European Journal of Computer Science and Information Technology, 14(4),48-69, 2026
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

A Deep Learning-Based Intrusion Detection System for Multiclass Cyber-Attack Detection in Smart Grids Advanced Metering Infrastructure

Daniel Asuquo[1,2], Emem Otu[3], Kingsley Attai[4], Kingsley Akputu[2], Bernard Ephraim[2], Kitoye Ebire Okonny[5], Kubiat Ekpo[6] and Isah Saidu[2]

[1]Department of Information Systems, Faculty of Computing, University of Uyo, Uyo, Nigeria
[2]Department of Computing Sciences, Faculty of Science, Admiralty University of Nigeria, Ibusa, Nigeria
[3]Department of Computer Science, Faculty of Computing, University of Uyo, Uyo, Nigeria
[4]Department of Computer Science, Faculty of Computing, Ritman University, Ikot Ekpene, Nigeria
[5]Department of Computer Science, Ignatius Ajuru University, Port Harcourt, Nigeria
[6]Department of Cyber Security, Faculty of Computing, National Open University of Nigeria

doi: https://doi.org/10.37745/ejcsit.2013/vol14n44869 Published June 28, 2026

Citation: Asuquo D., Out E., Attai K., Akputu K., Ephraim B., Okonny K.E., Ekpo K. and Saidu I. (2026) A Deep Learning-Based Intrusion Detection System for Multiclass Cyber-Attack Detection in Smart Grids Advanced Metering Infrastructure, *European Journal of Computer Science and Information Technology*, 14(4),48-69

Abstract: *Smart grids are promising innovations that integrate digital communication technologies, sensors, distributed energy resources, and storage systems to enable real-time monitoring, intelligent control, and efficient energy management. While these technologies improve reliability, efficiency, and responsiveness through two-way communication between utilities and consumers, they also expose Advanced Metering Infrastructure (AMI) systems to significant cybersecurity threats. To address these challenges, this work proposes a deep learning-based intrusion detection system for detecting cyber-attacks in smart grid environments. The framework emphasizes the need for scalable and intelligent Meter Data Management Systems capable of supporting real-time analytics, demand forecasting, distributed asset optimization, and enhanced cybersecurity. Using the BoT-IoT dataset, extensive preprocessing techniques were applied, including data cleaning, feature encoding, normalization, and sequence-based dataset restructuring. Two recurrent deep learning models, Recurrent Neural Network (RNN) and Bidirectional Long Short-Term Memory (Bi-LSTM), were developed for multiclass classification of network traffic into five categories: Distributed Denial of Service, Denial of Service, Reconnaissance, Theft, and Normal traffic. Experimental findings revealed that both models achieved strong detection capabilities. However, the Bi-LSTM model significantly outperformed the RNN model across all evaluation metrics. The Bi-LSTM achieved 99.12% accuracy, 87.26% precision, 97.82% recall, 91.81% macro F1-score, and 99.96% AUC-ROC, demonstrating superior ability in detecting minority attack classes while reducing false positives. The RNN model achieved accuracy (97.29%), precision (66.59%), recall (96.55%), macro F1-score (72.55%) and AUC-ROC (99.86%). The results confirm the effectiveness of bidirectional sequence learning in capturing temporal dependencies in network traffic and highlight the proposed framework's potential for strengthening cybersecurity and resilience in smart grid AMI systems.*

Keyword: Smart grids, AMI, network traffic, intrusion detection, Bi-LSTM, RNN, multiclass classification

European Journal of Computer Science and Information Technology, 14(4),48-69, 2026
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

INTRODUCTION

The world's energy sector is currently undergoing a fundamental transition with the adoption of intelligent power systems known as smart grids. Unlike conventional power systems, smart grids integrate advanced communication technologies, distributed energy resources, and intelligent control mechanisms to enhance efficiency, reliability, and sustainability (Wei et al., 2025). Figure 1 shows the smart grid architecture. This transition is particularly important in developing countries such as Nigeria, where traditional power infrastructure is often characterised by frequent outages, high transmission losses, carbon emissions, and limited operational efficiency (Adua et al., 2025; Adeshina et al., 2024).

