

Cybersecurity in Smart Grids: An AI and Blockchain-Based Approach for Secure and Resilient Power Systems

Author: **Shaila Noor**

B.tech Electrical Engineering

College: Government Engineering College Ajmer Rajasthan India

Year: 2026

Co-Author- **Dr S.N Joshi**

Department of electrical engineering

Assistant professor

Government Engineering College Ajmer Rajasthan India

Abstract

The Smart Grid is an advanced electrical power system that integrates digital communication, Internet of Things (IoT), smart meters, sensors, and automated control technologies to improve the efficiency, reliability, and sustainability of electricity generation, transmission, and distribution. Although these technologies provide significant advantages, they also introduce serious cybersecurity risks. Cyber attacks such as malware, ransomware, false data injection, denial-of-service (DoS), and smart meter hacking can disrupt the power supply, cause financial losses, and threaten national security.

This research paper reviews the major cybersecurity challenges in Smart Grids and studies the latest protection techniques developed by researchers. Existing solutions, including cryptography, intrusion detection systems (IDS), blockchain technology, artificial intelligence (AI), and machine learning (ML), are analyzed. The paper identifies current research gaps and proposes a hybrid AI-Blockchain-based intrusion detection framework for improving Smart Grid security. Future research directions, including quantum-safe cryptography, edge computing, federated learning, and zero-trust security architecture, are also discussed.

The proposed framework aims to improve attack detection accuracy, reduce false alarms, protect consumer privacy, and ensure secure communication among Smart Grid devices. This study contributes to the development of more resilient and intelligent power systems capable of resisting modern cyber threats.

Keywords

- Smart Grid
- Cybersecurity
- Artificial Intelligence
- Machine Learning
- Blockchain
- Intrusion Detection System (IDS)
- SCADA
- IoT
- Smart Meter
- Power System Security
- False Data Injection Attack
- Denial of Service (DoS)
- Edge Computing

- Privacy Protection

1. Introduction

Electricity has become one of the most essential resources in modern society. Traditional power systems were designed mainly for one-way electricity flow, where power plants generated electricity and consumers simply received it. These conventional grids had limited communication capabilities and very little automation.

To overcome these limitations, Smart Grid technology was introduced.

A Smart Grid is an intelligent electricity network that combines electrical infrastructure with digital communication, sensors, IoT devices, smart meters, cloud computing, artificial intelligence, and automated control systems. Unlike conventional grids, Smart Grids allow two-way communication between consumers and utility companies, enabling real-time monitoring, automatic fault detection, demand response, renewable energy integration, and efficient energy management.

The increasing use of digital communication, however, has created new cybersecurity challenges. Since Smart Grids are connected through the Internet and communication networks, attackers may exploit software vulnerabilities to disrupt electricity services.

Cyber attacks on Smart Grids may result in:

- Large-scale power outages
- Financial losses
- Data theft
- Equipment damage
- Consumer privacy violations
- Threats to national security

Because of these risks, cybersecurity has become one of the most important research areas in Electrical Engineering.

Modern researchers are investigating various security technologies, including:

- Artificial Intelligence
- Machine Learning
- Deep Learning
- Blockchain
- Cryptography
- Intrusion Detection Systems
- Zero Trust Architecture
- Edge computing

Despite significant progress, existing security solutions still face challenges such as high computational cost, delayed attack detection, false alarms, and poor scalability. Therefore, more intelligent and adaptive cybersecurity frameworks are required.

This research focuses on understanding existing Smart Grid cyber threats, analyzing current protection mechanisms, identifying research gaps, and proposing an AI-Blockchain-based framework for future Smart Grid security.

1.1 Objectives of the Research

- To study the architecture of Smart Grid systems.
- To analyze major cybersecurity threats.
- To review existing security mechanisms.
- To identify limitations in current research.
- To propose an AI-Blockchain-based intrusion detection framework.
- To suggest future research directions.

2. Literature Review

2.1 Introduction

In recent years, Smart Grid cybersecurity has become one of the most active research areas in Electrical Engineering. The integration of IoT, Artificial Intelligence (AI), cloud computing, smart meters, and renewable energy has improved power system efficiency but has also increased cyber risks.

