations, like Ethereum, also make trustworthy calculations possible. Smart contracts, for instance, may be used to transfer assets between peers and enforce agreements [8]. The blockchain network's consensus methods offer enhanced security and more efficient functioning. Key components from several consensus methods incorporate one another to generate hybrid consensus methods. This might be helpful in preventing 51% of assaults and double-spending [36]. Several unresolved issues with consensus algorithms must be resolved before blockchain technology is widely used in practical applications [1]. Scalability is a major issue as consensus processes need to process a large number of Transactions per second (Tx/s) in an efficient manner while maintaining decentralization and security [23]. Another significant concern is energy efficiency, particularly in Proof of Work (PoW) circumstances where excessive energy use is unsustainable and expensive over time. For real-world applications, creating new consensus algorithms that are more energy-efficient or enhancing current ones is essential [32]. Encouraging real-time apps to meet their expectations also presents the problem of ensuring quick transaction confirmation times. Blockchain technology's utility might be hampered by lengthy confirmation periods, therefore latency and transaction confirmation must be optimized [15]. Cyberattacks targeting SGs have become a significant concern as these systems

increasingly rely on interconnected devices and networks. One notable example is MiTM attacks, where cybercriminals intercept communication between devices to manipulate data or disrupt services. These attacks can compromise the confidentiality and integrity of the data exchanged within the grid. Another common threat is DDoS attacks, where attackers overwhelm the network with excessive traffic, rendering critical grid services unavailable. Additionally, malicious data injection attacks can manipulate sensor data, leading to incorrect system operations, while ransomware attacks may target control systems, demanding payments to restore access. These cyberattacks highlight the need for enhanced security measures, including blockchain-based solutions and machine learning algorithms, to safeguard SGs from such vulnerabilities. Consensus systems need to withstand assaults like double-spending, Sybil, and 51% attacks, since security remains a constant issue. Improving security protocols is essential to fostering confidence and achieving broad acceptance.

The main contribution of the article is enumerated as

- The objective of this article is to tackle the growing intricacy of cyberattacks that target SG systems, which are becoming a vital component of contemporary infrastructure. Particularly in real-time operations, existing cybersecurity frameworks can cause delays and risks. The study overcomes the shortcomings in existing frameworks by putting forth a decentralized, blockchain-based solution that fortifies grid defenses and improves operational efficiency.
- The grid-lock secure-chain consensus framework, a major development in utilizing blockchain technology for SG security, is introduced in the research.
- Because it blends secure transaction validation with decentralized voting, the Proof of Vote (PoV) consensus mechanism is very unique in its application, offering a special method of power system protection.
- This framework provides a scalable solution that is adaptable to other power system designs, in addition to addressing the unique vulnerabilities found in smart Direct Current-MicroGrid (DC-MG) systems. The framework is an innovative addition to the field of SG cybersecurity since it incorporates Secure Hash Algorithm (SHA-256) for secure data connecting, which further strengthens its resilience.

The rest of the article is structured as follows: The associated blockchain technology works for cyber risks are covered in section 2. The consensus-based mechanism with vote proof is presented in section 3. The efficiency of the suggested method is presented and shown using a simulation for an IEEE 118-bus system in section 4. The article is finally concluded in section 5.

2. Literature Survey

Ghiasi *et al*. [16] used the Hilbert-Huang transform methodology and blockchain-based ledger technology can retrieve the signal information and evaluate the voltage and current signals in smart sensors and controllers, thereby improving the security in smart DC-MGs and detecting False Data Injection Attacks (FDIAs). Because it depends on cosine similarity, the community identification server in a smart DC-MG system could be problematic. This might result in erroneous community detection, jeopardizing system stability and dependability in the event of a cyberattack.

Zhong *et al*. [39] offered a novel distributed Authentication and Authorization (A&A) protocol for SG networks based on blockchain technology to mitigate these threats. The proposed protocol integrates a distinct blockchain methodology with the immutable ledger and decentralized authentication features of blockchain architectures suitable for power systems that offer SG systems resource permission and identity authentication. Deliberate about the security and threat models of earlier A&A protocols, then show that the protocol fends off these attacks. It provides a strategy for an actual A&A protocol deployment utilizing the Financial Blockchain Shenzhen Consortium (FISCO) consortium platform and smart contract system algorithms. By incorporating blockchain technology, decentralized authorization, and sophisticated encryption into SG systems, real-time processes may become slower and system efficiency may be impacted by an increase in computing complexity and resource consumption.

Jha *et al*. [20] suggested a blockchain-based synchrophasor communication solution that protects the integrity and security of synchrophasor data. This study proposed a system for a blockchain-based synchrophasor communication system. The suggested structure's goal is to enhance synchrophasor measurement security and integrity. Moreover, the design leverages the resilience of a distributed, decentralized, hierarchical Phasor Data Concentrator (PDC) design by being created as a P2P distributed blockchain network. Moreover, mining time diminishes as the quantity of miners increases. However, because the consensus mechanism depends on the difficulty level, a trade-off exists between mining time and many miners.

Mahmud *et al*. [25] suggested a consensus-based distributed control approach for Distributed Energy Resources (DERs) that makes use of blockchain as a safe medium to exchange information channels for cyber resilience. To accomplish the global control objectives-wherein each DER connects to a local blockchain server powered by distributed ledger technology. This includes precise power sharing among the DERs as well as collective grid-forming capacity. This enables adjacent assets to securely share local measurements. Lyapunov function-based stability analysis is used to demonstrate

that when communication latency varies due to blockchain, distributed control can keep the system stable. Consensus-based control of blockchains may result in delays and computational costs, which might impair system resilience against cyberattacks and generate slower reaction times and inefficiencies.

Liu *et al*. [24] presented a secure energy trading solution for the SG based on blockchain and wireless networks. The power data gathered by the wireless network and stored on the blockchain might be used by the smart contract to make rational trading choices. The dual-chain architecture consisting of local energy trade blockchain and renewable energy trading blockchain enhances the effectiveness of power trading and renewable energy consumption. Create a blockchain-enabled renewable energy incentive system to raise the stability and size of renewable energy providers. A blockchain-enabled energy trading system that incorporates renewable energy sources and electric vehicles may see an increase in network complexity and transaction volume, which could lower the system's responsiveness and efficiency and possibly cause delays in transactions and challenges with real-time energy management.

Moniruzzaman *et al*. [28] suggested a unique method that encourages users to optimize their profit and safely transfer energy by fusing blockchain technology with cooperative game theory. With the help of the technology, customers may trade and save green energy credits on the blockchain as assets. Additionally, distribution line loss is a consensus method amongst blockchain energy trading participants to create an amended form of Proof of Energy Generation (PoEG). Next, to identify the victorious coalition as block miners, provide a coalition construction method based on the PoEG protocol and optimization approach. However, there might be negative effects as well, such as a possible mismatch between profit maximization and energy efficiency and higher processing requirements, which could lessen the system's ability to encourage the adoption of renewable energy sources.

