Journal of Emerging Technologies and Innovative Research Development (JETIRD)
Volume 1, Issue 1, January-February 2026 pp. 30-41

CYBER SECURITY FRAMEWORK FOR SMART ELECTRICAL GRIDS USING BLOCK CHAIN AND INTEGRATED TECHNOLOGY

Dr.Anil Pandurang Gaikwad
**Assistant Professor, Department of BBA, AISSMS College of Business Administration, Pune,*

Abstract
Smart electrical grids (smart grids) integrate advanced sensing, communication, and control technologies to support real-time monitoring, demand response, and integration of renewable energy sources. However, this increased connectivity significantly expands the cyber-attack surface, exposing critical infrastructure to threats such as data manipulation, false data injection, denial-of-service attacks, and unauthorized control of grid components. Traditional centralized security mechanisms often suffer from single points of failure, limited transparency, and poor scalability. This paper proposes a comprehensive cyber security framework for smart electrical grids that leverages blockchain technology integrated with IoT devices, edge computing, and AI-based anomaly detection. The proposed framework uses blockchain as a distributed, tamper-resistant ledger to secure control commands, measurement logs, and device identities. Smart contracts are employed to automate access control, authentication, and transaction validation among distributed energy resources (DERs), control centers, and prosumers. Edge computing nodes perform local preprocessing and AI-driven intrusion detection to minimize latency and reduce communication overhead. The paper presents the overall architecture, security requirements, and threat model for smart grids, followed by the design of the blockchain-enabled cyber security layer. A comparative analysis between traditional Public Key Infrastructure (PKI)-based security and the proposed blockchain-based model is discussed in terms of confidentiality, integrity, availability, scalability, and resilience. The study concludes that integrating blockchain with other emerging technologies can significantly enhance trust, transparency, and resilience in smart electrical grids, while highlighting implementation challenges such as interoperability, computational overhead, and regulatory issues.
Keywords: Smart grid, cyber security, blockchain, IoT, edge computing, distributed energy resources, intrusion detection, smart contracts.

1. Introduction

Smart electrical grids represent the evolution of traditional power systems into highly automated, digitally connected infrastructures. Advanced metering infrastructure (AMI), supervisory control and data acquisition (SCADA) systems, phasor measurement units (PMUs), distributed energy resources (DERs), and electric vehicles (EVs) are interconnected via IP-based networks. This digitalization enables real-time monitoring, optimized power flow, demand response programs, and integration of renewable energy sources.

However, the same connectivity that brings flexibility and intelligence also introduces significant cyber security risks. Attackers can exploit vulnerabilities in communication protocols, weak authentication mechanisms, and unpatched devices to manipulate meter readings, disrupt service, or destabilize the grid. Incidents such as malware attacks on energy sectors worldwide demonstrate that power systems are attractive and high-impact targets for cyber adversaries.

Traditional cyber security approaches in power systems rely heavily on centralized architectures, where a central authority manages keys, authentication, and event logs. These centralized models create single points of failure and can be difficult to scale with millions of IoT-enabled devices and prosumers.

To address these limitations, this paper proposes a blockchain-based cyber security f**ram**ework for smart electrical grids, integrated with IoT, edge computing, and AI-driven security analytics. Blockchain's distributed ledger, immutability, and consensus mechanisms are leveraged to provide tamper-proof logging, decentralized identity management, and secure transaction validation.

The main objectives of this paper are to:

- Identify the key cyber security requirements and threats in smart electrical grids.
- Design a blockchain-enabled security architecture integrating smart grid components, IoT devices, and control centers.
- Propose smart contract–based access control and authentication mechanisms.
- Present an integrated framework combining blockchain with edge computing and AI-based anomaly detection.
- Discuss the benefits, limitations, and future research directions of the proposed framework.