Researchers have proposed several techniques such as encryption, blockchain, machine learning, deep learning, intrusion detection systems (IDS), and zero-trust architectures. However, no single solution can completely secure Smart Grids against all cyber threats.

2.2 Research Progress (2022–2026)

2022: Machine Learning-Based Intrusion Detection

Research Focus

- Machine Learning algorithms were applied to detect cyber attacks in Smart Grid communication networks.

Algorithms Used

- Decision Tree
- Random Forest
- Support Vector Machine (SVM)
- K-Nearest Neighbor (KNN)

Advantages

- Better detection accuracy than rule-based systems.
- Automatic identification of abnormal network traffic.

Limitations

- Performance depends on high-quality labeled datasets.
 - Difficulty in detecting unknown (zero-day) attacks.
-

2023: Deep Learning for Smart Grid Security

Research Focus

- Machine Learning algorithms were applied to detect cyber attacks in Smart Grid communication networks.

Algorithms Used

- Decision Tree
- Random Forest
- Support Vector Machine (SVM)
- K-Nearest Neighbor (KNN)

Advantages

- Better detection accuracy than rule-based systems.
- Automatic identification of abnormal network traffic.

Limitations

- Performance depends on high-quality labeled datasets.
- Difficulty in detecting unknown (zero-day) attacks.

2023: Deep Learning for Smart Grid Security

Research Focus

- Deep Learning models were used for detecting complex cyber attacks.

Algorithms

- CNN
- RNN
- LSTM
- Autoencoders

Advantages

- Better performance on complex attack patterns.
- Lower false alarm rate.

Limitations

- Requires high computational power.
- Longer training time.

2024: Blockchain-Based Smart Grid Security

Research Focus

- Using Blockchain to secure Smart Grid transactions and protect data integrity.

Applications

- Smart Meter data protection
- Energy trading
- Consumer authentication

Advantages

- Tamper-resistant data.
- Decentralized trust.

Limitations

- Higher storage requirements.
- Increased transaction latency.

2025: AI + Edge Computing**Research Focus**

- Processing security data closer to devices using Edge Computing.

Benefits

- Faster attack detection.
- Reduced communication delay.
- Lower cloud dependency.

Challenges

- Limited computing resources at edge devices.
- Device management complexity.

2026: Hybrid AI + Blockchain Frameworks**Research Trend**

Recent studies increasingly combine AI with Blockchain to improve Smart Grid cybersecurity.

Expected Benefits

- Faster attack detection.
- Secure data sharing.
- Better privacy protection.
- Higher system reliability.

Current Challenges

- High computational overhead.
- Scalability.
- Real-time implementation in large Smart Grids.

Comparison of Existing Technologies

Technology	Advantages	Limitations
Cryptography	Strong data protection	Key management is difficult
Firewall	Blocks unauthorized access	Cannot detect insider attacks
IDS	Detects suspicious activities	False alarms
Machine Learning	Learns attack patterns	Needs training data
Deep Learning	Detects complex attacks	High computational cost
Blockchain	Data integrity and trust	Slow transactions
Edge Computing	Low latency	Limited resources
Zero Trust Security	Strong authentication	Complex implementation

2.4 Types of Cyber Attacks Studied

Researchers have mainly focused on the following attacks:

1. False Data Injection Attack (FDIA)

Attackers inject fake sensor values into the grid, leading to incorrect operational decisions.

2. Denial of Service (DoS)

The attacker floods communication channels, preventing normal data exchange.

3. Distributed Denial of Service (DDoS)

A large number of compromised devices simultaneously attack the Smart Grid.

4. Malware Attack

Malicious software infects Smart Grid systems, affecting operation.

5. Ransomware Attack

Critical data are encrypted by attackers, who then demand payment.

6. Smart Meter Hacking

Attackers manipulate meter readings, causing financial losses.

7. Phishing Attack

Utility employees are tricked into revealing login credentials.

