Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: https://www.science-gate.com/IJAAS.html

A lightweight machine learning-based intrusion detection system for smart grids

Laila Nassef*

Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

ARTICLE INFO

Article history:
Received 18 July 2025
Received in revised form
13 November 2025
Accepted 3 March 2026

Keywords:
Smart grid security
Intrusion detection
Lightweight models
Edge intelligence
Machine learning

ABSTRACT

A large volume of sensitive raw data is continuously collected from data acquisition systems within the monitoring and control networks of the power grid to support key applications in the centralized control system for smart grid operation, management, and planning. Although these communication networks provide wide-area and high-speed connectivity, they also increase the risk of cyberattacks that threaten the grid's critical physical infrastructure. The current centralized approach to intrusion detection cannot meet the strict quality-of-service requirements of latency-sensitive applications, and the growing size and complexity of learning models further increase communication and computation demands. Edge-intelligent access points offer a promising solution by enabling lightweight learning models to run close to data sources and provide fast responses to protect the core infrastructure. This paper proposes a lightweight machine learning-based intrusion detection system to support a shift toward distributed learning. Six learning models are used for feature extraction and classification, and the Synthetic Minority Oversampling Technique (SMOTE) is applied to balance the dataset. The model's performance is evaluated under binary and multiclass classification scenarios, and the results show excellent accuracy, short training time, and strong ability to distinguish various attack types, demonstrating its suitability for smart grid environments.

1. Introduction

With the proliferation of smart grid technologies and the exponential growth of physical infrastructure, a huge volume of data is generated within the monitoring and control networks of the smart grid to support the diverse applications. A smart grid is composed of three main domains of generation, transmission, and distribution (T&D), and consumers. The generation domain integrates a diversity of non-renewable energy sources, such as oil, coal, natural gas, and nuclear energy, and the renewable energy sources, including wind, solar, hydrogen, hydropower, geothermal, and biofuels (Islam et al., 2025). The T&D domain facilitates the high voltage transportation of energy from the generation sources to distribution stations and substations through transmission lines and transformers (Mejia-Ruiz et al., 2025). The third domain is the consumer's domain, which supplies energy to the residential, commercial, and industrial customers. Smart meters are deployed in this domain; however, smart meters have their own separate communication infrastructure called Advanced Metering Infrastructure (AMI).

Both the generation and T&D domains are monitored by three main data acquisition systems to collect real-time measurement data from the highly distributed physical infrastructure, such as current, voltage, phase, temperature, and relative humidity parameters. The traditional Supervisory Control and Data Acquisition (SCADA) collects data at low sampling rates and measures data at predefined time intervals. The Wide Area Monitoring System (WAMS) acquires data from advanced sensors called Phasor Measurement Units (PMUs) at a high sampling rate. The Wide Area Monitoring, Protection and Control (WAMPAC) complements both SCADA and WAMS systems with high sampling rates over a wider geographic area. Fig. 1 shows the synchro-phasor network of both generation and T&D

* Corresponding Author.
Email Address: lmohamed@kau.edu.sa
https://doi.org/10.21833/ijaas.2026.03.006
Corresponding author's ORCID profile:
https://orcid.org/0000-0001-9707-1259

domains of the Smart Grid, where renewable energy distributions are monitored by Micro-PMUs and integrated into T&D (Vahidi et al., 2023). The hierarchical architecture of the monitoring network collects and aggregates data from the wide area High Voltage Direct Current (HVDC) substations, with high capacity and long-distance power transmission, and is integrated with asynchronous Alternating Current (AC) transmission systems (Sundararajan et al., 2019). At the lowest level of physical infrastructure, PMUs are strategically installed at the critical components to capture synchronized measurements. Fig. 2 illustrates the collection of data from Current Transformers (CT) and Voltage Transformers (VT), which are merged by the Merging Unit (MU), and the local Remote Terminal Unit (RTU) converts data to digital form and forwards it to their local Phasor Data Concentrators (PDCs). Local PDCs have limited resources and only provide local validation checks and local data aggregation of concentrated synchro phasor data streams for the regional PDCs. Regional PDCs receive data from multiple local PDCs and forward data to the third level of Super PDC to perform further data aggregation and data quality checks. Multiple Super PDCs communicate raw measurement data to the Phasor GateWays (PGWs), which are interconnected with other PGWs in different regions. PGWs are equipped with communication gateways, typically found in routers and switches, to perform networking services such as addressing, routing, basic security, and encryption before uploading data to the utility Centralized Control System (CCS) for further analysis and inference (Presekal et al., 2024). Fig. 2 presents a simplified view of WAMPAC architecture.

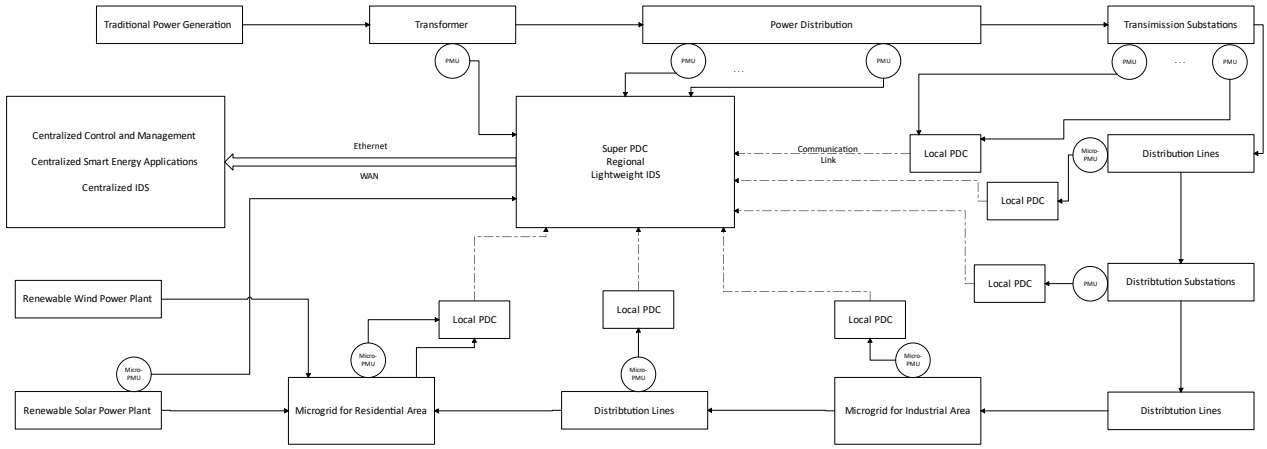

Fig. 1: Wide area synchro-phasor networks

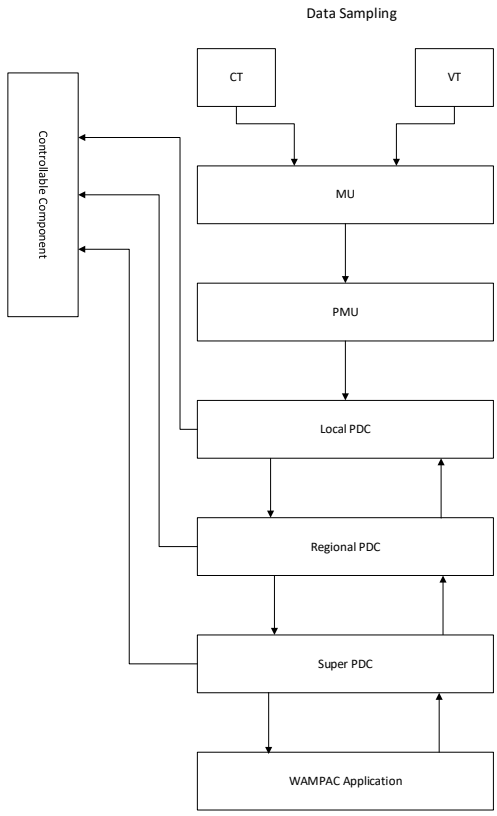

Fig. 2: Communication infrastructure of WAMPAC system

The bidirectional Communication Infrastructure (CI) transfers raw measurement data to feed the diverse applications, including WAMPAC. The corrective actions are propagated back to controllers to safeguard against system failure and wide spread of disturbances. The CI ensures seamless data transmission among various components of the smart grid; however, various proprietary systems with specialized protocols, such as the IEEE C37.118 protocol for substation automation and communication of PMUs to their local PDC, Electronic Devices (IEDs) IEC 61850 for communication beyond local PDCs, and Intelligent IEC 61850-90-5 for long-distance communication between PDCs and CCS. Other standard protocols include high-speed Ethernet wide area network to enable PGWs to communicate with CCS.

The integration of information and communication technologies has significantly enhanced the reliability, stability, and management of the power grid. However, the highly distributed nature of the power grid makes it difficult to physically protect the huge number of components. The traditional SCADA has limitations to handle the dynamics of modernization of the smart grid and was implemented with few or no security measures. The WAMPAC system did not consider security

during the design stage and was deployed without adequate security measures. The interdependencies between the physical infrastructure and CI increase the risk of cyberattacks motivated by cyber terrorists, adversarial nation states, and state-sponsored espionage to deliberately cause catastrophic damages, significant financial losses, and a severe threat to the nation's security.

Attackers generally compromise the confidentiality, integrity, and availability of the measurement data and control actions. Confidentiality attacks include unauthorized access to raw data collected by the acquisition system due to the lack of strong security measures, which could lead to data leakage and security breaches. Integrity attacks target the accuracy and completeness of measurement data and control actions of the critical components of substations, transformers, and circuit breakers. Unauthorized access to this critical data could lead to malfunctions in equipment, mismanagement of power flow, and disruption of power supply, with a serious influence on people's lives. Availability attacks target the availability of systems and applications. In addition, the communication of raw data could reveal sensitive information about the location of critical components, such as a nuclear power plant. The timeline and history of cybersecurity attacks against power grids are provided in Achaal et al. (2024).

