IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 1, December 2025

Impact Factor: 7.67

SecureGrid: Ensemble Learning Approach For Intrusion Detection

Raashid Ahmed R[1], Arpitha S[2], Sanjeevini B M[3], Varshini P[4], Prof. Harsha B R[5]

Students, Dept.Information Science and Engineering[1-4]
Assistant Professor, Dept.Information Science and Engineering[5]
Global Academy of Technology, Bengaluru, India
raashidahmed111@gmail.com, arpithasp444@gmail.com, sanjeevinimenasagi@gmail.com
varshini01p@gmail.com, harsha.br@gat.ac.in

Abstract: *Smart grids, as the next generation of electrical networks, are highly dependent on advanced communication and control systems, making them vulnerable to a wide range of cyber threats. Ensuring the security and reliability of these networks is crucial for stable power delivery and infrastructure protection. This study proposes an artificial intelligence-based ensemble modeling approach for intrusion detection in smart grids. By integrating multiple machine learning algorithms, the ensemble model leverages the strengths of individual classifiers to enhance detection accuracy and reduce false alarms. Experimental evaluations on benchmark smart grid datasets demonstrate that the proposed method effectively identifies both known and emerging cyber attacks, outperforming traditional single-classifier systems. The results highlight the potential of AI-driven ensemble techniques to strengthen smart grid cybersecurity and support the development of resilient energy infrastructures.*

Keywords*:* Smart Grids, Intrusion Detection System (IDS), Cybersecurity, Artificial Intelligence (AI), Machine Learning, Ensemble Modeling, Anomaly Detection, Network Security, Power Systems Security, Cyber Attack Detection

I. INTRODUCTION

The rapid evolution of power systems has led to the development of smart grids, which integrate advanced communication, automation, and control technologies to improve efficiency, reliability, and sustainability in electricity distribution. Unlike traditional grids, smart grids rely heavily on interconnected digital devices and communication networks, which makes them susceptible to a variety of cyber threats. Ensuring the security of these networks is critical, as any disruption can have significant economic and societal consequences.

Intrusion detection systems (IDS) play a pivotal role in protecting smart grids by monitoring network traffic and identifying malicious activities. Conventional IDS approaches, however, often struggle to detect sophisticated and evolving cyber-attacks due to their reliance on static rules or single-classifier models. These limitations necessitate more intelligent and adaptive methods capable of recognizing both known and novel threats in real time.

Artificial intelligence (AI) and machine learning (ML) have emerged as powerful tools for enhancing intrusion detection in smart grids. By learning patterns of normal and abnormal behavior from historical data, AI-based models can identify anomalies that may indicate cyber attacks. However, individual machine learning algorithms can sometimes be prone to overfitting or fail to generalize across different types of attacks, reducing detection accuracy.

Ensemble modeling, which combines multiple machine learning algorithms, offers a robust solution to this challenge. By aggregating the predictions of diverse classifiers, ensemble methods can exploit the strengths of each algorithm while mitigating their individual weaknesses. This approach has shown significant promise in improving detection rates, reducing false alarms, and adapting to the dynamic nature of smart grid environments.

This study focuses on developing an AI-based ensemble intrusion detection system for smart grids. The proposed system aims to enhance security by effectively identifying various cyber threats, including both known and emerging attacks. Through experimental evaluation on benchmark datasets, the study demonstrates that ensemble modeling can

DOI: 10.48175/IJARSCT-30123

outperform traditional IDS approaches, providing a more reliable and resilient solution for safeguarding critical smart grid infrastructure.