8. Insider Attack

Authorized users misuse their privileges.

2.5 Research Gap

Despite significant progress, several important issues remain unresolved:

- Existing AI models require large labeled datasets.
- Zero-day attacks are still difficult to detect.
- Blockchain increases computational overhead.
- Most IDS models generate false positives.
- Edge devices have limited processing capability.
- Consumer privacy protection remains insufficient.
- Few studies integrate AI, Blockchain, and Edge Computing into one framework.

2.6 Proposed Research Direction

This research proposes a hybrid framework that combines:

- Artificial Intelligence
- Blockchain
- Edge Computing
- Intrusion Detection System (IDS)

Expected Benefits

- Faster attack detection.
- Reduced false alarms.
- Secure communication.
- Better privacy protection.
- Improved scalability.
- Real-time cybersecurity for Smart Grids.

Summary

The literature indicates that while AI, Machine Learning, Deep Learning, Blockchain, and Edge Computing have significantly improved Smart Grid cybersecurity, challenges such as zero-day attacks, computational overhead, scalability, and privacy remain open. These gaps motivate the development of a hybrid AI–Blockchain–Edge Computing framework capable of providing more robust and adaptive protection for future Smart Grids.

Problem Statement, Research Gap, Objectives and Proposed Framework

3. Problem Statement

Smart Grid technology has transformed the traditional power system into an intelligent and automated electricity network. However, this transformation has also increased the risk of cyber attacks due to the extensive use of Internet communication, IoT devices, cloud computing, smart meters, and remote monitoring systems.

Existing cybersecurity solutions such as firewalls, encryption, and traditional Intrusion Detection Systems (IDS) are not fully capable of detecting modern attacks such as:

- Zero-Day Attacks
- False Data Injection Attacks (FDIA)
- Distributed Denial of Service (DDoS)
- Smart Meter Tampering
- Advanced Persistent Threats (APT)
- Insider Attacks

Many existing Artificial Intelligence models also require large labeled datasets and consume significant computational resources. Similarly, Blockchain provides data integrity but introduces higher latency and computational overhead.

Therefore, there is a need for a hybrid cybersecurity framework that provides:

- Real-time attack detection
- High detection accuracy
- Low false alarm rate
- Secure data sharing
- Consumer privacy protection
- Scalability for large Smart Grids

4. Research Gap

From the literature review, the following research gaps have been identified:

Gap 1: Limited Detection of Unknown Attacks

Most current IDS models detect only attacks they have already been trained on, making zero-day attack detection difficult.

Gap 2: High Computational Cost

Deep Learning models require powerful hardware and are difficult to deploy on edge devices.

Gap 3: Blockchain Scalability Issues

Blockchain improves security but can increase processing time and reduce system performance in large Smart Grids.

Gap 4: Lack of Integrated Security

Most studies focus on only one technology (AI or Blockchain). Few combine AI, Blockchain, and Edge Computing into a unified framework.

Gap 5: Privacy Protection

Consumer electricity usage data can reveal personal behavior. Many systems still do not provide adequate privacy protection.

5. Research Objectives

The objectives of this research are:

1. To study the cybersecurity challenges in Smart Grids.
2. To analyze different types of cyber attacks.
3. To evaluate existing cybersecurity techniques.
4. To identify current research gaps.
5. To design a Hybrid AI–Blockchain Intrusion Detection Framework.
6. To improve attack detection accuracy.
7. To reduce false positive rates.
8. To secure Smart Meter communication.
9. To protect consumer privacy.
10. To enhance the resilience of future Smart Grids.

7. Research Hypothesis

H₁ (Alternative Hypothesis):

A Hybrid AI–Blockchain–Edge Computing Intrusion Detection System provides significantly better cybersecurity performance than traditional security methods in Smart Grids.

H₀ (Null Hypothesis):

There is no significant improvement in Smart Grid cybersecurity when using a Hybrid AI–Blockchain–Edge Computing Intrusion Detection System compared to existing approaches.