2. Literature Review

The literature on smart grid cyber security highlights the increasing convergence of power systems with advanced digital technologies. This convergence enhances operational efficiency but simultaneously exposes the grid to new classes of cyber threats. Recent research has focused on strengthening communication systems, securing real-time data exchange, and establishing trust mechanisms among distributed energy resources. This section reviews existing studies on smart grid security, blockchain applications in energy systems, and the role of emerging technologies such as IoT, edge computing, and artificial intelligence (AI). The review concludes by identifying the research gaps that motivate the present study.

2.1 Smart Grids and Cyber Security

Smart grids integrate Information and Communication Technologies (ICT) with traditional electrical infrastructure to enable two-way communication between utilities and consumers. This integration supports advanced functionalities such as real-time monitoring, automated fault detection, and demand-side management, significantly improving the efficiency and reliability of electricity distribution. However, the increased dependence on digital communication introduces significant cyber vulnerabilities in systems such as Advanced Metering Infrastructure (AMI), SCADA, and Phasor Measurement Units (PMUs).

Standards and guidelines including NISTIR 7628, ISO/IEC 27019, and IEC 62351 have been developed to define best practices for securing smart grid communication and control. These frameworks emphasize confidentiality, integrity, availability, authentication, and non-repudiation as essential security requirements for grid operations. Despite the existence of these standards, smart grids continue to face a wide range of sophisticated cyber threats.

Common attack vectors include False Data Injection Attacks (FDIA), where adversaries manipulate sensor data to mislead grid operations; Man-in-the-Middle (MitM) attacks, which intercept or modify communications; Denial-of-Service (DoS) attacks targeting critical servers and control centers; and malware infections compromising SCADA or industrial control systems. Such attacks can destabilize grid performance, disrupt service delivery, compromise

billing accuracy, or even cause large-scale outages. Therefore, enhancing the cyber resilience of smart grids remains a major research priority.

2.2 Blockchain for Energy Systems

Blockchain technology has emerged as a promising tool for enhancing trust, transparency, and security in decentralized energy systems. A blockchain is essentially a distributed ledger in which transactions are stored in cryptographically linked blocks validated through consensus algorithms such as Proof-of-Work (PoW), Proof-of-Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). Because of its decentralized architecture, blockchain eliminates the need for a central authority and minimizes the risks associated with single points of failure. In the energy sector, blockchain applications have expanded rapidly. Researchers have explored its use in peer-to-peer (P2P) energy trading, allowing prosumers to directly trade excess renewable energy without relying on intermediaries. Blockchain has also been applied to decentralized electricity markets, enabling transparent pricing and automated settlements through smart contracts. Additionally, blockchain is increasingly used to secure metering data, ensuring that consumption records are tamper-proof, auditable, and verifiable.

The key advantages of blockchain include immutability, which prevents retroactive alteration of stored data; transparency, which allows authorized stakeholders to audit all system operations; decentralized trust, which distributes decision-making among network participants; and tamper-resistant audit trails, which strengthen accountability. These characteristics make blockchain a strong candidate for addressing security and trust challenges in smart grid environments.

2.3 Integrated Technologies: IoT, Edge Computing, and AI

The rapid proliferation of Internet of Things (IoT) devices—including sensors, smart meters, and PMUs enables granular data collection and real-time situational awareness in smart grids. However, these devices are often resource-constrained, making them highly susceptible to cyber-attacks such as device spoofing, unauthorized access, and firmware manipulation. Securing IoT endpoints has therefore become essential for maintaining the integrity of the entire grid. To address scalability and latency issues, edge computing has been introduced as a complementary architecture to cloud-based systems. Edge computing processes data closer to its source, reducing bandwidth consumption and enabling faster decision-making. In the context of smart grids, edge nodes can perform local authentication, preliminary data filtering, and run real-time intrusion detection algorithms without depending on distant cloud servers.