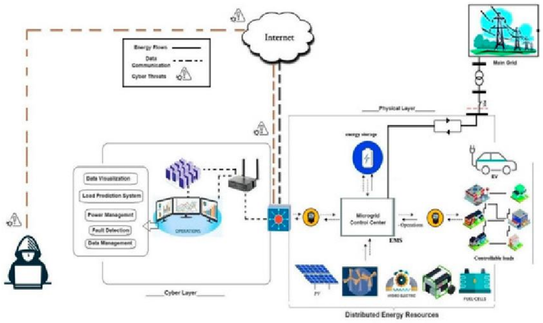

Figure 1: Detecting False Data Injection Attacks Using Machine Learning

The increasing integration of digital communication and control technologies in smart grids has significantly improved the efficiency and reliability of power distribution, but it has also introduced new cybersecurity vulnerabilities. Smart grids are highly susceptible to cyber-attacks such as data injection, denial-of-service, and malware infiltration, which can disrupt power delivery, compromise sensitive information, and cause substantial economic losses. Traditional intrusion detection systems often rely on static rules or single machine learning classifiers, limiting their ability to detect complex, evolving, or previously unknown attacks. This lack of adaptability and low detection accuracy poses a major challenge to securing smart grid infrastructure. Therefore, there is a critical need for intelligent and robust intrusion detection solutions capable of accurately identifying a wide range of cyber threats in real time, minimizing false alarms, and enhancing the overall resilience of smart grids.

To address the limitations of traditional intrusion detection in smart grids, this study proposes an artificial intelligence-based ensemble modeling approach. The proposed system combines multiple machine learning algorithms, leveraging the strengths of each to improve detection accuracy and reduce false positives. By integrating diverse classifiers, the ensemble model can identify both known and previously unseen cyber-attacks, adapting to the dynamic nature of smart grid networks. The approach involves preprocessing smart grid network data, extracting relevant features, and training the ensemble model to recognize patterns of normal and malicious activity. Experimental evaluation on benchmark datasets is conducted to validate the effectiveness of the proposed method, demonstrating enhanced performance compared to single-classifier systems and conventional IDS techniques. This AI-driven ensemble approach aims to provide a robust, reliable, and scalable solution for safeguarding smart grid infrastructures against evolving cyber threats.

II. RELATED WORKS

The integration of Artificial Intelligence (AI) and Machine Learning (ML) into intrusion detection systems (IDS) for smart grids has garnered significant attention in recent years. Traditional IDS approaches often rely on single classifiers, which may not effectively capture the complex and evolving nature of cyber threats in smart grid environments. To address these limitations, researchers have explored ensemble learning techniques, which combine multiple classifiers to improve detection accuracy and robustness.

A notable study by Alsirhani et al. (2025) proposed a fog-based AI framework utilizing ML and Deep Learning (DL)-based ensemble models to enhance intrusion detection in smart grid networks. The proposed system demonstrated improved accuracy in detecting intrusions by leveraging the strengths of multiple classifiers. This approach highlights the potential of ensemble learning in enhancing the security of smart grids

In a similar vein, AlHaddad et al. (2023) introduced a hybrid deep learning approach combining Convolutional Neural Networks (CNNs) and Gated Recurrent Units (GRUs) to detect Distributed Denial-of-Service (DDoS) attacks on smart grid communication infrastructure. Their method achieved a high accuracy rate of 99.86%, underscoring the effectiveness of combining different deep learning models for intrusion detection in smart grids

DOI: 10.48175/IJARSCT-30123

Another significant contribution by Alsirhani et al. (2025) involved the development of an ensemble model using classifiers such as Logistic Regression (LR), Random Forest (RF), K-Nearest Neighbors (KNN), Naive Bayes (NB), and Support Vector Machine (SVM). The model was evaluated using two datasets: the CIC-IDS-Collection and a Power System Intrusion dataset specifically designed for smart grid environments. The ensemble model demonstrated superior performance in terms of accuracy, precision, recall, and F1 scores compared to individual classifiers, highlighting the advantages of ensemble learning in smart grid intrusion detection

These studies collectively underscore the efficacy of AI-based ensemble modeling in enhancing intrusion detection systems for smart grids. By leveraging the strengths of multiple classifiers, ensemble methods can provide more accurate and reliable detection of cyber threats, thereby improving the security and resilience of smart grid infrastructures.

Data Collection and Preprocessing: The first module focuses on gathering network traffic and operational data from the smart grid environment. This data may include measurements from smart meters, substation sensors, and communication networks. Preprocessing steps such as normalization, missing value handling, and noise reduction are performed to ensure the data is clean and suitable for training. Feature selection techniques are applied to extract the most relevant attributes that can effectively distinguish between normal and malicious activities. This module is critical, as the quality of input data directly impacts the accuracy of the intrusion detection system.