8. Proposed Framework

The proposed framework combines:

- Artificial Intelligence (AI)
- Blockchain
- Edge Computing
- Intrusion Detection System (IDS)

Working Process

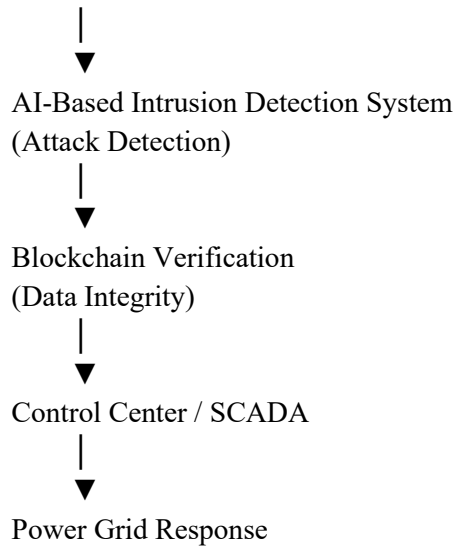
Smart Grid Devices



IoT Sensors & Smart Meters



Edge Computing Layer
(Local Data Processing)



Step 1: Data Collection

Smart Meters, IoT sensors, PMUs, and substations continuously generate data.

Step 2: Edge Computing

Instead of sending all data to the cloud, nearby edge devices process the data first. This reduces delay and bandwidth usage.

Step 3: AI-Based Detection

The AI model analyzes network traffic and sensor data to detect abnormal behavior such as malware, DDoS, or false data injection attacks.

Step 4: Blockchain Verification

Once the data are verified, they are stored securely using Blockchain to prevent tampering.

Step 5: Alert Generation

If an attack is detected, the system immediately sends alerts to the control center for rapid response.

10. Expected Advantages

- Real-time cyber attack detection
- High detection accuracy
- Reduced false alarms
- Secure communication
- Tamper-resistant data storage
- Low latency due to edge computing
- Better consumer privacy
- Improved system reliability
- Scalable for future Smart Grids

11. Innovation (Novel Contribution)

The key innovation of this research is the integration of **Artificial Intelligence, Blockchain, and Edge Computing** into a single cybersecurity framework for Smart Grids. Unlike approaches that rely on only one technology, this hybrid model aims to:

- Detect known and unknown attacks more effectively.
- Reduce the delay associated with centralized processing.
- Protect the integrity of operational data.
- Improve privacy and resilience without relying solely on cloud infrastructure.

Research Methodology

12. Research Methodology

12.1 Research Design

This research follows a **design-based experimental methodology**. The objective is to develop and evaluate a hybrid cybersecurity framework for Smart Grids by integrating Artificial Intelligence (AI), Blockchain, and Edge Computing.

The methodology consists of six major phases:

1. Data Collection
2. Data Preprocessing
3. AI-Based Attack Detection
4. Blockchain-Based Data Verification
5. Performance Evaluation
6. Comparative Analysis

Overall Research Flow

Smart Grid Devices

—|

—▼

Data Collection

—|

—▼

Data Preprocessing

—|

—▼

Feature Extraction

—|

—▼

AI-Based Attack Detection

—|

—▼

Blockchain Verification

—|

—▼

Alert Generation

—|

—▼

Performance Evaluation

Data Collection

The Smart Grid generates data from multiple sources:

- Smart Meters
- PMUs (Phasor Measurement Units)
- SCADA Systems
- IoT Sensors
- Renewable Energy Sources
- Distribution Substations

The collected data include:

- Voltage
- Current
- Frequency
- Power Consumption
- Network Traffic
- User Authentication Logs
- Event Logs
- Communication Packets

Data Preprocessing

Before training the AI model, the raw data are cleaned and prepared.

Steps:**Step 1**

Remove missing values.

Step 2

Remove duplicate records.

Step 3

Normalize numerical values.

Step 4

Encode categorical variables.

