Available online at www.HighTechJournal.org

HighTech and Innovation Journal

ISSN: 2723-9535

Vol. 5, No. 3, September, 2024

Real-Time Intrusion Detection in Power Grids Using Deep Learning: Ensuring DPU Data Security

Maoran Xiao [1, 2*], Qi Zhou [2], Zhen Zhang [1], Junjie Yin [1]

[1] *State Grid Jiangsu Electric Power Co., Ltd. Limited Information and Telecommunication Branch, Nanjing, Jiangsu, 210000, China.*

[2] *State Grid Jiangsu Electric Power Co., Ltd. Wuxi Power Supply Branch, Wuxi, Jiangsu, 214000, China.*

Received 15 May 2024; Revised 09 August 2024; Accepted 16 August 2024; Published 01 September 2024

Abstract

Deep learning technologies have revolutionized the management of energy, energy consumption, and data security within smart grids through non-intrusive load monitoring (NILM). This paper explores the use of deep learning for real-time intrusion detection in power grids with a primary focus on safeguarding the integrity and security of Data Processing Units (DPUs). An evaluation of various machine learning models, including Support Vector Machine (SVM), Linear Discriminant Analysis (LDA), Decision Trees, and Random Forests, is conducted to detect various types of intrusions, including Fault, Injection, Masquerade, Normal, and Replay. Random Forest produced AUC values of 1.00 for all classes and an overall F1-score of 0.99 for all classes. The Decision Tree model also shows robust performance for detecting Fault and Injection intrusions (AUC = 0.98), with an overall F1-score of 0.94. However, the LDA and SVM models do not perform well in detecting Injection intrusions with overall F1-scores of 0.83 and 0.86. Advances in machine learning can be used to improve smart grid security, reliability, and efficiency, according to this study. These findings highlight the potential of advanced machine learning techniques to enhance smart grid reliability and efficiency.

Keywords: Machine Learning; Intrusion Detection; Smart Grids; Data Integrity; Security; NILM; Real-Time Detection; Energy Management.

1. Introduction

The advancement of deep learning technologies has revolutionized various fields, and its application in power grids has been particularly transformative. Non-intrusive load monitoring (NILM) systems have greatly benefited from these advancements, leading to improved energy management, optimized consumption, and enhanced data security. However, despite these advancements, existing NILM systems continue to face significant challenges related to latency, accuracy, and privacy, particularly when applied to real-time monitoring in smart grids. This paper focuses on deploying deep learning for real-time intrusion detection in power grids, emphasizing the importance of safeguarding Data Processing Unit (DPU) data integrity and security. The need for effective and efficient energy management in smart grids has driven extensive research into NILM systems. NILM involves monitoring and disaggregating the power consumption of individual appliances from a single measurement point, typically without installing additional sensors. This approach offers numerous advantages, including cost reduction, spatial efficiency, and improved energy management capabilities. However, traditional NILM methods often struggle with key issues such as latency, limited accuracy in disaggregation, and potential privacy concerns related to data exposure.

* Corresponding author: maoranxiao@foxmail.com

http://dx.doi.org/10.28991/HIJ-2024-05-03-018

Deep-learning techniques have been incorporated into recent developments in order to address these challenges. SAMNet is a multi-task neural network based on Scale-and-Attention experts. By identifying the on/off states and energy consumption of appliances through multi-task deep learning, this innovative approach achieves latency-free NILM. In SAMNet, a shared expert learner uses correlations between tasks to construct a comprehensive feature summary, which improves performance over traditional methods [1]. Sequence-to-Sequence (Seq2Seq) deep learning algorithms have also shown promise in predicting appliance load signatures based on smart grid data. Despite their high accuracy in disaggregating household appliance loads, these algorithms raise privacy and disclosure concerns. For instance, NILM systems can reveal detailed energy consumption patterns that could expose sensitive information about household behavior, leading to what is termed "*disclosure risk*" [2]. Over the course of the evolution of NILM methodologies, several novel approaches have been introduced that further enhance the accuracy and efficiency of energy load disaggregation. To identify changes in appliance states, one approach involves measuring and processing the common supply current signal. It enables precise disaggregation of energy loads and contributes to more efficient energy management by identifying appliances based on their unique characteristics [3]. The development of non-intrusive AC-DC wide-bandwidth current sensors based on composite measurement principles is another significant development. Combining capacitive coupling and optical fiber sensing technologies, these sensors overcome the limitations of traditional power grid current sensors. As a result of this combination, the sensors are able to measure AC and DC signals simultaneously with high accuracy and a wide measurement range, making them suitable for various smart grid applications [4].

Despite these technological advancements, there remain several limitations in current NILM systems when addressing real-time security challenges. The focus has been primarily on improving energy disaggregation, but little attention has been given to real-time intrusion detection, particularly for safeguarding the integrity of DPUs in smart grids. The advancement of NILM technologies has also been facilitated by enhancements in event-detection algorithms. In order to identify appliance-specific events in real time, one algorithm uses multiple features from smart meter data. In addressing the limitations of current NILM methods, this approach achieves a higher recognition accuracy, demonstrating its potential for promoting supply-demand balance and energy conservation in residential settings [5]. NILM has adapted deep learning frameworks for specific applications, demonstrating their versatility and effectiveness. To detect pool pump operations, one innovative framework transforms time-series data into image-like data. This data is then segmented at a pixel level using a U-shaped convolutional neural network, achieving high accuracy in detecting pool pump activity. In particular, these methods demonstrate the potential of deep learning-based approaches in load monitoring for non-urgent, energy-intensive residential appliances [6]. The identification of appliances can also be accomplished using voltage-current trajectory-enabled deep supervised hashing. Electrical characteristics of appliances in different states can be represented using the V-I trajectory. In addition to providing efficient power management, this approach contributes to anomaly detection, demand response, and electricity management [7]. While these advancements have significantly improved NILM systems' ability to monitor and disaggregate energy consumption, they do not adequately address the critical need for securing smart grid operations from intrusions and other forms of cyber-attacks. The use of power-based condition monitoring methods is also beneficial for smart grid applications. These methods detect tampering of programs running on Distribution Terminal Units (DTUs) using power sensors and machine learning techniques. Smart grid operations can be improved with this approach [8]. The benefits and potential applications of NILM systems in smart grids are thoroughly evaluated. The NILM system monitors appliance consumption without adding additional sensors, reducing both costs and space restrictions. Machine learning algorithms can be used to decompose aggregate power absorption profiles into individual appliance profiles [9].

In this paper, we address the identified gaps by focusing on the critical issue of real-time intrusion detection in DPUs within smart grids. While NILM systems have improved energy efficiency and diagnostics, their application to security is still an emerging area that requires robust solutions. Although NILM systems are consistently supported, they are not well understood. The NILM system also facilitates diagnostics and automation, as well as increasing energy efficiency. Individual appliance profiles can be decomposed using machine learning algorithms. There are still several challenges to overcome when it comes to NILM technologies. One of the primary challenges is ensuring the real-time integrity and security of DPU data, as vulnerabilities in these units may compromise the reliability of the entire grid. The integrity and security of smart grid data processing units (DPUs) are becoming increasingly important as smart grids become more prevalent. The integrity and security of DPU data need to be protected in real-time, and vulnerabilities that may compromise the reliability of smart grids need to be addressed. Smart grid monitoring and security are the subject of several significant contributions in this paper. It emphasizes the importance of deep learning in enhancing accuracy, efficiency, and privacy in non-intrusive load monitoring (NILM) systems. Support Vector Machines (SVMs), LDA, Decision Trees, and Random Forests are also introduced and evaluated in the paper to detect intrusions in smart grids. Fault injection, masquerade, normal, and replay intrusions are classified using these techniques. By addressing these real-time threats, we propose a framework that significantly strengthens smart grid operations by incorporating robust machine learning techniques for real-time intrusion detection in DPUs. In the final part of the study, robust solutions for real-time intrusion detection in DPUs are proposed for data integrity and security. Smart grid operations will be

significantly strengthened by these advanced machine learning techniques for real-time intrusion detection. The method protects power grids from unauthorized access. By developing more secure and resilient smart grid technologies, we can create a more sustainable and efficient energy system.