Artificial Intelligence (AI) and Machine Learning (ML) play a crucial role in enhancing cyber resilience. AI-driven systems can detect anomalies in electricity consumption patterns, voltage fluctuations, and communication traffic, making them effective tools for identifying cyber-physical intrusions. Machine learning techniques such as Support Vector Machines (SVM), Random Forest classifiers, and Deep Learning models (e.g., LSTM networks) have been employed to identify malicious behavior with high accuracy. The integration of AI into smart grid operations thus enables proactive threat detection and rapid response to cyber incidents.

2.4 Research Gap

While existing research has explored blockchain applications, intrusion detection systems, and secure communication protocols for smart grids, most studies examine these technologies in isolation. Only a limited number of works propose a holistic security framework that integrates blockchain with IoT, edge computing, and AI-based analytics. Moreover, many existing models do not present clear architectural components, data flow mechanisms, or comprehensive security services tailored specifically for smart electrical grids.

This paper addresses these gaps by proposing an integrated cyber security framework that combines decentralized trust provided by blockchain, low-latency decision-making enabled by edge computing, and intelligent threat detection powered by AI. The framework outlines well-defined components, describes secure data pathways, and aligns security mechanisms with the operational needs of modern smart grids.

3. Problem Statement and Objectives

3.1 Problem Statement

Modern smart electrical grids operate as highly interconnected cyber-physical systems that incorporate millions of IoT-enabled devices, distributed energy resources, advanced metering systems, and digital control platforms. While this interconnectivity enhances efficiency and reliability, it also significantly increases the attack surface of the grid. The distributed nature of smart grids—combined with the use of heterogeneous communication technologies, legacy protocols, and resource-constrained devices—creates numerous vulnerabilities that can be exploited by cyber adversaries.

Traditional security mechanisms in power systems predominantly rely on centralized architectures, where a single entity manages authentication, authorization, data logging, and key distribution. This model introduces critical limitations, such as susceptibility to single points of failure, difficulty in scaling to millions of devices, and lack of transparency in event auditing. Furthermore, centralized systems often fail to provide the tamper-proof and trustless environment required to prevent manipulation of control commands, metering data, and device identities.

Therefore, there is a compelling need for a decentralized, transparent, scalable, and tamper-resistant cyber security framework capable of ensuring secure data exchange, authenticated device interactions, trustworthy control operations, and robust intrusion detection within smart electrical grids. Blockchain and integrated technologies such as IoT, edge computing, and AI provide promising capabilities for addressing these challenges.

3.2 Objectives of the Study

This study is guided by the following key objectives:

1. To analyze the security requirements and evolving threat landscape of smart electrical grids.
2. To design a blockchain-based cyber security architecture**.**
3. To develop an integrated cyber security framework.
4. To compare the proposed framework with traditional centralized security models**.**
5. To identify implementation challenges, limitations, and future research opportunities

4. Smart Grid Threat Model and Security Requirements

Smart electrical grids face a diverse set of cyber threats due to their hybrid cyber-physical architecture. A systematic threat model is essential for designing effective security mechanisms. This section describes the major cyber threats and outlines the core security requirements necessary for resilient grid operations.

4.1 Major Cyber Threats in Smart Electrical Grids

Smart grids are vulnerable to a range of cyber-attacks targeting communication networks, sensors, meters, substations, and control centers. Table 1 summarizes the major threats.

Table 1. Major Cyber Threats in Smart Electrical Grids

Threat Type	Description
False Data Injection Attacks (FDIA)	Attackers manipulate measurement data (e.g., voltage, frequency, consumption) to mislead state estimation and disrupt grid stability.
Replay Attacks	Previously valid messages are captured and resent to confuse devices or disrupt control logic.
Denial of Service (DoS/DDoS)	Adversaries overload communication channels, edge nodes, or control systems, causing delays or service outages.
Unauthorized Access / Privilege Escalation	Intruders gain access to system components, modify settings, or issue malicious control commands.
Privacy Breaches	Compromise of consumer usage data, revealing personal and behavioral information.
Malware and Ransomware Attacks	Infection of SCADA, substations, or AMI systems through malicious software, potentially leading to grid shutdowns or extortion attempts.