Step 5

Split the dataset:

- Training Data (70%)
- Testing Data (30%)

15. Feature Extraction

- Important features include:

Feature	Description
Voltage	Power system voltage
Current	Line current
Frequency	Grid frequency
Packet Size	Network traffic size
Login Attempts	Authentication records
Smart Meter ID	Device identification
Response Time	Communication delay
Energy Consumption	Consumer usage
16. AI Algorithms	
The proposed framework evaluates multiple machine learning algorithms.	
Random Forest	
Advantages:	
• High accuracy • Fast prediction	

Handles missing data well	
XGBoost Advantages: - Excellent classification performance - Handles complex data relationships - Efficient for structured datasets LSTM (Long Short-Term Memory) Advantages: - Suitable for time-series data - Detects sequential attack patterns - Useful for Smart Grid monitoring	
Autoencoder Advantages: - Detects anomalies - Works well for unknown attacks - Learns normal system behavior	

17. Blockchain Module

Blockchain is used after AI detection.

Functions:

- Secure data storage
- Tamper-proof records
- Transaction verification
- Identity validation

- Distributed trust

Consensus mechanism (example):

- Practical Byzantine Fault Tolerance (PBFT)
-

18. Edge Computing Layer

Instead of sending all data to a central cloud:

- Data are processed near substations.
 - Attack detection is faster.
 - Network delay is reduced.
 - Bandwidth usage decreases.
-

19. Performance Evaluation Metrics

The effectiveness of the proposed framework will be measured using:

Accuracy

Percentage of correctly classified samples.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision

Percentage of predicted attacks that are actually attacks.

$$\text{Precision} = \frac{TP}{TP + FP}$$

Recall

Percentage of actual attacks correctly detected.

$$\text{Recall} = \frac{TP}{TP + FN}$$

F1 Score

Harmonic mean of Precision and Recall.

$$F1 = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

Detection Time

Time required to detect an attack.

False Positive Rate

Percentage of normal events incorrectly classified as attacks.

20. Simulation Tools

The framework can be implemented using:

Tool	Purpose
Python	AI and Machine Learning
MATLAB/Simulink	Smart Grid Simulation
NS-3	Network Attack Simulation
OMNeT++	Communication Network Modeling
Hyperledger Fabric	Blockchain Implementation
Wireshark	Network Packet Analysis
Scikit-learn	Machine Learning
TensorFlow	Deep Learning
PyTorch	Neural Network Development

21. Experimental Setup

Hardware

- Intel Core i5/i7 Processor
- 16 GB RAM
- SSD Storage
- GPU (optional for deep learning)

Software

- Windows/Linux
- Python 3.x
- MATLAB
- Visual Studio Code
- Jupyter Notebook

22. Proposed Algorithm

1. Collect Smart Grid data.
2. Clean and preprocess the data.
3. Extract relevant features.
4. Train the AI model.
5. Detect abnormal behavior.
6. Verify critical records using Blockchain.