As adversaries become more sophisticated, protecting sensitive data to ensure security and preserve privacy is the most important challenge to the growth and deployment of the smart grid. Intrusion Detection Systems (IDSs) are able to identify subtle deviations from normal data behavior and detect any suspicious activities to alert security personnel to prevent potential threats from causing damage. Machine Learning (ML) and Deep Learning (DL) based IDSs are essential to ensure accurate detection and classifications of cyberattacks by performing continuous analysis to differentiate between normal and malicious classes of attacks (Sahani et al., 2023). IDSs receive huge amounts of communication from access points with a substantial increase in communication overheads, and with the bandwidth limitations, slow data rates, and connectivity problems typically found in a harsh smart grid environment, the communication delays increase, especially for long-distance transmissions and high-density deployments (Menzel et al., 2024). Additionally, the CCS could become a focal point of attacks with potential catastrophic consequences and threats to the nation's security. Furthermore, with the increase in size and complexity of IDS models, the model training time increases and influences the response time to cyberattacks. The high dimension and noisy data with complex relationships, and the dependence on specialized protocols with different data sizes and quality contribute to more performance degradation of IDS models. There is an urgent need to protect infrastructure against the increasing risk of cyberattacks and identify vulnerabilities and threats of cyberattacks closer to data sources.

Edge Intelligence (EI) is an enabling technology for the smart grid to reduce communication overheads, latencies, optimize bandwidth usage, and handle the increasing scalability of smart grid deployments. The development of distributed applications at edge and fog EI enabled access points facilitates distributing training and inference to accelerate response and overcome challenges associated with a centralized approach (Mahadevappa et al., 2024). Currently, EI computing is incorporated into major communication access points and is a potential candidate to host the lightweight IDSs for real-time attack detection. Fig. 3 presents the hierarchical distribution of IDS models depending on the capabilities of various levels of architecture (Molokomme et al., 2022). For the rest of this paper, only access points located closer to super PDCs will be considered.

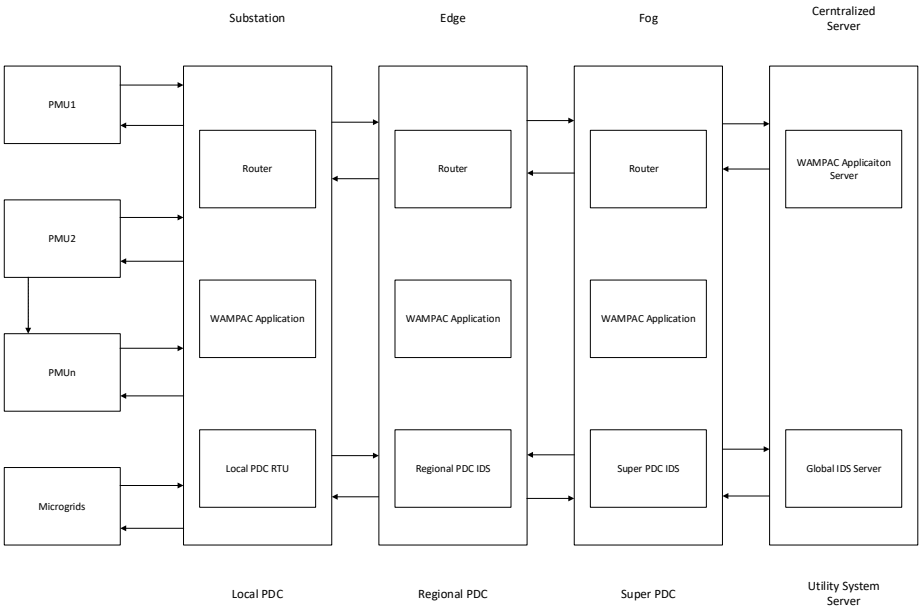

Fig. 3: Hierarchical distribution of the EI-WAMPAC system

With limited work found on distributing IDSs for the smart grid environment in general, the development of a lightweight IDS dedicated specifically to the resource-constrained access points is of great importance. The goal of this paper is to develop a lightweight IDS to solve the challenges associated with traditional centralized applications, including IDSs, to enable the shift toward distributing IDSs. Given that distributed learning is still in its early stages of development with many unsolved challenges, the design of a lightweight IDS provides an immediate solution to enable local training and inference.

This paper paves the way towards the next generation of distributed and collaborative IDSs. Towards that goal, a lightweight hybrid IDS to defend against cyberattacks to be distributed at communication access points is based on six powerful learning models to implement the proposed IDS. Three ensemble ML classifiers of two gradient boosting models of Light Gradient Boosting Model (LGBM) and Extreme Gradient Boosting (XGBoost), and one bagging model, such as Random Forest (RF). In addition to three DL models. Two models for classifications, namely Convolutional Neural Network (CNN) and the Long Short-Term Memory (LSTM), are a type of Recurrent Neural Network (RNN) architecture. The third DL model is the Auto-Encoder (AE) for feature extraction. The imbalanced data cannot be trusted to measure the performance of the developed model, and the Synthetic Minority Oversampling Technique (SMOTE) is implemented to balance the dataset.

The research questions are formulated as follows: How to enhance the model's performance with a powerful feature engineering tool, how to solve problems associated with an imbalanced dataset, how to select lightweight learning models, and how to develop an effective and lightweight IDS. The paper objectives are formulated as: utilize the AE to automate feature extraction and lower data dimensionality, apply SMOTE to balance the dataset, compare the performance of five different classifiers, and develop a lightweight model with four stages of processing, feature extraction, data balancing, classifications, and performance evaluation. The contribution of this research is the development of a lightweight hybrid IDS to locally train the models and overcome the limitations of current centralized IDSs. The key contributions are: Reduction of dimension of dataset, solving the negative impacts of imbalanced datasets on the performance of models, proposing a framework for the proposed lightweight IDS, and evaluating the performance of the proposed system in two scenarios of binary and multiclass classification based on four standard performance metrics.

The organization of this paper is as follows: Section two describes vulnerabilities of access points, security attacks, and current IDSs based on both ML and DL models. Section three proposes the framework for the lightweight IDS. Section four describes the different experiments and their evaluation. Finally, the conclusion and possible future enhancements are provided in section five.

2. Literature review

The heavy reliance on CI exposes raw measurement and control data to malicious attacks to exploit vulnerabilities in the software, hardware, and communication protocols to disrupt operational data with severe consequences. Recently, the frequency of attacks has increased, and many countries have been major targets for attacks due to the digital transformation and the huge adoption of recent technologies. Malicious activities can easily manipulate raw data, with the highest damage achieved by compromising raw measurement data and/or control actions to severely mislead the applications to take erroneous decisions and controllers to impose great damage.

Currently, WAMPAC has security measures such as message integrity and encryption to support authorization and authentication mechanisms to provide the first line of defense. However, these measures are unable to defend against cyberattacks, and a second line of defense is based on IDSs to detect potential attacks. IDSs identify cyberattacks by building a profile from normal traffic to detect any deviation from that profile as an anomaly and report to preventive systems to block the malicious traffic.

Lee et al. (2023) proposed a machine learning based IDS dedicated to photovoltaic power plants and renewable energy sources, to detect cyberattacks against the operational data, collected from power generation and the control actions issued by the SCADA system to manipulate data through Denial of Service (DoS) and man-in-the-middle attacks. Alsirhani et al. (2025) developed a machine learning ensemble model using soft voting and majority voting and trained the IDS over two datasets, one of which is specifically designed for the power system.

The following related works are selected based on their implemented models and datasets, while other related works are selected based on their learning models. Various models are implemented, including RF, XGBoost, and LightGBM.

Wang et al. (2022) advocated DL-based IDS for SCADA systems in power systems and gas pipeline systems. Feature extraction is based on recursive feature elimination (RFE). RF and the LSTM were used as classifiers and achieved good results using three datasets of UNSW-NB15, CIC-IDS2017, and NSL-KDD. Results reveal accuracy of 99.34, 99.75, and 98.31, respectively. In Verma and Ranga (2020), three datasets of CIDDS-001, UNSWNB15, and NSL-KDD are used. The IDS was designed to detect DoS attacks. RF, LGBM, and three others have trained and achieved an accuracy of 94.94. An IoT-based IDS for the smart city is developed in Rashid et al. (2020) using six ML models, including RF and four other classifiers. The training and testing of the model were done over two datasets, where UNSW-BC15

achieved 81.77%, while CICIDS2017 achieved 99.7%. In Almarshdi et al. (2023), an IDS for medical IoT (IoMT) environments is presented based on two DL models, where LSTM is used for classification, and CNN is used to extract features to detect DoS and distributed DoS (DDoS) attacks. The experimental results proved the effectiveness of the proposed system after applying SMOTE, and achieved a high accuracy of 92.89 % over the UNSW-NB15 dataset.

Tang et al. (2020) proposed IDS based on LGBM and AE, where the LGBM model was used for feature engineering and AE for classification. Training and testing were performed over KDD Cup 99, NSLKDD, and UNSW NB15. The model achieved an accuracy of 99.9 over UNSW NB15. A lightweight IoT IDS based on two-stage feature selection and Bayesian optimization is suggested by Zhang et al. (2025). Their results for LGBM indicate high classification accuracies of 96.08% and 97.22% over UNSW-NB15 and TON IoT datasets, respectively. Talukder et al. (2024) proposed an ML-based IDS, and training was performed over three datasets of UNSW-NB15, CIC-IDS-2017, and CIC-IDS-2018. Random oversampling method is used to balance the dataset and stacking feature embedding based on clustering, along with Principal Component Analysis (PCA) for dimension reduction. Results indicate RF as a classifier achieved 99.59%. Dinh et al. (2024) provided an IoT-based IDS based on multiple input AE with an embedded feature selection layer, and combined with RF as a classifier. Three datasets were used to train and test the model, and achieved accuracy of 75.3, 88.3, and 98.8 on the NSLKDD, UNSW-NB15, and IDS2017, respectively. Sayegh et al. (2024) developed an IDS for IoT that is developed on LSTM, and has implemented SMOTE to balance three datasets of CICIDS2017, NSL-KDD, and UNSW-NB15. Results indicate accuracies of 99.34, 99.75, and 98.31, respectively. The IDS developed in Zhao et al. (2023) is based on LGBM as a classifier and combined with CNN as a feature extraction. They trained the model over TON-IoT and BoT-IoT to detect DoS and DDoS attacks. Results show strong detection capability and a more lightweight proposed model with good accuracy of 90.66%. Okey et al. (2022) implemented boosting ensemble learning models based on five classifiers, including RF, LGBM, and XGBoost, among others.