These threats underscore the necessity for a comprehensive, multi-layered cyber security strategy capable of protecting both physical assets and digital infrastructure.

4.2 Security Requirements

To ensure reliable and secure operation, smart electrical grids must satisfy several fundamental security requirements:

Confidentiality

Sensitive operational data, control messages, and consumer usage information must remain protected from unauthorized disclosure. This is critical for preventing espionage and preserving consumer privacy.

Integrity

Data collected from sensors, meters, and communication networks must remain unaltered during transmission and storage. Integrity ensures that control decisions are based on accurate and trustworthy information.

Availability

Grid resources—such as substations, meters, communication networks, and control centers—must remain continuously accessible even during cyber-attacks. Disruptions in availability can lead to blackouts or cascading failures.

Authentication and Authorization

A robust identity verification mechanism is required to ensure that only legitimate devices, users, and control systems participate in smart grid operations. Role-based access control must restrict actions based on predefined privileges.

Non-repudiation and Traceability

All interactions—such as data updates, control commands, and configuration changes—must be recorded in a manner that prevents denial of responsibility. Traceability ensures full auditability of system events.

Resilience

Smart grids must detect, withstand, and recover from cyber-attacks with minimal impact on operations. Resilience includes redundancy, rapid fault isolation, and self-healing capabilities.

5. Proposed Blockchain-Enabled Cyber Security Framework

This section presents the core contribution of the study: an integrated cyber security framework for smart electrical grids using blockchain, IoT, edge computing, and AI-driven intrusion

detection. The framework aims to provide a decentralized and tamper-resistant mechanism to secure communication, authenticate devices, safeguard operational data, and ensure resilience against cyber-attacks. The proposed architecture is organized into four distinct layers, each providing specialized functions that collectively enhance the overall security posture of smart grid operations.

5.1 High-Level Architecture

The proposed cyber security framework adopts a layered architecture, allowing seamless coordination between physical devices, computational nodes, decentralized security services, and grid operation platforms. Figure 1 conceptually illustrates the architecture.

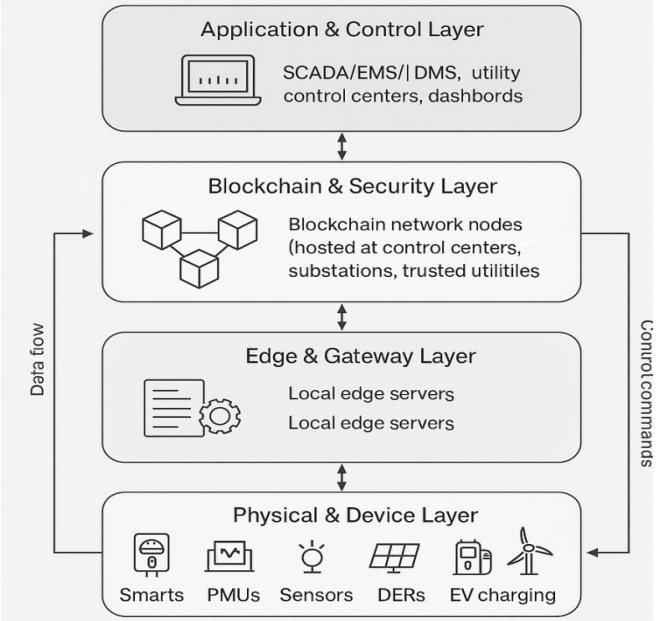


Fig 1 Blockchain enabled cyber security architecture integrating device

Layer 1: Physical & Device Layer (Bottom)

This foundational layer consists of the core operational devices responsible for measurement, monitoring, communication, and control within the smart grid. It includes:

- Smart meters
- Phasor Measurement Units (PMUs)
- Remote Terminal Units (RTUs)
- Environmental and operational sensors
- Distributed Energy Resources (DERs) such as solar PV, wind units, and microgrids
- Electric Vehicle (EV) charging stations

These devices generate high-frequency data and interact continuously with grid control systems. Due to their distributed deployment and limited security capabilities, they are prone to cyber intrusions, making protection at this layer critical.

