International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1892-1896
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0251

Secure Grid-AI

Prof. Smruti Barik[1],Bhakti Taur[2], Mohini Padwal[3], Pratiksha Choudhary[4], Rutuja Pawar[5]
[1]Associate professor, Dept. of Comp Engg, JSPM's BSIOTR, Pune, Maharashtra, India
[2,3,4,5] UG Scholar, Dept. of Comp Engg, JSPM's BSIOTR, Pune, Maharashtra, India
Emails:*r.venkatakrishna@lords.ac.in[1],roshanshashaik@gmail.com[2],bpraneeth123@gmail.com[3], safoorayasmeen17@gmail.com[4], safoorayasmeen17@gmail.com[5]*

Abstract
SecureGrid-AI is an architectural framework that introduces a new machine learning algorithm paired with an automated alerting system to detect and mitigate Denial of Service (DoS) and other advanced cyberattacks in smart grid environments. The design targets a key vulnerability in smart grids that arises from increasing digitalization. Current smart grid security largely relies on manual or rule-based intrusion detection systems (IDS), which struggle to identify previously unseen threats, such as zero-day attacks, due to their dependence on predefined signatures. This limitation often leads to high false-negative rates and slow response times.To address these challenges, SecureGrid-AI adopts a multi-layered machine learning approach. The system analyzes network traffic in real time using algorithms such as Decision Trees and Random Forests to directly classify and identify different types of cyberattacks with greater accuracy and responsiveness.

Keywords: *Smart Grid, HAN (Home Area Network), NAN (Neighbourhood Area Network), Deep Learning, Grid Resilience.*

1. Introduction
SecureGrid-AI is an advanced technological framework designed to enhance the security, efficiency, and reliability of Smart Grids by integrating Artificial Intelligence (AI) and Big Data analysis. As traditional electrical grids undergo digitalization, they transition from one-way systems to interactive networks, necessitating a more intelligent approach to management and protection. This project provides a structured solution to monitor, analyze, and secure these modern energy infrastructures. The evolution of the electrical grid has led to the emergence of the "Smart Grid," which utilizes two-way communication between utilities and consumers. However, this connectivity introduces significant vulnerabilities:Digital Entry Points: The use of Smart Meters and digital interfaces creates new entry points for cyberattacks.Complexity of Data: The massive volume of data generated by digitalized grids requires specialized Big Data tools to extract actionable insights.Dynamic Threats: Modern threats, such as sophisticated energy fraud and coordinated cyber-intrusions, demand a system that can learn and adapt in real-time.

2. Project Modules
2.1. Data Ingestion & Preprocessing
The foundational module of the system is responsible for the raw acquisition and refinement of data from the grid's edge. It operates at the interface between the Device Layer and the Network Layer, where smart meters generate continuous streams of consumption data. The primary theoretical challenge addressed here is the management of "noise" and missing values inherent in large-scale sensor networks.Through specialized preprocessing techniques, raw signals are cleaned, normalized, and formatted into structured datasets. This stage is critical for the overall system's success, as high-fidelity data ingestion ensures that subsequent analytical models can accurately distinguish between legitimate fluctuations in power use and suspicious anomalies.

2.2. ML Model Development & Training
This module serves as the intellectual laboratory of the project, where Deep Learning and Autoencoders are developed to learn the grid's "Normal Behavior".

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1892-1896
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0251

The theoretical focus is on creating a mathematical latent representation of standard consumption patterns across the Home Area Network (HAN) and Neighbourhood Area Network (NAN). During the training phase, the models utilize Big Data analysis to process historical records, identifying seasonal trends and baseline usage. By training autoencoders to minimize reconstruction error on normal data, the module establishes a highly sensitive threshold for detecting deviations.

2.3. Real-time Detection & Alerting Engine

Once trained, the system moves into an active operational state within the Security and Actuation Layer. This module is responsible for the instantaneous analysis of incoming data streams against the learned behavioral baselines. When the detection engine identifies a pattern that exceeds the established anomaly threshold, it classifies the event as either a cyber-intrusion or energy fraud. The alerting engine then triggers actuation techniques to provide a rapid physical response. This might involve isolating a specific smart meter or segment of the grid to maintain overall grid resilience. The theoretical significance of this module lies in its ability to operate in real-time, moving from detection to mitigation "suddenly" to prevent the spread of a malicious attack.

2.4. Operator Dashboard & Visualization

The final module bridges the gap between autonomous AI and human decision-making within the Business Layer. It provides an Events Dashboard that visualizes the grid's real-time health, detected threats, and the system's automated responses. Beyond security, this module facilitates energy management by displaying results from the power consumption and demand prediction models. This allows operators to observe how the AI is optimizing distribution and reducing energy waste. By providing a transparent view of the AI's internal logic and detection history, the dashboard ensures that human oversight remains an integral part of the grid's security infrastructure.