Two oversampling techniques, including SMOTE, are employed to balance the dataset, and the GridSearchCV method is used for feature extraction. The model was trained and tested over three datasets of CSE-CIC-IDS2018 and CIC-IDS2017, and results indicate significant improvement in accuracy after implementing SMOTE with RF. The achieved accuracy for RF was 98.4%, LGBM achieved 98.8, and XGBoost achieved 98.9%. The ML-based IDS presented in Faysal et al. (2022) used RF for feature extraction and XGBoost for classification. The model was trained over the N-BaIoT dataset and achieved an accuracy of 99.94%. Table 1 summarizes the related works.

Table 1: Comparison of the related works

Reference	Domain	Dataset	Feature extraction	Data balancing	Classification type	Classifier models	Accuracy (%)
Wang et al. (2022)	Gas pipelines	CIC-IDS2017 NSL-KDD UNSW-NB15	RFE	SMOTE	Multiclass	LSTM	99.34 99.75 98.31
Verma and Ranga (2020)	IoT	CIDDS-001 UNSW-NB15	MLP	SMOTE	Binary	RF XGBoost	94.0 99.53
Rashid et al. (2020)	Smart cities	UNSW-NB15 CIC-IDS2017	Information gain ratio	Not used	Multiclass	RF + ML models	81.77 99.7
Tang et al. (2020)	Computer networks	NSL-KDD	LGBM	Not used	Binary	AE + other models	89.82
Talukder et al. (2024)	General	UNSW-NB15 CIC-IDS2017 CIC-IDS2018	Stacking clustering + PCA	Oversampling	Multiclass	RF	99.59 99.59 99.59
Dinh et al. (2024)	IoT	NSL-KDD UNSW-NB15 IDS2017	AE	Not used	Multiclass	RF	75.3 88.3 98.8
Sayegh et al. (2024)	IoT	CIC-IDS2017 NSL-KDD UNSW-NB15	LGBM	SMOTE	Multiclass	RF	99.34 99.75 98.31
Zhao et al. (2023)	General	TON-IoT BoT-IoT	CNN	Not used	Multiclass	LGBM	99.33 98.24
Okey et al. (2022)	IoT	CSE-CIC-IDS2018 CIC-IDS2017	Stacking	SMOTE + ADASYN	Multiclass	XGBoost LightGBM RF	98.7 98.8 98.9
Faysal et al. (2022)	IoT	N-BaIoT	RF	Not used	Multiclass	XGBoost	99.94

The related works are based on different datasets with different types of attacks. The UNSW-NB15 dataset (Moustafa and Slay, 2015) has demonstrated excellent detection performance and lightweight characteristics. The UNSW-NB15 has nine types of attacks, such as exploits, backdoor, reconnaissance, generic, fuzzers, shellcode, and worm attacks that typically target the smart grid. The nine types of attacks are defined as follows. Exploit attacks are attacks that enable attackers to know vulnerabilities and gain unauthorized access to sensitive data. Backdoor attacks allow attackers to access systems without authentication to learn the control commands to perform other attacks. Reconnaissance attacks allow attackers to discover vulnerabilities in the network, which could be exploited to initiate

actual attacks, including all kinds of system scanning, such as IP addresses, ports, services, and operating systems. Analysis attacks allow attackers to gain access to systems. Generic attacks allow an attacker to gain access to block ciphers using a hash function. Fuzzers attacks allow attackers to gain access by inserting randomly generated data. Shellcode attacks use a piece of code to enable vulnerabilities and force a jump to shellcode to execute the attacker's commands. The worm attack is a malicious piece of code that replicates itself on the infected systems.

The UNSW NB15 is highly imbalanced and has a bias towards the majority class, which increases the risk of overfitting in training data without using SMOTE to balance the data. Some papers have employed different methods to balance the dataset to increase the performance of their models, to effectively enable the models to learn the patterns of the minority, to reduce the risk of the model overfitting by generating synthetic samples for the minority classes, and to ensure that the minority classes are adequately represented during training.

The six learning models, three ML and three DL models, are selected based on their high performance. The three ensemble learning ML models are XGBoost and LGBM, as gradient boosting models, and the RF as a bagging model. These ensemble models combine multiple decision trees for more accurate predictions and have the ability to handle complex datasets, are robust against overfitting, and have good generalization, which makes them powerful models for developing the lightweight IDS. The lightweight characteristics of LGBM reduce memory usage for large datasets while maintaining high accuracy, which is beneficial for resource-constrained access points. These models have parallel and distributed computing capabilities to speed up training on large datasets. On the other side, the two learning models of CNN and LSTM are employed as classifiers with distinct characteristics. CNN handles spatial data, while LSTMs handle sequential data and long-term dependencies to overcome the vanishing gradient problem. The third DL model is the AE to extract the most important features and reduce the dimensionality of data by discovering hidden relationships within the dataset to make the models effectively handle the large datasets. AE performs different tasks and is generally used as a classifier; however, this research utilizes AE to extract features and reduce data dimensionality to enhance the performance of five classifiers. In general, ML models are more computationally efficient than DL models, especially in terms of training time, and are able to deal with high-dimensional datasets.

Currently, the centralized IDS approach is unable to guarantee the strict quality of service requirements for latency-sensitive applications, including IDSs. In addition, the high dimension and noisy data with complex relationships require high computational requirements and longer training time, causing more delays for fast detection and reaction to cyberattacks (Powell et al., 2024). Consequently, the development of a new generation of lightweight IDSs for future distribution closer to data sources is demanded to enable fast detection and reaction before they become actual data breaches. In general, few works have developed lightweight models that are suitable for distribution at the resource-constrained access points, and, to the best of our knowledge, none have considered developing IDS to defend against cyberattacks targeting the critical WAMPAC architecture. In addition, most of the studied works did not consider the importance of model training time, which is crucial for IDSs. Therefore, this paper sheds light on the development of a lightweight IDS for the WAMPAC system and raises the main question of how to design a lightweight IDS to enhance performance and enable future distribution closer to data sources for future distribution and collaboration among IDSs to enable the shift toward fully distributed IDSs.

3. Proposed work

The proposed model includes four stages of data pre-processing, feature selection, data balancing, and classification. The model training and testing are performed on the UNSW NB15 dataset, which requires data pre-processing to convert the raw data into a suitable input format required by the learning models.

The first stage of preprocessing tackles the problems of noise, missing values, and the removal of redundant and constant features to accelerate the training time of the data. The missing and duplicated values are generally solved with a data interpolation method. Pre-processing is based on two methods. The first method is the data normalization using the min-max normalization method to scale the text value into a numeric range by mapping different values of attributes, feature instances, to a range between [0, 1]. This is achieved by subtracting the minimum of all data (data in one column of the dataset) from each value and dividing it by the difference between the minimum value and the maximum one.

The source files of the UNSW-NB15 dataset support many protocols with a hybrid of realistic and recent normal network traffic and synthesized malicious attacks. Data is extracted from the set of features obtained from the analyzed network packets, which contains categorical features to identify attributes of the protocol's data. The dataset has more than 2 million records in four files in "CSV" format and four types of data values, with total numbers indicated of binary (30), numeric (38), nominal (6), and time stamps (2). The dataset contains 49 features including packet-based features, flow-based features, content features, and time features. The feature label for binary classification is 0 for normal and 1 for attacks, however, there is 49 features and some are not required for binary classification. The dataset also contains some non-numerical data that needs pre-

processing to convert the non-numerical attributes to numerical values. The four categorical features of protocol type, service, and flag are converted into numerical values by using the one hot encoder method to assign a number of bits as a binary value to each one, as models do not work with text. The different classes of attacks are encoded as normal (6), generic (5), exploits (3), fuzzers (4), DoS (2), reconnaissance (7), analysis (0), backdoor (1), shellcode (8), and worms (9). Fig. 4 indicates the various categories of attacks, while Fig. 5 shows the encoding of attacks into number.

The second stage employs the AE, which consists of an encoder to convert the input data vector, and then the decoder reconstructs the original input from the compressed vector. The AE extracts the most important features; nevertheless, the decoder part of the AE is not required after training data, as indicated in Fig. 6. The third stage solves the problems associated with the imbalanced dataset, which pushes the models to become biased toward the majority class due to a high number of normal classes as compared to malicious classes. The SMOTE is employed to introduce variability and reduce the risk of the model overfitting to enable models to effectively learn the patterns of the minority classes.