Layer 2: Edge & Gateway Layer

This layer consists of **local edge servers** deployed at distribution substations, microgrids, or cluster nodes. Edge devices serve three primary functions:

1. **Local Data Processing and Pre-Filtering** Incoming data from devices is aggregated at edge gateways, which reduce redundant or noisy signals before forwarding critical information.
2. **Local Storage and Temporary Event Logging** Edge nodes maintain short-term logs to reduce bandwidth load and prevent dependence on centralized data stores.
3. **AI-Based Intrusion Detection Execution** Machine learning models run directly on edge hardware to detect anomalies in real-time, enabling rapid threat mitigation without relying on remote control centers.

By hosting both computational and security services locally, the edge layer supports low-latency processing and enhances grid resilience.

Layer 3: Blockchain & Security Layer

The blockchain layer functions as the trust and security backbone of the framework. It is implemented as a permissioned blockchain, where nodes are distributed across trusted utility stakeholders such as:

- Control centers
- Substations
- Utility companies
- Regulatory authorities

Key functionalities include:

- **Distributed Ledger for Event Logging:** All critical operations—meter readings, device authentication requests, control commands, configuration changes—are stored as immutable transactions.
- **Smart Contract Enforcement:** Policies for access control, role verification, authorization, anomaly responses, and P2P energy transactions are encoded into smart contracts.
- **Decentralized Identity Management:** Devices and stakeholders are assigned tamper-proof identities through cryptographic key pairs stored on the blockchain.
- **Consensus-Based Validation:** The system uses energy-efficient algorithms such as PBFT (Practical Byzantine Fault Tolerance) or Raft, ensuring reliable and low-latency validation without the overhead of PoW.

Layer 4: Application & Control Layer (Top)

The topmost layer comprises operational systems and user interfaces:

- SCADA (Supervisory Control and Data Acquisition)
- EMS (Energy Management Systems)
- DMS (Distribution Management Systems)
- Utility dashboards
- Billing systems
- Consumer service applications

These applications interact with blockchain-validated data and rely on authenticated control commands to ensure secure real-time grid management.

Data Flow Representation

Arrows in the architecture diagram should show:

- **Upstream Flow:** Devices → Edge nodes → Blockchain layer → Application/Control layer
- **Downstream Flow:** Control center → Blockchain validation → Edge nodes → Devices

This bi-directional flow ensures both secure data ingestion and authenticated command dissemination.

6. Comparison of Traditional vs Blockchain-Based Security

Table 1 Comparison between Traditional Centralized Security and Proposed Blockchain-Based Framework

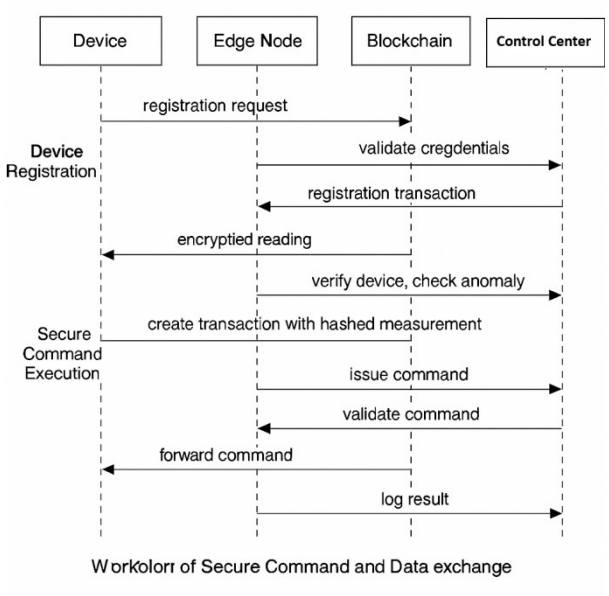
Security Criterion	Traditional Centralized Model	Proposed Blockchain-Based Framework
Architecture	Central server / PKI authority	Distributed ledger with multiple validating nodes
Single Point of Failure	High – compromise of central server affects entire system	Low – no single authority; redundancy across nodes
Data Integrity	Relies on database security and backups	Cryptographic hashing; tamper-evident blocks
Transparency & Audit	Limited log integrity; logs may be altered	Immutable audit trail of all critical events
Scalability	Central server becomes bottleneck as devices grow	Horizontally scalable with additional blockchain nodes
Trust Model	Requires trust in central authority	Distributed trust via consensus among authorized nodes
Latency	Lower (no consensus)	Slightly higher (consensus overhead) but optimized with permissioned chain
Key/Identity Management	Centralized PKI	Decentralized identity and key management on chain
Resilience to Attacks	Vulnerable to DoS on central services	More resilient due to distributed validation and storage