Feature Extraction and Selection: In this module, important patterns and characteristics are extracted from the preprocessed data. Various statistical and machine learning-based methods, such as Principal Component Analysis (PCA) or Mutual Information, can be used to reduce dimensionality while retaining critical information. By selecting the most informative features, the system reduces computational complexity and enhances detection performance. This step ensures that the ensemble model receives high-quality, meaningful input for effective classification of network events.

Individual Classifier Training: The third module involves training multiple machine learning classifiers individually. Common algorithms include Random Forest (RF), Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Logistic Regression (LR). Each classifier is trained to identify normal and anomalous network behavior based on the extracted features. By allowing each model to specialize in detecting certain patterns, the ensemble benefits from diverse perspectives, which improves overall system accuracy and reduces the risk of misclassification.

Ensemble Model Construction: This module combines the predictions from all trained classifiers to form the ensemble model. Techniques such as majority voting, weighted averaging, or stacking can be used to aggregate the outputs. The ensemble approach leverages the strengths of individual models while compensating for their weaknesses. This integration ensures that the final detection system is robust, capable of identifying a wide range of cyber attacks, and more reliable than any single classifier approach.

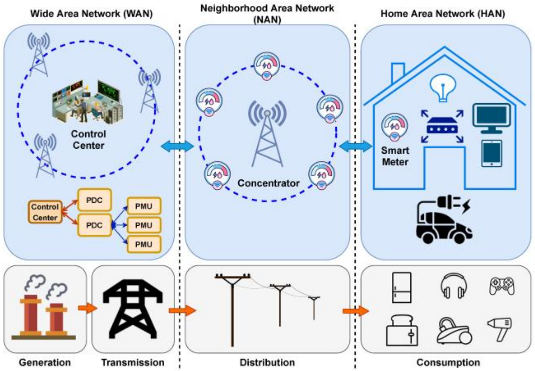

Figure 2: Detecting Cyber Attacks in Smart Grids

Intrusion Detection and Alert Generation: The final module deploys the ensemble model in a real-time smart grid environment for monitoring and detection. The system continuously analyzes incoming network traffic, classifying events as normal or suspicious. Upon detection of a potential threat, alerts are generated and sent to network administrators for further action. This module ensures timely response to cyber-attacks, enhancing the security and resilience of smart grid infrastructure.

Performance Evaluation: This optional but important module evaluates the performance of the intrusion detection system using metrics such as accuracy, precision, recall, F1-score, and false positive rate. Benchmark datasets and real-world smart grid traffic can be used for validation. This step helps in fine-tuning the ensemble model and ensuring it meets the desired security standards.

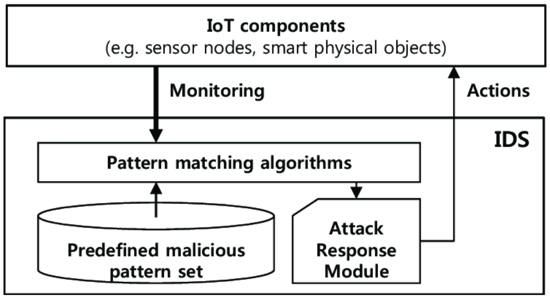
IoT components
(e.g. sensor nodes, smart physical objects)
Monitoring
Actions
IDS
Pattern matching algorithms
Predefined malicious pattern set
Attack Response Module

Figure: 3 Intrusion detection systems

The use of artificial intelligence,-based ensemble modeling for intrusion detection in smart grids offers several key advantages. By combining multiple machine learning classifiers, the system significantly improves detection accuracy and reliability compared to single-classifier approaches. It is capable of identifying both known and previously unseen cyber threats, making it highly adaptive to the evolving nature of smart grid attacks. Ensemble models also reduce false positive rates, minimizing unnecessary alerts and improving operational efficiency. Additionally, the approach is scalable and can handle large volumes of network and sensor data in real time, ensuring continuous monitoring and timely threat mitigation. Overall, this AI-driven method enhances the resilience, security, and stability of smart grid infrastructures, supporting reliable power distribution and safeguarding critical energy systems.