Yapa *et al*. [38] presented a new Blockchain-as-a-Service for Energy Trading (BaaSET) platform for SG applications that provides reputation-based services via smart contracts. Smart contracts installed on a blockchain enable the autonomous execution of reputation-based grid actions. Grid measurements yield power quality and reliability indices, which are used to determine reputation. The accuracy of AI and ML decisions may be impacted by a decrease in latency on the BaaSET platform as nodes merge. Affordability and scalability are essential for drawing in stakeholders. The consensus algorithm is impacted by latency, which is mostly determined by the block generation time.

As a result, the conventional technique faces difficulties as cosine similarity may be a challenge for the community identification server in a smart DC-MG system, leading to the possibility of cyberattack vulnerabilities and mistaken detection. Due to increasing computer complexity and resource consumption, blockchain technology, decentralized authorization, and encryption may slow down real-time activities and affect system performance. More miners might result in a reduction in mining time, however, consensus procedures might trade off difficulty levels. Blockchains that use consensus-based control may have delays and computational expenses, which would reduce the system's ability to withstand cyberattacks. An energy trading system with blockchain capabilities may complicate the network and increase transaction volume, which might lead to delays and difficulties in real-time energy management. Latency may influence the expense and scalability of AI and ML choices. Hence there is a need to develop a novel blockchain-based framework to detect the cyber threats in SG.

3. Proposed Methodology

The cyber security of advanced power systems is gaining traction in research and industries, leading to the development of detection and protection mechanisms for cyber-attacks. The previously proposed frameworks face the issues of the community identification server in a smart DC-MG system, leading to the possibility of cyberattack vulnerabilities and mistaken detection. Due to increasing computer complexity and resource consumption, blockchain technology, decentralized authorization, and encryption may slow down real-time activities and affect system performance. More miners might result in a reduction in mining time, however, consensus procedures might trade off difficulty levels. In this research, a novel, grid-lock secure-chain consensus framework is proposed to improve modern power systems' self-defense capabilities against cyber-attacks. Every network meter node has a public and private key assigned to it, which are used to validate a node's identification and actions. Before being sent to other nodes, the information gathered by every node needs to be encrypted. Each metering node stores the following vital data: the private key of that node, the public keys of all other nodes, preset consensus, and collected blocks. All acquired data in the proposed framework is recorded in a ledger in the arrangement of linked units that spread across the storage space of each meter. The distributed blockchain network's recorded information is cryptographically connected block by block, with transmitted data including encryption and signatures. To address the challenge of condensing encryption in the current block, the SHA-256 hash algorithm is employed. The verification outcome is then put to a vote using the address-based distributed voting process, guaranteeing that only legitimate blocks are added to the blockchain. This approach ensures that the current block is only permitted if sufficient nodes concur on the nonce value, and cryptographically link to the prior ledger. A new consensus technique, PoV, is proposed, allowing

distributed nodes owned by Meter nodes to obtain consensus and engage in decentralized arbitration through voting. PoV distinguishes between voting and accounting privileges while maintaining distinct security identities for meter nodes. Members of the core consortium vote to select which PoV blocks are generated and verified. Each meter-private node's key is used to encrypt its message digest, resulting in a signature that can be decrypted using its public key. Subsequently, the information is transmitted to every other meter node via the exchange of information network. When broadcast data is received, all meter nodes need to decode it and verify the information. Consequently, the proposed blockchain technology may boost the reliability and safety of the electricity system by using meters as nodes in a distributed system that encodes meter data into blocks. Figure 1 depicts the block diagram of the proposed work shown below. The blockchain network will be discussed below.

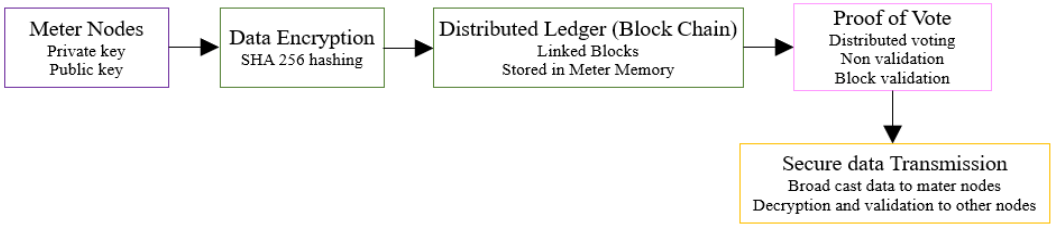

Figure 1. Block schematic illustrating the proposed approach.

3.1. Blockchain Network

Blockchain is the name of a technology that uses an ever-growing collection of data structures called blocks. Cryptography is utilized to connect and secure these blocks, ensuring their integrity and security. The technology, which depends on an extremely complex encryption system, allows for secure data transmission. Similar to a business ledger, it keeps meticulous records of each P2P record and carefully documents every transaction. Every block has a timestamp, transaction information, and information about when it was created. It is also connected to the block before it. Once the data is approved by the network, it cannot be altered. Blockchain technology is intended to prevent data manipulation and fraud. Every transaction is kept in a block, which is subsequently joined together to form a chain. Each block has important information that is displayed in Figure 2. This data consists of the current block value, transaction time of execution, previous block address, random number (nonce), and current block header. The block structure serves as the primary storage for the quantity and specifics of the collected data. Furthermore, data saved on the Blockchain is always available and permanent. The acquired data is protected and rendered unreplicable through the use of digital signatures in the shape of Merkle trees. Because the received data is processed by the Merkle-tree hash function, the Merkle-root value remains distinctive within blocks.

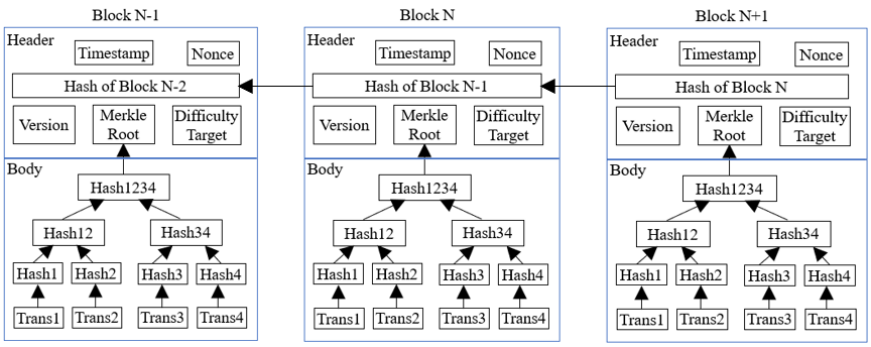

Figure 2. Blockchain structure and Merkle hash tree.

