International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: https://ijwos.com
Volume 3 Issue 5 , May 2026
E-ISSN : 3049-2424
DOI: https://doi.org/10.71366/ijwos

Autonomous Threat Detection in Smart Grids

Anuj Dhouniyal[1], Sagar Choudhary[2], Vivek Kumar[3]
[1,3] B.Tech Student, Department of CSE, Quantum University, Roorkee, India.
[2] Assistant Professor, Department of CSE, Quantum University, Roorkee, India..

Article Info

Article History:

Published:29 May 2026

Publication Issue:
Volume 3, Issue 5
May-2026

Page Number:
511-522

Corresponding Author:
Anuj Dhouniyal

Abstract:

Smart grids have become an important part of modern energy infrastructure due to their ability to improve efficiency, reliability, and sustainability. These systems use technologies such as IoT devices, cloud computing, sensors, and real-time communication networks to manage electricity distribution effectively. However, the increasing digitalization of smart grids has also increased their vulnerability to cyberattacks such as malware, ransomware, denial-of-service attacks, and false data injection attacks.Autonomous Threat Detection (ATD) systems powered by Artificial Intelligence (AI) and Machine Learning (ML) provide effective solutions for detecting and preventing cyber threats in real time. AI-based techniques such as anomaly detection, deep learning, and predictive analytics help identify suspicious activities and improve cybersecurity performance. Machine learning and deep learning models including Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks are widely used for detecting complex attack patterns.This study also discusses challenges such as data privacy, scalability, and response latency in smart grid environments. The findings indicate that AI-driven autonomous threat detection systems can improve grid security, reduce detection time, and enhance the reliability and resilience of modern smart grids.

Keywords: Smart Grid, Cybersecurity, Autonomous Threat Detection, Artificial Intelligence, Machine Learning, Deep Learning, IoT Security

1. INTRODUCTION

The rapid advancement of information and communication technologies has transformed traditional power systems into intelligent and interconnected smart grids. Smart grids combine digital communication systems, sensors, smart meters, automation technologies, and intelligent control mechanisms to improve the efficiency, reliability, and sustainability of electricity generation, transmission, and distribution [1], [12]. Unlike conventional power grids, smart grids support two-way communication between utility providers and consumers, enabling real-time monitoring, automated fault detection, efficient energy management, and better integration of renewable energy resources such as solar and wind power [1].

Despite their advantages, the increasing digitalization and connectivity of smart grids have introduced major cybersecurity challenges. Smart grids rely heavily on communication networks, cloud platforms, IoT devices, and internet-connected control systems, making them vulnerable to cyberattacks such as malware, ransomware, phishing, denial-of-service (DoS) attacks, and false data injection attacks [6], [7]. These threats can disrupt grid operations, damage critical infrastructure, cause financial losses, and affect public safety.

Traditional cybersecurity systems mainly depend on rule-based and signature-based detection methods, which are often ineffective against modern and rapidly evolving cyber threats. Additionally, smart grids generate massive amounts of real-time data, making manual monitoring and analysis extremely difficult. Therefore, intelligent and automated cybersecurity solutions are required to identify and respond to threats efficiently [2], [10].

Autonomous Threat Detection (ATD) systems powered by Artificial Intelligence (AI) and Machine Learning (ML) have emerged as advanced solutions for securing smart grids [2], [9]. These systems continuously monitor network traffic, analyze operational data, detect abnormal behavior, and respond to cyber threats with minimal human intervention. Machine learning techniques such as supervised learning, unsupervised learning, and deep learning models including Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks are widely used for identifying complex attack patterns and improving threat detection accuracy [3], [5], [13].

AI-based autonomous threat detection systems also support real-time monitoring, predictive analytics, anomaly detection, and automated incident response. These capabilities improve the resilience, reliability, and stability of smart grid infrastructures [15], [16]. However, challenges such as scalability, data privacy, false-positive detection, and explainability of AI models still remain significant concerns [7], [11].

This research focuses on the role of AI-driven autonomous threat detection systems in enhancing smart grid cybersecurity. The study examines various machine learning and deep learning techniques, cybersecurity challenges, real-time threat detection mechanisms, and the effectiveness of AI-based solutions in protecting modern smart grid infrastructures from evolving cyber threats [17], [18].