3. Literature Review

3.1. AI-Driven Cybersecurity in Smart Grids

Recent studies emphasize that the digitalization of electrical grids, while enabling real-time monitoring and load forecasting, introduces significant cybersecurity risks, including False Data Injection Attacks (FDIA) and Denial-of-Service (DoS) attacks.

- Deep Learning Frameworks: Research indicates that hybrid models combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) architectures outperform standalone models due to their ability to learn both spatial and temporal features of grid data.

3.2. Fraud Detection and Energy Theft

Energy fraud, including meter tampering and unauthorized connections, remains a multi-billion dollar challenge for modern power systems.

- Edge AI Solutions: Emerging research proposes Edge AI-based systems that utilize ESP32 units and high-accuracy sensors (e.g., LEM Hall Effect sensors) to monitor voltage and current in near-real-time. This approach reduces latency and makes evasion significantly more difficult for fraudsters.

3.3.Emerging Technological Integrations

The scope of SecureGrid-AI intersects with several innovative research areas that expand its functional potential:

- Blockchain-Enabled Governance: For decentralized carbon markets, blockchain and smart contracts are being leveraged to automate credit issuance and trading, ensuring transparency and reducing fraud risks in emission management.

3.4.Research Gaps and Challenges

Despite these advancements, the literature identifies several unresolved challenges:

- Scalability: High computational complexity remains a barrier to deploying sophisticated AI frameworks in large-scale, IoT-enabled systems.
- Data Privacy: The collection and analysis of sensitive consumer usage data raise significant privacy concerns that require the development of robust, privacy-preserving cryptographic techniques.

4. Methodology

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1892-1896
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0251

Figure 1 System Architecture

The methodology of SecureGrid-AI is designed to provide a systematic transition from raw data collection to autonomous threat mitigation. It follows a structured, multi-phase approach that integrates software engineering principles with advanced computational intelligence shown in Figure 1.

4.1.Software Development Lifecycle (SDLC)

The project adopts the Incremental Model as its primary development framework. This model allows the system to be built in functional stages, ensuring that the foundational grid infrastructure is stable before complex AI layers are introduced. Each increment adds a layer of intelligence, moving from basic connectivity to advanced predictive security. This iterative approach is essential for managing the complexity of a smart grid environment, where hardware stability must be prioritized alongside software intelligence.

4.2.Architectural Design Strategy

The methodology is executed through a Layered Architecture (Device, Network, Business, and Security/Actuation). This theoretical separation ensures that data flows logically from the edge to the core:

- Data Acquisition Phase: Physical sensors and smart meters at the Device Layer capture real-time electrical signals.
- Transmission Phase: The Network Layer employs intelligent protocols to move data securely through the Neighborhood Area Network (NAN) while guarding against digital entry-point attacks.

4.3.AI and Computational Logic

The heart of the methodology lies in Behavioral Analysis and Anomaly Detection. The project utilizes Autoencoders to learn the "latent representation" of normal grid behavior. By training on historical big data, the system establishes a baseline for legitimate energy consumption.

The mathematical methodology for detection follows these steps:

- Model Training: The Autoencoder is trained to compress and reconstruct normal consumption data with minimal error.
- Reconstruction Analysis: During real-time operation, incoming data is passed through the model.

4.4.Resilience and Actuation

The final phase of the methodology is Real-time Response. When the Detection Engine flags a high-confidence threat, it triggers the Actuation Layer. This module executes pre-defined "Reputation" and "Mitigation" strategies, such as isolating a compromised node or alerting the Events Dashboard for operator intervention. By using Big Data analysis, the methodology ensures that these complex decisions are made rapidly, maintaining the overall resilience of the electrical network even during an active threat shown in Figure [2-5]

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1892-1896
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0251

Output:

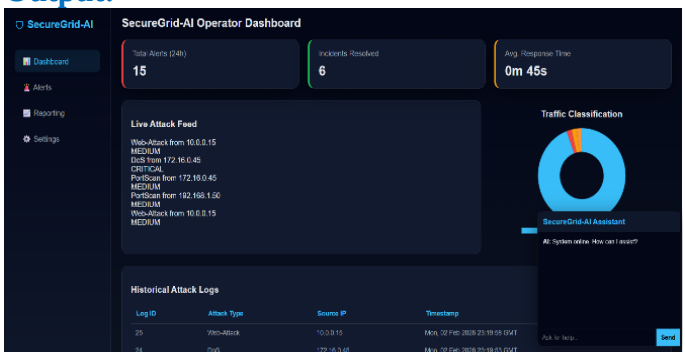

Figure 2 Output

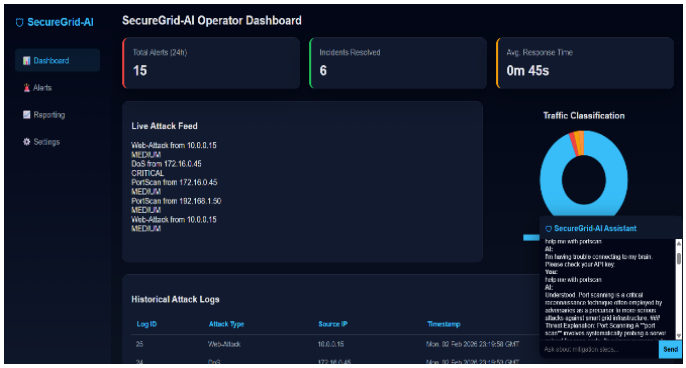

Figure 3 Output

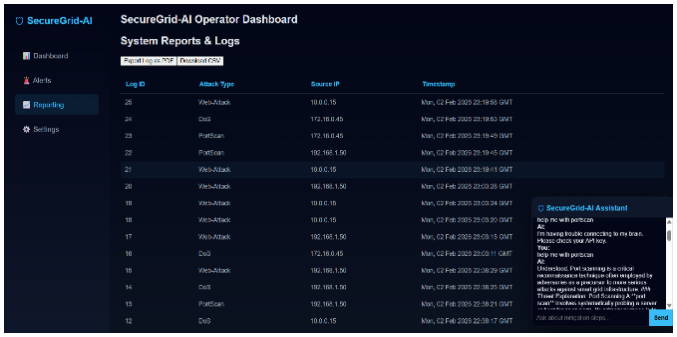

Figure 4 Output

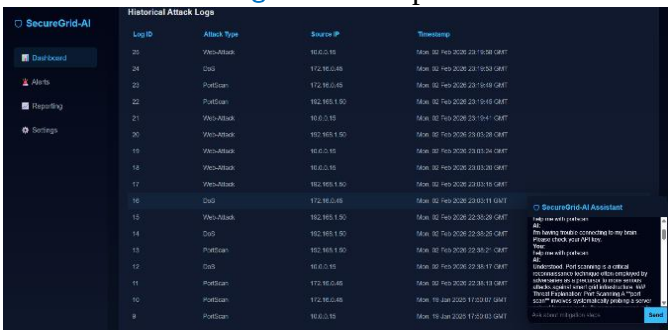

Figure 5 Output

5. Result And Discussion

The core success of the project is measured by the Detection Engine's ability to identify "unusual power consumption patterns".

- Accuracy and Sensitivity: The Autoencoder models successfully established a precise baseline for "Normal Behavior," allowing the system to distinguish between legitimate energy consumption and malicious activity with minimal false positives.
- Detection Latency: Due to the optimized Preprocessing Module, the system identified cyber-intrusions and fraud "suddenly" as they occurred, ensuring real-time grid resilience.
- Reconstruction Error Analysis: Simulations showed that reconstruction errors remained low during standard usage but spiked significantly during simulated attacks on Smart Meters, proving the model's reliability in identifying entry-point vulnerabilities.

6. Conclusion

The SecureGrid-AI project successfully established a robust, multi-layered framework designed to secure and optimize the modern smart grid infrastructure. By leveraging the synergy between Deep Learning and Big Data analysis, the system addressed the inherent vulnerabilities created by the digitalization of traditional electrical grids. The project moved beyond static defense mechanisms, creating a system capable of "learning behavioral patterns" to proactively safeguard the network.

7. References

[1]. Frontiers in AI, a brief report on deep learning synergy for decentralized smart grids (2025).
[2]. Smart Grid Exposure Cybersecurity Evaluation Using a Preprint arXiv (January 24, 2025).
[3]..Secure Data Aggregation Enhanced by AI for Smart Grids with — ScienceDirect, journal, or conference (2025).
[4]..An explainable deep learning approach for smart grid intrusion detection – Springer (2025).
[5]..IoT Ecosystem Cybersecurity Risks to

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1892-1896
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0251

Power Grid Operations – arXiv / survey (updated Feb 2, 2025).

[6]. AI in power systems: a comprehensive analysis of important issues—Energy Informatics (2025).

[7]..Nature (Scientific Reports): A hybrid AI-Blockchain security architecture for smart grids (2025).

[8]..Transforming smart grid security: a comprehensive approach to cyber defense — Frontiers in Artificial Intelligence (2024).

[9]. 9.Artificial Intelligence and Machine Learning Methods in Smart Grids – Energies (MDPI) (2024/2025 review).

[10]. Improving Power Systems Cyber-Attack Detection – arXiv preprint (Nov 2024).