2. Literature Review

Smart grid intrusion detection systems have been significantly improved by recent advances in machine learning and deep learning. Silva & Liu [10] reviewed recent studies on Non-Intrusive Load Monitoring (NILM) and its integration with Machine Learning (ML). The authors found that NILM has become a promising approach for energy management, providing affordable solutions using aggregated load data from smart meters. The study concluded that integrating ML approaches with NILM can lead to more efficient energy management systems, offering real-time solutions for practical implementation. The authors emphasized the importance of considering both theoretical and experimental aspects when developing reliable EM solutions using NILM and ML techniques. Adewole & Tan [11] introduce a new concept called energy disaggregation risk, which refers to the potential privacy issues that arise when energy disaggregation algorithms are used to analyze aggregated smart grid data. In this study, Sequence-to-Sequence (Seq2Seq) NILM deep learning algorithm is compared with three activation extraction methods and three inference attacks are explored. Compared with other event detection methods, Variance Sensitive Thresholding (VST) is the most resilient to energy disaggregation risk. Kommey et al. [12] investigated an artificial intelligence-based non-intrusive load monitoring system for energy consumption optimization using a modified K-Nearest Neighbor algorithm. The study aimed to address the challenges of intrusive load monitoring methods, which are often costly and inconvenient. The proposed approach used machine learning techniques to predict and classify energy consumption patterns without requiring direct access to appliances or meters. Results showed that the non-intrusive method effectively predicted energy consumption with high accuracy (94.5%) and classified appliance types correctly (92.3%). This innovative solution has potential applications in reducing power wastage, improving energy efficiency, and minimizing financial burdens on households and businesses.

A key step in non-intrusive load monitoring (NILM) is the detection of events using geometric features of cumulative sums [13]. Energy shortages and greenhouse gas emissions have prompted experts worldwide to focus on solving energy management problems, with smart grid construction one of the most important technologies for managing energy use. The study found that traditional event detection methods, including those developed using the cumulative sum (CUSUM) method, while reasonable in terms of accuracy, lack precision. Zhao et al. [5] proposed a nonintrusive load monitoring method to detect multiple events, addressing issues related to setting hyper-parameters and detecting multiple events. In order to extract local features from aggregated data within a sliding window, the authors used convolutional neural networks, followed by multi-head self-attention mechanisms that could distinguish similar events based on correlations between event sequences and contextual information. Table 1 presents an overview of recent advances in NILM. There is potential for this technology to be applied to customer-side intelligent sensing and ubiquitous power Internet of Things applications.

Table 1. Overview of Recent Advancements in NILM and Related Technologies

Author	Year	Method	Type	Key Results
Liu et al. [14]	2022	Scale-and Attention-experts based multi-task neural network (SAMNet)	NILM	Achieved latency-free NILM by identifying on/off states and energy consumption from aggregate loads
Adewole & Torra [2]	2023	Sequence-to-Sequence (Seq2Seq) deep learning algorithm	NILM	High accuracy in disaggregating appliance loads but with privacy risks
Dowalla et al. [3]	2022	Common supply current signal processing	NILM	Effectively identified appliances based on unique characteristics, enabling energy load disaggregation
Tan et al. [4]	2022	AC-DC wide-bandwidth current sensor	Sensor	High accuracy (0.1% or less) and wide measurement range (-50 A to 100 A)
Zhao et al. [5]	2021	Event-detection algorithm	NILM	Higher recognition accuracy compared to existing NILM techniques
Bucci et al. [9]	2021	Overview of NILM systems	Overview	Highlighted benefits and potential applications of NILM systems
Ma et al. [6]	2021	Deep learning framework (PUMPNET)	NILM	Effectively detected pool pump operations with 95.6% accuracy and 92.5% precision
Han et al. [7]	2021	Voltage-current trajectory enabled asymmetric deep supervised hashing (ADSH)	NILM	Accurately identified appliances and their states, improving smart power consumption management
Zhang et al. [8]	2020	Power-based non-intrusive condition monitoring	Condition Monitoring	Feasibility of detecting tampering in DTUs using power consumption data.
Seyedi et al. [15]	2020	Reliability assessment of synchrophasor communications	Reliability	Effectively reduced missed synchrophasor data frames over successive timestamps
Green et al. [16]	2020	Multi-scale framework for nonintrusive load identification	NILM	More accurate and robust NILM by leveraging multiple algorithms.
Xia et al. [17]	2020	Composite deep long short-term memory network	NILM	Improved accuracy and efficiency in load disaggregation
Pereira et al. [18]	2019	NILM Performance Evaluation dataset	Dataset	Provided ground-truth data, model specifications, and performance metrics

Huang et al. [19]	2018	Review of energy-efficient smart buildings	Review	Highlighted key areas in smart buildings driven by new technologies
Henao et al. [20]	2018	Probabilistic non-intrusive approach	NILM	Accurate recognition of electric space heater power profiles
Otoum et al. [21]	2017	Hybrid architecture for intrusion detection	Intrusion Detection	Effectively identified intrusions in critical applications
Villani et al. [22]	2017	Contactless and energy-neutral power meter	Power Meter	Efficient control of electric loads in Smart Grids.
Eibl & Engel [23]	2015	Impact of data granularity on smart meter privacy	Privacy	Detection rate declines as time interval between measurements increases beyond half the on-time of an appliance.

Also, Chan & Zhou [24] investigated non-intrusive methods of protecting legacy SCADA systems against false command injection attacks. The authors emphasize the limitations of patching old-generation devices with cryptographic defenses due to resource constraints. Rather than modifying the protocol at the protocol level, they proposed add-on solutions. In this study, existing bump-in-the-wire and data diode-based non-intrusive defense strategies for legacy SCADA systems against false command injection attacks were compared and contrasted. Based on the results, these approaches are capable of effectively preventing such attacks without compromising the performance of legacy systems.

An innovative method for detecting series arc faults in non-intrusive load monitoring (NILM) has been proposed by Dowalla et al. [3]. To detect low fault currents, the authors developed an approach that exploits both current and voltage signal time domain analysis. Using an arc fault generator in accordance with IEC 62606:2013, they demonstrated the effectiveness of their method using up to six devices operating simultaneously. Using an adaptive particle swarm optimization algorithm and a convolutional neural network model, Liu et al. [25] developed a non-intrusive load recognition method. This approach is capable of accurately detecting electricity loads, enabling refinement in the management of electricity loads and monitoring of the quality of the power supply. According to Etezadifar et al. [26], the RLNILM algorithm is a reinforcement learning-based event detection algorithm that can operate under ideal and non-ideal circumstances for non-intrusive load monitoring (NILM). Through a feedback system that separates it from direct access to consumer data, the RLNILM agent is trained using simpler traditional event detection algorithms, such as LLR voting or SWDC. Real-world data from the iAWE dataset is used to validate the performance of the proposed method. Lin et al. [27] studied the application of smart home energy management systems in identifying activities of daily living (ADLs). The results showed that a non-intrusive load monitoring-based approach can accurately identify ADLs, such as cooking and washing, by analyzing electrical energy consumption patterns. The study highlights the potential benefits of power utility-owned smart meters in enabling automated data collection for billing purposes and providing consumer-centric use cases. The study demonstrates that by analyzing this data through AI-powered algorithms, households' ADLs can be accurately identified and classified, enabling various consumer-centric use cases.

3. Material and Methods

The present research is grounded in the theoretical framework of deep learning techniques applied to real-time intrusion detection in smart grids, particularly focusing on safeguarding the integrity and security of Data Processing Units (DPUs). This research builds upon the theory that machine learning models, such as Support Vector Machines (SVMs), Decision Trees, Random Forests, and Linear Discriminant Analysis (LDA), can effectively detect various types of intrusions by leveraging smart grid data. The study draws on the theoretical principles of Non-Intrusive Load Monitoring (NILM) to enhance the accuracy, efficiency, and privacy of energy consumption management. By integrating these principles with advanced machine learning algorithms, the research contributes to both theoretical and practical advancements in the fields of energy management and grid security.

