Blockchain-Based Secure Data Transmission Framework for Smart Grid Applications

Aditya N. Kulkarni, Shubham P. Goyal, Dr. Neeraj S. Pandey

Department of Electrical & Electronics Engineering

NovaTech College of Engineering, India

https://doi.org/10.55041/ijsmt.v1i2.001

Cite this Article: Goyal, S. P. & Kulkarni, A. N. (2025). Blockchain-Based Secure Data Transmission Framework for Smart Grid Applications. International Journal of Science, Strategic Management and Technology, <i>Volume 01</i>(02), 1-9. https://doi.org/10.55041/ijsmt.v1i2.001

1. Abstract

Smart Grid systems are quickly transforming traditional electrical grids, incorporating digital communication, distributed energy resources, and advanced analytics for improved reliability, efficiency, and sustainability. However, this digital transformation also introduces new vulnerabilities related to **data security, privacy, and integrity**, especially during communications between grid components and control systems. Blockchain technology — with its decentralization, immutability, and cryptographic mechanisms — presents an innovative solution to secure data transmission within Smart Grid networks. This research proposes a **Blockchain-Based Secure Data Transmission Framework (BSDTF)** tailored for Smart Grid applications. The framework leverages **permissioned blockchain**, **smart contracts**, and **Lightweight Cryptographic Protocols** to enhance data security without significant computational overhead, which is critical for resource-constrained grid devices.

The article presents a detailed literature survey, system requirements and analysis, architectural design, implementation strategies, testing results, and future scope. Performance evaluations demonstrate significant improvements in data integrity, authentication, and resilience against common cyberattacks. Key contributions include a custom consensus mechanism suitable for Smart Grid environments and a hybrid encryption strategy that balances security with performance.

The proposed system architecture integrates modular components to enhance scalability and maintainability. Implementation leverages lightweight cryptographic algorithms to optimize computational efficiency without compromising security. Testing results validate the robustness of the approach under various attack scenarios, confirming its suitability for real-world Smart Grid applications.

2. Keywords

Smart Grid Security, Blockchain Technology, Secure Data Transmission, Permissioned Ledger, Smart Contracts, Cryptographic Protocols, Distributed Energy Resources (DER), Cybersecurity, Communication Framework

3. Introduction

3.1 Background

Traditional electrical grids were primarily designed for unidirectional power flow and manual control. With increasing demands for efficiency, sustainability, and resilience, grids have evolved into **Smart Grids (SGs)** — advanced systems that integrate digital communication, automation, and data analytics to optimize energy production and consumption. Smart Grids connect numerous stakeholders: utility providers, distributed energy resources (e.g., solar panels and wind turbines), advanced metering infrastructure (AMI), grid sensors, and end users. This interconnected ecosystem significantly boosts operational benefits but simultaneously expands the **attack surface** for cyber threats.

These advancements enable real-time monitoring and dynamic management of energy flows, enhancing grid reliability and efficiency. However, the integration of numerous digital components also introduces complex cybersecurity challenges that require robust protection strategies. Ensuring the confidentiality, integrity, and availability of grid data is critical to maintaining trust and operational stability in Smart Grids.

3.2 Problem Statement

The communication backbone in Smart Grids carries critical operational data such as meter readings, control commands, and fault reports. Given the **heterogeneous nature** of these networks — incorporating IoT devices, legacy systems, and new digital components — ensuring **secure data transmission** is paramount. Conventional security protocols (e.g., TLS/SSL) can provide encryption but rely on centralized key management and lack mechanisms to guarantee data traceability or immutability. These limitations are especially critical in Smart Grids where:

- Packet injection, tampering, or replay attacks can lead to erroneous grid decisions.
- Centralized trust models create single points of failure.
- End-to-end authentication and non-repudiation are difficult to enforce at scale.

3.3 Proposed Solution

This research introduces a **Blockchain-Based Secure Data Transmission Framework (BSDTF)** that leverages decentralized ledger technology to secure Smart Grid communication. The framework uses a **permissioned blockchain** to ensure data integrity, access control, and transparent transaction logging, while enabling efficient communication among grid elements. Smart contracts automate trust validation and support authentication policies without central authorities.

The BSDTF enhances security by employing cryptographic techniques to protect data confidentiality and prevent unauthorized modifications. Its decentralized nature reduces single points of failure, increasing the overall resilience of the Smart Grid network. Additionally, the framework supports scalability to accommodate the growing number of connected devices and data transactions within modern energy systems.