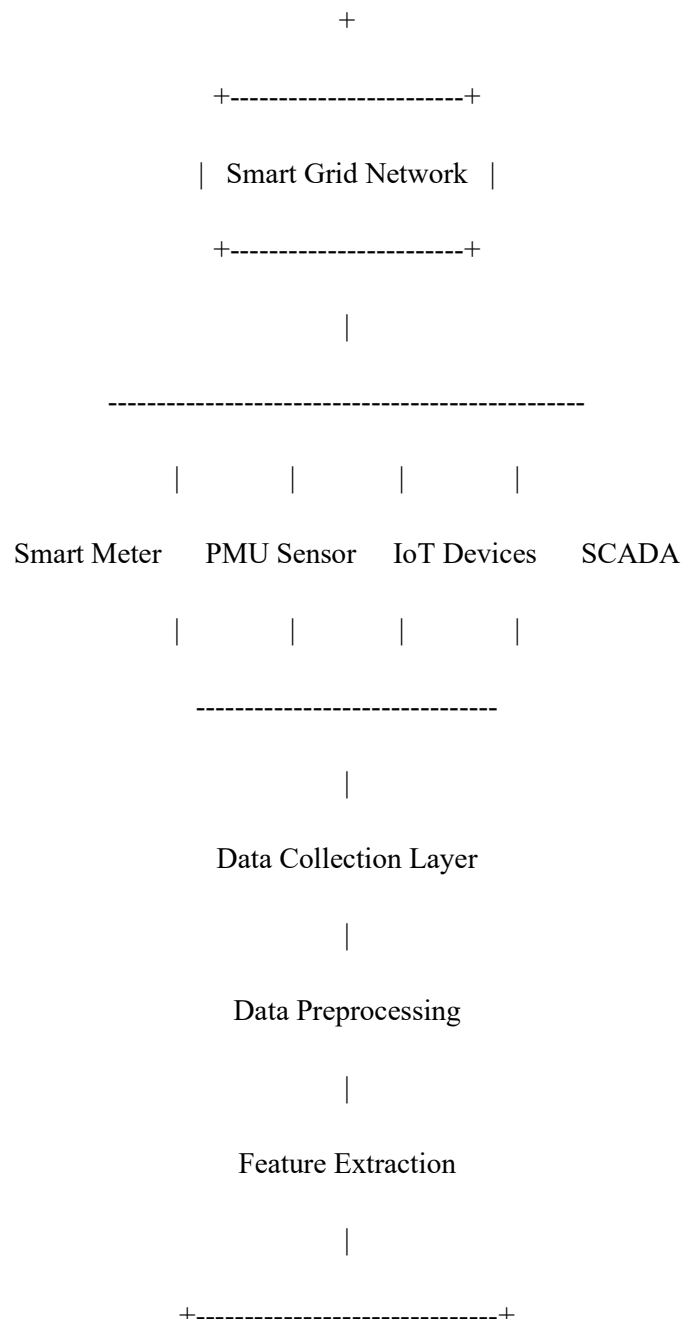
7. Generate alerts for suspicious activities.
8. Store verified events securely.
9. Evaluate performance using Accuracy, Precision, Recall, and F1 Score.
10. Compare results with existing methods.

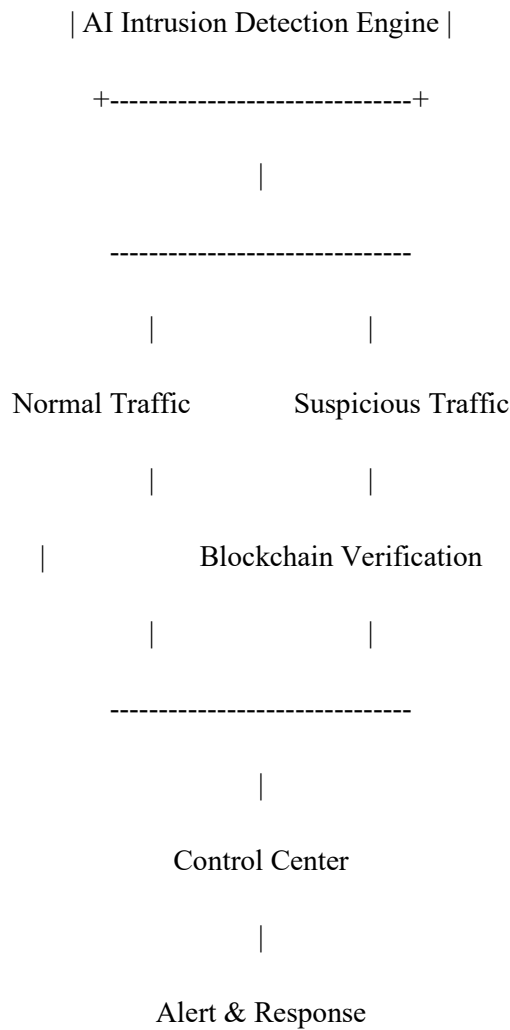
23. Expected Results

The proposed framework is expected to:

- Increase attack detection accuracy.
- Reduce false positives.
- Detect attacks more quickly.
- Improve data integrity through Blockchain.
- Lower communication delay using Edge Computing.
- Enhance privacy and overall Smart Grid resilience.