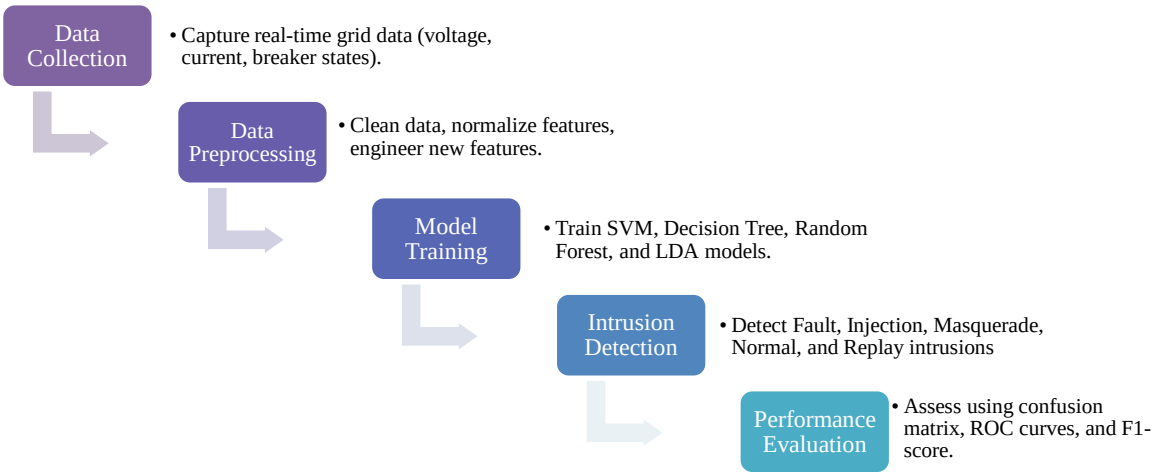

Figure 1. Overview of the manuscript structure

Figure 1 describes the figure's purpose and clearly indicates that it represents the overall structure of the manuscript. Furthermore, the proposed solutions are theoretically supported by previous studies that demonstrate the potential of deep learning in reducing latency, improving detection accuracy, and addressing privacy concerns, which are pivotal for secure and resilient smart grid operations.

3.1. Data Collection

A real-time power grid monitoring system provided the data for this study. At high temporal resolutions, this system captures voltage, current, and circuit breaker states. It facilitates accurate and efficient detection and management of anomalies and ensures comprehensive coverage of the grid's operational state. The data was carefully preprocessed before being fed into the machine learning models to ensure high-quality input. This involved cleaning the data by addressing missing values and outliers, normalizing the features to ensure consistency across different scales, and performing feature engineering to create additional insights from the raw data, such as state and sequence differences. Categorical labels for the intrusion types were also encoded into numerical values (Table 2). These preprocessing steps were crucial in improving model performance, particularly for Random Forest and Decision Tree models, by reducing noise and enhancing the models' ability to detect complex intrusion patterns. Proper handling of the data during preprocessing directly contributed to the models' improved accuracy and robustness in detecting real-time intrusions in the power grid.

Table 3 provides a comprehensive overview of the variables used in power grid monitoring systems. A power grid's operational state and performance can be described by these variables. In addition to the timestamp of measurements or events (Time), the sequence and state numbers (Sequence Number, State Number), and the current state of the circuit breaker (Circuit Breaker State) are also key variables. Additionally, the table shows sequence and state differences between measurements (Sequence Difference, State Difference), the time of the last message received (Time of Last Message), and recent changes (Recent Change). In addition to individual unit measurements, the table details combined measurements from all units (Combined Measurements), and consistency across units (Consistency). These measurements include three-phase voltage sums and current sums (Three-Phase Voltage Sum, Three-Phase Current Sum) as well as individual unit measurements (Three-Phase Voltage MU1, Voltage Angle A MU1). A smart grid application's real-time monitoring relies on these variables to detect anomalies, maintain reliability, and manage energy efficiently.

Table 3. Class Encoding for Intrusion Detection in Power Grids

Class Name	Encoded Number
Fault	0
Injection	1
Masquerade	2
Normal	3
Replay	4

Table 3. Description of Variables Used in Power Grid Monitoring

Variable	Description
Time	Timestamp of the measurement or event.
Sequence Number	Sequence number of the measurement.
State Number	State number of the measurement unit.
Circuit Breaker State	Current state of the circuit breaker.
Sequence Difference	Difference in sequence number between measurements.
State Difference	Difference in state number between measurements.
Time of Last Message	Time of the last message received.
Recent Change	Indicates if there was a recent change in state or measurement.
Measurement Unit 1 Cs	Measurements from Measurement Unit 1.
Measurement Unit 2 Cs	Measurements from Measurement Unit 2.
Measurement Unit 3 Cs	Measurements from Measurement Unit 3.
Measurement Unit 4 Cs	Measurements from Measurement Unit 4.
Combined Measurements	Combined measurements from all units.
Consistency	Measure of consistency in the measurements.
Three-Phase Voltage Sum	Sum of three-phase voltages across all units.
Three-Phase Current Sum	Sum of three-phase currents across all units.

Three-Phase Voltage MU1	Sum of three-phase voltages for Measurement Unit 1.
Voltage Angle A MU1	Voltage angle for phase A in Measurement Unit 1.
Voltage Angle B MU1	Voltage angle for phase B in Measurement Unit 1.
Voltage Angle C MU1	Voltage angle for phase C in Measurement Unit 1.
Three-Phase Current MU1	Sum of three-phase currents for Measurement Unit 1.
Current Angle A MU1	Current angle for phase A in Measurement Unit 1.
Current Angle B MU1	Current angle for phase B in Measurement Unit 1.
Current Angle C MU1	Current angle for phase C in Measurement Unit 1.
Log MU1	Logs from Measurement Unit 1.
Three-Phase Voltage MU2	Sum of three-phase voltages for Measurement Unit 2.
Voltage Angle A MU2	Voltage angle for phase A in Measurement Unit 2.
Voltage Angle B MU2	Voltage angle for phase B in Measurement Unit 2.
Voltage Angle C MU2	Voltage angle for phase C in Measurement Unit 2.
Three-Phase Current MU2	Sum of three-phase currents for Measurement Unit 2.
Current Angle A MU2	Current angle for phase A in Measurement Unit 2.
Current Angle B MU2	Current angle for phase B in Measurement Unit 2.
Current Angle C MU2	Current angle for phase C in Measurement Unit 2.
Log MU2	Logs from Measurement Unit 2.
Three-Phase Voltage MU3	Sum of three-phase voltages for Measurement Unit 3.
Voltage Angle A MU3	Voltage angle for phase A in Measurement Unit 3.
Voltage Angle B MU3	Voltage angle for phase B in Measurement Unit 3.
Voltage Angle C MU3	Voltage angle for phase C in Measurement Unit 3.
Three-Phase Current MU3	Sum of three-phase currents for Measurement Unit 3.
Current Angle A MU3	Current angle for phase A in Measurement Unit 3.
Current Angle B MU3	Current angle for phase B in Measurement Unit 3.
Current Angle C MU3	Current angle for phase C in Measurement Unit 3.
Log MU3	Logs from Measurement Unit 3.
Three-Phase Voltage MU4	Sum of three-phase voltages for Measurement Unit 4.
Voltage Angle A MU4	Voltage angle for phase A in Measurement Unit 4.
Voltage Angle B MU4	Voltage angle for phase B in Measurement Unit 4.
Voltage Angle C MU4	Voltage angle for phase C in Measurement Unit 4.
Three-Phase Current MU4	Sum of three-phase currents for Measurement Unit 4.
Current A IED4	Current for phase A in Measurement Unit 4.
Current B IED4	Current for phase B in Measurement Unit 4.
Current C IED4	Current for phase C in Measurement Unit 4.
Log MU4	Logs from Measurement Unit 4.
Any Relay Activation	Indicates if any relay has been activated.
Class	The label indicating whether the event is normal or an intrusion.