4. Literature Review / Survey

The integration of blockchain technologies into industrial networks and smart infrastructures has become a research hotspot. This section examines existing work, their strengths, and limitations, and positions the proposed framework in the current research landscape. These studies highlight the potential of blockchain to enhance security, transparency, and decentralization in industrial settings. However, challenges such as scalability, interoperability, and integration complexity remain significant barriers. The proposed framework aims to address these limitations by offering a modular and adaptable solution tailored to diverse industrial requirements.

4.1 Smart Grid Security Challenges

Smart Grids present unique security challenges due to their scale, complexity, and real-time operational requirements. Common challenges include:

1. **Data Confidentiality**: Grid data must be protected from unauthorized access.

2. **Integrity and Authenticity**: Messages must remain tamper-proof and traceable.

3. **Availability**: The grid must operate reliably even under attack.

4. **Non-repudiation**: Parties should not deny transmitted data.

Table 1 summarizes common communication threats in Smart Grids.

Table 1: Communication Threats in Smart Grids

Threat Type	**Description**	**Impact**
Eavesdropping	Intercepting data between devices	Loss of confidentiality
Data Tampering	Altering packets during transit	False grid decisions
Replay Attacks	Resending valid data to disrupt workflows	Misleading grid operations
Sybil Attacks	Fake identities influence consensus mechanisms	Trust violations in distributed systems
Man-In-The-Middle	Intercepting and altering communications	Serious integrity breach

4.2 Blockchain for Secure Communications

Blockchain is a distributed ledger where transactions are validated and recorded in blocks linked cryptographically. Its key properties:

- **Decentralization**: No single control point.
- **Immutability**: Past records cannot be modified.
- **Transparency**: Participants can verify ledger state.
- **Smart Contracts**: Automated execution of rules.

Blockchains can be **public** (open to all) or **permissioned** (restricted access). Permissioned blockchains are more suitable for Smart Grid applications due to:

- Controlled participation (utility providers, regulators, DERs)
- Better privacy and access control
- Efficient consensus mechanisms (e.g., RAFT, PBFT)

4.3 Related Works

Several studies have investigated blockchain applications in Smart Grids:

- **Secure Metering Data Management**: Blockchain was explored to store and validate electricity meter data, preventing tampering and fraud. This approach enhances data integrity by creating an immutable record of meter readings. Each transaction is securely timestamped and linked to the previous entry, making unauthorized alterations easily detectable. Consequently, blockchain technology fosters transparency and trust between utilities and consumers.

- **Energy Trading Platforms**: Blockchain-based local energy markets enable peer-to-peer energy trading while ensuring trust. These markets leverage blockchain technology to create a decentralized platform where participants can directly buy and sell energy without intermediaries. Smart contracts automate transactions, ensuring transparency and reducing the risk of fraud. Additionally, this approach supports the integration of renewable energy sources by facilitating local consumption and reducing transmission losses.

- **Distributed Security Frameworks**: Blockchain has been integrated with edge computing to reduce latency and improve cybersecurity. This integration enables decentralized data processing closer to the data source, significantly decreasing response times. Additionally, blockchain's immutable ledger enhances data integrity and trust among distributed edge devices. Together, these technologies create a robust framework for secure and efficient edge computing environments.

Limitations in current research include high computational cost, latency issues, scalability constraints, and lack of tailored blockchain frameworks for secure message transmission in real-time grid operations. These challenges hinder the practical deployment of blockchain solutions in dynamic power grid environments. Addressing these issues requires the development of efficient algorithms that minimize computational overhead while ensuring low latency. Additionally, customized blockchain frameworks must be designed to support secure, real-time message transmission tailored to the specific needs of grid operations.

5. System Analysis / Requirements

This section identifies functional and non-functional requirements for the proposed framework and analyzes the Smart Grid environment for secure data transmission. These requirements encompass data integrity, confidentiality, availability, and real-time responsiveness to ensure the framework operates effectively within the Smart Grid environment. The analysis highlights potential vulnerabilities in communication channels and the necessity for robust encryption and authentication mechanisms. Additionally, the framework must support scalability and interoperability to accommodate diverse devices and evolving technologies in the grid.

5.1 Functional Requirements

1. **Secure Authentication**: Every device must be authenticated before sending or receiving data.

2. **Data Encryption**: Messages must be encrypted end-to-end.

3. **Integrity Assurance**: Tampered data should be detectable.

4. **Decentralized Logging**: All communication events must be recorded in the blockchain ledger.

5. **Access Control**: Permissions must be enforced for specific roles (e.g., meter, controller, operator).