The information contained in each block varies based on the type of blockchain. Every block is uniquely identified by its hash code, which functions as a fingerprint. This hash code is updated whenever block material is modified. The previous block's hash, which acts as its identifier, also plays a role in creating the chain as a whole. Because every change made to one block affects the consistency of the following blocks, the Blockchain is both interconnected and impervious to tampering. Take into consideration blockchain technology as a distinct kind of ledger technology. It records transactional data and works similarly to a digital notepad. This notebook is organized as a series of blocks that get longer as more entries are made. Every time new data is added, a new block is created. Every new block that is inserted is connected to the previous ones via unique codes. This creates a secure, unchangeable record in the Blockchain. Consider the first block as the link at the start of a chain, and the subsequent information-containing blocks as the links. Any effort to alter the

information in the second block will cause connections with the third and subsequent blocks to break. This happens because each block is linked together by a unique code called a hash. Modifications to a block's contents affect its hash, making it incompatible with blocks that come after it. Thus, once data is written, the architecture of the Blockchain helps guarantee that it cannot be easily changed by anybody. A consensus algorithm is one of the algorithms used by blockchain technology. This research introduces PoV, a novel consensus method that enables distributed nodes owned by Meter nodes to reach a consensus and participate in voting-based decentralized arbitration. PoV maintains the core idea that meter nodes should have unique security identities while making a distinction between voting and accounting privileges. The results of votes among core consortium members determine the generation and verification of PoV blocks, in contrast to uncontrollably high public awareness or third-party intermediaries.

A popular cryptographic method known as Secure Hashing Technique 256, or SHA-256, generates a 32-byte, fixed-length 256-bit hash result. The objective of the SHA-256 algorithm create a distinct digital fingerprint for each piece of data like a file or message. A complex mathematical method that yields a distinct output value is applied to the input data to generate a SHA-256 hash. The hash serves as both an output value and a digital fingerprint of the input information. Digital signatures, password authentication, and blockchain technology are among the uses of the SHA-256 algorithm. Technique for Secure Hashing any text may be transformed using the cryptographic hash method SHA-256 into a distinct 256-bit alphanumeric string that is known as a hash or hash value. One important characteristic of hash functions is collision resistance, which is the impossibility of obtaining the same hash output from two distinct inputs. The goal of SHA-256 is to prevent collisions.

3.2. Consensus Mechanism Based on Proof of Vote (PoV)

In the proposed approach, a new consensus technique is termed PoV, in which distributed nodes owned by meter nodes can obtain consensus and engage in decentralized arbitration through voting. PoV distinguishes between voting and accounting privileges while retaining the fundamental principle of having specific security identifies for meter nodes. Unlike the outcomes of votes between core consortium members decide the generation and validation of PoV blocks, regardless of the involvement of third parties or uncontrollably high awareness among the public.

In the PoV mechanism, commissioners are selected based on their previous performance and reputation within the system. Each node's performance is monitored to ensure that only reliable nodes are chosen as commissioners. The selection process involves a reputation-based algorithm where nodes with a history of accurate block generation and validation are prioritized.

In the proposed PoV algorithm, the consensus procedure consists of several commissioners signified as $N(C)$. $N(B)$ denotes the number of butlers, $N(BC)$ represents the number of butler candidates, and $N(OU)$ represents the number of ordinary users. Meanwhile, a node also has several identities, $N(All)$ represents the number of all roles, and fulfils

$$N(All) = \leq N(C) + N(B) + N(BC) + N(OU) \quad (1)$$

Which is considered constant. Let us assume every butler has an integer between zero and zero. $N(B\text{-}1)$. If $N(BC)<N(B)$ then, all the terms are considered insufficient for bulter candidates. The system function is designed correctly when the butlers are assigned multiple numbers. Let us assume the $N(B)=8$ and $N(BC)=6$, the butlers were represented by integers 0 through 7 in the framework.

$$\{B(1), B(2), B(3), B(4), B(5), B(6), B(1), B(2)\} \quad (2)$$

The two butlers who have received the most votes get two butler numbers are regarded as being the butler $B(1)$ and $B(2)$. Valid blocks are created if the butler's tenure is for each tenure. The election outcome for the butler and other relevant details are included in the final specialized block. The valid block is considered when the block at least collects $\left[\frac{N(C)}{2}\right] + 1$ signatures from various commissioners. A servant must create a legal block in the fixed period, the packing cycle. The voting process in PoV follows a predefined set of rules. Each commissioner casts a vote for a butler candidate based on their judgment of the candidate's legitimacy and capabilities. The voting power of each commissioner may vary depending on their previous contributions to the network. This weighted voting ensures that well-established nodes with proven reliability have a greater influence on the consensus process. Figure 3 represents the consensus model of one tenure cycle.

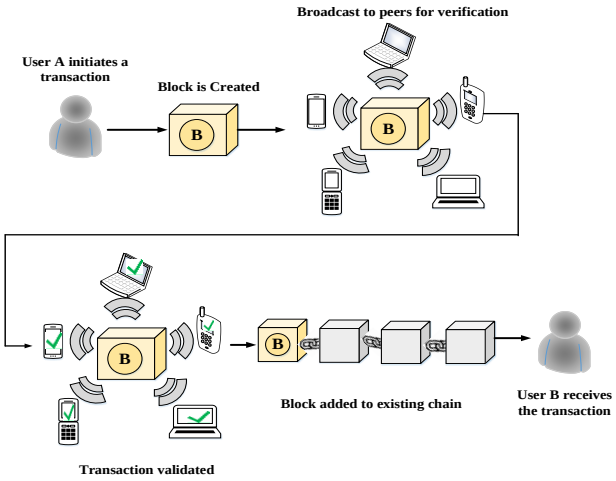

Figure 3. Model of consensus for a single tenure cycle.

A process of agreement denotes the generation of a legitimate block by a servant. Which rounds of agreement generated a legitimate block tenure cycle $B(w+1)$. A random number like R, $0 \leq R \leq N(B)$.

Then, in the subsequent round of unanimity, the servant whose number matches R is tasked with coming up with a block. If no valid block is generated in the $T(B)$ time, the $(R+1)^{th}$ butler will regenerate the block and let it $R=(R+1) MOD\ N(B)$. The network will eventually agree if most single servants perform regularly. The majority of signatures can only be obtained by one block during a packing cycle $T(B)$, every legal block has a conclusion, and the chain won't split. The special block developed throughout the term is expressed as

$$B(w+1)^{th} \tag{3}$$

The present butlers and butler candidates fight in this consensus process to become the following tenure's butlers. The most popular $N(B)$ applicants will ultimately prevail in the selection, each commissioner providing a voting list. The election results and associated data are added to this special area. The fresh valets started working in the fresh term when this special block was made, and present butlers officially resigned at that time. To mitigate potential attacks, the PoV mechanism employs several security measures. For instance, it uses a combination of cryptographic encryption and digital signatures to ensure the authenticity of votes and blocks. Additionally, the decentralized nature of the voting process makes it resistant to Sybil attacks, where an attacker might attempt to falsify votes by creating multiple fake nodes. The system also prevents double-spending by ensuring that each block is validated by a majority of commissioners, making it difficult for malicious actors to manipulate the blockchain.