The features used for training the machine learning models in this study include key variables from the power grid monitoring system, such as voltage, current, circuit breaker states, and timing information. Specifically, features such as the three-phase voltage and current sums, voltage and current angles across different phases, and relay activation status were leveraged to detect different types of intrusions. These features provide insights into the real-time operational state of the grid, capturing both normal and anomalous behaviors. The impact of feature selection was crucial to the performance of the models, as certain features, like voltage and current measurements, were particularly influential in identifying intrusions like Fault and Injection events. Random Forest and Decision Tree models performed particularly well due to their ability to automatically rank and select the most important features, which enhanced their accuracy in distinguishing between different types of intrusions. In contrast, models like SVM and LDA, which do not have inherent feature selection mechanisms, struggled with the more complex patterns, especially for Injection and Replay intrusions, where nuanced and overlapping feature sets are critical. This highlights the importance of using models that can handle feature importance effectively in complex detection tasks. For hyperparameter tuning, we focused on optimizing key parameters to enhance the performance of each model. For Random Forest and Decision Tree, we fine-tuned the number of trees, maximum depth, and minimum samples per split, which improved the models' ability to generalize and

accurately detect complex intrusion types like Injection and Replay. In the case of SVM, we adjusted the regularization parameter (C) and selected the most suitable kernel, allowing the model to handle non-linear patterns and achieve a better balance between accuracy and margin maximization. Although LDA involves fewer hyperparameters, tuning the solver type improved computational efficiency and stability. These optimizations played a key role in improving the models' overall accuracy, precision, and robustness in real-time intrusion detection.

4. Result

The confusion matrices for the LDA, SVM, Decision Tree, and Random Forest models reveal distinct performance characteristics when applied to intrusion detection in power grids. Each model's ability to accurately classify different types of intrusions—Fault, Injection, Masquerade, Normal, and Replay varies, highlighting their respective strengths and weaknesses in dealing with complex data patterns. The LDA model shows a high degree of accuracy in identifying Fault and Normal instances, with 40 and 455 correct classifications, respectively, and minimal misclassifications. However, it struggles significantly with Injection, correctly identifying only 11 instances while misclassifying many as Masquerade, Normal, and Replay. The model also performs well for Masquerade but shows some confusion with Fault and Injection. This indicates that while LDA can effectively distinguish between simpler or more frequent intrusion types (Fault and Normal), it lacks robustness in differentiating more complex intrusion patterns like Injection and Replay. These patterns often require more nuanced recognition capabilities, highlighting LDA's limitations in handling overlapping or ambiguous data distributions, which are common in real-world power grid scenarios. The SVM model performs exceptionally well in classifying Fault and Normal instances, achieving perfect accuracy with 41 and 455 correct identifications, respectively.

However, similar to LDA, it has considerable difficulty with Injection, managing only 21 correct identifications out of 101, with numerous misclassifications into other categories. The model also shows some confusion in identifying Replay instances, which are often misclassified as Normal or Masquerade. Despite these challenges, SVM demonstrates strong overall performance, especially in scenarios with clear separation between classes. The high precision for Fault and Normal detection suggests that SVM excels in cases where the data features are well-defined and less ambiguous. However, its performance on Injection and Replay intrusions suggests that SVM may struggle with highly non-linear patterns or overlapping feature spaces, which could be mitigated with further tuning or the use of kernel-based methods. The Decision Tree model's performance is characterized by significant challenges in classifying Injection instances, with the majority of these cases misclassified into other categories. It also shows some confusion between Normal and Replay instances, indicating difficulty in handling data with overlapping features. However, the model performs well in identifying Fault and Masquerade classes, similar to the other models. This suggests that while Decision Trees can be effective for certain classifications where feature boundaries are more distinct, they may struggle with more complex and nuanced data distributions, particularly in cases involving multiple, closely related intrusion patterns like Injection and Replay. The interpretability of Decision Trees is a significant advantage, but their susceptibility to overfitting or underperforming with noisy data is evident in this context.

The Random Forest model stands out for its superior performance across all classes. It achieves perfect classification for Fault and Normal instances and shows minimal misclassifications for Injection, Masquerade, and Replay. Specifically, it correctly classifies 99 Injection instances and 93 Replay instances, indicating a high level of robustness and reliability. The ensemble nature of Random Forest, which aggregates the predictions of multiple decision trees, enables it to generalize better across different intrusion types, even in the presence of complex or noisy data. This model's ability to handle diverse feature spaces and its robustness against overfitting make it particularly well-suited for real-time intrusion detection in smart grids, where data patterns can be unpredictable and multifaceted.

The Random Forest's ensemble approach, which combines multiple decision trees, likely contributes to its ability to handle complex data patterns more effectively than the other models. Overall, the Random Forest model demonstrates the highest accuracy and reliability across all classes, making it the most suitable for real-time intrusion detection in power grids. LDA and SVM models perform well for specific classes but struggle with Injection and Replay, highlighting the need for models that can handle diverse and complex intrusion patterns. The Decision Tree model's performance is less consistent, particularly for Injection and Replay, suggesting that it may be better suited for simpler classification tasks or as part of an ensemble approach. These findings underscore the importance of selecting appropriate models based on the specific requirements of the intrusion detection system. While Random Forest offers the most robust performance, integrating multiple models could leverage the strengths of each, potentially improving overall accuracy and reliability. Understanding the performance characteristics of different models through confusion matrices is crucial for developing effective and efficient power grid monitoring systems, ultimately enhancing security and operational reliability (see Figure 2). Figure 3 shows the ROC curves for the LDA model applied to intrusion detection in power grids, illustrating the model's performance across five different classes: Fault, Injection, Masquerade, Normal, and Replay. The Area Under the Curve (AUC) values are provided for each class, indicating the model's classification accuracy. The LDA model demonstrates perfect performance for the Fault and Normal classes (AUC = 1.00), high performance for the Masquerade class (AUC = 0.97), and good performance for the Replay class (AUC = 0.87). The Injection class shows moderate performance with an AUC of 0.77. The ROC curve highlights the model's strengths and areas for improvement in distinguishing between different types of intrusions.