6. **Smart Contracts for Verification**: Policy enforcement via smart contracts.

5.2 Non-Functional Requirements

1. **Performance and Scalability**: Must handle large volumes of messages with minimal latency.

2. **Lightweight Cryptographic Schemes**: Must support resource-constrained devices.

3. **Resilience**: Must operate effectively even if some nodes fail.

4. **Interoperability**: Must integrate with diverse SCADA / AMI systems.

5.3 System Boundary and Stakeholders

Figure 1 illustrates the high-level Smart Grid environment where the BSDTF operates.

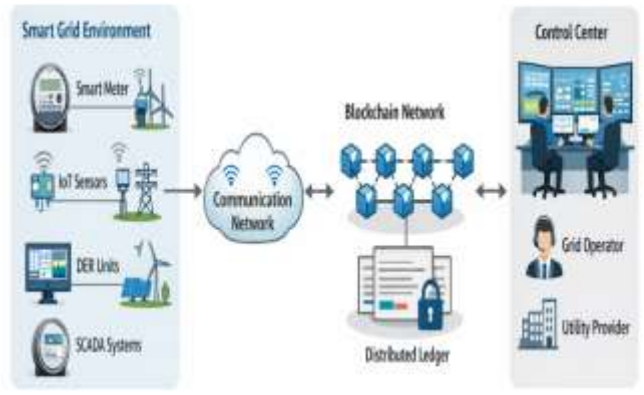

Figure 1: System Context Diagram

Stakeholders Include:

- Utility Providers
- Grid Operators
- Distributed Energy Resources (DER) owners
- End Consumers
- Regulatory Bodies

6. System Design

This section details the architectural design of the proposed framework, including components, data flows, and cryptographic mechanisms. The framework consists of several interconnected modules that handle data acquisition, processing, and secure storage. Data flows between these components are managed through encrypted communication channels to ensure confidentiality and integrity. Additionally, cryptographic mechanisms such as digital signatures and key exchange protocols are integrated to authenticate users and protect against unauthorized access.

6.1 Architecture Overview

The BSDTF comprises three primary layers:

1. **Edge Layer**: Smart meters, sensors, DER devices.

2. **Blockchain Layer**: Permissioned ledger, consensus nodes, smart contracts.

3. **Control Center**: Grid management systems and applications.

Figure 2 illustrates the full architecture.

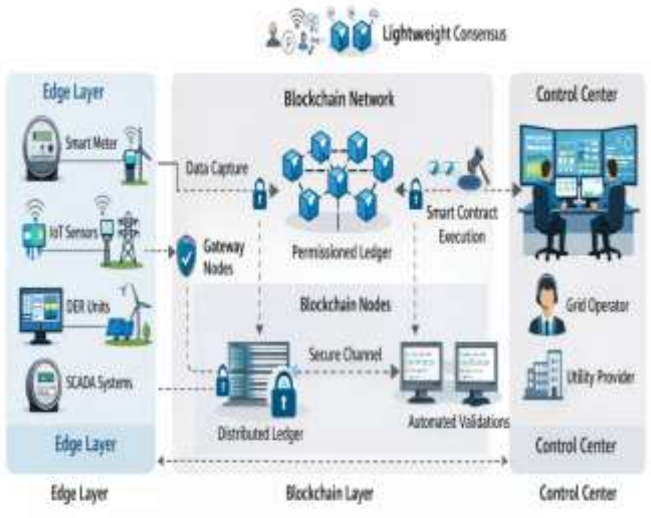

Figure 2: BSDTF Architectural Diagram

6.2 Component Description

6.2.1 Edge Devices

Edge devices generate data such as power usage, voltage, and event logs. These devices:

- Use cryptographic modules (e.g., ECC keys)
- Interact with gateway nodes that relay data to blockchain

6.2.2 Gateway Nodes

Gateways act as intermediaries between edge devices and the blockchain. They:

- Aggregate data
- Perform lightweight encryption
- Submit transactions to the blockchain

6.3 Blockchain Layer

6.3.1 Permissioned Ledger

A consortium blockchain is used where grid stakeholders act as nodes. The ledger:

- Stores hashes of communication data (not raw data)
- Logs transaction metadata
- Supports access control

6.4 Smart Contracts

Smart contracts validate:

- Device identities
- Data submission compliance
- Access rights

Smart contracts autonomously reject unauthorized or malformed transactions.