A key component of smart grid architecture is the Advanced Metering Infrastructure (AMI), which enables bidirectional communication between utilities and consumers (Abdullah et al., 2023). AMI facilitates real-time monitoring, automated billing, and efficient energy management through interconnected smart meters and communication networks (Koukouvinos et al., 2025; Zhang et al., 2024; Abdullah et al., 2023). The Meter Data Management System (MDMS) further supports this framework by aggregating and processing large volumes of metering data for operational decision-making.

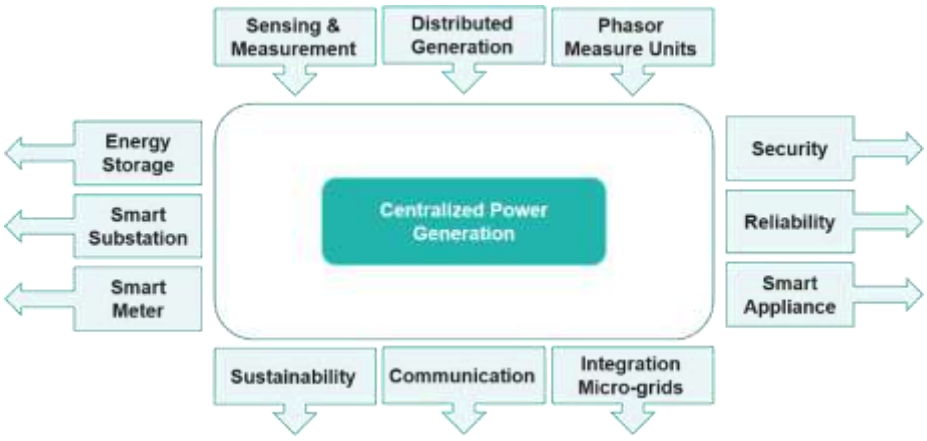


Figure 1: Architecture of Smart Grid System

The MDMS serves as the central component of the AMI in smart grids. Its major functions include collecting meter data from different metering technologies, validating data quality, estimating missing or erroneous values, processing and storing information, and supplying formatted data to utility billing and operational systems. MDMS also enables interaction with important utility management systems such as the Outage Management System (OMS), Consumer Information System (CIS), Geographic Information System (GIS), and Distribution Management System (DMS). In a centralized AMI architecture, a single MDMS located at the utility control center stores and manages data from all concentrators, which improves accessibility and processing speed. However, as the number of concentrators increases, the

centralized architecture faces scalability and communication challenges. Figure 2 shows the MDMS of the AMI.

The communication network framework of the AMI provides a two-way communication channel between utilities and consumers (Panda and Das, 2021), enabling real-time monitoring of electricity consumption and the transmission of pricing or control signals. The framework relies heavily on concentrators, which are categorized into local concentrators and backbone concentrators. Local concentrators gather data from smart meters and forward it to the backbone network, while backbone concentrators communicate with the utility control center or MDMS. Thus, the AMI communication network is divided into two layers: the smart meter network and the backhaul network. While the smart meter network connects smart meters through Neighbourhood Area Networks (NANs), often using mesh communication, the backhaul network links backbone concentrators to the control center. Together, these layers support efficient data collection, command dissemination, and reliable communication across the smart grid infrastructure. Figure 3 shows a typical framework of AMI communication network.