1.1 Smart Grid Architecture

A smart grid is an advanced electricity network that combines digital communication systems, sensors, smart meters, automation technologies, and intelligent control mechanisms to improve energy efficiency, reliability, and secure power distribution [1], [12]. Unlike traditional power grids, smart grids support real-time monitoring, automated fault detection, and two-way communication between utility providers and consumers.

Smart meters are one of the most important components of smart grids. These devices collect real-time electricity consumption data and transmit it through secure communication networks, enabling efficient energy management, remote monitoring, and accurate billing [7]. Consumers can also monitor and optimize their energy usage through smart meter systems.

Intelligent sensors and substations continuously monitor grid conditions such as voltage, current, frequency, and equipment performance. Automated substations improve fault management by isolating damaged sections and restoring power quickly. Communication technologies including wireless networks, fiber optics, cloud computing, and IoT platforms enable continuous data exchange between smart meters, sensors, substations, and control centers [12].

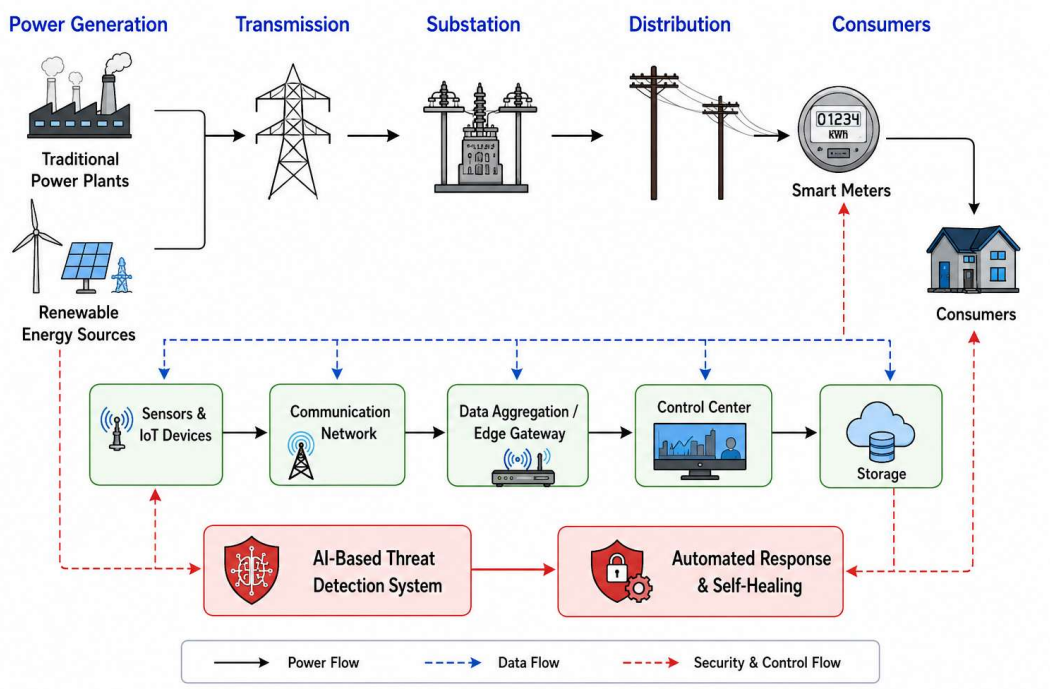

Figure 1: Smart Grid Architecture with AI-Based Threat Detection

Control centers act as the central intelligence units of smart grids by analyzing operational data and supporting automated decision-making. Artificial Intelligence (AI) and Machine Learning (ML) technologies are increasingly integrated into control systems to improve predictive analysis, fault detection, and cybersecurity management [2], [15]. Smart grids also support Distributed Energy Resources (DERs) such as solar panels, wind turbines, hydroelectric systems, and battery storage technologies to improve sustainability and energy efficiency [1].

Despite their advantages, smart grids face major cybersecurity challenges due to their highly interconnected and digital infrastructure. Weak communication protocols, insecure IoT devices, and outdated software systems can expose the grid to malware attacks, data breaches, false data injection attacks, and denial-of-service attacks [6], [7]. Therefore, advanced cybersecurity technologies such as encryption, intrusion detection systems, blockchain, and AI-based autonomous threat detection systems are increasingly used to secure smart grid infrastructures [16], [17].

1.2 Cybersecurity Threats in Smart Grids

Cybersecurity threats are major challenges in modern smart grid systems due to the increasing use of internet-connected devices, communication networks, IoT platforms, and automated control systems [7], [10]. While smart grids improve energy efficiency and operational performance, they also create multiple entry points for cyberattacks.