III. LITERATURE SURVEY

Intelligent Intrusion Detection Scheme for Smart Power-Grid Using Optimized Ensemble Learning on Selected Features: This paper presents an intelligent intrusion detection scheme for smart power grids that employs Binary Grey Wolf Optimization (BGWO) for feature selection and ensemble learning to classify attacks. The method enhances detection accuracy by selecting relevant features and combining multiple classifiers, thereby improving the system's ability to identify and mitigate cyber threats in smart grid environments.

AI-enhanced Smart Grid Framework for Intrusion Detection and Mitigation: This paper introduces an Artificial Intelligence-powered Smart Grid Framework (AI-SGF) developed to tackle intrusion detection and mitigation specifically in smart grid environments. The framework integrates AI techniques to enhance the security of smart grids by detecting and responding to cyber threats in real-time, thereby ensuring the resilience and reliability of power distribution systems.

Advanced Mathematical Modeling of Mitigating Security Risks in Smart Grids Using Deep Ensemble Learning: This study develops a novel Mountain Gazelle Optimization with Deep Ensemble Learning (MGODEL-ID) technique for intrusion detection in smart grid environments. The approach utilizes deep learning models to analyze network data, recognize complex attack patterns, and adapt to dynamic threats in real-time, thereby strengthening the reliability and resilience of the grid against cyber-attacks.

Dataset Collection and Visualization

In smart grid intrusion detection systems, dataset collection is a critical step that involves gathering both operational and network data from multiple components of the grid. Data is typically sourced from smart meters, substations, transformers, and communication networks, capturing electrical parameters such as voltage, current, and frequency, as well as network traffic features like packet size, source and destination IP addresses, and protocol information. The dataset includes both normal operational data and anomalous events representing cyber-attacks, such as Denial-of-Service (DoS), data injection, or man-in-the-middle attacks. Once collected, the data is preprocessed, cleaned, and

DOI: 10.48175/IJARSCT-30123

labeled to facilitate training of AI-based ensemble models. For visualization, a tabular representation can show rows of timestamped events with columns for each feature, while charts like bar graphs can illustrate the distribution of normal versus attack data. Additionally, schematic diagrams can depict the data flow from smart grid devices to the intrusion detection system, helping stakeholders understand how raw sensor readings and network traffic are transformed into structured datasets suitable for machine learning analysis.

IV. PROPOSED TECHNIQUES

The implementation of artificial intelligence-based ensemble modeling for intrusion detection in smart grids offers several notable advantages. By combining multiple machine learning classifiers, ensemble models achieve higher detection accuracy and robustness compared to individual models, enabling the identification of both known and novel cyber threats. This approach reduces false positives, minimizing unnecessary alerts and enhancing operational efficiency. Additionally, ensemble techniques are highly adaptive, capable of learning from evolving attack patterns, which is critical for the dynamic environment of smart grids. They also support real-time analysis of large volumes of heterogeneous data generated by smart meters, substations, and network communications, ensuring continuous monitoring and prompt threat mitigation. Overall, this methodology strengthens the security, reliability, and resilience of smart grid infrastructures, contributing to uninterrupted power distribution and protection of critical energy assets.

V. FUTURE WORK

The future of intrusion detection in smart grids using AI-based ensemble modeling is highly promising, as smart grids continue to evolve with increased automation, distributed energy resources, and Internet of Things (IoT) integration. Future research can focus on developing more adaptive and self-learning ensemble models that can detect previously unseen cyber threats in real time. Integration of edge computing and fog computing can enable faster data processing closer to the source, reducing latency and enhancing the grid’s resilience to attacks. Additionally, hybrid approaches combining machine learning, deep learning, and reinforcement learning can improve detection accuracy while minimizing false alarms, making the system more reliable for real-world deployment.

Moreover, as smart grids generate ever-increasing volumes of heterogeneous data, future studies can explore scalable and privacy-preserving AI techniques to protect sensitive customer and operational information. Incorporating explainable AI (XAI) into intrusion detection systems can help stakeholders understand the reasoning behind threat predictions, facilitating better decision-making and faster mitigation strategies. Overall, advancing AI-based ensemble modeling will not only strengthen the security and stability of smart grids but also contribute to the development of smarter, safer, and more resilient energy infrastructure worldwide.