3.3. Block Creation

A round of consensus might proceed with M packing cycles $T(B)$. If the butler B_i fails to produce a legal block within $T(B)$ the period, the servant will be given the authority to make this block B_{i+1}. The overall period for a round of consensus $T(C)$ is $M \times T(B)$, this indicates that some M-1 invalid blocks have been dropped from this consensus. The actions $M \leq N(B)$ listed below must be taken to create a valid column;

- S_1-represent the connections created by regular users and have their signatures. They simultaneously receive transactions, check their legitimacy, and transmit the successful ones to other commissioners and servants.
- S_2-represents that the butlers keep track of transfers and add legitimate ones to their local pool. The NTP times of each butler and commissioner in the network are synced regularly.

The preceding block is the final valid special block of the tenure if this is the first block of the tenure. If the genesis block is to be generated by this agreement, R defaults to 0. (the initial block of the network).

- S_4-represents the duty butler $B_i(i=R)$ denotes the transaction used for the local pool; this compiles them into a pre-block and distributes it to each commissioner. The cutoff time of this block is represented as $T_{cut}=GetPreviousblockConfirmTime()+M \times T_b$.
- S_5-the commissioners check a pre-legitimacy block after receiving it, but they also approve of the block's construction; they transmit their autograph and the current time stamp back to the butler.
- S_6-the job valet gathers at least $\left[\frac{N(C)}{2}\right]+1$ a few autographs from each commissioner arrange them into a string in ascending order of time-stamp, and then add the string to the pre-header. Next, it evaluates by the following equation;

$$\text{R=Get PreviousblockrandomNum()} \tag{4}$$

To create the final header, add the R-value and the block time that has the highest value in the time-stamp list that the commissioners have returned. The duty butler will revise the pre-header with the necessary signatures if the block time is earlier $T(Cut)$, confirming its job and moving on to S_8.

- S_7-the current block will no longer be valid if the time is over $T(Cut)$. Let us consider

$$R = (R+1) MOD\ N(B) \tag{5}$$

$$\text{and } M = (M+1) \tag{6}$$

then jump to S_4.

- S_8-Butler-Block Reporter (Butler-BR) delivers the final to all commissioners after creating a legitimate block distributed to other nodes. When over 50% of the commissioners acknowledge that they have acquired the legitimate block, the block receives the final approval and is given legal standing in the system.
- S_9-when the assistants and officials acquire a viable block, they take the transfers from their public pool, get the random number R, and start the next consensus phase.

The goal of the last block in a tenure cycle is to take the butler team for the following tenure.

- P_1 the duty butler receives a sequence that the commissioner created from the list of butler applicants and present butlers to construct a vote.
- P_2 votes are collected from all commissioners and placed in a local pool by the commissioners and the present butlers.
- P_3 the duty butler determines if the total number of votes cast surpasses half of the commissioner's total. If yes, carry out $P_4 - P_8$ to create a new special block; else, hold off on substituting the duty of the butler

until an expiration time happens.

- P_4-P_8 like S_4-S_8 of the regular block generation, the special block requires commissioner signatures before agreeing. Voting transactions are present in the special block but not regular data transactions, which is how it differs from the usual block. The election will be won by the topNb nodes, who will then take over as the new butlers for the upcoming term.
- P_9 the butlers of the present term are released from their duties and the pertinent voting transactions are deleted from the resident pool following the creation of the special block.

With a height of zero, the consortium blockchain's genesis block is its most distinctive feature. It contains the information from the first batch of butler nodes and the initial consortium nodes, which establishes the framework for later blocks. Its generation process is as follows:

- T_4: to confirm online, the consortium's primary commissioner nodes exchange messages with one another. Every node possesses an address hash. The genesis block is created by the member acting as a proxy commissioner who has the lowest hash value.

T_2: the updating transaction is forwarded to the proxy commissioner by the primary commissioner.

- T_3: the commissioners who wish to run for butler positions also submit identity change requests. The commissioners received these transactions and added them to their local pool.
- T_4: from their local pool of candidate addresses, the commissioner chooses at least K butler addresses. These addresses are serialized into a vote, signed by the commissioner, and sent to the proxy commissioner.
- T_5: a pre-block is created by the proxy commissioner by integrating all of the transactions and distributing it to each commissioner after calculating the voting data. The genesis block can be released once the proxy commissioner has received the pre-block signatures from every commissioner (this step verifies that every commissioner can interact with every other commissioner, indicating the establishment of the consortium blockchain network). This procedure is comparable to S_4-S_8 for creating a regular block.
- T_4: following the receipt of the genesis block by each commissioner, the unconfirmed transactions in the local pool are deleted.

3.4. Producing a Random Number

The next duty butler is chosen at random by each block, which generates a random number. The following is the algorithm used to generate random numbers: Let us assume that the duty butler has obtained the signatures and timestamps from K commissioners, denoted by ⟨*C-time*(*i*), *C-sign*(*i*)⟩ ($0 \leq i < K$, $\left\lceil \frac{N(C)}{2} \right\rceil < K \leq N(c)$). After that, they will be arranged by the on-duty butler in ascending order of *C-time*, so the largest is *C-time*(*K*-1). Calculate R_{sor}=*C-time*(*K*-1)⊕*C-Sign*(*K*-1). Indicate that *R* is the function that takes the final 32 bits of the string and stores it as *SubStringEnd*32 (*string*) using Equation (7).

$$R = StrToInt\left(SubstringEnd32\left(Hash(R_{sor})\right)\right) mod\ N_b \quad (7)$$

Because each block header's value is random, it can produce a variable R_{sor} and a random number *R*, eliminating the chance that butlers will band together to increase revenue by manipulating R- elements displayed up in a particular sequence.

3.5. Procedure for Voting

Two different types of votes are used in the consensus mechanism to represent the concept of PoV. The first is the butler team vote, and the other is voting for block production. The commissioners cast their votes by signing back.

The PoV on blocks is processed by generating the blocks with B_i a butler and transmitting it to all commissioners. If the commissioner is satisfied with generating the block, the signature and time stamp are returned to the butler B_i after the block header and time stamp have been encrypted. Suppose the butler B_i receives at least $\left\lceil \frac{N(C)}{2} \right\rceil + 1$ signatures during the period specified to a valid block. If not, the block and the butler are invalid B_{i+1}.

When the commissioners reach a final accord throughout the term, they send the signed voting transactions to the duty butler B_i. It creates a special block with the election results and associated documents after gathering and calculating the votes. The block will then be sent to all commissioners for verification by butler B_i.

The voting data for the commissioners consists of two different types of tickets combined:

1. Score tickets: a list of the butler candidates' scores is kept by each commissioner, who then chooses a sequence of candidates with the highest scores.
2. Designated tickets: to improve the butler's mobility, the commissioner either randomly selects candidates or selects a specific group of candidates while taking human factors into account.

PoV can considerably reduce blockchain transaction authentication delays guaranteeing algorithm precision, and enhancing the consortium blockchain's performance. This is dependent on the reliable attributes of the nodes in the consortium and the right consensus decision. Under the right parameter settings, PoV can guarantee that the butlers produce valid blocks consistently and without interruption. The system can always respond to a user's operation request in a finite amount of time.