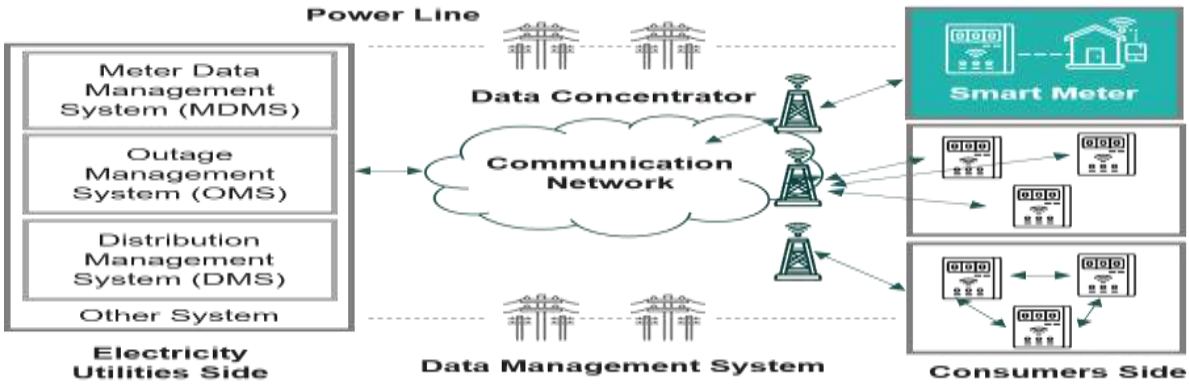


Figure 2: Data Management System of the AMI

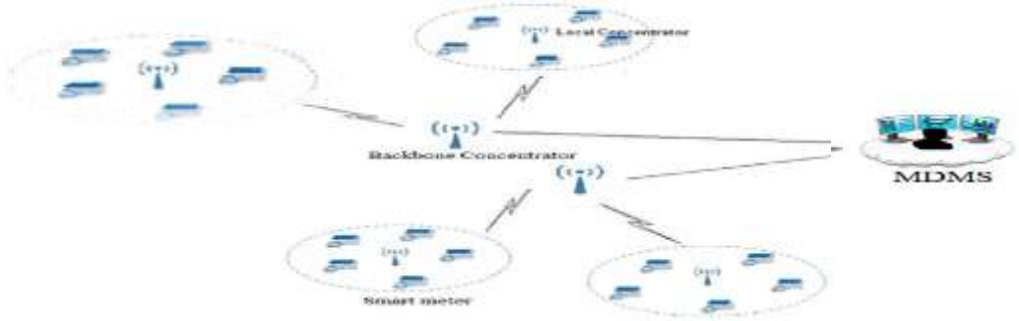


Figure 3: A Typical Communication Network of the AMI

However, the integration of communication networks into power systems significantly increases the cybersecurity risks associated with smart grids. The distributed and

interconnected nature of AMI exposes it to various cyber threats, including Denial of Service (DoS), Distributed DoS (DDoS), reconnaissance attacks, and data manipulation (Abiramasundari et al., 2025; Szczepaniuk & Szczepaniuk, 2025; Paul et al., 2024; Ali et al., 2022). These attacks can compromise data confidentiality, integrity, and availability (CIA), potentially resulting in inaccurate billing, service disruption, and large-scale power outages.

In a typical smart grid attack sequence, an adversary first conducts reconnaissance by scanning networks, monitoring traffic, and identifying devices, protocols, and vulnerabilities. This intelligence is then used to launch DoS attacks from a single source or DDoS attacks from many compromised devices, flooding control centers, gateways, substations, or smart meters with excessive traffic. These attacks disrupt communication, delay operational data transmission, and may prevent operators from monitoring or controlling the grid effectively. The risk of service interruptions and power outages also increases. After gaining access, attackers may perform data manipulation or data theft by altering, injecting, deleting, or stealing metering, billing, and operational data. Manipulated data can lead to incorrect control decisions, inaccurate billing, and reduced grid stability, while stolen information compromises customer privacy and utility security. Collectively, these attacks threaten the CIA triad of smart grid systems, resulting in operational disruptions, financial losses, reduced reliability, and diminished public trust in smart grid services.

The adoption of Intrusion Detection Systems (IDS) has become widespread as a means of addressing these security concerns. Traditional IDS approaches, such as signature-based and anomaly-based methods, exhibit notable limitations. Signature-based systems are known as knowledge-based detection or misuse detection systems and are ineffective against unknown attacks. On the other hand, anomaly-based methods have the ability to identify zero-day attacks by detecting abnormal user activities without relying on a signature database. However, it often suffers from high false positive rates and limited capability in modeling complex traffic patterns (Kumar et al., 2026; Alnasser et al., 2025; Diana et al., 2025; Ravindran et al., 2025). These challenges are further compounded by the high dimensionality and temporal nature of modern network traffic data.