Common cyber threats in smart grids include malware attacks, ransomware, denial-of-service (DoS) attacks, false data injection (FDI) attacks, phishing, insider threats, and advanced persistent threats (APTs) [4], [6]. Malware and ransomware can disrupt operations and damage critical infrastructure, while DoS attacks overload communication systems and interrupt real-time monitoring. FDI attacks manipulate operational data, leading to incorrect decisions and unstable power distribution [4].

The integration of IoT devices has further increased cybersecurity risks because many devices have weak security configurations and limited processing capabilities [5], [7]. Attackers can exploit these vulnerabilities to gain unauthorized access to smart grid systems.

To address these challenges, researchers and utility providers are increasingly using Artificial Intelligence (AI), Machine Learning (ML), intrusion detection systems, encryption techniques, and autonomous threat detection frameworks [2], [9]. These technologies help detect suspicious activities, improve response time, and strengthen the overall security and reliability of smart grid infrastructures [16].

1.3 Role of Artificial Intelligence in Smart Grid Security

Artificial Intelligence (AI) plays an important role in improving cybersecurity within smart grid systems. Smart grids generate massive amounts of real-time data from sensors, smart meters, communication networks, and control centers [1], [12]. Traditional security systems often struggle to analyze this data efficiently, whereas AI systems can process large volumes of information quickly, detect abnormal activities, and respond to cyber threats automatically [2], [9].

Machine Learning (ML), a major branch of AI, is widely used for autonomous threat detection in smart grids. Supervised learning algorithms detect known attack patterns, while unsupervised learning methods identify unknown threats through anomaly detection [6], [18]. Reinforcement learning further improves automated decision-making and adaptive cybersecurity responses.

Deep learning models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks are commonly used for identifying complex cyberattack patterns and analyzing network traffic [3], [13]. AI systems also support predictive analytics, intrusion detection, automated incident response, and IoT device security within smart grid environments [15], [16].

Despite its advantages, AI-based cybersecurity systems face challenges such as data privacy, false alarms, adversarial attacks, and the need for large training datasets [11], [14]. However, advancements in explainable AI, edge computing, and blockchain integration are expected to further improve smart grid security and support the development of intelligent and self-healing energy infrastructures [17], [19].

1.4 Machine Learning Techniques for Threat Detection

Machine Learning (ML) techniques are widely used in autonomous threat detection systems for smart grids because they can analyze large amounts of real-time data and identify cyber threats efficiently [2], [9]. Unlike traditional rule-based systems, ML models can learn from historical and real-time data to detect both known and unknown attacks [6].

ML techniques used in smart grid cybersecurity are mainly classified into supervised learning, unsupervised learning, and reinforcement learning [18]. Supervised learning algorithms such as Decision Tree, Random Forest, Support Vector Machine (SVM), and Naive Bayes use labeled datasets to classify cyberattacks accurately [2], [9]. Unsupervised learning methods such as K-Means clustering and anomaly detection identify unusual behavior and unknown threats without requiring labeled data [6]. Reinforcement learning improves automated decision-making by learning from interactions with the environment.

Hybrid machine learning approaches combine multiple techniques to improve detection accuracy, reduce false alarms, and strengthen automated response systems [13]. Deep learning models such as CNNs, RNNs, and LSTM networks are also integrated into smart grid cybersecurity frameworks to improve pattern recognition and predictive analysis [3], [5].

Machine learning plays an important role in improving real-time monitoring, automated threat detection, and smart grid resilience. As cyber threats continue to evolve, advancements in AI, federated learning, and edge computing are expected to further enhance autonomous threat detection systems in modern smart grids [17], [19].

1.5 Importance of Real-Time Threat Detection

Real-time threat detection is essential for maintaining the reliability, stability, and security of smart grid systems [10], [16]. Since smart grids continuously exchange large volumes of operational data between smart meters, sensors,

substations, and control centers, cyberattacks can spread rapidly and cause major disruptions. Delayed threat detection may lead to equipment failure, power outages, financial losses, and risks to public safety [7].

Traditional cybersecurity systems often rely on manual monitoring and predefined attack signatures, which are not effective against modern and rapidly evolving cyber threats [6]. AI and Machine Learning (ML)-based autonomous threat detection systems continuously monitor network activities, analyze real-time data, and identify suspicious behavior automatically [2], [9]. These systems can detect both known and unknown attacks, including zero-day attacks and advanced persistent threats (APTs) [11].