The comparison in Table 1 demonstrates that the blockchain-based security framework provides substantial improvements in reliability, transparency, and resilience compared to traditional centralized models. Centralized systems depend on a single authority for authentication, logging, and key management, making them highly susceptible to single-point failures and limiting their scalability as the number of grid-connected devices increases. In contrast, the blockchain-based approach distributes trust and data storage across multiple validating nodes, reducing vulnerability to attacks and eliminating reliance on a central server. Data integrity is significantly enhanced through cryptographic hashing and tamper-evident block structures, while immutable audit trails ensure transparent and traceable system operations. Although centralized architectures offer lower latency due to the absence of consensus mechanisms, permissioned blockchain networks mitigate this issue by providing optimized, low-latency validation suitable for real-time applications. Additionally, decentralized identity management strengthens authentication by addressing traditional PKI limitations, and the distributed architecture greatly improves resilience against DoS and other cyber-attacks. Overall, the blockchain-enabled framework provides a more secure, scalable, and fault-tolerant solution for protecting smart electrical grids from evolving cyber threats.

7. Framework Workflow

The operation of the proposed blockchain-enabled cyber security framework can be explained through the workflow of secure device registration, data reporting, and control command execution. Figure 2 illustrates this workflow as a sequence diagram with four main entities: Device, Edge Node, Blockchain Network, and Control Center.

Figure 2 Sequence Diagram Description



W orkolorr of Secure Command and Data exchange

Step 1: Device Registration

1. **Registration Request**

- A smart meter (or any grid-connected device) initiates the process by sending a **registration** request to the nearest **edge node**.

2. **Credential Validation at Edge**

- The edge node verifies the device's credentials (e.g., manufacturer ID, MAC address, pre-shared keys, or certificates).
- If validation succeeds, the edge node prepares a registration transaction containing the device's public key and identity attributes.

3. **On-Chain Registration**

- The registration transaction is submitted to the blockchain network.
- A smart contract checks the authenticity of the submitted information and validates whether the registering entity is authorized to join the grid network.
- Upon successful verification, the device identity is stored on the distributed ledger, creating a tamper-proof record of its existence and cryptographic identity.

Step 2: Secure Data Reporting

1. **Encrypted Measurement Upload**

- The registered smart meter periodically sends encrypted measurement data (e.g., energy consumption, voltage, frequency) to the edge node.

2. **Verification and Anomaly Check**

- The edge node authenticates the sending device using its on-chain identity.
- AI/ML-based **anomaly detection** is executed locally on the data and associated network traffic to identify suspicious patterns.

3. **Blockchain Logging of Valid Data**

- If the data is classified as legitimate, the edge node computes a cryptographic hash of the measurement and creates a blockchain transaction containing this hash and relevant metadata (timestamp, device ID, location, etc.).
- The transaction is validated by the blockchain network and appended to a new block, thereby providing an immutable record of the reported measurements without exposing raw data.