Proposed System Architecture





32. Conclusion

The increasing digitization of Smart Grids has significantly improved the efficiency and reliability of modern power systems, but it has also expanded the cyber attack surface. Existing security mechanisms often struggle with evolving threats such as zero-day attacks, false data injection, and large-scale distributed attacks.

This research proposes a hybrid framework integrating Artificial Intelligence, Blockchain, and Edge Computing to enhance Smart Grid cybersecurity. The proposed approach aims to improve attack detection, strengthen data integrity, reduce detection latency, and protect consumer privacy. Although the framework requires experimental validation, it provides a structured direction for building more secure and resilient Smart Grids.

. Expected Results

The proposed Hybrid Artificial Intelligence and Blockchain-based Cybersecurity Framework is expected to significantly improve the security, reliability, and resilience of Smart Grid systems. By integrating AI-based intrusion detection with Blockchain-enabled secure data management, the framework aims to detect cyber attacks at an early stage while maintaining data integrity and protecting consumer privacy.

The AI-based Intrusion Detection System (IDS) is expected to accurately identify both known and unknown cyber attacks, including False Data Injection Attacks (FDIA), Distributed Denial of Service (DDoS), malware, ransomware, insider attacks, and smart meter tampering. Compared with conventional security mechanisms, the proposed framework is expected to reduce false alarms and improve the overall detection rate.

Blockchain technology is expected to provide a decentralized and tamper-resistant platform for storing critical Smart Grid data. This ensures that unauthorized users cannot modify operational records, thereby improving trust and transparency within the power system.

The Edge Computing layer is expected to reduce communication latency by processing data closer to the source. This enables faster attack detection and minimizes the delay associated with cloud-based processing.

Overall, the proposed framework is expected to:

- Improve cyber attack detection accuracy.
- Reduce false positive rates.
- Enhance data integrity through Blockchain.
- Minimize response time.
- Protect consumer privacy.
- Increase the reliability and resilience of Smart Grid operations.

7. Advantages of the Proposed Framework

The proposed Hybrid AI–Blockchain Cybersecurity Framework offers several advantages over traditional Smart Grid security solutions.

- Real-time detection of cyber attacks.
- High accuracy in identifying malicious activities.
- Secure and tamper-proof data storage using Blockchain.
- Reduced communication delay through Edge Computing.
- Enhanced consumer privacy and data confidentiality.
- Improved scalability for large Smart Grid networks.
- Better resistance against advanced cyber threats.

9. Future Scope

Cybersecurity in Smart Grids is an evolving research area, and several opportunities exist for future work.

Future research may focus on:

- Integration of Quantum Cryptography for next-generation security.
- Application of Explainable Artificial Intelligence (XAI) to improve decision transparency.
- Development of Federated Learning models for privacy-preserving attack detection.
- Adoption of Digital Twin technology for real-time cyber risk assessment.
- Implementation of Zero Trust Security Architecture.
- Integration with 6G communication networks.
- Development of self-healing Smart Grid systems capable of automatic cyber attack recovery.
- Enhancement of energy trading security using advanced Blockchain platforms.

10. Conclusion

Smart Grids have revolutionized modern power systems by integrating advanced communication technologies, automation, Internet of Things (IoT), and Artificial Intelligence. However, this digital transformation has also introduced significant cybersecurity challenges that threaten the stability, reliability, and safety of electrical power systems.

This research reviewed the major cyber threats affecting Smart Grids and analyzed existing cybersecurity solutions, including cryptography, Intrusion Detection Systems (IDS), Artificial Intelligence, Machine Learning, Blockchain, and Edge Computing. The study identified several research gaps, including limited detection of zero-day attacks, high computational overhead, privacy concerns, and scalability issues.

To address these challenges, a Hybrid Artificial Intelligence and Blockchain-based Cybersecurity Framework was proposed. The framework combines AI-based attack detection, Blockchain-enabled data integrity, and Edge Computing for real-time analysis. The proposed approach aims to improve attack detection accuracy, reduce false alarms, enhance consumer privacy, and strengthen the overall resilience of Smart Grid infrastructure.