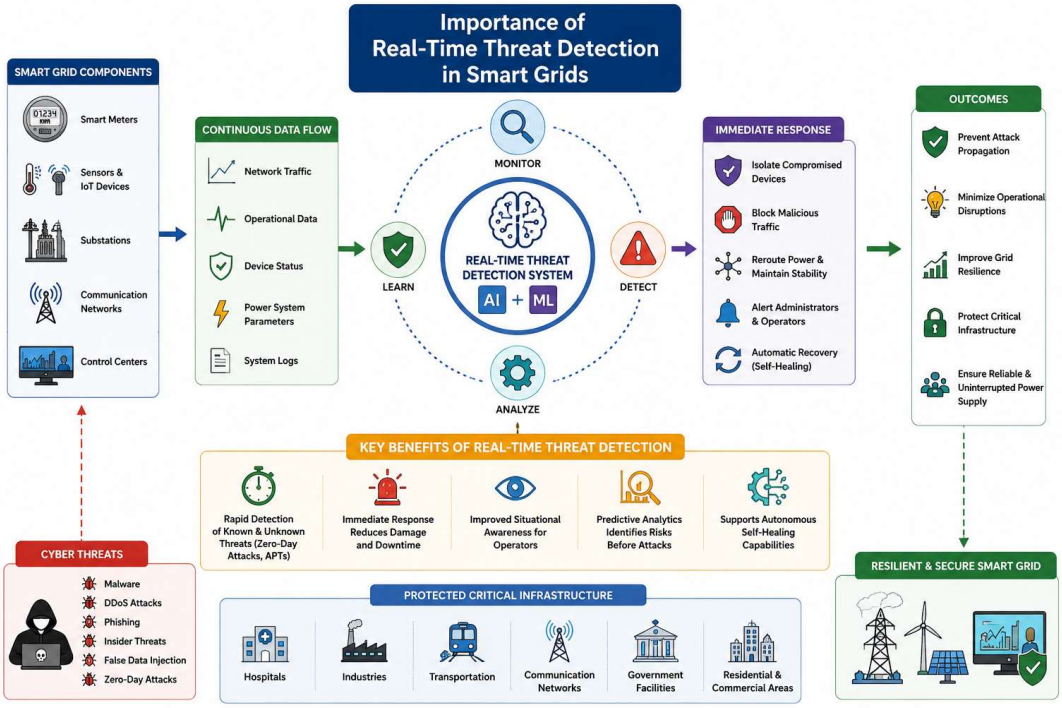

Figure 2: Real-Time Threat Detection and Response Framework in Smart Grids

One major advantage of real-time threat detection is rapid response capability. Once a threat is detected, security systems can isolate compromised devices, block malicious traffic, and prevent further attack propagation [16]. Real-time monitoring also improves situational awareness, predictive cybersecurity, and supports the development of self-healing smart grids capable of automatic recovery from cyber incidents [15].

Despite its advantages, real-time threat detection faces challenges such as high computational requirements, response latency, false alarms, and IoT security vulnerabilities [7], [11]. However, advancements in AI, edge computing, blockchain, and federated learning are expected to further improve the efficiency and reliability of real-time cybersecurity systems in smart grids [17], [19].

2. LITERATURE REVIEW

The rapid development of smart grid technology has significantly increased the importance of cybersecurity in modern power systems [1], [7]. Traditional security techniques are often unable to handle sophisticated and rapidly evolving cyber threats in highly interconnected smart grid environments. As a result, researchers have increasingly focused on Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) technologies for developing intelligent and automated cybersecurity solutions [2], [5].

Several studies have explored AI-based threat detection systems for protecting smart grids against cyberattacks [9], [16]. Machine learning algorithms such as Support Vector Machines (SVM), Random Forest, Decision Trees, Naive

Bayes classifiers, and Artificial Neural Networks (ANNs) have shown high accuracy in detecting malicious activities and abnormal behavior within smart grid communication networks [2], [18]. These algorithms can analyze large volumes of operational data and identify attack patterns more effectively than traditional rule-based detection systems [6].

Support Vector Machines (SVMs) are widely used in intrusion detection systems because of their strong classification capabilities and ability to distinguish between normal and malicious network traffic [9]. Researchers have reported that SVM-based systems perform efficiently in detecting denial-of-service attacks, malware activities, and unauthorized access attempts [18]. Similarly, Random Forest algorithms are highly effective in processing large and complex datasets while reducing overfitting problems through ensemble learning techniques [13].