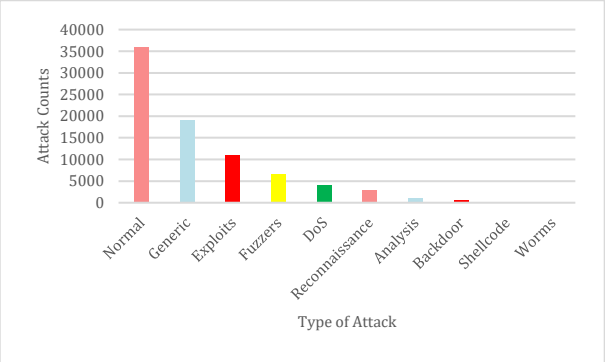

Fig. 4: Attacks distribution

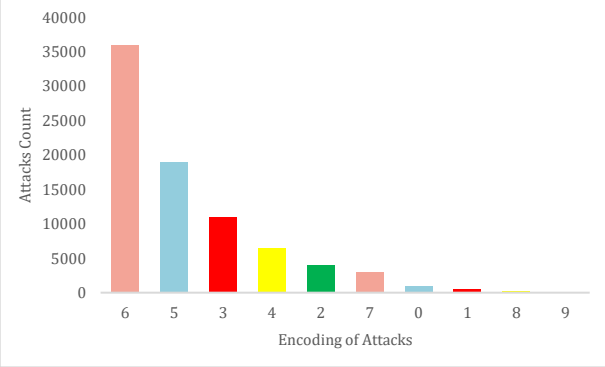

Fig. 5: Encoding of various categories of attacks

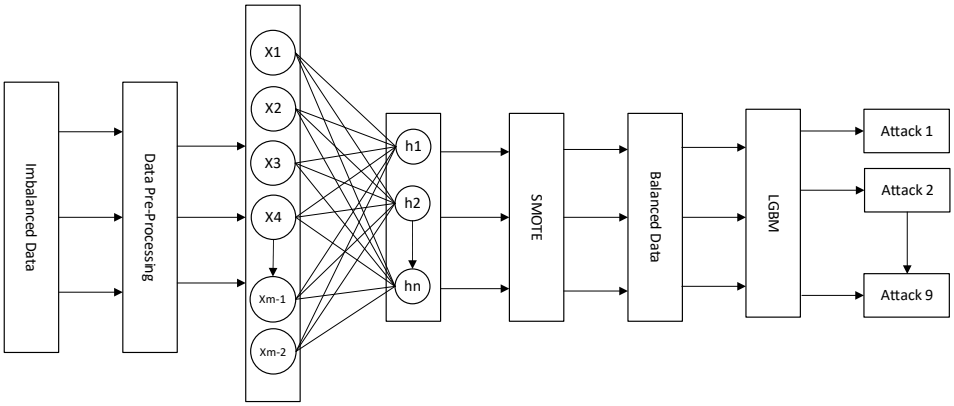

Fig. 6: The proposed AE-SMOTE-LGBM IDS

The fourth stage is the five classifiers to detect attack behaviors and classify the nine different types of attacks. Finally, the model's performance is evaluated based on four standard metrics, and a comparison between the five classifiers is carried out. The hyperparameters of the five classifiers are set to their default values for fair comparison, while EA parameters are set as follows: batch size = 512, maximum epochs = 100, and Adam optimizer.

Fig. 7 summarizes the data flow diagram of the proposed IDS with four stages of pre-processing, feature extraction, data balancing, and classification.

3.1. Performance evaluation

The training of models aims to fine-tune the model's parameters, such as the weights and biases. The testing set is independent of the training set and is used to test the model's performance. The dataset is partitioned into a training set with 175341 records (56000 for normal flow and 119341 for attack flow), and a testing set with 82332 records (37000 for normal flow and 45332 for attack flow), respectively. In the training set, the proportion of normal samples and attack instances are 31.94% and 68.06%, respectively. In the test set, the proportion of normal samples and attack instances are 44.94% and 55.06%, respectively. Both sets contain the records belonging to 9 different attack classes as well as the normal class. Exploits, generic, and normal instances make up a large portion of subsamples at 16%, 22%, and 38% of the overall instances in the training subset, respectively. As an extreme case, worms attack instances form a mere 0.06% of both training and test sets.

The dataset suffers from class imbalance between classes and within classes. Between-class imbalance occurs due to the unequal distribution, with normal records constitute 87% of all records, and the combined malicious record count of only 13%. The normal class has 2,218,761 records, while malicious attacks are categorized into nine groups of attacks:

fuzzers, analysis, backdoors, DoS, exploits, generic, reconnaissance, shellcode, and worms that represent 24246, 2677, 2329, 16535, 44525, 215481, 13987, 1511, and 174 records, respectively. Also, attacks are not equally distributed, as 65% of all attack records belong to the generic attack class, while only 0.0008% of all attack records belong to the worm attack.

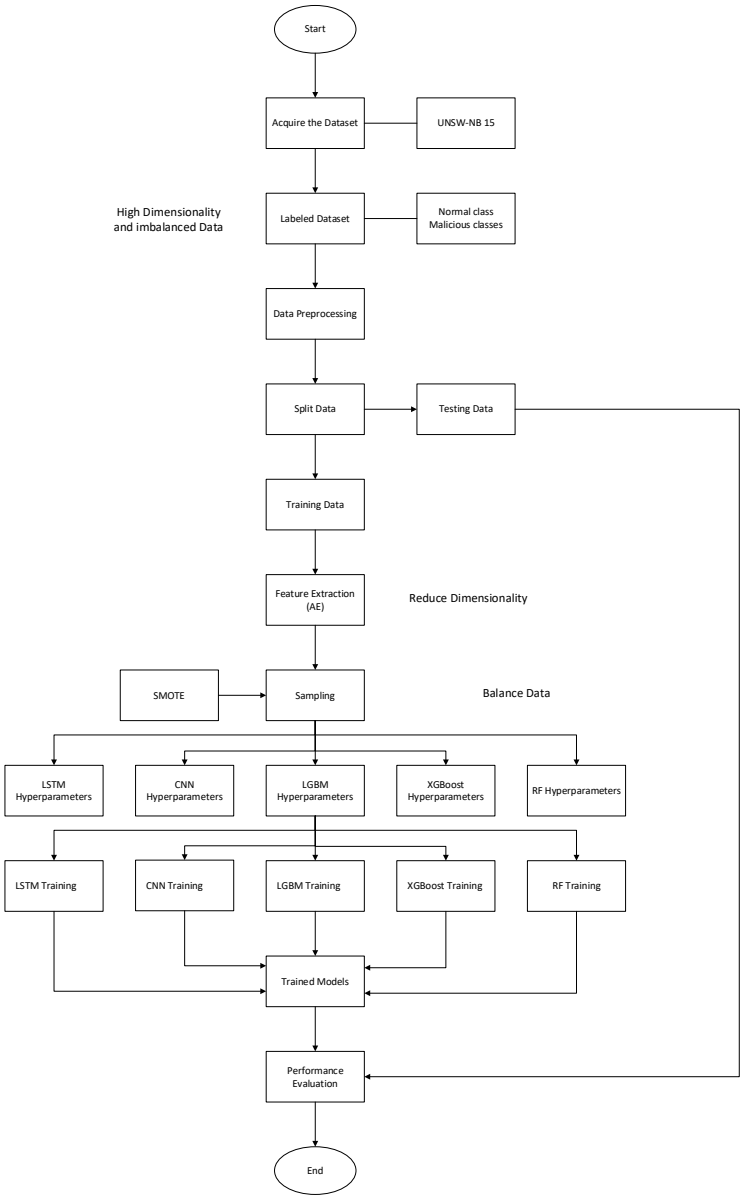

Fig. 7: Dataflow of the proposed intrusion detection system

The performance is evaluated based on four standard performance evaluation metrics of Accuracy, Precision, Recall, and F1-Score as defined by the following four equations. They depend on values of true positive (TP), in which intrusion samples are classified correctly as intrusion, true negative (TN) in which normal samples are classified as normal, false positive (FP) in which normal samples are misclassified as intrusion, and false negative (FN) in which intrusion samples are misclassified as normal. The four metrics are defined as follows:

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+FP+TN+FN}} \quad (1)$$

$$\text{Precision} = \frac{\text{TP}}{\text{PT+FN}} \quad (2)$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \quad (3)$$

$$\text{F1} - \text{Score} = 2 \times \frac{\text{Precion} \times \text{Recall}}{\text{Precion+ Recall}} \quad (4)$$

The confusion matrix shows the number of TP, TN, FP, and FN to provide details about the performance of models, while the Receiver Operating Characteristic (ROC) curve graphically represents the TP rate against the FP rate to show the model's ability to differentiate between classes.

4. Results and discussion

The experiments are implemented online using the Graphical Processing Unit (GPU) provided by Google Colab, where various libraries are available, such as Pandas for data manipulation, visualization and analysis, NumPy to provide a set of mathematical and numerical features to support the multidimensional array and matrix data structures, and matplotlib Scikit to offer common utility functions for feature scaling and data encoding. In

addition to libraries for ML models that are written in Python, and libraries of DL models based on pre-implemented libraries supported by Keras that run on top of Tensor Flow. Two scenarios are implemented. In the first scenario, a set of experiments was conducted to evaluate the performance for binary classification and early detection of attacks. In the second scenario, a set of experiments is implemented for the multiclass classifications. Due to space limitations, the confusion matrix and ROC graphs are only provided for the SOMTE-LGBM binary model and the proposed multiclass model. Fig. 8 shows the distribution of attacks, where Normal is 0, and Attacks are 1. Fig. 9 indicates the impact of SMOTE on data distributions for binary models.

In the second set of experiments, five models are implemented to show the impact of SMOTE on attack distribution for a multiclass scenario, as indicated in Fig. 10. While Fig. 11 indicates the encoding of Attacks: Normal 6 and multiclass Attacks 1-5, 7-9.

4.1. Scenario 1: Performance evaluation of binary models

Results of binary ML models without SMOTE indicate a little impact of data balancing on models, as it only differentiates between two classes. In terms of all of the four standard metrics, LSTM has achieved a high percentage of 99%. Both XGBoost and LGBM have achieved a high percentage of accuracy, while CNN has achieved the lowest performance. Considering the training time consumed by all models, RF has consumed the shortest time, followed by LGBM, then XGBoost, while CNN has consumed the longest time. Applying SMOTE to balance the dataset has accelerated training time, due to reduced complexity of binary classifiers, and has enabled the models to learn and generalize even with an imbalanced dataset of ML models.