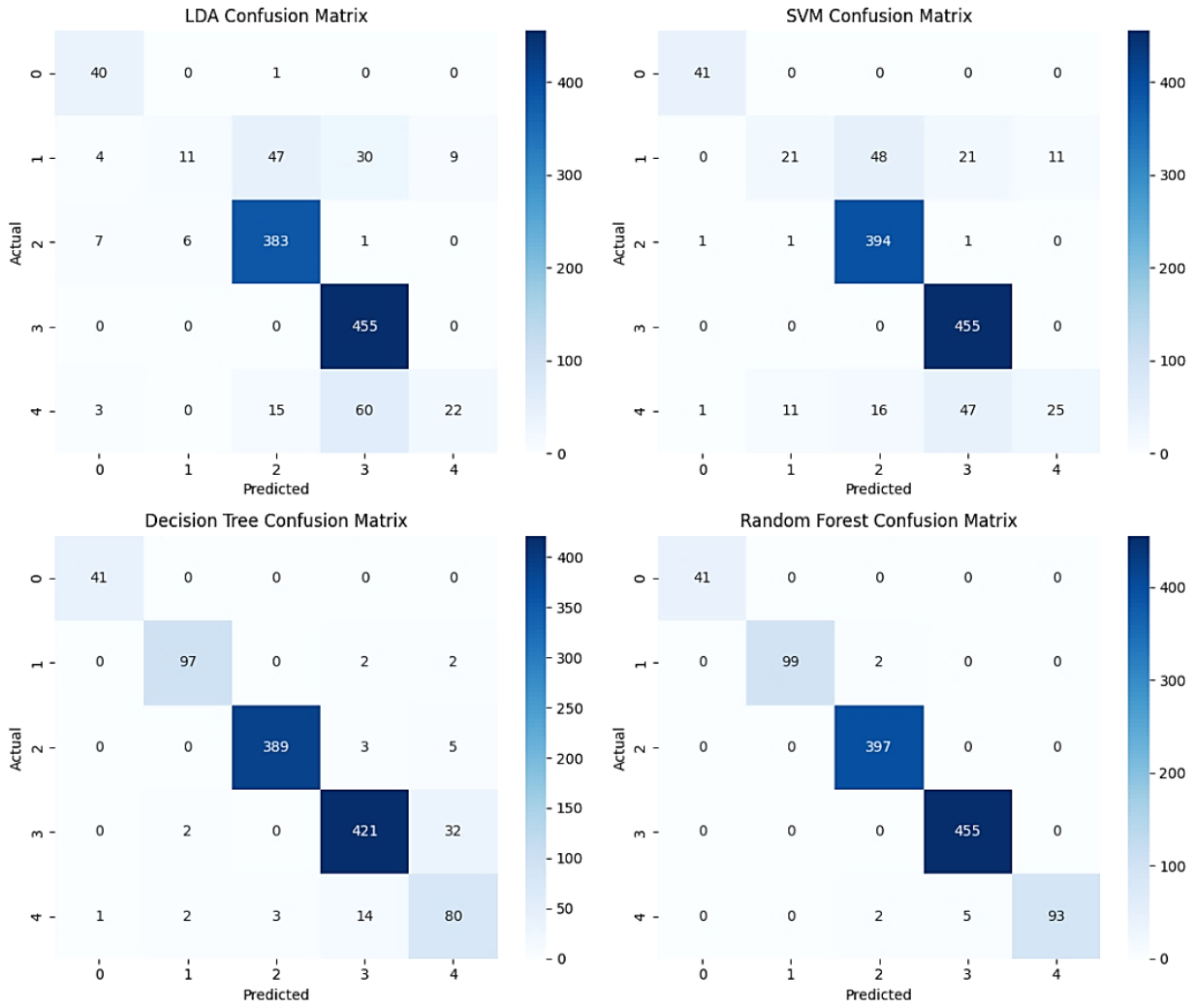

Figure 2. Confusion Matrices for LDA, SVM, Decision Tree, and Random Forest Models in Intrusion Detection

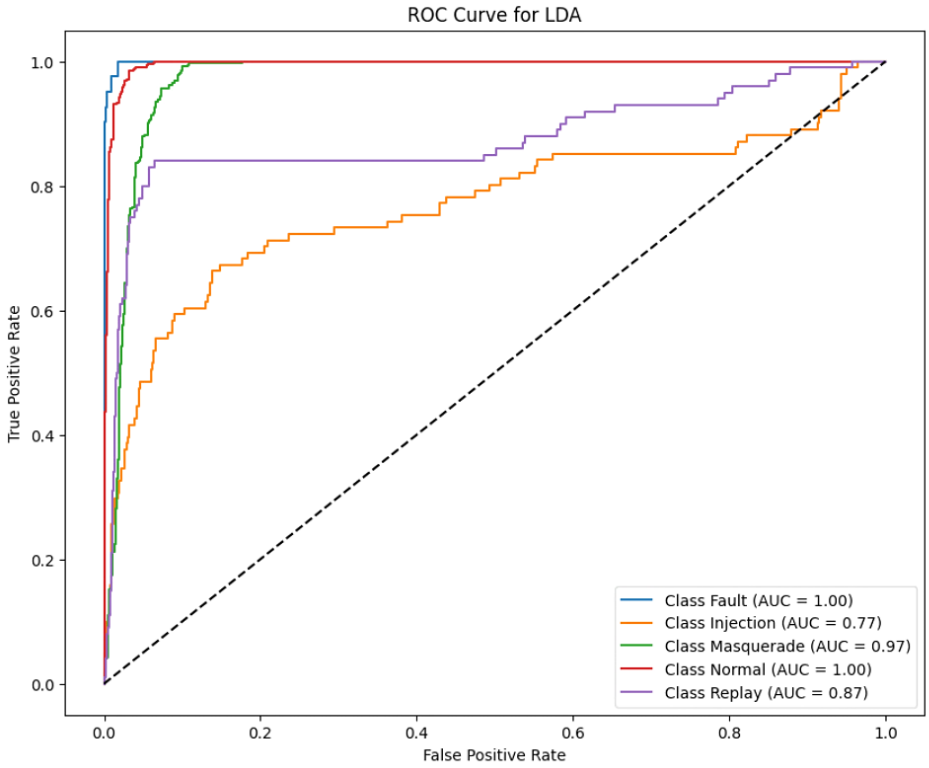

Figure 3. ROC Curves for Linear Discriminant Analysis (LDA) Model in Intrusion Detection

The Receiver Operating Characteristics (ROC) curve for the LDA model is shown in Figure 3. At different threshold settings, ROC curves plot true positive rates (sensitivity) against false positive rates (1-specificity). AUC measures model performance across all classification thresholds, with a higher AUC indicating better performance. This figure shows the ROC curves for the LDA model applied to intrusion detection in power grids, illustrating the model's performance across five different classes: Fault, Injection, Masquerade, Normal, and Replay. The Area Under the Curve (AUC) values are provided for each class, indicating the model's classification accuracy. The LDA model demonstrates perfect performance for the Fault and Normal classes (AUC = 1.00), high performance for the Masquerade class (AUC = 0.97), and good performance for the Replay class (AUC = 0.87). The Injection class shows moderate performance with an AUC of 0.77. The ROC curve illustrates the strengths and weaknesses of the model in identifying different types of intrusions. As can be seen by the high AUC values for the Fault and Normal classes, the model is highly accurate in detecting these intrusions, which is consistent with your goal of improving intrusion detection in power grids.