VI. CONCLUSION

Intrusion detection in smart grids is a critical aspect of ensuring the reliability, security, and efficiency of modern power systems. The integration of artificial intelligence-based ensemble modeling provides a robust approach to detecting both known and emerging cyber threats by combining the strengths of multiple machine learning classifiers. This methodology improves detection accuracy, reduces false positives, and adapts to the dynamic nature of smart grid networks, making it highly suitable for real-time monitoring and protection of critical energy infrastructure.

Furthermore, AI-driven ensemble models not only enhance the resilience of smart grids against cyber-attacks but also support efficient management of large-scale heterogeneous data generated by smart meters, substations, and communication networks. The ability to process and analyze complex patterns enables proactive threat identification and timely mitigation. As smart grids continue to evolve with distributed energy resources and IoT integration, AI-based ensemble intrusion detection systems will play an increasingly vital role in securing the future of intelligent, reliable, and sustainable energy systems.

REFERENCES

[1]. Hassan Muhammad, Rania Kora, and Rania Kora "Intrusion Detection in Smart Grids Using Artificial Intelligence-Based Ensemble Modeling," Cluster Computing, 2025.

DOI: 10.48175/IJARSCT-30123

[2]. Ulaa AlHaddad, Alaa Khamis, and Ibrahim Khalil "Ensemble Model Based on Hybrid Deep Learning for Intrusion Detection in Smart Grid Networks," Sensors, 2023.

[3]. M. Panthi, R. K. Gupta, and B. B. Gupta, "Intelligent Intrusion Detection Scheme for Smart Power-Grid Using Optimized Ensemble Learning on Selected Features," Procedia Computer Science, 2022.

[4]. A R. Singh, S. K. Singh, and A. K. Mishra, "AI-enhanced Smart Grid Framework for Intrusion Detection and Mitigation," Journal of Electrical Engineering & Technology, 2025.

[5]. S. A. Sharaf, M. A. Hossain, and M. R. Islam, "Explainable AI-based Innovative Hybrid Ensemble Model for Intrusion Detection," Journal of Cloud Computing, 2024.

[6]. Ali Dehghantanha, Reza M. Parizi, and Kim-Kwang Raymond Choo, "A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids," IEEE Access, 2020.

[7]. Hossein Mohammadi Rouzbahani, Hadis Karimipour, and Lei Lei, "An Ensemble Deep Convolutional Neural Network Model for Electricity Theft Detection in Smart Grids," arXiv, 2021.

[8]. Zakaria El Mrabet, Hassan El Ghazi, and Naima Kaabouch, "A Performance Comparison of Data Mining Algorithms Based Intrusion Detection System for Smart Grid," arXiv, 2019.

[9]. Sathya Narayana Mohan, Gelli Ravikumar, and Manimaran Govindarasu, "Distributed Intrusion Detection System using Semantic-based Rules for SCADA in Smart Grid," arXiv, 2024.

[10]. FS Alsubaei, M. A. Hossain, and M. R. Islam, "Smart Deep Learning Model for Enhanced IoT Intrusion Detection in Smart Grids," Scientific Reports, 2025.

[11]. Ali Dehghantanha, Reza M. Parizi, and Kim-Kwang Raymond Choo, "Artificial Intelligence and Machine Learning for Smart Grids," Elsevier, 2025.

[12]. Cengiz Kaygusuz, Leonardo Babun, and Hidayet Aksu, "Detection of Compromised Smart Grid Devices with Machine Learning and Convolution Techniques," arXiv, 2018.

[13]. Imtiaz Ullah, Qusay H. Mahmoud, and Imtiaz Ullah, "Intrusion Detection Framework Architecture for the Smart Grid," ResearchGate, 2017.

[14]. Brij B. Gupta, Deepak Kalra, and Ammar Almomani, "Innovations in Modern Cryptography," IGI Global Scientific Publishing, 2024.

[15]. YM Banad, A. R. Singh, and S. K. Singh, "Artificial Intelligence for Biometrics and Cybersecurity," IET Press, 2023

DOI: 10.48175/IJARSCT-30123