Recent advances in deep learning (DL) have demonstrated significant potential in improving intrusion detection performance. In particular, Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and Bidirectional LSTM (Bi-LSTM) models have been widely adopted for analyzing network traffic due to their ability to capture temporal dependencies in sequential data (Tayebi and El Kafhali, 2025; Jablaoui and Liouane, 2025; Mienye et al., 2024). Among these, Bi-LSTM models provide enhanced contextual representation by processing input sequences in both forward and backward directions, thereby capturing richer temporal patterns in network behaviour (Krichen & Mihoub, 2025; Hassan et al. 2024). Recent studies (Khalifa et al., 2026; Qian et al., 2023; Chui et al., 2022) demonstrate that DL-based IDS models, while achieving high overall accuracy, remain biased toward majority classes due to imbalanced datasets. This results in poor detection of minority and rare attack types, a

limitation that persists even in smart grid environments (Acharya et al., 2026), thereby reducing their real-world effectiveness. While RNNs are effective for modeling temporal patterns in smart grid data, Bi-LSTMs provide superior performance by utilizing information from both past and future time steps and by maintaining long-term memory through specialized gating mechanisms. Despite the growing adoption of DL-based IDS in smart grids, identifying the architecture that offers optimal accuracy, robustness, and effectiveness in detecting sophisticated cyber-attacks remains a significant challenge. Addressing this challenge requires a comprehensive comparative evaluation of RNN, LSTM, and Bi-LSTM models to determine their suitability for securing modern smart grid environments.

RNNs are computationally efficient and capable of learning sequential patterns, but they struggle with long-term dependencies due to the vanishing gradient problem. LSTMs overcome this limitation by incorporating memory cells and gating mechanisms that retain relevant information over extended periods, making them more effective for detecting cyber-attacks in smart grids. Bi-LSTMs further enhance performance by processing data in both forward and backward directions, enabling them to capture richer contextual information and achieve superior accuracy in detecting sophisticated attacks such as false data injection, DDoS, reconnaissance, and data manipulation attacks. Consequently, Bi-LSTM generally provides the highest detection performance, LSTM offers a balance between accuracy and computational cost, while RNN provides the lowest computational overhead but the least detection capability among the three

A typical RNN architecture consists of (see Figure 4) : 1) Input Layer, that receives sequential smart grid data such as voltage measurements, current readings, power consumption records, network traffic logs, and sensor outputs; 2) Hidden Recurrent Layer(s), that contains recurrent connections that allow information from previous time steps to be retained through a hidden state (memory). This enables the model to learn temporal dependencies and behavioural patterns in the data seen. However, their memory is short term and cannot maintain long-term time series; and 3) Output Layer, that produces the final prediction, such as normal operation or a specific cyber-attack category. A recurrent network in its simplest form contains just one internal memory h_t, which is computed from Eqn. (1) as follows:

$$h_t = g\left(W x_t + U_f h_{t-1} + b\right) \quad (1)$$

where, $g(\,)$ is the activation function, U and W are flexible weight matrices of the h layer, b is the bias, and X is the input vector (Kratzert et al., 2018).

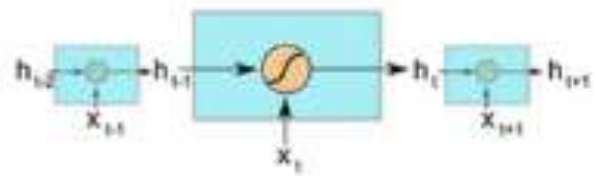


Figure 4: Architecture of a Simple RNN

LSTM is an advanced RNN architecture developed to overcome the limitations of traditional RNNs in handling sequential data. Unlike simple RNNs, LSTM incorporates memory cells and specialized gating mechanisms namely, the input, forget, and output gates, to regulate the flow of information and retain relevant data over extended periods (Witten et al., 2016). This design enables LSTM to effectively learn and preserve long-term dependencies, which are essential for sequence prediction tasks that require information from earlier time steps. While conventional RNNs are limited to capturing short-term relationships and highly susceptible to vanishing gradient problem, LSTMs can maintain and utilize long-range temporal information, with the forget gate controlling the extent to which previous information is retained or discarded. Figure 5 shows the architecture of LSTM. The hidden state h_t, for LSTM is calculated as:

$$i_t = \sigma(W_i X_t + U_i h_{t-1} + b_i) \quad (2)$$

$$f_t = \sigma\left(W_f X_t + U_f h_{t-1} + b_f\right) \quad (3)$$

$$o_t = \sigma(W_o X_t + U_o h_{t-1} + b_o) \quad (4)$$

$$\zeta_t = \tanh(W_c X_t + U_c h_{t-1} + b_c) \quad (5)$$

$$C_t = f_t * C_{t-1} + i_t * \zeta_t \quad (6)$$

$$h_t = \tanh(C_t) * o_t \quad (7)$$

where i_t, f_t, and o_t denotes the input, forget, and output gates at time t, respectively. W_i, W_f, W_o, and W_c
denote the weights that map the hidden layer input to the three gates of input, forget, and output while U_i, U_f, U_o, and U_c denote the weights matrices that map the hidden layer output to gates. While b_i, b_f, b_o, and b_c are the bias vectors; C_t and h_t $denote$ the outcome of the cell and the outcome of the layer, respectively (Cui et al., 2017). The activation function is denoted by σ, and its choice significantly impact the network's behaviour. According to (Ciaburro &Venkateswaran, 2017), it introduces non-linearity that enables the network to learn complex data patterns.

Among the commonly used activation functions, the hyperbolic tangent (tanh) maps input values to the range [−1,1], providing a zero-centered representation that is well suited for modeling sequential data containing both positive and negative values. Similarly, the Rectified Linear Unit (ReLU) is a widely used activation function that outputs positive inputs directly while mapping negative values to zero, helping to reduce the vanishing gradient problem by improving gradient flow. Variants such as Leaky ReLU address the "dying ReLU" issue by allowing small gradients for negative inputs, while Exponential Linear Unit (ELU) further improves learning by producing negative outputs that stabilize and speed up training. In addition, the sigmoid function compresses inputs into the range [0,1], making it suitable for probability-based outputs, whereas the softmax function is typically used in classification tasks to convert raw model outputs into normalized probabilities for multi-class prediction (Mienye et al., 2024).