Step 3: Control Command Execution

1. **Command Generation at Control Center**

- The **control center** (e.g., SCADA/EMS/DMS) issues a control command such as load shedding, voltage adjustment, or DER dispatch.

2. **Command Encapsulation as Transaction**

- The command is encapsulated in a **transaction** that includes the sender's identity, target device or group, and operation type.
- This transaction is submitted to the blockchain network.

3. **Smart Contract Validation**

- A dedicated **access-control smart contract** checks:
- The role and authorization level of the sender,
- The current status and registration of the target device(s),
- Any applicable security policies or constraints.
- Only if all conditions are satisfied is the command approved and confirmed on the ledger.

4. **Command Delivery and Execution**

- The edge node monitoring the blockchain detects the approved command and forwards it securely to the relevant device(s).

5. **Result Logging for Traceability**

- Once the device executes the command, an acknowledgment and the outcome (e.g., successful load reduction) are returned to the edge node.
- A summary of the result is logged again on the blockchain, creating a fully traceable chain of events: who issued the command, when it was validated, and how it was executed.
-

8. Evaluation (Conceptual / Theoretical)

In the absence of empirical testbed results, a conceptual evaluation helps assess how the proposed blockchain-enabled framework meets the essential security requirements of smart electrical grids. The evaluation is based on analyzing confidentiality, integrity, availability, resilience, authentication, and access control.

Confidentiality

The framework ensures confidentiality through strong encryption mechanisms (e.g., TLS-based secure channels and symmetric key encryption) between smart devices, edge nodes, and control centers. Because the blockchain stores only hashed values and metadata, sensitive raw measurement data never appears on-chain. This design protects consumer privacy while still providing verifiable integrity. The use of distributed identity management also minimizes unauthorized access.

Integrity and Non-Repudiation

Blockchain inherently supports integrity due to its immutable ledger, where every block is linked cryptographically to the previous one. Digital signatures ensure that each transaction—whether a data reading or control command—can be traced back to its originator. This prevents data tampering and ensures non-repudiation. Once a transaction is confirmed, neither users nor attackers can deny or alter it, enabling trusted audit and accountability.

Availability and Resilience

Traditional centralized architectures suffer from single points of failure and are vulnerable to DoS attacks. The proposed framework addresses this through distributed ledger replication across multiple validating nodes, ensuring that system functions continue even if some nodes

fail. Edge computing further enhances availability by allowing devices to continue operating locally during connectivity issues. This layered redundancy increases grid resilience in the face of cyber disruptions.

Authentication and Access Control

Device identities are stored and verified using blockchain-based cryptographic keys, eliminating dependence on vulnerable centralized PKI. Smart contracts enforce role-based access control**,** ensuring only authorized users and devices can initiate operations. Unauthorized attempts trigger alerts or automated actions, reducing the risk of misuse or manipulation.

Table 2. Qualitative Evaluation of Security Requirements

Security Requirement	**Traditional Model**	**Proposed Blockchain-Based Framework**
Confidentiality	Medium	High
Integrity	Medium	High
Non-repudiation	Low–Medium	High
Availability	Medium	High
Authentication & Access Control	Medium	High
Resilience	Low–Medium	High

This conceptual evaluation indicates that the proposed blockchain-enabled architecture provides significant improvements across all security dimensions, making it a promising approach for securing smart grid operations.

9. Challenges and Limitations

Despite its benefits, the proposed framework faces several important challenges that must be considered before large-scale implementation.

Performance and Latency

Consensus algorithms and cryptographic operations introduce processing delays. For time-sensitive functions such as fault detection or voltage control, even small delays may be critical. Permissioned blockchains reduce latency, but real-time performance must still be optimized.

Scalability Issues

Smart grids consist of millions of IoT devices producing continuous data streams. Logging all events on the blockchain may lead to ledger bloat, high storage overhead, and increased computational requirements. Efficient off-chain storage and selective logging strategies are necessary.