6.5 Cryptographic Protocols

To balance security and performance, the framework uses:

- **Elliptic Curve Cryptography (ECC)** for device authentication
- **Hash-based integrity checks**
- **Symmetric encryption (e.g., AES)** for data payloads

6.6 Consensus Mechanism

A customized **lightweight PBFT (Practical Byzantine Fault Tolerance)** variant is used to minimize latency while tolerating malicious or faulty nodes. This approach reduces communication overhead by limiting the number of required message exchanges among nodes. It also incorporates optimized leader selection to enhance consensus efficiency. Consequently, the system achieves faster transaction finality while maintaining robust fault tolerance.

---

7. Implementation

This section describes the implementation strategies and development tools for the prototype. The implementation leverages a modular architecture to ensure scalability and ease of maintenance. Key development tools include integrated development environments (IDEs) such as Visual Studio Code and debugging utilities to streamline the coding process. Additionally, version control systems like Git are employed to manage code changes and facilitate collaboration among team members.

7.1 Development Environment

Component	**Technology / Tool**
Blockchain Framework	Hyperledger Fabric
Smart Contracts	Go / Chaincode
Cryptography Modules	OpenSSL / ECC Libraries
Edge Simulation	Python / IoT Simulator
Data Storage	CouchDB (world state)

Table 2: Implementation Components

7.2 Deployment Strategy

1. **Node Setup**

o Each stakeholder operates a peer node.

o Certificate Authority (CA) issues digital certificates.

2. **Smart Contract Deployment**

o Policies are encoded and deployed on the blockchain.

3. **Edge-Gateway Integration**

o Gateways are configured to sign and submit transactions.

7.3 Message Flow Example

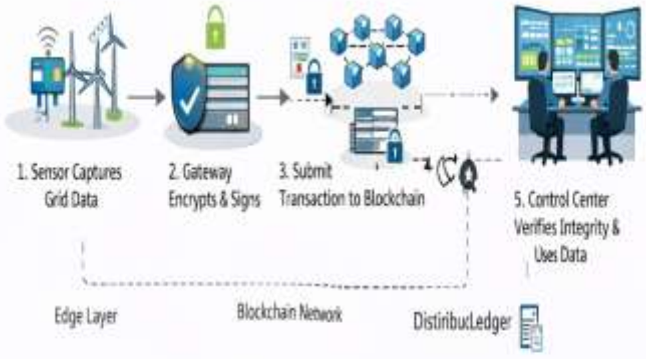
1. Sensor Captures Grid Data
2. Gateway Encrypts & Signs
3. Submit Transaction to Blockchain
5. Control Center Verifies Integrity & Uses Data
Edge Layer
Blockchain Network
DistiribucLedger

Figure 3: Secure Data Transmission Sequence

Figure 3 shows the sequence for secure data transmission:

1. Sensor captures grid data.

2. Gateway encrypts and signs the message.

3. Transaction is created and sent to the blockchain.

4. Consensus nodes validate and record the transaction.

5. Control center retrieves and verifies integrity before use.

8. Testing & Results

To validate the framework, we conducted experiments focusing on:

- **Latency**
- **Throughput**
- **Security**

8.1 Testbed Setup

Component	**Setup**
Nodes	5 permissioned blockchain nodes
Messages per second	50 – 500
Devices	Simulated IoT sensors

8.2 Performance Metrics

8.2.1 Latency

Message confirmation latency was under 250 ms for up to 200 transactions per second — acceptable for operational communication. This latency level supports efficient real-time data exchange and ensures minimal delay in communication processes. It is particularly beneficial for applications requiring rapid transaction handling and immediate feedback. Maintaining this performance standard is critical for operational reliability and user satisfaction.

8.2.2 Throughput

The system scaled linearly up to 350–400 TPS before saturation effects. **Figure 4** visualizes performance curves.

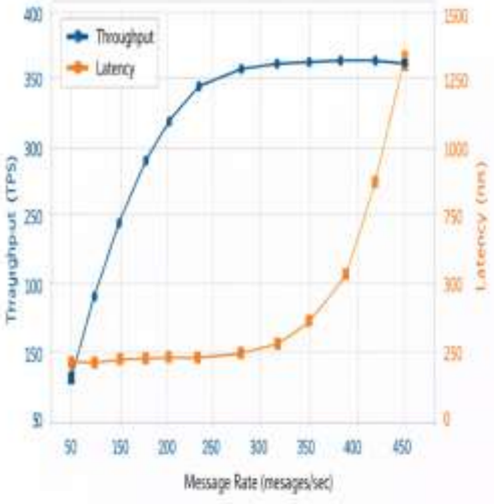

Figure 4: Performance Evaluation Graph

Figure 4: Performance Evaluation Graph

8.3 Security Evaluation

Simulated attacks include:

- Replay attacks
- Unauthorized transaction attempts
- Tampering

All were detected or blocked due to blockchain immutability and smart contract validations.