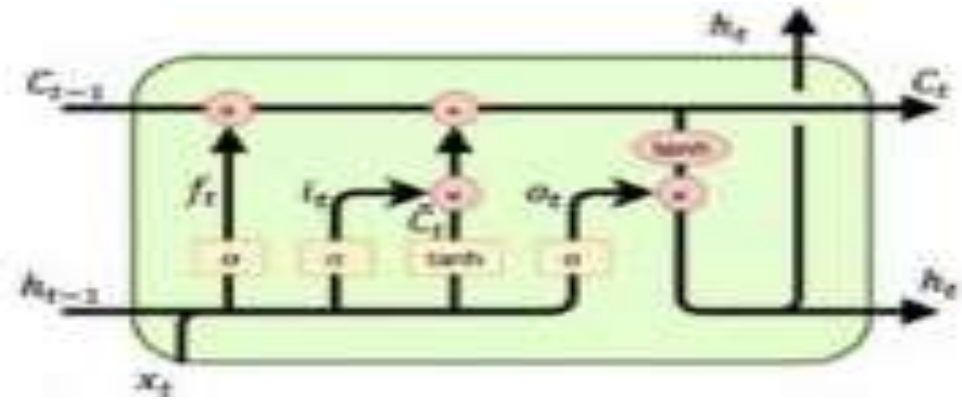


Figure 5: Architecture of LSTM

The Bi-LSTM extends the conventional LSTM architecture by processing sequential data in two directions namely, forward and backward, using separate hidden layers. The forward LSTM analyzes data in chronological order, while the backward LSTM processes the sequence in reverse order, enabling the network to capture contextual information from both past and future observations (Cui et al. 2017). The outputs from both directions are combined to generate a more comprehensive representation of the input sequence, thereby improving learning and prediction performance. To reduce overfitting and enhance generalization, dropout is applied between layers by randomly deactivating neurons during training. Additionally, the learning rate serves as a critical hyperparameter for model optimization and is typically selected within a range of 1 to 1×10^{-7} (Apaydin et al., 2020). Bi-LSTM exploits past and future contextual information to improve attack detection accuracy, learn long-term dependencies, identify sophisticated cyber-attacks and subtle anomalies, and enhance classification performance in evolving smart grid environments.

Its architecture, shown in Figure 6, typically includes: 1) Input Layer, that accepts sequential smart grid operational and communication data; 2) Forward LSTM Layer, that processes data from past to future, learning dependencies from previous observations; 3) Backward LSTM Layer, that processes data from future to past, capturing contextual information from subsequent observations; 4) Memory Cells, that store relevant long-term information while filtering irrelevant data; 5) Gates (Input, Forget, and Output Gates) where the Input Gate controls what new information enters the memory cell; the Forget Gate removes irrelevant or outdated information while the Output Gate determines what information is passed to the next layer and output; 6) Concatenation Layer, that combines outputs from both forward and backward LSTM layers; and 7) Output Layer, that classifies traffic as normal or malicious and may identify the attack type.

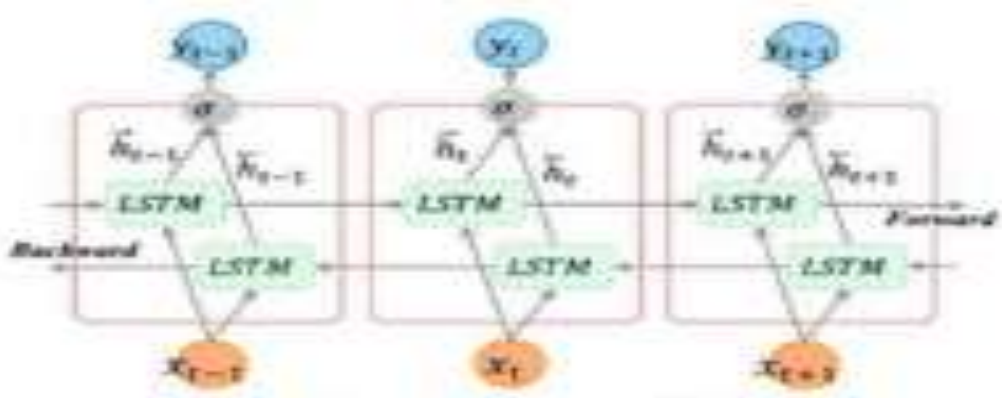


Figure 6: Architecture of Bi-LSTM

In a Bi-LSTM network, the forward hidden state output $\overrightarrow{h_t}$ is generated by processing the input sequence in chronological order from time $T - n$ to $T - 1$, whereas the backward hidden state output $\overleftarrow{h_t}$ is obtained by processing the same sequence in reverse order over the corresponding time steps. The outputs of both the forward and backward layers are computed similarly to those in a standard unidirectional LSTM using Eqns. (8) and (9). The final Bi-LSTM output, Y_t, is then determined using Eqn. (10) as follows:

$$\overrightarrow{h_t} = \sigma_h\left(W_{xh}X_t + W_{hh}\overrightarrow{h_{t-1}} + b_h\right) \quad (8)$$

$$\overleftarrow{h_t} = \sigma_h\left(W_{xh}X_t + W_{hh}\overleftarrow{h_{t-1}} + b_h\right) \quad (9)$$

$$Y_t = \sigma_y\left(W_{hy}[\overrightarrow{h_t}; \overleftarrow{h_t}] + b_y\right) \quad (10)$$

where, σ is the activation function used to concatenate two $\overrightarrow{h_t}$ and $\overleftarrow{h_t}$ outputs while [;] denotes concatenation.