Interoperability Constraints

Integrating blockchain with legacy SCADA systems, diverse vendor equipment, and existing communication protocols is complex. Lack of standardized blockchain interfaces for energy systems limits seamless interoperability.

Regulatory and Policy Barriers

Critical infrastructure regulations require strict compliance with national cyber security frameworks, data protection laws, and power sector standards. Blockchain's decentralized nature may conflict with certain regulatory mandates requiring centralized oversight.

Resource Constraints on IoT Devices

Many smart meters and sensors have limited processing power and cannot operate as full blockchain nodes. Running blockchain services directly on such devices is infeasible. Hence, the framework relies heavily on edge nodes and lightweight client configurations.

10. Conclusion

This paper presented a comprehensive blockchain-enabled cyber security framework designed to strengthen the protection, transparency, and resilience of smart electrical grids. As modern power systems increasingly depend on digital communication, IoT devices, and automated control functions, traditional centralized security mechanisms are no longer sufficient to address the growing complexity and sophistication of cyber threats. The proposed framework integrates blockchain technology, edge computing, and AI-based intrusion detection to provide a decentralized, tamper-proof, and intelligent defense architecture.

Through conceptual evaluation, the study demonstrates that blockchain significantly enhances data integrity, non-repudiation, secure event logging, and decentralized identity management. Smart contracts automate authorization policies and maintain consistent, trustless interactions among grid components, while edge computing ensures low-latency processing and rapid anomaly detection. Compared to legacy PKI-based centralized systems, the blockchain-enabled approach offers superior scalability, fault tolerance, and resistance to distributed cyber-attacks.

However, challenges remain related to latency introduced by consensus algorithms, scalability concerns with large-scale deployment, interoperability issues with legacy SCADA systems, regulatory compliance, and the limited processing capabilities of resource-constrained devices. Addressing these challenges requires future work on privacy-preserving blockchain techniques, optimized consensus mechanisms, hybrid on-chain/off-chain architectures, and standardized interfaces for energy-sector interoperability.

Overall, the proposed framework provides a forward-looking foundation for enhancing cyber resilience in smart electrical grids and contributes meaningfully to the development of secure, transparent, and sustainable energy infrastructures.

References

1. Aitzhan, N. Z., & Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing, 15*(5), 840–852.
2. Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., ... Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews, 100*, 143–174.
3. Baumeister, M., & Haar, R. (2020). Enhancing security in smart grids using blockchain technology. *International Journal of Energy Research, 44*(10), 7902–7915.*
4. Gai, K., Wu, Y., Zhu, L., Zhang, B., & Shen, M. (2019). Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Transactions on Industrial Informatics, 15*(6), 3548–3558.
5. Hahn, A., Ashok, A., Sridhar, S., & Govindarasu, M. (2013). Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Transactions on Smart Grid, 4*(2), 847–855.
6. Kuzlu, M., Pipattanasomporn, M., & Rahman, S. (2014). Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Computer Networks, 67*, 74–88.
7. Liu, C., Sun, K., Wang, X., & Liu, S. (2011). A cyber-attack defense system for automatic generation control. *IEEE Transactions on Smart Grid, 2*(4), 782–792.
8. NIST. (2014). *NISTIR 7628 Rev. 1: Guidelines for smart grid cyber security.* National Institute of Standards and Technology.
9. Rahman, M. M., Sargolzaei, A., & Bingham, J. (2020). A survey on secure communication protocols for smart grid. *IEEE Communications Surveys & Tutorials, 22*(1), 243–270.
10. Zhang, Y., Wang, L., Sun, W., & Esmalifalak, M. (2018). Blockchain-based secure data sharing for smart grid. *Security and Communication Networks, 2018*, 1–12.
11. Zhou, Y., & Wu, J. (2021). A blockchain-based distributed security architecture for next-generation power systems. *Electric Power Systems Research, 190*, 106–700.