In conclusion, the proposed framework represents a promising direction for future Smart Grid cybersecurity research. Further validation through simulations and real-world implementation can demonstrate its effectiveness in protecting next-generation intelligent power systems against increasingly sophisticated cyber threats.

Acknowledgement

I would like to express my sincere gratitude to everyone who supported and guided me throughout the completion of this research paper entitled **"Cybersecurity in Smart Grids: An AI and Blockchain-Based Approach for Secure and Resilient Power Systems."**

First and foremost, I would like to thank my project guide and faculty members of the Department of Electrical Engineering for their valuable guidance, continuous encouragement, and constructive suggestions during this research work. Their knowledge and support helped me understand the subject in greater depth.

I would like to extend my appreciation to the authors, researchers, and publishers whose published research papers, books, and technical articles provided valuable insights and references for this work.

Finally, I express my heartfelt gratitude to my family and friends for their constant motivation, patience, and encouragement throughout the preparation of this research paper.

This work has greatly enhanced my understanding of Smart Grid cybersecurity, Artificial Intelligence, Blockchain technology, and modern power system security.

References

- [1] J. Ruan, G. Liang, J. Zhao, H. Zhao, J. Qiu, F. Wen, and Z. Y. Dong, "Deep Learning for Cybersecurity in Smart Grids: Review and Perspectives," *Energy Conversion and Economics*, vol. 4, pp. 233–251, 2023. doi: 10.1049/enc2.12091.
- [2] T. Alladi, V. Chamola, J. J. P. C. Rodrigues, and S. A. Kozlov, "Blockchain in Smart Grids: A Review on Different Use Cases," *Sensors*, vol. 19, no. 22, p. 4862, 2019. doi: 10.3390/s19224862.
- [3] V. K. Mololoth, S. Saguna, and C. Åhlund, "Blockchain and Machine Learning for Future Smart Grids: A Review," *Energies*, vol. 16, no. 1, p. 528, 2023. doi: 10.3390/en16010528.
- [4] "Artificial Intelligence and Blockchain Technology for Secure Smart Grid and Power Distribution Automation: A State-of-the-Art Review," *Sustainable Energy Technologies and Assessments*, vol. 57, 103282, 2023. doi: 10.1016/j.seta.2023.103282.

- [5] “Review on Cyber-Physical and Cyber-Security System in Smart Grid: Standards, Protocols, Constraints, and Recommendations,” *Journal of Network and Computer Applications*, vol. 209, 103540, 2023. doi: 10.1016/j.jnca.2022.103540.
- [6] “Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions,” *Energies*, vol. 15, no. 18, p. 6799, 2022. doi: 10.3390/en15186799.
- [7] “Cybersecurity and Resilience of Smart Grids: A Review of Threat Landscape, Incidents, and Emerging Solutions,” *Applied Sciences*, 2026.
- [8] “Cybersecurity in Smart Grids: A Domain-Centric Review,” *Systems*, vol. 13, no. 12, 2025.
- [9] “AI-Powered Cybersecurity for Smart Grid Communication: A Systematic Review of Intrusion Detection and Threat Mitigation Systems,” *Energy Conversion and Management: X*, vol. 29, 101416, 2026. doi: 10.1016/j.ecmx.2025.101416.
- [10] H. Lakhal, M. Zegrari, and A. Bahasse, “Next-Generation Smart Grid Cybersecurity: A Systematic Review of OT Cyber Threats, AI-Driven Defense, Cyber Deception Techniques, and Emerging Security Strategies,” *IEEE Access*, vol. 13, 2025. doi: 10.1109/ACCESS.2025.3623834.
- [11] T. Zheng, M. Liu, D. Puthal, P. Yi, Y. Wu, and X. He, “Smart Grid: Cyber Attacks, Critical Defense Approaches, and Digital Twin,” *arXiv*, 2022.
- [12] A. Zibaeirad, F. Koleini, S. Bi, T. Hou, and T. Wang, “A Comprehensive Survey on the Security of Smart Grid: Challenges, Mitigations, and Future Research Opportunities,” *arXiv*, 2024.