To address the challenges, this study proposes a DL-based intrusion detection framework for smart grids AMI using RNN and Bi-LSTM models. The framework leverages the BoT-IoT dataset to perform multiclass classification of network traffic into five categories: DoS, DDoS, Reconnaissance, Theft, and Normal traffic. A comprehensive preprocessing pipeline is employed to improve data quality and feature representation. The proposed approach aims to enhance detection accuracy, reduce false positives, and provide a scalable and reliable solution for securing smart grid infrastructures.

The rest of the paper is structured in the following way: Section 2 describes the methodology, explaining the proposed framework, attributes of the dataset, data preprocessing and feature engineering tasks as well as optimized hyperparameters for training the deep learning models. Section 3 presents the results from implementation of the proposed framework in Python software, evaluating the models' performance with implications for cyber-attack detection in smart grids environment. Finally, section 4 concludes the paper, giving direction for future works.

European Journal of Computer Science and Information Technology, 14(4),48-69, 2026
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

METHODOLOGY

This study proposes a DL-based intrusion detection framework for classifying cyber-attacks in smart grids AMI. The methodology comprises dataset acquisition, data preprocessing, model development, training configuration, and performance evaluation.

Dataset Description

The proposed DL-based intrusion detection framework for smart grids AMI using RNN and Bi-LSTM models is shown in Figure 7. It comprises three distinct layers namely, data layer containing dataset components, middle layer describing activities like data preprocessing, feature extraction and model training, and evaluation layer, unfolding the performance of the models in detecting and classifying the attack types in smart grids environment. The BoT-IoT dataset, obtained from the Kaggle repository, was used in this work. It is a benchmark dataset widely adopted in network intrusion detection research due to its realistic representation of IoT network traffic. The dataset contains approximately 1,000,000 instances with diverse network flow features, including protocol information, port numbers, packet statistics, timestamps, and behavioural attributes. These features enable effective discrimination between normal and malicious traffic. The problem was formulated as a five-class classification task consisting of DoS, DDoS, Reconnaissance, Theft, and Normal traffic. This multiclass formulation enables fine-grained attack detection beyond binary classification.