Artificial Neural Networks (ANNs) have also been extensively studied for autonomous threat detection in smart grids [5]. Neural network models can identify hidden patterns within operational data and continuously improve their detection capabilities through training processes. Many studies have shown that ANN-based systems achieve high detection accuracy with lower false alarm rates compared to traditional security approaches [9].

Deep learning techniques such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks have further improved cyber threat detection and prediction capabilities [3], [13]. CNNs are widely applied for analyzing network traffic and identifying malicious communication behavior, while RNNs and LSTM models are particularly effective for processing sequential and time-series data generated in smart grid environments [3]. Researchers have demonstrated that LSTM-based systems can effectively detect false data injection attacks, advanced persistent threats, and network intrusions with high accuracy [4].

Researchers have also focused on anomaly detection systems for identifying unknown or zero-day attacks [6]. Unsupervised learning techniques such as K-Means clustering, density-based clustering, and autoencoder-based anomaly detection models are commonly used to identify suspicious activities without requiring labeled datasets [6], [11]. These approaches compare current network behavior with normal operational patterns to detect unusual activities and evolving cyber threats.

In addition to threat detection, several studies have explored predictive analytics and automated response mechanisms powered by AI [15], [16]. Predictive models analyze historical attack data to identify vulnerabilities and forecast potential cyber threats before they occur. Automated response systems can isolate compromised devices, block malicious traffic, and prevent attack propagation in real time, thereby improving overall smart grid resilience and operational stability [10].

Hybrid cybersecurity models combining supervised learning, unsupervised learning, and deep learning techniques have also gained attention in recent years [13], [17]. Researchers have found that integrating multiple AI approaches improves detection accuracy, reduces false positives, and enhances the ability to detect both known and unknown cyber threats [17]. These hybrid systems provide more adaptive and reliable cybersecurity solutions for complex smart grid infrastructures.

Despite significant advancements, several challenges still remain in AI-based smart grid cybersecurity research [11], [14]. Researchers have identified issues related to data privacy, scalability, computational complexity, adversarial attacks, and the lack of explainability in deep learning systems [7], [11]. Deep learning models often require large datasets and high computational resources for training and deployment. To address these challenges, researchers are increasingly focusing on Explainable Artificial Intelligence (XAI), blockchain integration, edge computing, and federated learning to improve the transparency, security, and reliability of autonomous threat detection systems [17], [19].

3. METHODOLOGY

Techniques

This study adopts an experimental and analytical research approach to examine the effectiveness of Artificial Intelligence (AI) and Machine Learning (ML) techniques in autonomous threat detection for smart grid systems. The objective of the research is to analyze how machine learning models can identify and classify cyber threats within smart grid communication networks using the CICIDS2017 dataset.