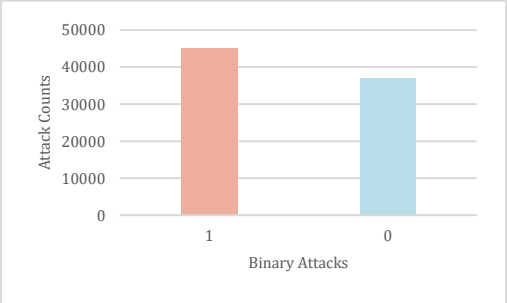

Fig. 8: Normal and attacks binary distribution

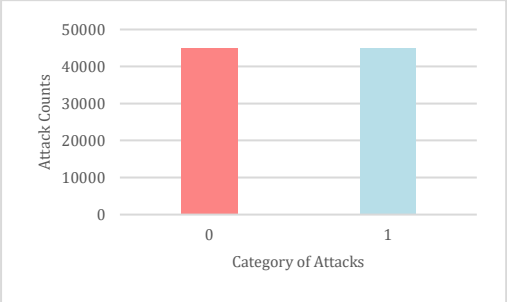

Fig. 9: Impact of SMOTE on binary models

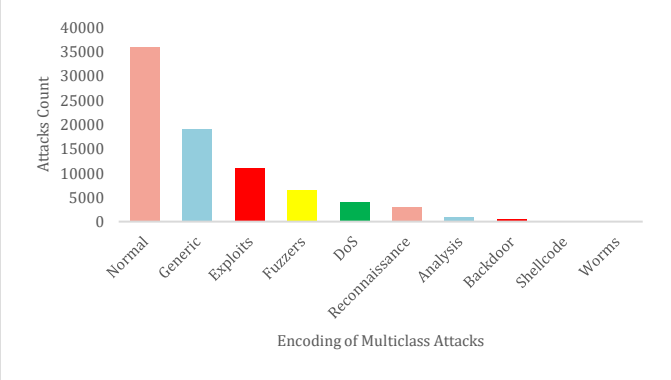

Fig. 10: Multiclass attack's distribution

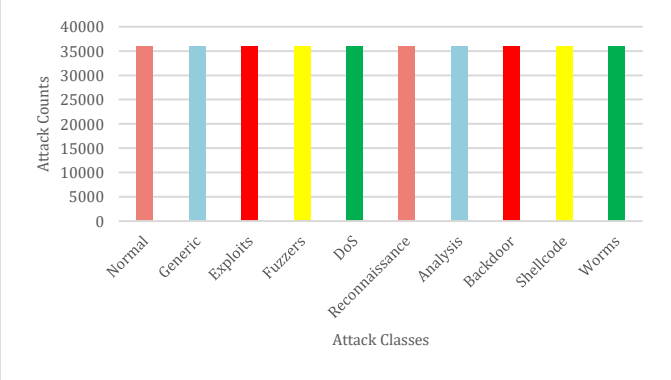

Fig. 11: Impact of SMOTE on multiclass attacks

Results, in Fig. 12 without applying SMOTE and Fig. 13 after applying SMOTE, indicate that XGBoost, RF, and LGBM have achieved high accuracy regardless of their family with less complicated computations and have effectively differentiated between normal and malicious classes. Furthermore, results reveal that XGBoost, LSTM, and LGBM are able to successfully identify 99% of malicious attacks due to the reduced complexity of binary classifiers, which enabled models to learn and generalize even with an imbalanced dataset.

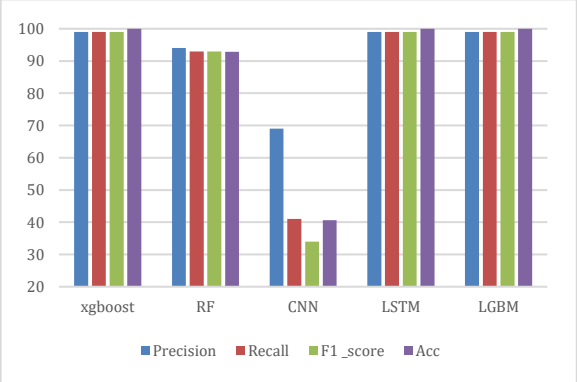

Fig. 12: Performance of binary models without SMOTE

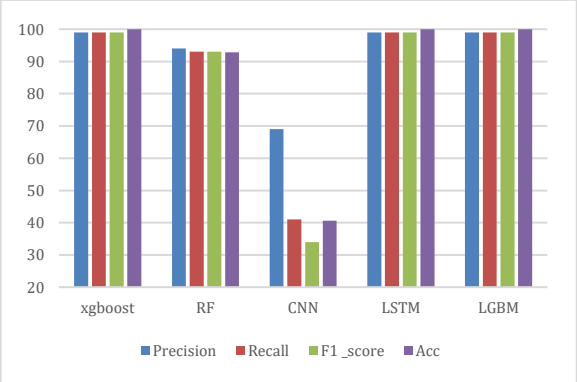

Fig. 13: Performance of binary models with SMOTE

The training time of the five ML models—XGBoost, RF, and LGBM—was shorter than that of the DL models, CNN and LSTM. The application of SMOTE further contributed to reducing the training time for all models. Among them, the SMOTE-LGBM model achieved the best performance with a training time of 0.027 s in this binary classification scenario and demonstrated superior accuracy compared with the other models.

DL models required longer training times due to their higher architectural complexity. In particular, LGBM produced strong results for binary classification and proved to be a lightweight, efficient, and accurate classifier for the early detection of attack indicators. Its efficiency makes it suitable for deployment closer to data sources, enabling rapid detection of attacks before significant damage occurs.

Given the promising results obtained in the binary classification scenario, further experiments should focus on extending the approach to multiclass attack classification.

The confusion matrices of the LGBM binary classifier without SMOTE and with SMOTE are presented in Fig. 14 and Fig. 15, respectively. The results indicate that the use of SMOTE is not necessary for binary classification, as the classifier can effectively distinguish between the two classes without additional resampling.

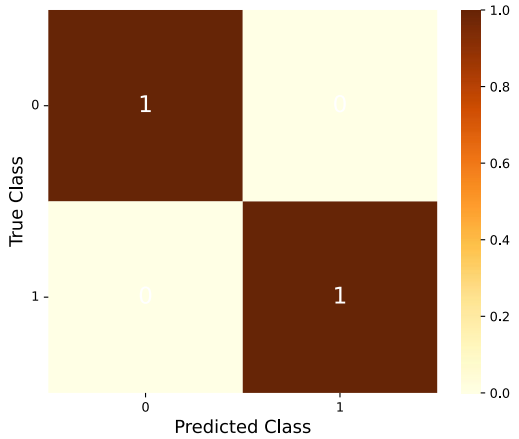

Fig. 14: Binary LGBM confusion matrix without SMOTE

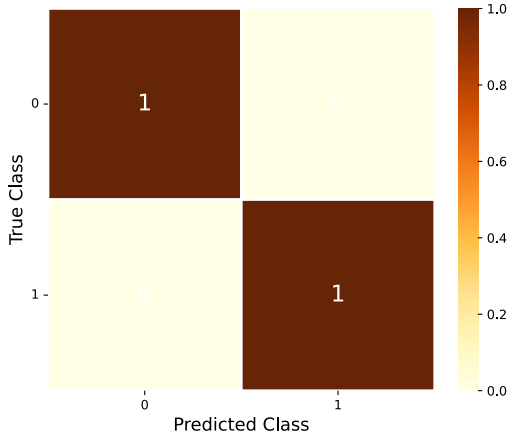

Fig. 15: Binary LGBM confusion matrix with SMOTE

The ROC graphs of binary classifiers, without and with SMOTE, are presented in Fig. 16 and Fig. 17, respectively.

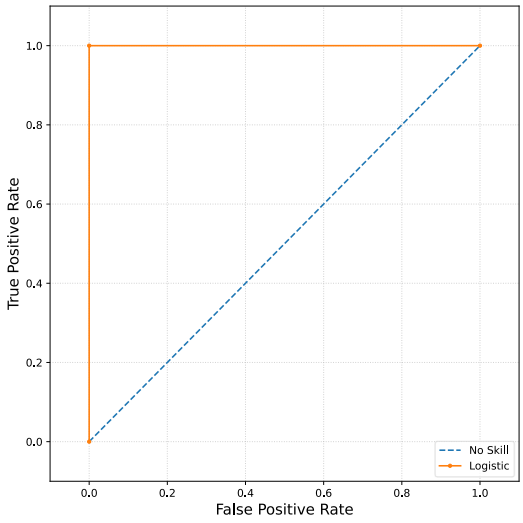

Fig. 16: Binary LGBM ROC without SMOTE

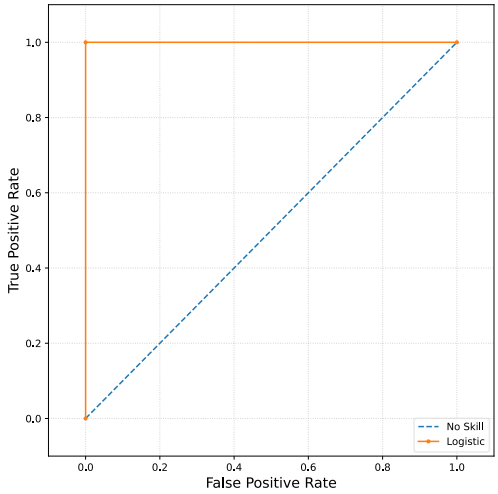

Fig. 17: Binary LGBM ROC graph with SMOTE

Adding AE has enabled the AE-SMOTE-LGBM binary model to have excellent performance, as shown in the confusion matrix in Fig. 18 and the ROC in Fig. 19, respectively.