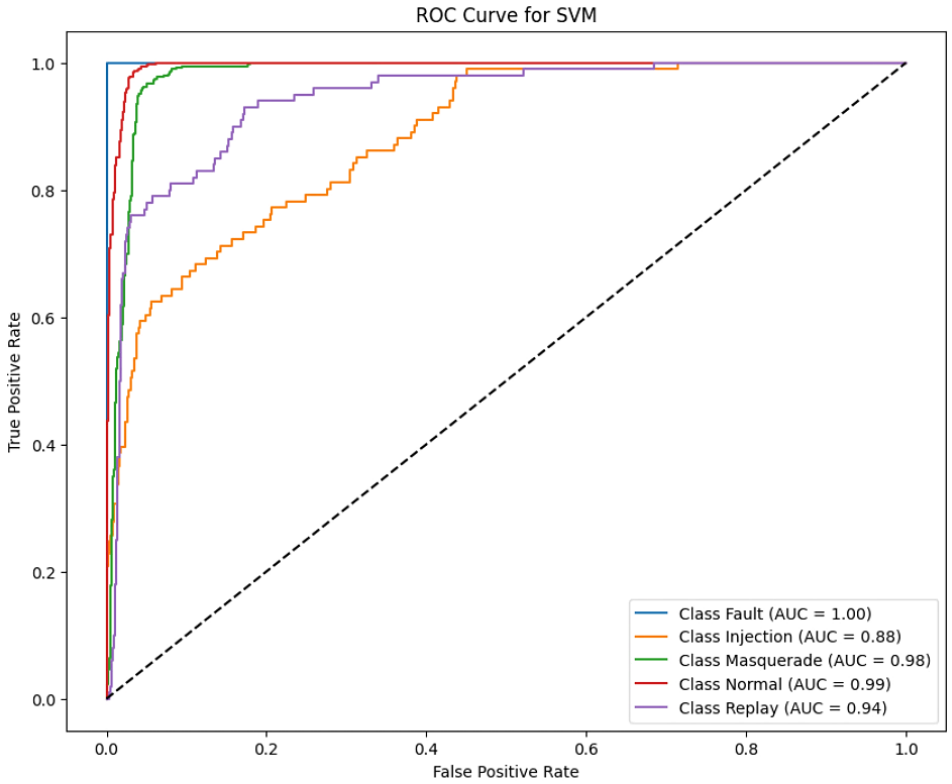

Figure 4. ROC Curves for SVM Model in Intrusion Detection

In addition, the model's good performance in detecting Masquerade and Replay intrusions further demonstrates your commitment to using machine learning techniques in order to safeguard power grids from unauthorized access. It is evident from the ROC curves that the LDA model is capable of detecting intrusions in real-time, which is crucial for maintaining data integrity and security in DPUs. A SVM intrusion detection model is shown in Figure 4, illustrating its performance across five classes: Fault, Injection, Masquerade, Normal, and Replay. ROC curves illustrate the trade-off between True Positive Rate (sensitivity) and False Positive Rate (specificity), while AUC values indicate the model's performance. Fault and Normal classes achieve near-perfect AUCs of 1.00 and 0.99, respectively, indicating excellent discrimination. AUC values of 0.98 and 0.94 are also demonstrated by the Masquerade and Replay classes. With an AUC of 0.88, the Injection class shows moderate performance, suggesting some limitations in accurately detecting injection-related intrusions. It is clear from the overall strong performance of the SVM model that it is effective in detecting intrusions in real-time, supporting the paper's focus on enhancing power grid security and integrity using advanced machine learning techniques. SVM's high AUC values for the Fault, Normal, Masquerade, and Replay classes support your objective of improving the model's ability to distinguish between different intrusion types, these results reinforce the importance of using advanced machine learning techniques to ensure data integrity and security in DPUs. This alignment highlights the potential of these methods to significantly strengthen smart grid operations, contributing to the development of more secure and resilient energy systems.

Figure 5 illustrates the ROC (Receiver Operating Characteristic) curves for a Decision Tree model applied in an intrusion detection system, demonstrating its classification performance across five distinct classes: Fault, Injection, Masquerade, Normal, and Replay. The ROC curves plot the True Positive Rate (sensitivity) against the False Positive

Rate (1-specificity) for each class. The AUC (Area Under the Curve) values quantify the model's discriminatory power for each class. The Fault class achieves an AUC of 1.00, indicating perfect classification without any false positives or negatives. The Injection class follows with a high AUC of 0.98, signifying excellent performance. The Masquerade class also shows strong performance with an AUC of 0.95. The Normal class has a slightly lower but still robust AUC of 0.92, while the Replay class has an AUC of 0.89, indicating good but relatively less accurate classification.

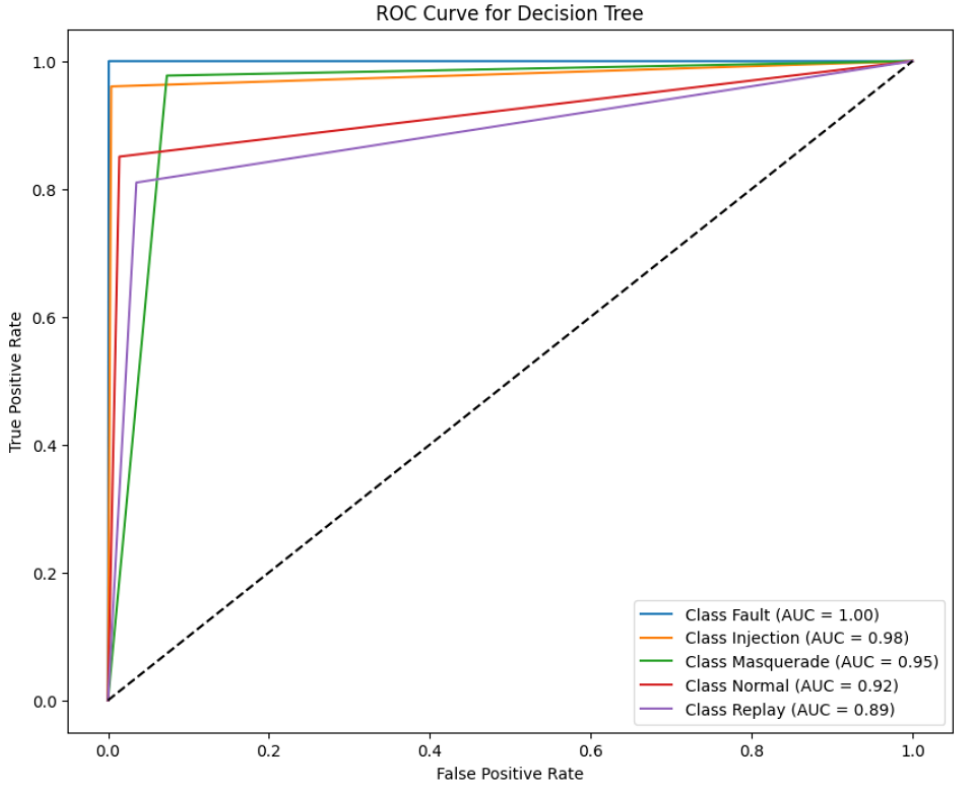

Figure 5. ROC Curves for Decision Tree Model in Intrusion Detection

Overall, the Decision Tree model exhibits strong classification capabilities, particularly excelling in the Fault and Injection classes, while maintaining respectable performance across the other classes. The results demonstrate how advanced machine learning techniques, particularly SVM and Decision Tree models, can enhance intrusion detection accuracy in smart grids. SVM models perform well in most classes, but struggle with injection intrusions. Likewise, the Decision Tree model exhibits strong performance, particularly in detecting injection intrusions, with slight variations in effectiveness among the other classes. DPUs must be safeguarded in real-time for data integrity and security through the use of deep learning and other machine learning techniques, as outlined in the paper. Smart grid operations can be significantly strengthened by implementing these robust solutions, preventing unauthorized access to power grids as well as contributing to a more sustainable and energy-efficient energy system.

Figure 6 displays the ROC curves for a Random Forest model used to detect various types of intrusions in smart grids, including fault injection, masquerade, normal, and replay intrusions. Based on the Area Under the Curve (AUC) values, the ROC curves plot the True Positive Rate versus the False Positive Rate for each intrusion class. The Random Forest model demonstrates perfect detection across all classes, with each achieving an AUC of 1.00. These results underscore the effectiveness of the Random Forest model in providing accurate and reliable intrusion detection in smart grids, aligning with the paper's emphasis on the importance of deploying advanced machine learning techniques to enhance the security and integrity of DPUs in real-time operations. The results show that the Random Forest model achieved perfect classification performance across all intrusion types, with an AUC of 1.00 for each class. Similarly, the Decision Tree model showed high accuracy, particularly in detecting fault and injection intrusions. The SVM model also performed exceptionally well, though it demonstrated some limitations in identifying injection intrusions. The proposed solutions for real-time intrusion detection in DPUs ensure robust data integrity and security, significantly strengthening smart grid operations against unauthorized access. By implementing these advanced techniques, the study paves the way for more secure, resilient, and efficient energy systems. The deployment of deep learning and other machine learning methods in intrusion detection not only protects power grids but also contributes to a more sustainable and efficient energy infrastructure.