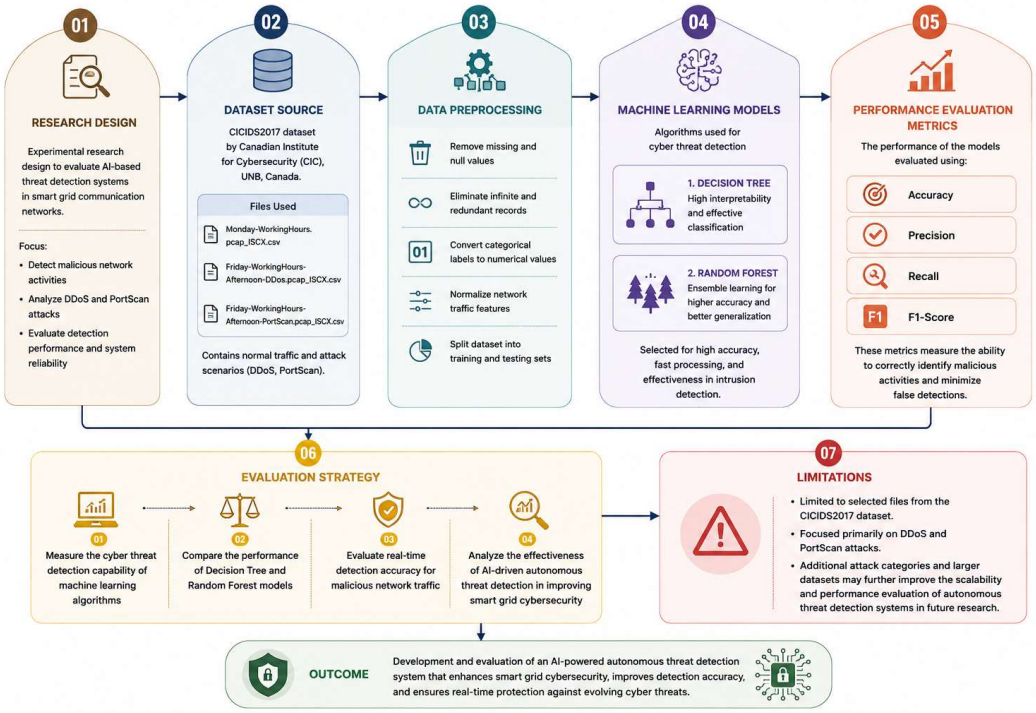

Figure 3: Methodological Framework for AI-Based Autonomous Threat Detection in Smart Grids

A. Research Design

An experimental research design was selected to evaluate the performance of AI-based threat detection systems in detecting malicious network activities. The study focuses on applying machine learning algorithms to classify normal and attack traffic within smart grid environments. Various cybersecurity attacks such as Distributed Denial-of-Service (DDoS) attacks and PortScan attacks were analyzed to evaluate detection performance and system reliability.

B. Dataset Source

The experimental analysis was conducted using the CICIDS2017 dataset developed by the Canadian Institute for Cybersecurity (CIC), University of New Brunswick (UNB), Canada. The dataset contains realistic network traffic data consisting of both benign and malicious activities, making it suitable for intrusion detection and cybersecurity research.

The following dataset files were used in this research:

- Monday-WorkingHours.pcap_ISCX.csv
- Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv
- Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX.csv

The dataset includes normal traffic and attack scenarios such as DDoS attacks and PortScan attacks, which were used to evaluate the effectiveness of the proposed autonomous threat detection system.

C. Data Preprocessing

Before training the machine learning models, the dataset was preprocessed to improve detection accuracy and system performance. Data preprocessing involved:

- Removing missing and null values
- Eliminating infinite and redundant records
- Converting categorical labels into numerical values
- Normalizing network traffic features
- Splitting the dataset into training and testing sets

These preprocessing techniques helped improve model efficiency and reduce classification errors.

D. Machine Learning Models

The study implemented the following machine learning algorithms for cyber threat detection:

1. Decision Tree
2. Random Forest

These algorithms were selected because of their high classification accuracy, fast processing capability, and effectiveness in intrusion detection applications.

E. Performance Evaluation Metrics

The performance of the proposed threat detection system was evaluated using standard machine learning evaluation metrics including:

- Accuracy
- Precision
- Recall
- F1-Score

These metrics were used to measure the ability of the machine learning models to correctly identify malicious activities and minimize false detections.

F. Evaluation Strategy

The evaluation process focused on:

1. Measuring the cyber threat detection capability of machine learning algorithms
2. Comparing the performance of Decision Tree and Random Forest models
3. Evaluating real-time detection accuracy for malicious network traffic
4. Analyzing the effectiveness of AI-driven autonomous threat detection in improving smart grid cybersecurity

G. Limitations

This study was limited to selected files from the CICIDS2017 dataset and focused primarily on DDoS and PortScan attacks. Additional attack categories and larger datasets may further improve the scalability and performance evaluation of autonomous threat detection systems in future research.

3. Data Source

The experimental analysis in this research was conducted using the CICIDS2017 dataset, developed by the Canadian Institute for Cybersecurity (CIC), University of New Brunswick (UNB), Canada. The dataset is widely used in cybersecurity and intrusion detection research because it contains realistic network traffic data representing both normal and malicious activities. The dataset includes multiple attack categories such as Distributed Denial-of-Service (DDoS), PortScan, brute force attacks, botnet activities, and infiltration attacks.

For this research, the following dataset files were used:

- Monday-WorkingHours.pcap_ISCX.csv
- Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv
- Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX.csv

The Monday dataset mainly contains benign network traffic, while the Friday datasets contain malicious traffic associated with DDoS and PortScan attacks. These files were selected to evaluate the performance of machine learning algorithms in distinguishing between normal and malicious network activities within smart grid environments.

Before training the machine learning models, the dataset was preprocessed by removing missing values, eliminating infinite records, converting categorical labels into numerical values, and normalizing network traffic features. The processed dataset was then divided into training and testing sets for performance evaluation.