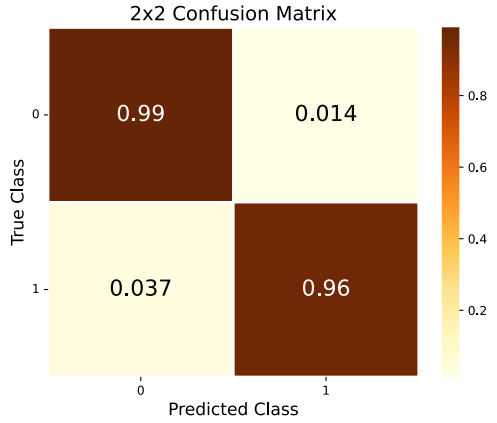

Fig. 18: Binary AE-SMOTE LGBM confusion matrix

4.2. Scenario 2: Performance evaluation of the multiclass models

The accuracy for different models indicates that most of the attacks are not properly detected without a balanced dataset due to uneven distribution of attacks, as indicated in Fig. 20. Results reveal that XGBoost and RF models have achieved an accuracy of 83.93% and 76.46%, respectively, and have consumed an identical amount of time of 0.02 seconds. XGBoost achieved the highest precision of 82%. LSTM seems to perform much better than CNN in terms of accuracy, with LSTM achieved 73.04% and CNN achieved 36.33%, and having relatively similar long times of 14.85 and 15.98 seconds.

Fig. 21 depicts that applying SMOTE data balancing has enabled all learning models to achieve excellent performance in detecting normal class and correctly differentiate between normal and malicious attacks, except for CNN, with an accuracy of 95%. DL models have better performance compared with the previous case of not employing SMOTE, but still consume a longer time in classifications and have the lowest accuracy. All models could not detect three attacks of analysis, DoS, and Backdoor. In addition, LGBM could not detect worm attacks. The DL is unable to detect five attacks out of nine, including DoS, analysis, shellcode, backdoor attacks, and worms.

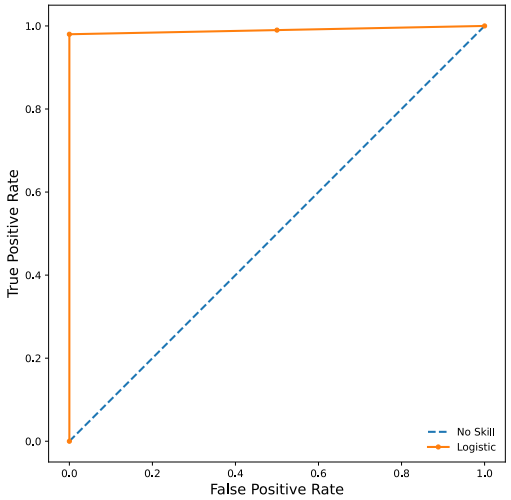

Fig. 19: Binary AE-SMOTE LGBM ROC graph

The SMOTE-XGBoost model achieved the highest accuracy of 80.45%, which is slightly higher than that of SMOTE-LGBM, which achieved an accuracy of 80.07%. Both models demonstrated efficient training times of 0.026 s and 0.29 s, respectively. In comparison, SMOTE-RF achieved an accuracy of 74.77% with a training time of 0.55 s.

Overall, the training time required for DL models, namely CNN and LSTM, was generally longer than that of the machine learning (ML) models. However, SMOTE-LGBM achieved the best overall performance in terms of precision (86%), recall (80%), and F1-score (82%). These results indicate that the application of SMOTE improved the performance of LGBM while maintaining low training time, making LGBM a suitable candidate for deployment at multiple access points in network environments. Moreover, SMOTE-LGBM further improved multiclass attack detection, producing promising results even for attacks with limited training samples, except for the analysis attack category.

Both LGBM and XGBoost successfully detected most types of attacks with considerable performance. In particular, LGBM demonstrated superior detection performance for DoS, backdoor, shellcode, and worms, whereas SMOTE-XGBoost performed better in detecting exploits, fuzzers, and reconnaissance attacks. However, all models showed difficulty in correctly classifying analysis attacks, which remained the most challenging category.

Although the performance of the DL models improved, the improvement for CNN was not as significant as expected, likely due to the use of default hyperparameter settings.

The confusion matrices of the LGBM multiclass model without and with SMOTE are presented in Fig. 22 and Fig. 23, respectively. The corresponding ROC curves are illustrated in Fig. 24 and Fig. 25.