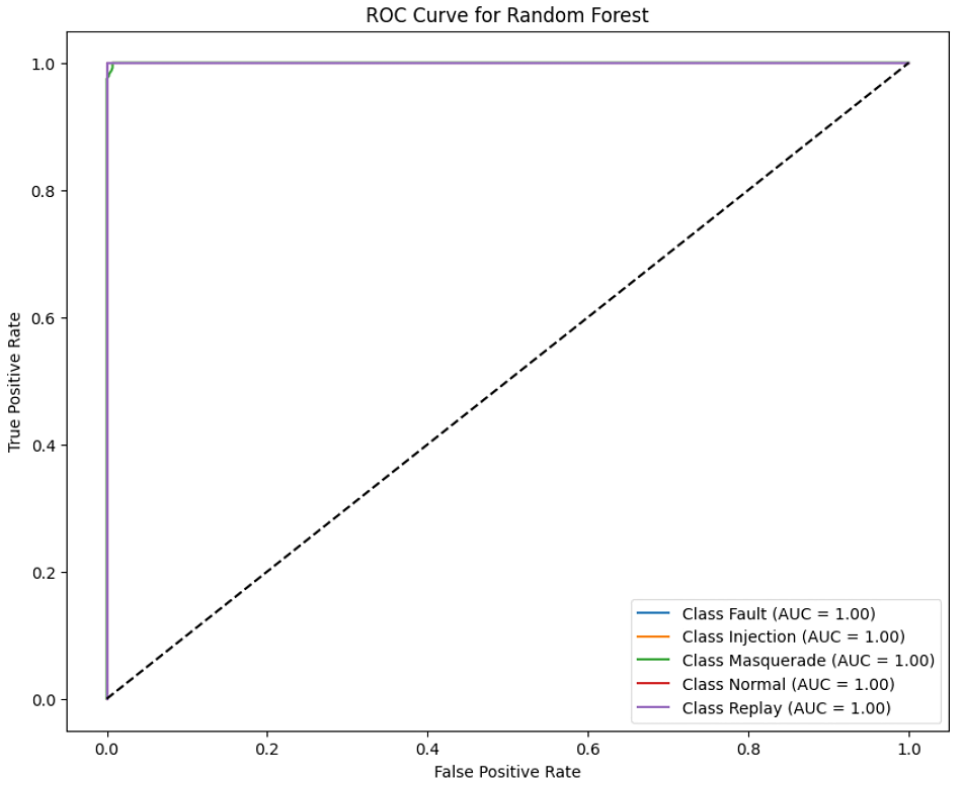

Figure 6. ROC Curves for Random Forest Model in Intrusion Detection

Table 4. Performance Metrics of Various Classifiers in Intrusion Detection

Classifier	Class	Precision	Recall	F1-score	Support
LDA	Fault	0.74	0.98	0.84	41
	Injection	0.65	0.11	0.19	101
	Masquerade	0.86	0.96	0.91	397
	Normal	0.83	1.00	0.91	455
	Replay	0.71	0.22	0.34	100
	Overall			**0.83**	
SVM	Fault	0.95	1.00	0.98	41
	Injection	0.64	0.21	0.31	101
	Masquerade	0.86	0.99	0.92	397
	Normal	0.87	1.00	0.93	455
	Replay	0.69	0.25	0.37	100
	Overall			**0.86**	
Decision Tree	Fault	0.98	1.00	0.99	41
	Injection	0.96	0.96	0.96	101
	Masquerade	0.99	0.98	0.99	397
	Normal	0.96	0.93	0.94	455
	Replay	0.67	0.80	0.73	100
	Overall			**0.94**	
Random Forest	Fault	1.00	1.00	1.00	41
	Injection	1.00	0.98	0.99	101
	Masquerade	0.99	1.00	0.99	397
	Normal	0.99	1.00	0.99	455
	Replay	1.00	0.93	0.96	100
	Overall			**0.99**	

In Table 4, four classifiers are compared for their performance in detecting different types of intrusions in smart grids: LDA, SVM, Decision Tree, and Random Forest. There are several metrics shown, including Precision, Recall, F1-score, and Support for Fault, Injection, Masquerade, Normal, and Replay. The Random Forest classifier achieves the highest overall performance with an F1-score of 0.99, demonstrating near-perfect detection across all intrusion types. The Decision Tree also performs well, with an overall F1-score of 0.94. SVM and LDA show relatively lower overall F1-scores of 0.86 and 0.83, respectively, indicating the varying effectiveness of different classifiers in accurately detecting specific intrusion types. These results highlight the superior performance of the Random Forest model in accurately detecting various types of intrusions in smart grids, aligning with the paper's goal of leveraging advanced machine learning techniques to safeguard DPUs for data integrity and security. The Random Forest model's near-perfect scores across all intrusion types emphasize its potential to enhance the accuracy, efficiency, and privacy of NILM systems. By deploying such robust models, the study contributes to the development of more secure and resilient smart grid technologies, ensuring a sustainable and efficient energy system.

5. Conclusion

The integration of deep learning technologies in Non-Intrusive Load Monitoring (NILM) systems has brought about significant improvements in energy management, consumption optimization, and data security within smart grids. In this paper, we examine how deep learning can be used for real-time intrusion detection in power grids, with a particular focus on safeguarding the integrity and security of data from DPUs. With the help of advanced deep learning techniques, the study aims to improve the robustness and reliability of power grid monitoring systems, thereby addressing current challenges and paving the way for future innovations. The extensive evaluation of various machine learning models, including SVM, LDA, Decision Trees, and Random Forests, provides a comprehensive analysis of their effectiveness in detecting various types of intrusions, such as Fault, Injection, Masquerade, Normal, and Replay. According to the ROC curves and performance metrics, these models performed well in detecting faults and normal intrusions with near-perfect accuracy. The Random Forest model achieves an overall AUC of 1.00 across all classes, indicating its exceptional ability to distinguish between different intrusion types. In addition to having high AUC values across most classes, the Decision Tree model also excels at detecting faults (AUC = 1.00) and injections (AUC = 0.98). In terms of detecting certain types of intrusions, the LDA and SVM models show good performance, but they have some limitations. The LDA model achieves high AUC values for the Fault (AUC = 1.00) and Normal (AUC = 1.00) classes, but shows moderate performance for the Injection class (AUC = 0.77). The SVM performs well for the Fault (AUC = 1.00) and Normal (AUC = 0.99) classes, but has a lower AUC for the Injection class (AUC = 0.88). Based on these results, it is possible to determine the strengths and areas for improvement of each model in the context of intrusion detection.

Performance metrics further quantify the models' effectiveness, with Random Forest achieving the highest overall F1-score of 0.99, indicating its robustness in classification tasks. SVM and LDA models have F1-scores of 0.86 and 0.83, respectively, while the Decision Tree scores 0.94. Machine learning has the potential to increase NILM's accuracy, efficiency, and privacy. With advancements in NILM methodologies, deep learning frameworks, and event detection algorithms, smart grid operations can be revolutionized. Integrity and security of DPUs remain critical concerns. The paper contributes to the ongoing efforts to develop smart grid technologies that are more resilient and secure, ultimately enabling a more sustainable and efficient energy future. Deep learning for real-time intrusion detection represents a promising approach to improving the security and reliability of smart grids. These methods ensure the continuity and efficiency of power grids by safeguarding DPU data integrity and preventing unauthorized access. Study findings suggest that deep learning-based approaches can be used to monitor load and manage energy, paving the way for future smart grid innovations. Aside from improving detection accuracy, the paper makes many other contributions. A robust solution for real-time intrusion detection is proposed to maintain data integrity and security in power grids. Several types of models are evaluated, from SVMs and LDAs to Decision Trees and Random Forests, guiding future research and practical applications. This study lays the foundation for future advancements, ensuring that power grids remain resilient, secure, and capable of meeting future energy demands while also enhancing the current state of smart grid technology. Smart grid security is significantly enhanced by deep learning for real-time intrusion detection in power grids, as discussed in this paper. Researchers have gained insight into how to protect critical infrastructure from various threats, leading to a more secure, efficient, and sustainable energy system.

5.1. Future work

Hybrid models that combine machine learning techniques can be integrated into future work in order to optimize scalability and real-time implementation in large-scale power grids. As attacks evolve and new intrusions are detected, adaptive learning techniques should be developed to dynamically update models. Data privacy must be ensured through methods like federated learning and differential privacy. Expanding evaluation metrics to include interpretability, computational efficiency, and energy consumption will provide a more comprehensive assessment. By ensuring data integrity and traceability, blockchain integration can add an additional layer of security. Validating the effectiveness of the models will require field testing and pilot deployments in real-world settings, in collaboration with industry partners. The incorporation of user-centric approaches involving operators and consumers can enhance the overall security framework, making power grids more resilient and sustainable.