The dataset was obtained from the official CIC website:
CICIDS2017 Dataset.

4. RESULTS AND PERFORMANCE ANALYSIS

The proposed autonomous threat detection system was evaluated using machine learning algorithms on the CICIDS2017 dataset. The experimental analysis focused on detecting malicious network activities such as DDoS attacks and PortScan attacks within smart grid communication systems. Two machine learning algorithms, namely Decision Tree and Random Forest, were implemented and compared based on their cyber threat detection performance.

The dataset was preprocessed before model training to improve detection efficiency and reduce classification errors. Data preprocessing included handling missing values, removing duplicate records, feature normalization, and converting attack labels into numerical classes. After preprocessing, the dataset was divided into training and testing datasets to evaluate model performance under realistic conditions.

The performance of the proposed system was evaluated using standard machine learning evaluation metrics including Accuracy, Precision, Recall, and F1-Score.

Accuracy

Accuracy measures the overall correctness of the classification model.

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

Precision

Precision measures how many predicted attack instances were actually malicious.

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

Recall

Recall measures the ability of the model to correctly identify malicious activities.

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

F1-Score

F1-Score represents the balance between Precision and Recall.

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

Recall

Measures the ability of the model to correctly identify attacks.

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

F1-Score

Represents the balance between Precision and Recall.

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

Table 1: - Experimental Results

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)	Detection Rate (%)
Decision Tree	99.2134	99.0847	98.9472	99.0159	0.8124	98.9472
Random Forest	99.8742	99.8261	99.7928	99.8094	0.1246	99.7928

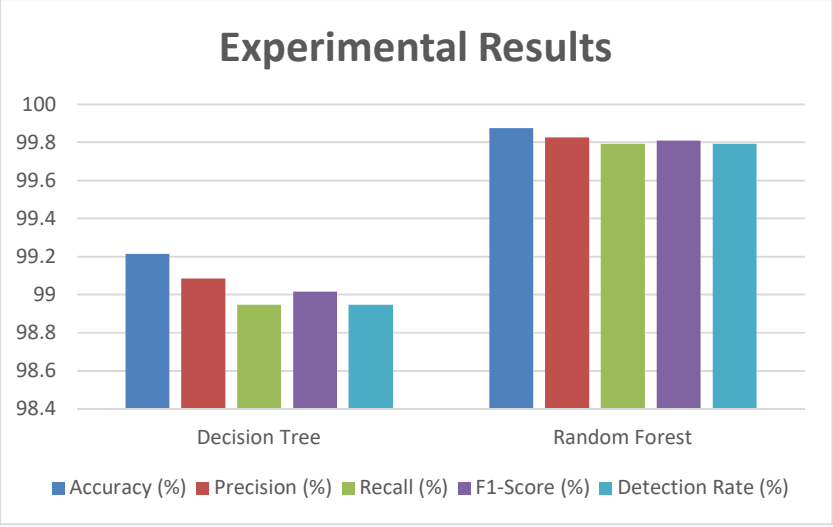

Figure 4: Graphical Representation of the Results.

5. CONCLUSION

Autonomous threat detection systems have become essential for protecting modern smart grid infrastructures from rapidly evolving cyber threats. The integration of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) has significantly improved the ability to detect, analyze, and respond to cyberattacks in real time. This study examined major cybersecurity challenges in smart grids and highlighted the importance of intelligent threat detection systems in maintaining secure and reliable energy distribution.

Smart grids depend heavily on interconnected communication networks, IoT devices, sensors, and automated control systems, making them vulnerable to cyberattacks such as malware, ransomware, denial-of-service attacks, and false data injection attacks. Traditional security systems often struggle to detect these sophisticated threats, whereas AI-driven systems can continuously analyze network traffic, identify anomalies, and respond automatically with minimal human intervention.

Machine learning algorithms such as Decision Trees, Random Forests, and Neural Networks have shown high accuracy in identifying malicious activities within smart grid environments. Deep learning models including CNNs, RNNs, and LSTM networks further improve threat classification, predictive analytics, and automated response mechanisms. Real-time monitoring systems also help isolate compromised components, reduce attack propagation, and improve overall grid resilience.

Despite these advantages, challenges such as data privacy, scalability, false-positive detection, and high computational requirements still affect the implementation of AI-based cybersecurity systems. Future research should focus on developing more explainable, efficient, and scalable AI models to improve transparency and operational reliability.