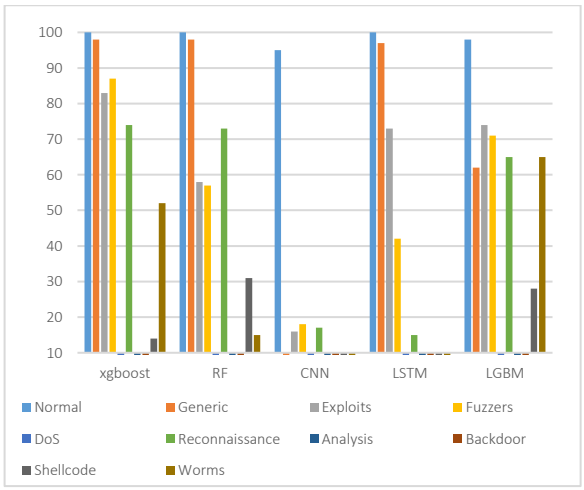

Fig. 20: Performance of multiclass models without SMOTE

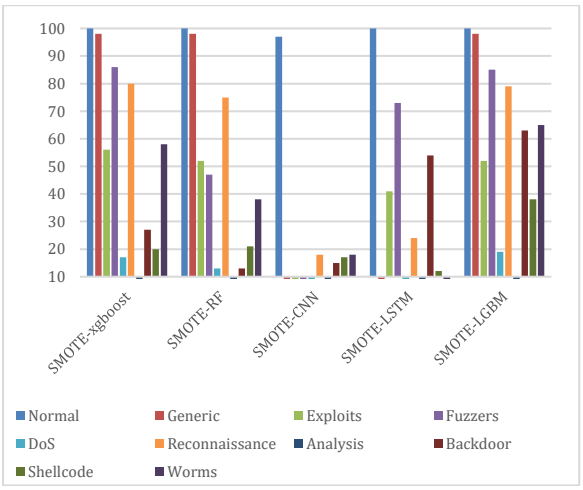

Fig. 21: Performance of multiclass models with SMOTE

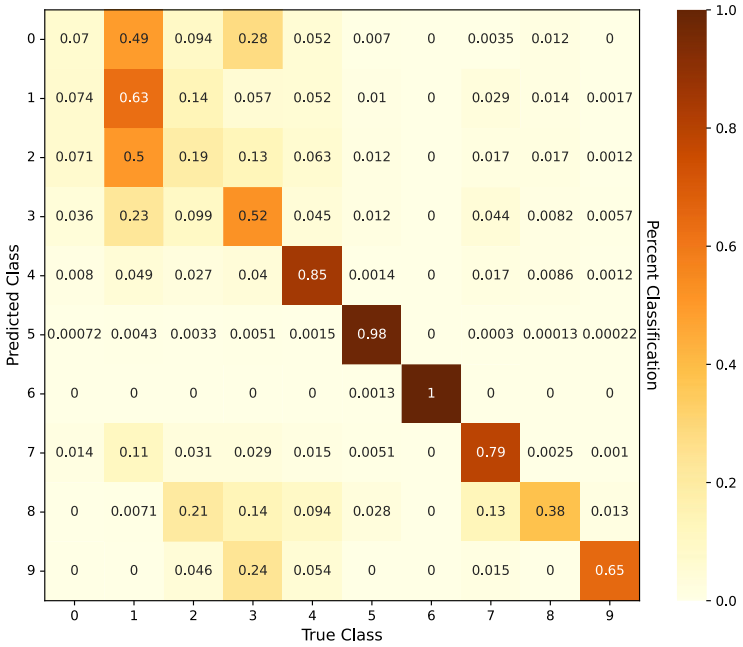

Fig. 22: Confusion matrix LGBM without SMOTE

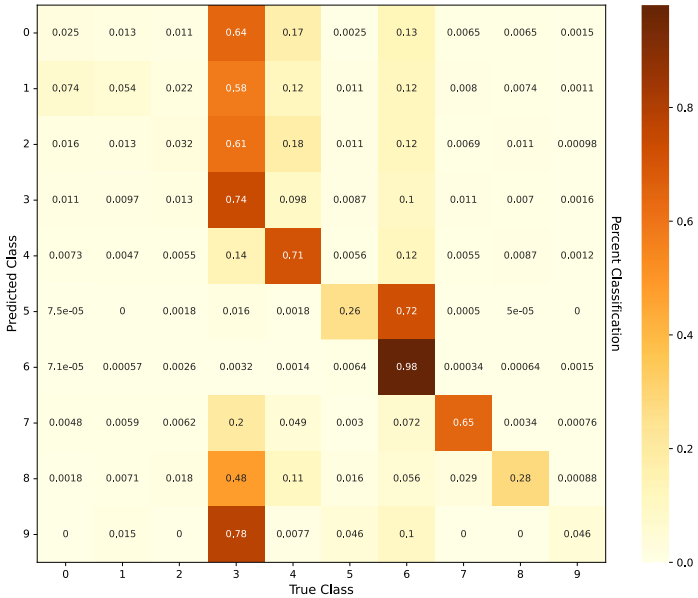

Fig. 23: Confusion matrix of LGBM with SMOTE

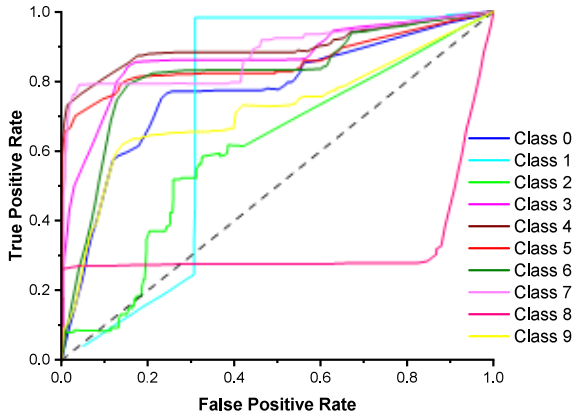

Fig. 24: ROC for multiclass LGBM without SMOTE

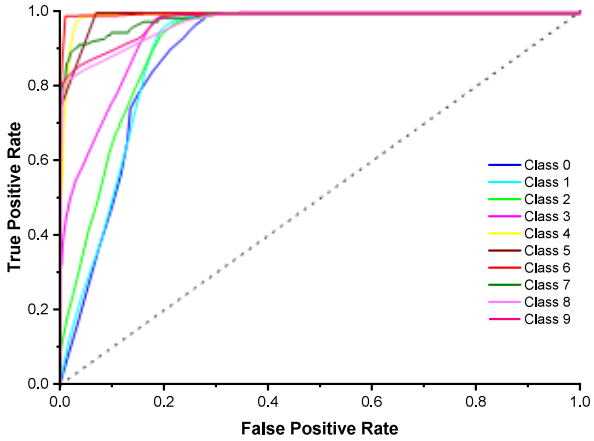

Fig. 25: ROC for multiclass LGBM with SMOTE

4.3. Performance results and analysis of the proposed AE-SMOTE-LGBM

The application of an AE for feature extraction prior to attack classification produced excellent results for both XGBoost and LGBM, achieving accuracies of 99.16% and 97.06%, respectively, with similar training times of 0.026 s and 0.028 s. The performance of the deep DL models, CNN and LSTM, also improved considerably compared with the previous experiment. However, these models still required longer training times than the ML models, with LSTM exhibiting the longest training time. The use of AE reduced computational complexity and effectively captured representative features from the data, which accelerated training and improved the models' generalization capability across different attack classes.

A comparison between SMOTE-LGBM and the proposed AE-SMOTE-LGBM model for multiclass classification indicates that AE successfully extracted meaningful feature representations and reduced data dimensionality, which further enhanced classifier performance. In this experiment, AE-SMOTE-XGBoost achieved the highest accuracy of 65.16% with a training time of 0.027 s, effectively distinguishing between normal and malicious traffic. In contrast, the AE-SMOTE-LGBM model achieved a lower accuracy of 61.16% with a longer training time of 0.42 s. These relatively lower accuracies are primarily attributed to the use of default hyperparameter settings across all models to ensure a fair comparison. The confusion matrix of the proposed AE-SMOTE-LGBM model is presented in Fig. 26, while the corresponding ROC curve is shown in Fig. 27. These results demonstrate that incorporating AE improves the performance of the SMOTE-LGBM framework. Among the evaluated models, AE-SMOTE-XGBoost achieved the highest overall performance, followed by AE-SMOTE-LGBM.

Furthermore, AE significantly improved the performance of the DL models; however, they continued to require longer training times compared with ML models. CNN outperformed LSTM, while LSTM remained the most computationally expensive model. The performance of these DL models could potentially be further enhanced through systematic hyperparameter optimization.

The overall results of both binary and multiclass classification experiments reveal strong competition between AE-SMOTE-XGBoost and AE-SMOTE-LGBM. Their accuracies vary depending on the attack type, achieving 65.16% and 61.22%, respectively, with training times of 0.027 s and 0.42 s. In terms of computational efficiency, the ML models consistently outperformed the DL models on the UNSW-NB15 dataset. The relatively short training times enable the deployment of IDSs that maintain good detection accuracy while ensuring rapid processing.

A comparison of the experimental results shows that XGBoost achieved the shortest training time and the highest computational efficiency, whereas LGBM demonstrated stronger capability in differentiating between multiple attack types. All ML models—XGBoost, RF, and LGBM—achieved acceptable accuracy levels. Among them, RF required slightly longer training time, while XGBoost consumed the shortest time.

Considering that these models are typically trained offline, the slightly longer training time of LGBM is acceptable. Consequently, the proposed AE-SMOTE-LGBM model remains a promising solution due to its enhanced classification capability across multiple attack categories.

The proposed AE-SMOTE-LGBM model successfully detected seven out of nine attack types, failing only to detect shellcode and worm attacks. In contrast, AE-SMOTE-XGBoost effectively detected four attack categories, including generic, exploits, fuzzers, and reconnaissance attacks. However, all models struggled to correctly classify analysis attacks, indicating that this attack category remains particularly challenging.

Furthermore, the integration of AE significantly improved the performance of the DL models, although the degree of improvement varied depending on the classifier and the evaluation metric used.

5. Conclusion

The developed lightweight IDS was trained and evaluated using the UNSW-NB15 dataset under both imbalanced and balanced data distributions. This

dataset contains attack characteristics similar to those typically observed in smart grid environments, enabling the learning models to generalize underlying attack patterns and distributions present in the training data. The negative impact of the dataset's imbalanced distribution was mitigated using SMOTE, which balanced the minority and majority classes.

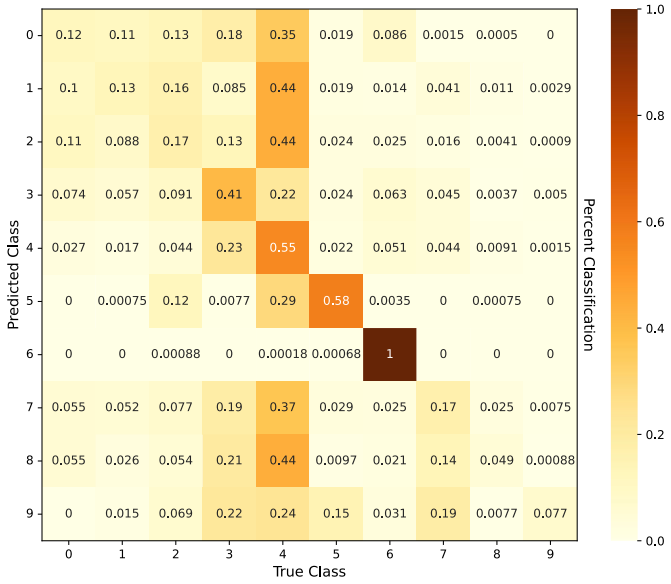

Fig. 26: Confusion matrix of multiclass AE-SMOTE LGBM

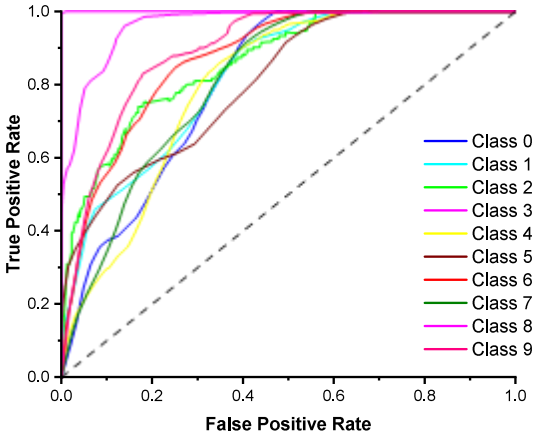

Fig. 27: ROC graph of multiclass AE-SMOTE LGBM

Two classification scenarios were evaluated: binary classification and multiclass classification, using four standard evaluation metrics. The results obtained from the five classifiers indicate that binary classification achieved higher performance than multiclass classification, primarily because binary classification involves distinguishing between only two classes. In contrast, multiclass classification increases model complexity by requiring the differentiation among a larger number of attack categories. The reduced complexity of binary classifiers enables models to learn more effectively and generalize better even when trained on imbalanced datasets.

In multiclass scenarios, the presence of multiple classes and the imbalanced dataset contributed to performance degradation, and some models struggled to learn effective representations for minority classes. To address this issue, data preprocessing, class balancing with SMOTE, and feature extraction using AE were applied. These techniques significantly improved the performance of the learning models by reducing data dimensionality and extracting more representative features.

Among the evaluated models, LGBM and CNN successfully detected seven out of nine attack types while maintaining strong accuracy and efficient training times. In particular, LGBM demonstrated superior performance in multiclass attack detection, whereas RF produced competitive results in terms of accuracy. The strong performance of ML models can be attributed to their lower model complexity and reduced computational requirements compared with DL models, making them more suitable for deployment in environments with limited computational resources. In particular, the lightweight nature of the LGBM model satisfies the requirements of resource-constrained access points while maintaining strong multiclass detection capabilities with short processing times.

The proposed AE-SMOTE-LGBM model demonstrated advantages over other models in detecting certain attack types, including the analysis attack, which other classifiers struggled to identify. Additionally, the CNN model showed significant improvement after incorporating AE, becoming the only model capable of detecting minority attack categories such as shellcode and worm attacks. Nevertheless, although DL models generally perform well on larger datasets, they require higher computational power and hardware resources, making them less suitable for deployment in resource-constrained access points.

Future work will focus on evaluating the proposed IDS using multiple datasets and real-world network traffic to further improve model generalization and ensure practical deployment in

real-world environments. In addition, further research will explore few-shot learning approaches, enabling models to learn from limited training samples and detect previously unseen attack patterns, commonly referred to as zero-day attacks.

The highly heterogeneous environment of smart grids, characterized by numerous distributed access points deployed across wide geographical areas, introduces several challenges. These environments involve heterogeneous communication protocols and varying data characteristics, which may produce location-specific data patterns. Variations in feature distributions, local dataset sizes, and attack characteristics across different locations complicate data analysis and model inference.