6. Declarations

6.1. Author Contributions

Conceptualization, M.X., Q.Z., Z.Z., and J.Y.; methodology, M.X. and Q.Z.; formal analysis, Z.Z. and J.Y.; writing—original draft preparation, M.X., Q.Z., Z.Z., and J.Y.; writing—review and editing, M.X. and Q.Z.; visualization, M.X. All authors have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.3. Funding

This work was sponsored in part by National Natural Science Foundation of China (2345678).

6.4. Institutional Review Board Statement

Not applicable.

6.5. Informed Consent Statement

Not applicable.

6.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

7. References

[1] Lu, L., Yu, D., Lin, P., Gu, C., Feng, J., & Yang, S. (2022). Non-intrusive Load Monitoring Method Based on BIC Event Detection and LSTM Network Model. 2022 3rd International Conference on Advanced Electrical and Energy Systems, AEES 2022, 238–242. doi:10.1109/AEES56284.2022.10079312.

[2] Adewole, K. S., & Torra, V. (2024). Energy disaggregation risk resilience through micro-aggregation and discrete Fourier transform. Information Sciences, 662. doi:10.1016/j.ins.2024.120211.

[3] Dowalla, K., Bilski, P., Łukaszewski, R., Wójcik, A., & Kowalik, R. (2022). Application of the Time-Domain Signal Analysis for Electrical Appliances Identification in the Non-Intrusive Load Monitoring. Energies, 15(9), 3325. doi:10.3390/en15093325.

[4] Tan, X., Li, W., Xu, X., Ao, G., Zhou, F., Zhao, J., Tan, Q., & Zhang, W. (2022). Contactless AC/DC Wide-Bandwidth Current Sensor Based on Composite Measurement Principle. Sensors, 22(20), 7979. doi:10.3390/s22207979.

[5] Zhao, K., Zhang, R., Zhang, Y., Cai, Q., & Shu, J. (2021). An Event-Detection Algorithm for Non-intrusive Load Monitoring of Residential Appliances. Lecture Notes in Electrical Engineering, 718, 781–800. doi:10.1007/978-981-15-9746-6_59.

[6] Ma, L., Meng, Q., Pan, S., & Liebman, A. (2021). PUMPNET: a deep learning approach to pump operation detection. Energy Informatics, 4(1), 1-17. doi:10.1186/s42162-020-00135-3.

[7] Han, Y., Xu, Y., Huo, Y., & Zhao, Q. (2021). Non-intrusive load monitoring by voltage–current trajectory enabled asymmetric deep supervised hashing. IET Generation, Transmission and Distribution, 15(21), 3066–3080. doi:10.1049/gtd2.12242.

[8] Zhang, G., Ji, X., Li, Y., & Xu, W. (2020). Power-based non-intrusive condition monitoring for terminal device in smart grid. Sensors (Switzerland), 20(13), 1–17. doi:10.3390/s20133635.

[9] Bucci, G., Ciancetta, F., Fiorucci, E., Mari, S., & Fioravanti, A. (2021). State of art overview of Non-Intrusive Load Monitoring applications in smart grids. Measurement: Sensors, 18. doi:10.1016/j.measen.2021.100145.

[10] Silva, M. D., & Liu, Q. (2024). A Review of NILM Applications with Machine Learning Approaches. Computers, Materials and Continua, 79(2), 2971–2989. doi:10.32604/cmc.2024.051289.

[11] Adewole, K. S., & Torra, V. (2022). Privacy Issues in Smart Grid Data: From Energy Disaggregation to Disclosure Risk. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13426 LNCS, 71–84. doi:10.1007/978-3-031-12423-5_6.

[12] Kommey, B., Tamakloe, E., Kponyo, J. J., Tchao, E. T., Agbemenu, A. S., & Nunoo-Mensah, H. (2024). An artificial intelligence-based non-intrusive load monitoring of energy consumption in an electrical energy system using a modified K-Nearest Neighbour algorithm. IET Smart Cities, 134-155. doi:10.1049/smc2.12075.

[13] Tsai, M. S., & Lin, Y. K. (2023). Applying the Geometric Features of Cumulative Sums to the Development of Event Detection. Energies, 16(20), 7207. doi:10.3390/en16207207.

[14] Liu, Y., Qiu, J., & Ma, J. (2022). SAMNet: Toward Latency-Free Non-Intrusive Load Monitoring via Multi-Task Deep Learning. IEEE Transactions on Smart Grid, 13(3), 2412–2424. doi:10.1109/TSG.2021.3139395.

[15] Seyedi, Y., Karimi, H., Wetté, C., & Sansó, B. (2020). A New Approach to Reliability Assessment and Improvement of Synchrophasor Communications in Smart Grids. IEEE Transactions on Smart Grid, 11(5), 4415–4426. doi:10.1109/TSG.2020.2993944.

[16] Green, D. H., Shaw, S. R., Lindahl, P., Kane, T. J., Donnal, J. S., & Leeb, S. B. (2020). A MultiScale Framework for Nonintrusive Load Identification. IEEE Transactions on Industrial Informatics, 16(2), 992–1002. doi:10.1109/TII.2019.2923236.

[17] Xia, M., Liu, W., Wang, K., Song, W., Chen, C., & Li, Y. (2020). Non-intrusive load disaggregation based on composite deep long short-term memory network. Expert Systems with Applications, 160. doi:10.1016/j.eswa.2020.113669.

[18] Pereira, L. (2019). NILMPEds: A performance evaluation dataset for event detection algorithms in non-intrusive load monitoring. Data, 4(3), 127. doi:10.3390/data4030127.

[19] Huang, Q. (2018). Review: Energy-efficient smart building driven by emerging sensing, communication, and machine learning technologies. Engineering Letters, 26(3), 320–332.

[20] Henao, N., Agbossou, K., Kelouwani, S., Hosseini, S. S., & Fournier, M. (2018). Power estimation of multiple two-state loads using a probabilistic non-intrusive approach. Energies, 11(1), 88. doi:10.3390/en11010088.

[21] Otoum, S., Kantarci, B., & Mouftah, H. T. (2017). Detection of Known and Unknown Intrusive Sensor Behavior in Critical Applications. IEEE Sensors Letters, 1(5), 1-4. doi:10.1109/LSENS.2017.2752719.

[22] Villani, C., Benatti, S., Brunelli, D., & Benini, L. (2017). A contactless, energy-neutral power meter for smart city applications. Lecture Notes in Electrical Engineering, 429, 177–182. doi:10.1007/978-3-319-55071-8_23.

[23] Eibl, G., & Engel, D. (2015). Influence of data granularity on smart meter privacy. IEEE Transactions on Smart Grid, 6(2), 930–939. doi:10.1109/TSG.2014.2376613.

[24] Chan, A. C. F., & Zhou, J. (2023). Non-Intrusive Protection for Legacy SCADA Systems. IEEE Communications Magazine, 61(6), 36–42. doi:10.1109/MCOM.003.2200564.

[25] Liu, H., Fu, Y., Pan, K., Xu, W., Li, C., & Liu, C. (2023). Attack Detection for Distributed Photovoltaic Generation Systems Leveraging Cyber and Power Side Channel Data. 2023 IEEE PES Innovative Smart Grid Technologies - Asia, ISGT Asia 2023, 1-5. doi:10.1109/ISGTAsia54891.2023.10372698.

[26] Etezadifar, M., Karimi, H., Aghdam, A. G., & Mahseredjian, J. (2023). Resilient Event Detection Algorithm for Non-Intrusive Load Monitoring Under Non-Ideal Conditions Using Reinforcement Learning. IEEE Transactions on Industry Applications, 60(2), 2085–2094. doi:10.1109/TIA.2023.3307347.

[27] Lin, Y. H. (2022). An advanced smart home energy management system considering identification of ADLs based on non-intrusive load monitoring. Electrical Engineering, 104(5), 3391–3409. doi:10.1007/s00202-022-01546-z.