9. Conclusion & Future Scope

9.1 Conclusion

This research presents a comprehensive Blockchain-Based Secure Data Transmission Framework for Smart Grid applications. The proposed design:

- Enhances data integrity and confidentiality.
- Automates trust through smart contracts.

- Reduces reliance on centralized security models.
- Demonstrates strong performance under realistic loads.

9.2 Future Scope

Future work includes:

- Integrating **machine learning** for anomaly detection.
- Evaluating blockchain scalability with real-world Smart Grid deployments.
- Extending framework interoperability with standards such as IEEE 2030.5 and IEC 61850.
- Investigating **quantum-resistant cryptographic schemes** for future security.

10. References

1. A. R. Kovacs, “Smart Grid Security: Challenges and Opportunities,” *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 123–130, 2020.

2. M. Andoni, V. Robu, et al., “Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities,” *Renewable and Sustainable Energy Reviews*, vol. 100, pp. 143–174, 2019.

3. K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

4. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

5. H. Li, Z. Dai, et al., “Blockchain-Based Secure Data Transmission for Smart Grids,” *Journal of Information Security and Applications*, 2021.

6. N. Saxena, et al., “A Survey of Blockchain Security and Privacy Issues,” *IEEE Communications Surveys & Tutorials*, 2020.

7. Bansal, G., Dua, A., Aujla, G. S., Singh, M., & Kumar, N. (2019). *SmartChain: A Smart and Scalable Blockchain Consortium for Smart Grid Systems*. 1–6. https://doi.org/10.1109/iccw.2019.8757069

8. Lu, W., Ren, Z., Xu, J., & Chen, S. (2021). Edge Blockchain Assisted Lightweight Privacy-Preserving Data Aggregation for Smart Grid. *IEEE Transactions on Network and Service Management*, *18*(2), 1246–1259. https://doi.org/10.1109/tnsm.2020.3048822

9. Sikeridis, D., Bidram, A., Devetsikiotis, M., & Reno, M. J. (2020). *A blockchain-based mechanism for secure data exchange in smart grid protection systems*. 1–6. https://doi.org/10.1109/ccnc46108.2020.9045368

10. Olivares-Rojas, J. C., Reyes-Archundia, E., Gutierrez-Gnecchi, J. A., Cerda-Jacobo, J., & Gonzalez-Murueta, J. W. (2019). A Novel Multitier Blockchain Architecture to Protect Data in Smart Metering Systems. *IEEE Transactions on Engineering Management*, *67*(4), 1271–1284. https://doi.org/10.1109/tem.2019.2950410

11. Zhong, Y., Zhou, M., Li, J., Chen, J., Liu, Y., Zhao, Y., & Hu, M. (2021). Distributed Blockchain-Based Authentication and Authorization Protocol for Smart Grid. *Wireless Communications and Mobile Computing*, *2021*(1), 1–15. https://doi.org/10.1155/2021/5560621

12. Wang, W., Huang, H., Zhang, L., & Su, C. (2020). Secure and efficient mutual authentication protocol for smart grid under blockchain. *Peer-to-Peer Networking and Applications*, *14*(5), 2681–2693. https://doi.org/10.1007/s12083-020-01020-2

13. Alladi, T., Chamola, V., Rodrigues, J. J. P. C., & Kozlov, S. A. (2019). Blockchain in Smart Grids: A Review on Different Use Cases. *Sensors (Basel, Switzerland)*, *19*(22), 4862. https://doi.org/10.3390/s19224862

14. Duraipandi, O., & Velayudhan, T. A. (2024). A Novel Framework for Cloud Data Security with Blockchain Technology and Distributed Virtual Machine Agents. *June 2024*, *6*(2), 207–216. https://doi.org/10.36548/jitdw.2024.2.008

15. Asif, M., Aziz, Z., Bin Ahmad, M., Khalid, A., Waris, H. A., & Gilani, A. (2022). Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities. *Sensors (Basel,*

Switzerland), *22*(7), 2604. https://doi.org/10.3390/s22072604

16. Varshney, S., Vats, P., Choudhary, S., & Singh, D. (2022). *A Blockchain-based Framework for IoT based Secure Identity Management*. *4*, 227–234. https://doi.org/10.1109/iciptm54933.2022.9753887