Furthermore, access points in real smart grid deployments are heterogeneous in terms of computational and communication capabilities. Computational capabilities include processing power and storage capacity, while communication capabilities involve transmission media, protocols, data rates, and channel conditions. These variations present significant challenges for deploying distributed IDS solutions.

Such data and system heterogeneity hinder the development of a unified IDS, highlighting the need for customized IDS solutions that can learn the unique characteristics of local data and adapt to the specific constraints of resource-limited access points. Therefore, adaptive IDS architectures capable of dynamically adjusting to both data heterogeneity and system constraints are urgently required.

The primary objective of this research was to design a lightweight IDS capable of detecting cyberattacks closer to the data sources, enabling rapid response and minimizing potential damage. The long-term goal is to develop distributed and collaborative IDS frameworks based on advanced DL approaches while addressing the challenges of model complexity, system heterogeneity, and data privacy.

To achieve this objective, future research must focus on reducing DL model complexity, improving model performance, and preserving sensitive data privacy, while ensuring compatibility with resource-constrained access points. This will require dynamic and adaptive optimization of model parameters, including hyperparameters, to address multiple conflicting objectives and system constraints. Formulating the problem mathematically and selecting appropriate optimization methods will be essential to identify optimal trade-offs among model complexity, computational resources, detection performance, and scalability, thereby enabling the deployment of the next generation of distributed and collaborative IDS systems.

List of abbreviations

AC	Alternating current
AE	Auto-encoder
AMI	Advanced metering infrastructure
CCS	Centralized control system
CI	Communication infrastructure
CNN	Convolutional neural network
CSV	Comma-separated values
CT	Current transformer
DDoS	Distributed denial of service
DL	Deep learning
DoS	Denial of service
EI	Edge intelligence
FN	False negative
FP	False positive
GPU	Graphical processing unit
HVDC	High voltage direct current
IDS	Intrusion detection system
IDSs	Intrusion detection systems
IEDs	Intelligent electronic devices
IoMT	Internet of medical things
IoT	Internet of things
KDD	Knowledge discovery in databases
LGBM	Light gradient boosting model
LSTM	Long short-term memory
ML	Machine learning
MU	Merging unit
PCA	Principal component analysis
PDC	Phasor data concentrator
PGW	Phasor gateway
PMU	Phasor measurement unit
RF	Random forest
RFE	Recursive feature elimination
RNN	Recurrent neural network
ROC	Receiver operating characteristic
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SMOTE	Synthetic minority oversampling technique
T&D	Transmission and distribution
TN	True negative
TP	True positive
VT	Voltage transformer
WAMPAC	Wide area monitoring, protection and control
WAMS	Wide area monitoring system
XGBoost	Extreme gradient boosting

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Achaal B, Adda M, Berger M, Ibrahim H, and Awde A (2024). Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. Cybersecurity, 7: 10. https://doi.org/10.1186/s42400-023-00200-w **PMid:38707764 PMCid:PMC11062904**

Almarshdi R, Nassef L, Fadel E, and Alowidi N (2023). Hybrid deep learning based attack detection for imbalanced data classification. Intelligent Automation and Soft Computing, 35(1): 297-320. https://doi.org/10.32604/iasc.2023.026799

Alsirhani A, Tariq N, Humayun M, Naif Alwakid G, and Sanaullah H (2025). Intrusion detection in smart grids using artificial intelligence-based ensemble modelling. Cluster Computing, 28: 238. https://doi.org/10.1007/s10586-024-04964-9

Dinh PV, Hoang DT, Uy NQ, Nguyen DN, Bao SP, and Dutkiewicz E (2024). Multiple-input auto-encoder for IoT intrusion detection systems with heterogeneous data. In the ICC 2024-IEEE International Conference on Communications, IEEE,

Denver, USA: 2707-2712. https://doi.org/10.1109/ICC51166.2024.10622942

Faysal JA, Mostafa ST, Tamanna JS, Mumenin KM, Arifin MM, Awal MA, Shome A, and Mostafa SS (2022). XGB-RF: A hybrid machine learning approach for IoT intrusion detection. Telecom, 3(1): 52-69. https://doi.org/10.3390/telecom3010003

Islam U, Ullah H, Khan N, Saleem K, and Ahmad I (2025). AI-enhanced intrusion detection in smart renewable energy grids: A novel Industry 4.0 cyber threat management approach. International Journal of Critical Infrastructure Protection, 50: 100769. https://doi.org/10.1016/j.ijcip.2025.100769

Lee JH, Shin J, and Seo JT (2023). Solar power plant network packet-based anomaly detection system for cybersecurity. Computers, Materials and Continua, 77(1): 757-779. https://doi.org/10.32604/cmc.2023.039461

Mahadevappa P, Murugesan RK, Al-Amri R, Thabit R, Al-Ghushami AH, and Alkawsi G (2024). A secure edge computing model using machine learning and IDS to detect and isolate intruders. MethodsX, 12: 102597. https://doi.org/10.1016/j.mex.2024.102597 **PMid:38379716 PMCid:PMC10877948**

Mejia-Ruiz GE, Marasini G, Zhihua Q, Kundu S, and Pushpak S (2025). Cybersecurity challenges in power networks with distributed energy resources: A comprehensive survey. Renewable and Sustainable Energy Reviews, 224: 116100. https://doi.org/10.1016/j.rser.2025.116100

Menzel V, Speckamp J, and Remke A (2024). Developing a robust communication infrastructure for a distributed smart grid IDS. In the 2024 IEEE International Conference on Cyber Security and Resilience, IEEE, London, UK: 1-8. https://doi.org/10.1109/CSR61664.2024.10679379

Molokomme DN, Onumanyi AJ, and Abu-Mahfouz AM (2022). Edge intelligence in smart grids: A survey on architectures, offloading models, cyber security measures, and challenges. Journal of Sensor and Actuator Networks, 11(3): 47. https://doi.org/10.3390/jsan11030047

Moustafa N and Slay J (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In the 2015 Military Communications and Information Systems Conference, IEEE, Canberra, Australia: 1-6. https://doi.org/10.1109/MilCIS.2015.7348942

Okey OD, Maidin SS, Adasme P, Rosa RL, Saadi M, Carrillo Melgarejo D, and Zegarra Rodríguez D (2022). BoostedEnML: Efficient technique for detecting cyberattacks in IoT systems using boosted ensemble machine learning. Sensors, 22(19): 7409. https://doi.org/10.3390/s22197409 **PMid:36236506 PMCid:PMC9572777**

Powell J, McCafferty-Leroux A, Hilal W, and Gadsden SA (2024). Smart grids: A comprehensive survey of challenges, industry applications, and future trends. Energy Reports, 11: 5760-5785. https://doi.org/10.1016/j.egyr.2024.05.051

Presekal A, Jorjani M, Rajkumar VS, Goyel H, Cibin N, Semertzis I, Ştefanov A, and Palensky P (2024). Cyber security of HVDC systems: A review of cyber threats, defense, and testbeds. IEEE Access, 12: 165756-165773. https://doi.org/10.1109/ACCESS.2024.3490605

Rashid MM, Kamruzzaman J, Hassan MM, Imam T, and Gordon S (2020). Cyberattacks detection in IoT-based smart city applications using machine learning techniques. International Journal of Environmental Research and Public Health, 17(24): 9347. https://doi.org/10.3390/ijerph17249347 **PMid:33327468 PMCid:PMC7764956**

Sahani N, Zhu R, Cho JH, and Liu CC (2023). Machine learning-based intrusion detection for smart grid computing: A survey. ACM Transactions on Cyber-Physical Systems, 7(2): 11. https://doi.org/10.1145/3578366

Sayegh HR, Dong W, and Al-Madani AM (2024). Enhanced intrusion detection with LSTM-based model, feature selection, and SMOTE for imbalanced data. Applied Sciences, 14(2): 479. https://doi.org/10.3390/app14020479

Sundararajan A, Khan T, Moghadasi A, and Sarwat AI (2019). Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies. Journal of Modern Power Systems and Clean Energy, 7(3): 449-467. https://doi.org/10.1007/s40565-018-0473-6

Talukder MA, Islam MM, Uddin MA, Hasan KF, Sharmin S, Alyami SA, and Moni MA (2024). Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. Journal of Big Data, 11: 33. https://doi.org/10.1186/s40537-024-00886-w

Tang C, Luktarhan N, and Zhao Y (2020). An efficient intrusion detection method based on LightGBM and autoencoder. Symmetry, 12(9): 1458. https://doi.org/10.3390/sym12091458

Vahidi S, Ghafouri M, Au M, Kassouf M, Mohammadi A, and Debbabi M (2023). Security of wide-area monitoring, protection, and control (WAMPAC) systems of the smart grid: A survey on challenges and opportunities. IEEE Communications Surveys & Tutorials, 25(2): 1294-1335. https://doi.org/10.1109/COMST.2023.3251899

Verma A and Ranga V (2020). Machine learning based intrusion detection systems for IoT applications. Wireless Personal Communications, 111: 2287-2310. https://doi.org/10.1007/s11277-019-06986-8

Wang W, Harrou F, Bouyeddou B, Senouci SM, and Sun Y (2022). A stacked deep learning approach to cyber-attacks detection in industrial systems: Application to power system and gas pipeline systems. Cluster Computing, 25: 561-578. https://doi.org/10.1007/s10586-021-03426-w **PMid:34629940 PMCid:PMC8490144**

Zhang D, Huang D, Chen Y, Lin S, and Li C (2025). A lightweight IoT intrusion detection method based on two-stage feature selection and Bayesian optimization. AIMS Electronics and Electrical Engineering, 9(3): 359-389. https://doi.org/10.3934/electreng.2025017

Zhao G, Wang Y, and Wang J (2023). Intrusion detection model of Internet of Things based on LightGBM. IEICE Transactions on Communications, 106(8): 622-634. https://doi.org/10.1587/transcom.2022EBP3169