4. Result and Discussion

The outcome, performance analysis, comparison and discussion section examines the efficiency of the proposed approach. Utilizing a consensus based on PoV, the proposed approach created a practical smart contract and tested it on the Ethereum network. In the experiment, key network configurations were varied, including the number of nodes, transaction volumes (high, moderate, and low), and consensus mechanisms such as the grid-lock secure-chain, Practical Byzantine Fault Tolerance (PBFT), and PoW. Each configuration was tested across a minimum of 10 independent trials to ensure reliability and minimize the effects of random fluctuations. Essential performance metrics, including throughput Tx/s and latency (in seconds), were tracked throughout the experiment. To assess the consistency and variability of the results, the mean, Standard Deviation (SD), and 95% Confidence Intervals (CI) for each metric were calculated.

4.1. Experimental Setup

The proposed approach's setup includes 16GB of RAM, a 64-bit operating system, and an Intel Core i5-6200U processor. The design of the system satisfies the requirements of consensus-based operations, guaranteeing the efficient execution and verification of transactions in the context of the blockchain. Blockchain has the potential to significantly reduce vulnerabilities found in traditional SCADA systems, as demonstrated by the empirical evaluation conducted across IEEE 118-bus topologies. This work uses the IEEE 118 bus method against cyber-attacks in SG network systems. Transmission lines, generators, loads, and capacitor banks make up the system. Deploying a meter in each node collects analogue information like current, voltage, power stream, etc. Every branch set up a breaker to gather digital data to find the line's status, whether opened or closed. Two meters are installed on the corners of every line by every branch to collect analogue data such as the power flows, voltage, current, etc. Figure 4 shows the illustration of the IEEE 118 bus system.

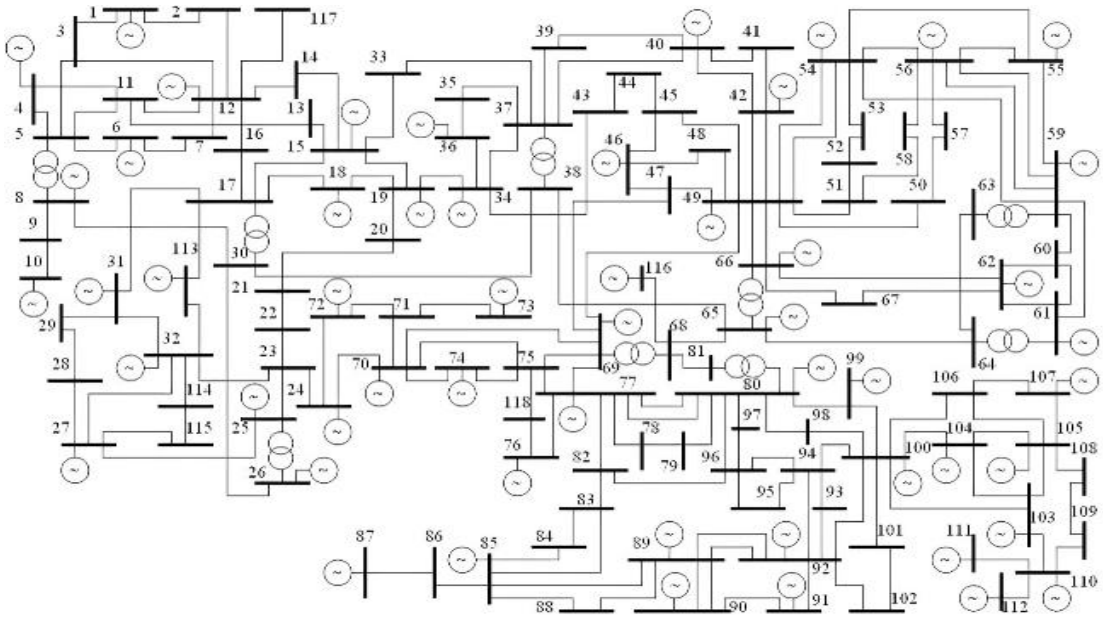

Figure 4. IEEE 118 bus system.

4.2. Performance Analysis

To assess the effectiveness of the IEEE 118 bus systems, the PoV consensus method in the proposed blockchain architecture is chosen. The time it takes to mine a block successfully is chosen as the performance indicator to assess the BC architecture's performance for demonstration purposes. Figure 5 illustrates the performance of the proposed blockchain design for IEEE 118 bus systems.

The time needed to mine each blockchain block using a PoV consensus process is shown in Figure 5. At the beginning of the blockchain, the first four blocks (numbered 1 through 4) are virtually entirely mined in the same amount of time, demonstrating effective consensus with no computing cost. A progressive increase in mining time is noted with an increasing block number; this increase appears to be greatest between blocks 5 and 8, which is indicative of the growing difficulty of reaching agreement as additional blocks are added. Beginning with block 9, there is a noticeable rise in mining time. Block 9 takes about 57 milliseconds, and by block 12, the time has increased significantly to roughly 1091 milliseconds. Due to the cumulative impacts of a bigger blockchain, which demands more votes and computing work to maintain consensus, there has been a significant increase in mining time. As the blockchain grows, the figure illustrates the PoV mechanism's ability to balance security and efficiency

by requiring more processing power to ensure that only legitimate blocks are added to the chain.

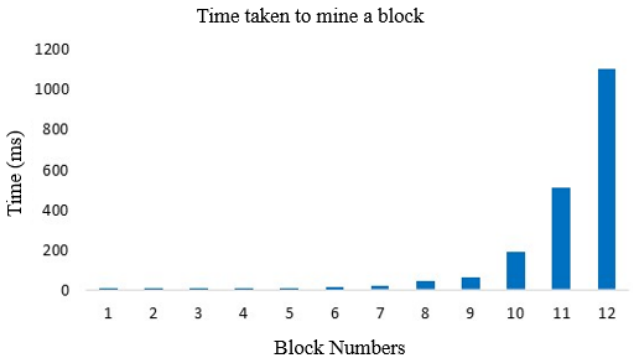

Figure 5. Time taken performance for IEEE 118 bus systems.

Specifically applied to the IEEE 118 bus system, Figure 6 shows the throughput performance in a blockchain network employing a PoV consensus process. At first, the throughput increases gradually as the number of relay Tx/s increases from 0 to 100, peaking at about 80 TPS at 50 relay Tx/s . This indicates that the PoV method, which preserves a linear connection between relay transactions and throughput, can effectively manage growing transaction loads within the IEEE 118 bus system. The throughput increases more quickly between 100 and 150 relay Tx/s , reaching about 130 TPS at 150 relay Tx/s . This shows that the PoV method is successfully maintaining consensus, and the system is scaling well under increased transaction volumes. Nevertheless, the throughput reaches a level at around 160 TPS when the number of relay Tx/s approaches 200.