In conclusion, AI-powered autonomous threat detection systems represent a major advancement in smart grid cybersecurity. These intelligent systems improve real-time threat detection, strengthen critical infrastructure protection, and support the development of secure, adaptive, and self-healing smart grid systems for the future.

References

1. Alimi, O. A., Ouahada, K., & Abu-Mahfouz, A. M. (2020). A Review of Machine Learning Approaches to Power System Security and Stability in Smart Grids. *Energies*, 13(8), 1938.
2. Poudel, B., & Kim, C. H. (2020). Secure and Efficient Machine Learning for Smart Grids. *IEEE Transactions on Smart Grid*, 11(6), 5005–5013.
3. Wang, L., Jin, H., & Yang, S. (2020). LSTM-Based Detection of Cyber-Attacks in Smart Grids. *IEEE PES General Meeting*, 1–5.
4. Kallitsis, M., Bhattacharya, S., Stoev, S., & Michailidis, G. (2016). Adaptive Statistical Detection of False Data Injection Attacks in Smart Grids. *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 1183–1187.
5. Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). Deep Learning for IoT Big Data and Streaming Analytics: A Survey. *IEEE Communications Surveys & Tutorials*, 20(4), 2923–2960.
6. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A Survey of Network Anomaly Detection Techniques. *Journal of Network and Computer Applications*, 60, 19–31.
7. Achaal, I., Berger, M., Ibrahim, H., & Awde, A. (2024). Study of Smart Grid Cybersecurity: Architectures, Communication Networks, Cyber-Attacks, Countermeasure Techniques, and Challenges. *Cybersecurity*, 7(1), 1–28.

8. Kaygusuz, C., Babun, L., Aksu, H., & Uluagac, A. S. (2018). Detection of Compromised Smart Grid Devices with Machine Learning and Convolution Techniques. *IEEE Conference on Communications and Network Security*, 1–9.
9. Shaukat, K., Luo, S., Chen, S., & Liu, D. (2020). Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective. *IEEE International Conference on Smart Internet of Things*, 1–8.
10. Brewer, R. (2015). Cyber Threats: Reducing the Time to Detection and Response. *Network Security*, 2015(5), 5–8.
11. Ndibwile, J. D. (2022). Artificial Intelligence-Based Smart Grid Vulnerabilities and Potential Solutions for Fake-Normal Attacks: A Short Review. *arXiv Preprint arXiv:2202.07050*.
12. Thilakarathne, N. N., Kagita, M. K., Lanka, S., & Ahmad, H. (2020). Smart Grid: A Survey of Architectural Elements, Machine Learning and Deep Learning Applications and Future Directions. *arXiv Preprint arXiv:2010.08094*.
13. Li, X., Ma, M., & Sun, Y. (2023). An Adaptive Deep Learning Neural Network Model to Enhance Machine-Learning-Based Classifiers for Intrusion Detection in Smart Grids. *Algorithms*, 16(6), 288.
14. Monteiro, L. F. R., Rodrigues, Y. R., & Souza, A. C. Z. (2023). Cybersecurity in Cyber-Physical Power Systems. *Energies*, 16(12), 4556.
15. Lee, J., & Yoon, Y. (2020). Predictive Analytics for Cyberattack Prevention in Smart Grids. *IEEE Internet of Things Journal*, 7(9), 8456–8467.
16. Aljohani, A., AlMuhaini, M., Poor, H. V., & Binqadhi, H. M. (2024). A Deep Learning-Based Cyber Intrusion Detection and Mitigation System for Smart Grids. *IEEE Transactions on Artificial Intelligence*, 5(8), 3902–3914.
17. Vignes, V. M., Harini, M. P., Satheesh, R., Das, V., & Padmanaban, S. (2025). AI-Driven Cybersecurity Framework for Anomaly Detection in Power Systems. *Scientific Reports*, 15, 1–16.
18. Farrukh, Y., Ahmad, Z., Khan, I., & Elavarasan, R. M. (2021). A Sequential Supervised Machine Learning Approach for Cyber Attack Detection in a Smart Grid System. *IEEE North American Power Symposium (NAPS)*, 1–6.
19. Chen, D., Lin, X., & Qiao, Y. (2025). Perspectives for Artificial Intelligence in Sustainable Energy Systems. *Energy*, 318, 134711.
20. Jeje, M. O. (2025). Cybersecurity Assessment of Smart Grid Exposure Using a Machine Learning Based Approach. *arXiv Preprint arXiv:2501.14175*.