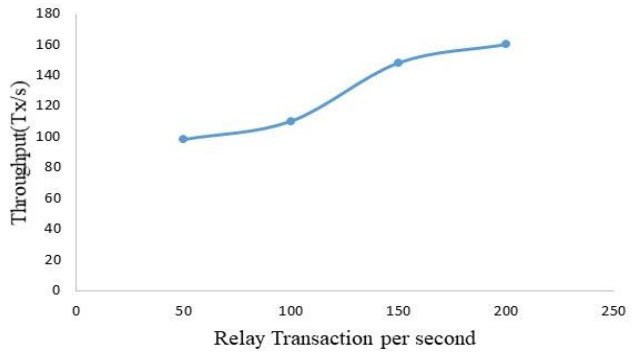

Figure 6. Throughput performance for IEEE 118 bus systems.

A graph of latency performance for IEEE 118 bus systems is shown in Figure 7, which is offered. The graph shows an increasing trend, indicating that latency rises as the number of relay Tx/s rises. In particular, latency decreases to about 0.2 seconds at low transaction rates from 0.91 seconds when the transaction rate gets closer to 200 per second. The effectiveness of the blockchain-based consensus mechanism, more especially the proof-of-vote technique, is responsible for this latency performance. The network in these systems grows more efficient at processing and reaching consensus as the quantity of relay transactions rises, maximizing total latency. By facilitating quicker consensus among nodes, the PoV technique probably improves the network's scalability and responsiveness. Because of this, the system performs better in terms of latency as it processes more Tx/s.

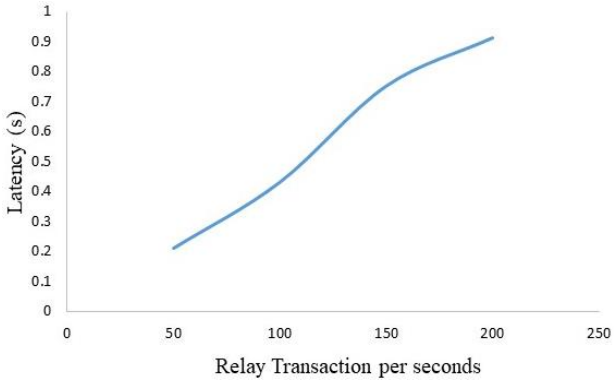

Figure 7. Latency performance for IEEE 118 bus systems.

To ensure statistical rigor, t-tests and ANalysis Of VAriance (ANOVA) were conducted to determine if the performance differences between the grid-lock secure-chain and the traditional consensus mechanisms PBFT and PoW were statistically significant. The results of the t-tests indicated that the grid-lock secure-chain outperformed PBFT with a 53% increase in throughput and showed a 25% higher throughput than PoW. Additionally, the grid-lock secure-chain reduced latency by 19% compared to PBFT and improved it by 11% over PoW. These performance improvements were confirmed to be statistically significant, with p-values falling below the conventional threshold, ensuring that the observed enhancements were not due to random variation.

Furthermore, the consistent improvements in throughput and latency observed under various conditions reinforced the reliability of the grid-lock secure-chain framework. By employing multiple experimental runs, calculating statistical metrics (mean, SD, 95% CI), and conducting significance testing (t-tests, ANOVA), it was demonstrated that the observed improvements in performance were both statistically significant and indicative of a genuine enhancement in blockchain efficiency, rather than being attributed to chance. Table 1 illustrates the statistical summary of block chain performance.

Table 1. Statistical summary of blockchain performance.

Consensus mechanism	Mean throughput (Tx/s)	Std. Dev. (throughput)	95% Confidence interval (Tx/s)	Mean latency (sec)	Std. Dev. (latency)	95% Confidence interval (latency)
Grid-lock secure-chain	150	5	[148, 152]	0.89	0.1	[0.85, 0.93]
PBFT	98	3	[96, 100]	11	0.5	[10.5, 11.5]
PoW	120	4	[116, 124]	1	0.3	[0.7, 1.3]

4.3. Comparative Analysis

To compare the performance such as throughput and latency of the proposed method with other existing consensus methods such as PBFT and PoW without IEEE bus for given below.

Table 2. Performance comparison of the proposed method with existing method.

Consensus mechanism	Throughput (Tx/s)	Latency(s)
PBFT without IEEE bus	98	11
PoW without IEEE bus	120	1
PoV with IEEE bus	150	0.89

Table 2 compares the effectiveness of two well-known consensus mechanisms such as PBFT and PoW against the proposed PoV consensus mechanism when it is used within the IEEE bus system. Both mechanisms are assessed independently of the IEEE bus system. Throughput, expressed in Tx/s, and delay, expressed in seconds, are the measures taken into consideration. According to the findings, the PoV method outperforms PBFT, which has a throughput of 98 Tx/s and a latency of 11 seconds, and PoW, which has a throughput of 120 Tx/s and a latency of 1 second, by achieving a throughput of 150 Tx/s and a latency of 0.89 seconds. The PoV mechanism's uniqueness and effectiveness are demonstrated by this notable increase in throughput and latency, especially when combined with the IEEE bus system. The PoV can process more transactions than more conventional techniques, as seen by its better throughput of 150 Tx/s. This is important because in a SG setting, maintaining system security and stability depends on rapid data processing. This benefit is further enhanced by the decreased latency of 0.89 seconds, which guarantees almost real-time transaction processing a crucial aspect of timely cyber threat identification and response.

4.4. Discussion

The PoV consensus method is innovative in that it may reconcile low latency and high throughput, therefore mitigating the frequent trade-offs encountered by other consensus systems. Although PBFT offers some fault tolerance, its high latency makes it unsuitable for applications that need fast reaction times. PoW reduces latency but requires a lot of energy and processing resources, which may be expensive in large-scale systems like the IEEE 118 bus network. On the other hand, PoV minimizes both methods' drawbacks while combining their advantages. PoV speeds up transaction processing times by lowering energy and computing costs through the use of a special voting-based consensus architecture. Furthermore, because of its connection with the IEEE bus system, it is more applicable in SG networks, where preventing and detecting cyberattacks is crucial. PoV is a better option for protecting SG infrastructure since it can handle large transaction volumes quickly and effectively, offering an innovative solution to the problems with conventional consensus methods.

5. Conclusions

The grid-lock secure-chain consensus framework, which uses a revolutionary PoV consensus mechanism, provides a big step forward in protecting electricity power networks from intrusions. By facilitating decentralized voting between network meter nodes, this framework improves on the established security measures and guarantees transparent and reliable consensus processes. The system is strengthened against any breaches by the use of public and private keys for every meter node, extensive data encryption, and a distributed ledger protected by the SHA-256 hashing technique. The novel strategy of dividing accounting and voting rights fortifies the security of the system by thwarting illegal changes and guaranteeing the blockchain's integrity. The proposed structure maintains excellent system performance while reducing the danger of cyberattacks by improving encryption methods and decentralizing permissions. The 118-bus topology study shows that the grid-lock secure-chain consensus framework outperforms other approaches in terms of throughput and latency. This attests to its effectiveness in enhancing power systems' operating efficiency and resilience. Overall, this framework offers a revolutionary advancement in the use of blockchain technology to power system security, strengthening the grid's defenses in the process. Subsequent efforts will concentrate on including adaptive algorithms to enhance the grid-lock secure-chain consensus framework's functionality in ever-changing surroundings. Further investigation into the framework's scalability for bigger and more intricate power systems is essential for wider deployment.

References

[1] Abdelmaboud A., Ahmed A., Abaker M., Eisa T., Albasheer H., Ghorashi S., and Karim F., "Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions," *Electronics*, vol. 11, no. 4, pp. 1-35, 2022. https://doi.org/10.3390/electronics11040630

[2] Acarali D., Rao K., Rajarajan M., Chema D., and Ginzburg M., "Modelling Smart Grid IT-OT Dependencies for DDoS Impact Propagation," *Computers and Security*, vol. 112, pp. 102528, 2022. https://doi.org/10.1016/j.cose.2021.102528

[3] Ahmed S., Alam M., Hassan M., Rozbu M., Ishtiak T., Rafa N., and Gandomi A., "Deep Learning Modelling Techniques: Current Progress, Applications, Advantages, and Challenges," *Artificial Intelligence Review*, vol. 56, no. 11, pp. 13521-13617, 2023.

[4] Al-Mousa M., Amer W., Abualhaj M., Albilasi S.,

Nasir O., and Samara, G., "Agile Proactive Cybercrime Evidence Analysis Model for Digital Forensics," *The International Arab Journal of Information Technology*, vol. 22, no. 3, pp. 627-636, 2025. https://doi.org/10.34028/iajit/22/3/15

[5] Amin M., El-Sousy F., Aziz G., Gaber K., and Mohammed O., "CPS Attacks Mitigation Approaches on Power Electronic Systems with Security Challenges for Smart Grid Applications: A Review," *IEEE Access*, vol. 9, pp. 38571-38601, 2021. DOI:10.1109/ACCESS.2021.3063229

[6] Arvindhan M., Thirunavukarasan M., and Daniel A., *Handbook of Green Computing and Blockchain Technologies*, CRC Press, 2021. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003107507-8/blockchain-technology-energy-sector-arvindhan-thirunavukarasan-daniel

[7] Babar M., Tariq M., and Jan M., "Secure and Resilient Demand Side Management Engine Using Machine Learning for IoT-Enabled Smart Grid," *Sustainable Cities and Society*, vol. 62, pp. 102370, 2020. https://doi.org/10.1016/j.scs.2020.102370

[8] Barreto C., Eghtesad T., Eisele S., Laszka A., Dubey A., and Koutsoukos X., "Cyber-Attacks and Mitigation in Blockchain Based transactive Energy Systems," *in Proceedings of the IEEE Conference on Industrial Cyberphysical Systems*, Tampere, pp. 129-136, 2020. DOI:10.1109/ICPS48405.2020.9274708

[9] Bashir A., Khan S., Prabadevi B., Deepa N., Alnumay W., Gadekallu T., and Maddikunta P., "Comparative Analysis of Machine Learning Algorithms for Prediction of Smart Grid Stability," *International Transactions on Electrical Energy Systems*, vol. 31, no. 3, pp. e12706, 2021. https://doi.org/10.1002/2050-7038.12706

[10] Chen X., Shen J., Cao Z., and Dong X., "A Blockchain-based Privacy-Preserving Scheme for Smart Grids," *in Proceedings of the 2nd International Conference on Blockchain Technology*, Hilo, pp. 120-124, 2020. https://doi.org/10.1145/3390566.3391667

[11] Chen Z., Amani A., Yu X., and Jalili M., "Control and Optimisation of Power Grids Using Smart Meter Data: A Review," *Sensors*, vol. 23, no. 4, pp. 1-26, 2023. https://doi.org/10.3390/s23042118

[12] Dileep G., "A Survey on Smart Grid Technologies and Applications," *Renewable Energy*, vol. 146, pp. 2589-2625, 2020. https://doi.org/10.1016/j.renene.2019.08.092

[13] Ding J., Qammar A., Zhang Z., Karim A., and Ning H., "Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions," *Energies*, vol. 15, no. 18, pp. 1-37, 2022. https://doi.org/10.3390/en15186799

[14] Faheem M., Al-Khasawneh M., Khan A., and Madni S., "Cyberattack Patterns in Blockchain-based Communication Networks for Distributed Renewable Energy Systems: A Study on Big Datasets," *Data in Brief*, vol. 53, pp. 110212, 2024. https://doi.org/10.1016/j.dib.2024.110212

[15] Gadekallu T., Pham Q., Nguyen D., Maddikunta P., Deepa N., Prabadevi B., and Hwang W., "Blockchain for Edge of Things: Applications, Opportunities, and Challenges," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 964-988, 2021. DOI:10.1109/JIOT.2021.3119639

[16] Ghiasi M., Dehghani M., Niknam T., Kavousi-Fard A., Siano P., and Alhelou H., "Cyber-Attack Detection and Cyber-Security Enhancement in Smart DC-Microgrid Based on Blockchain Technology and Hilbert Huang Transform," *IEEE Access*, vol. 9, pp. 29429-29440, 2021. DOI:10.1109/ACCESS.2021.3059042

[17] Gunduz M. and Das R., "Cyber-Security on Smart Grid: Threats and Potential Solutions," *Computer Networks*, vol. 169, pp. 107094, 2020. https://doi.org/10.1016/j.comnet.2019.107094

[18] Hasan M., Abdulkadir R., Islam S., Gadekallu T., and Safie N., "A Review on Machine Learning Techniques for Secured Cyber-Physical Systems in Smart Grid Networks," *Energy Reports*, vol. 11, pp. 1268-1290, 2024. https://doi.org/10.1016/j.egyr.2023.12.040

[19] Hasankhani A., Hakimi S., Bisheh-Niasar M., Shafie-Khah M., and Asadolahi H., "Blockchain Technology in the Future Smart Grids: A Comprehensive Review and Frameworks," *International Journal of Electrical Power and Energy Systems*, vol. 129, pp. 106811, 2021. https://doi.org/10.1016/j.ijepes.2021.106811

[20] Jha A., Appasani B., Gupta D., Ainapure B., and Bizon N., "A Blockchain-Enabled Approach for Enhancing Synchrophasor Measurement in Smart Grid 3.0," *Sustainability*, vol. 15, no. 19, pp. 1-20, 2023. https://doi.org/10.3390/su151914451

[21] Kumar P., Kumar R., Aljuhani A., Javeed D., Jolfaei A., and Islam A., "Digital Twin-Driven SDN for Smart Grid: A Deep Learning Integrated Blockchain for Cybersecurity," *Solar Energy*, vol. 263, pp. 111921, 2023. https://doi.org/10.1016/j.solener.2023.111921

[22] Kumari A., Gupta R., and Tanwar S., "Amalgamation of Blockchain and IoT for Smart Cities Underlying 6G Communication: A Comprehensive Review," *Computer Communications*, vol. 172, pp. 102-118, 2021. https://doi.org/10.1016/j.comcom.2021.03.005

[23] Liu C., Zhang X., Chai K., Loo J., and Chen Y., "A Survey on Blockchain-Enabled Smart Grids: Advances, Applications and Challenges," *IET Smart Cities*, vol. 3, no. 2, pp. 56-78, 2021. https://doi.org/10.1049/smc2.12010

[24] Liu Z., Wang D., Wang J., Wang X., and Li H., "A

Blockchain-Enabled Secure Power Trading Mechanism for Smart Grid Employing Wireless Networks," *IEEE Access*, vol. 8, pp. 177745-177756, 2020. DOI:10.1109/ACCESS.2020.3027192

[25] Mahmud R. and Seo G., "Blockchain-Enabled Cyber-Secure Microgrid Control Using Consensus Algorithm," *in Proceedings of the IEEE 22nd Workshop on Control and Modelling of Power Electronics*, Cartagena, pp. 1-7, 2021. DOI:10.1109/COMPEL52922.2021.9645973

[26] Mazhar T., Irfan H., Khan S., Haq I., Ullah I., Iqbal M., and Hamam H., "Analysis of Cyber Security Attacks and their Solutions for the Smart Grid Using Machine Learning and Blockchain Methods," *Future Internet*, vol. 15, no. 2, pp. 1-37, 2023. https://doi.org/10.3390/fi15020083

[27] Mirzaee P., Shojafar M., Cruickshank H., and Tafazolli R., "Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures)," *IEEE Access*, vol. 10, pp. 52922-52954, 2022. DOI:10.1109/ACCESS.2022.3174259

[28] Moniruzzaman M., Yassine A., and Benlamri R., "Blockchain and Cooperative Game Theory for Peer-to-Peer Energy Trading in Smart Grids," *International Journal of Electrical Power and Energy Systems*, vol. 151, pp. 109111, 2023. https://doi.org/10.1016/j.ijepes.2023.109111

[29] Park K., Lee J., Das A., and Park Y., "BPPS: Blockchain-Enabled Privacy-Preserving Scheme for Demand-Response Management in Smart Grid Environments," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 2, pp. 1719-1729, 2022. DOI:10.1109/TDSC.2022.3163138

[30] Prieto Gonzalez L., Fensel A., Gomez Berbis J., Popa A., and De Amescua Seco A., "A Survey on Energy Efficiency in Smart Homes and Smart Grids," *Energies*, vol. 14, no. 21, pp. 1-16, 2021. https://doi.org/10.3390/en14217273

[31] Reda H., Anwar A., Mahmood A., and Tari Z., "A Taxonomy of Cyber Defence Strategies against False Data Attacks in Smart Grids," *ACM Computing Surveys*, vol. 55, no. 14s, pp. 1-37, 2023. https://doi.org/10.1145/3592797

[32] Sapra N., Shaikh I., and Dash A., "Impact of Proof of Work (PoW)-based Blockchain Applications on the Environment: A Systematic Review and Research Agenda," *Journal of Risk and Financial Management*, vol. 16, no. 4, pp. 1-29, 2023. https://doi.org/10.3390/jrfm16040218

[33] Sheng C., Yao Y., Fu Q., and Yang W., "A Cyber-Physical Model for SCADA System and Its Intrusion Detection," *Computer Networks*, vol. 185, pp. 107677, 2021. https://doi.org/10.1016/j.comnet.2020.107677

[34] Singh P., Masud M., Hossain M., and Kaur A., "Blockchain and Homomorphic Encryption-Based Privacy-Preserving Data Aggregation Model in Smart Grid," *Computers and Electrical Engineering*, vol. 93, pp. 107209, 2021. https://doi.org/10.1016/j.compeleceng.2021.107209

[35] Tushar W., Saha T., Yuen C., Smith D., and Poor H., "Peer-to-Peer Trading in Electricity Networks: An Overview," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3185-3200, 2020. DOI:10.1109/TSG.2020.2969657

[36] Venkatesan K. and Rahayu S., "Blockchain Security Enhancement: An Approach Towards Hybrid Consensus Algorithms and Machine Learning Techniques," *Scientific Reports*, vol. 14, no. 1, pp. 1-24, 2024. https://doi.org/10.1038/s41598-024-51578-7

[37] Xia X., Xiao Y., Liang W., and Cui J., "Detection Methods in Smart Meters for Electricity Thefts: A Survey," *Proceedings of the IEEE*, vol. 110, no. 2, pp. 273-319, 2022. DOI:10.1109/JPROC.2021.3139754

[38] Yapa C., De Alwis C., Liyanage M., and Ekanayake J., "Utilization of a Blockchainized Reputation Management Service for Performance Enhancement of Smart Grid 2.0 Applications," *Journal of Industrial Information Integration*, vol. 39, pp. 100580, 2024. https://doi.org/10.1016/j.jii.2024.100580

[39] Zhong Y., Zhou M., Li J., and Chen J., et al., "Distributed Blockchain-based Authentication and Authorization Protocol for Smart Grid," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, pp. 5560621, 2021. https://doi.org/10.1155/2021/5560621

[40] Zhuang P., Zamir T., and Liang H., "Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 3-19, 2020. DOI:10.1109/TII.2020.2998479

Rashi Saxena is currently pursuing her Doctoral Programme at Koneru Lakshmaiah Education Foundation, located in Hyderabad, Telangana. She is working as Assistant Professor in Department of Data Science at Gokaraju Rangaraju Institute of Engineering and Technology, she holds an M. Tech from JVW University, Jaipur, Rajasthan Her field of specialization is Cyber Security, Blockchain Artificial Intelligence and Machine Learning. She has published 12 articles in reputed peer-reviewed national and international journals and 2 book chapters, 5 Patents and also has 2 Global certifications in "Certified Blockchain Expert" and "Certified Cybersecurity Expert" by the Blockchain Council. She has attended/presented the research papers in various Seminars, conferences and workshop at national and international level.

Lalitha Kumari is presently working as Professor in the Department of Computer Science and Engineering at Koneru Lakshmaiah Education Foundation, located in Hyderabad, Telangana, India. Dr. Kumari obtained her Ph.D. in Computer Science and Engineering from Jawaharlal Nehru Technological University, Hyderabad, Telangana, India. Additionally, she has been recognized as a "Certified Blockchain Expert" by the Blockchain Council and has received an "Award of Excellence in Research" from the Novel Research Academy. She received the 'Master Educator in Academic Leadership Award" from the Artificial Intelligence Medical and Engineering Researchers Society (AIMERS) in March 2024. Her professional contributions extend beyond teaching and research, as she actively participates as a reviewer for various esteemed journals and conferences. Dr. Kumari has made significant contributions to the field, with a portfolio that includes publishing over 12 National and International patents covering IoT, Machine Learning, and Cyber Security. She has also authored 8 book chapters. She is the author of the book "Fundamentals of Data Structures using Python." Additionally, she has published more than 35 research articles and papers in reputable journals and has presented her work at conferences hosted by Springer and IEEE.