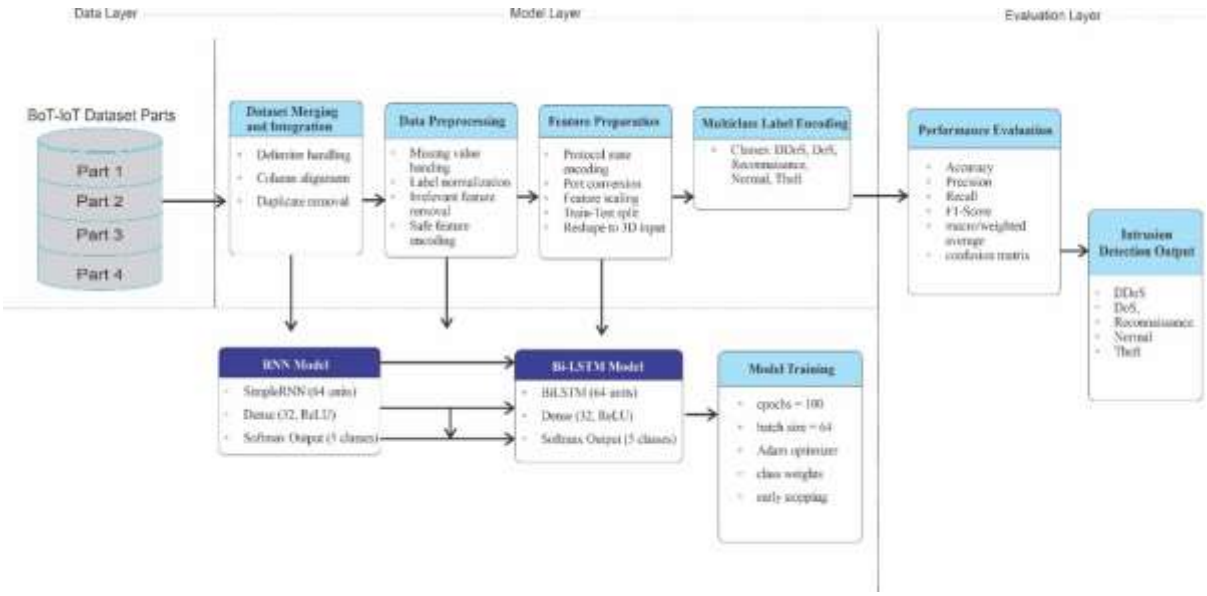


Figure 7: The proposed DL-based framework for multi-class cyber-attacks detection in smart grids AMI

The dataset consists of network traffic protocols mainly including Address Resolution Protocol (ARP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP), with source and destination IP addresses largely in Class C ranges and a few Class A addresses such as 192.168.100.x and 8.8.8.x. It also includes state indicators like CON, INT, and RST, along with

various service port numbers (e.g., 138, 139, 37214, 51838, 57950, 58999, 58360, and 36663) that may be targeted by attackers. These state values describe how network sessions behave or terminate where CON denotes Connection Established and Terminated Normally, typically represents normal traffic; INT denotes Interrupted Connection, indicates incomplete or suspicious connections often linked to scans or attacks, and RST denotes Connection Reset, suggests port scanning, DoS activity, or connection resets after probing. In general, normal traffic is dominated by CON states, while malicious activities such as botnet probes, scanning, and DoS attacks are characterized by higher occurrences of INT and RST due to incomplete handshakes, rejected connections, and abnormal traffic spikes detectable by monitoring systems.

Data Preprocessing and Feature Engineering

To ensure that the data attains desirable quality and is suitable for training the deep learning models, data preprocessing activities were performed. First, dataset integration and cleaning were conducted by merging relevant data segments and removing duplicate, inconsistent, and irrelevant records. Missing and invalid values were handled to ensure dataset consistency. A total of 800,039 data points (samples) and 46 features were used in this study. Categorical features such as protocol type and connection state were transformed into numerical representations using encoding techniques. Feature scaling was applied using Min-Max normalisation to standardise feature ranges, as shown in Eqn. (11):

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \quad (11)$$

Relevant statistical and behavioural features, including packet counts, byte rates, and flow durations, were retained for model training. These features are critical for capturing anomalous traffic patterns. Feature importance was further examined using model-based techniques such as attention mechanism. This enhance the interpretability of these “black box” models as it is difficult to directly see which input features or time steps influenced a prediction. It also supports trust in AI-based IDS systems. The dataset was split into training and testing sets in the ratio of 7:3, and the input data was reshaped into a three-dimensional format suitable for sequence-based models.

Deep Learning Models

Two recurrent DL architectures were implemented to capture temporal dependencies in network traffic data. The RNN model consists of a Simple RNN layer with 64 units, followed by a dense layer with 32 neurons and ReLU activation, and a Softmax output layer. The model captures sequential dependencies by retaining information from previous inputs. The Bi-LSTM model extends sequence learning by processing input data in both forward and backward directions. It comprises a bidirectional LSTM layer with 64 units, a dense layer with 32 neurons (ReLU), and a Softmax output layer. This architecture enhances contextual learning and improves classification performance.

Model Training Configuration and Performance Evaluation

Both models were trained under identical conditions to ensure fair comparison. The training configuration includes 100 epochs, batch size of 64, and the Adam optimizer. Categorical crossentropy was used as the loss function L, for multiclass classification, as represented in Eqn. (12):

$$L = -\sum_{i=1}^{N}\sum_{j=1}^{C} y_{ij}\log(\hat{y}_{ij}) \quad (12)$$

where, i is the sample, j is the class, and N is the total number of samples, $y_{ij}$and $\hat{y}_{ij}$ represent the true and predicted class probabilities, respectively.

The Softmax activation function was applied at the output layer to generate probability distributions across the five classes. Model implementation was carried out using Python with TensorFlow/Keras, NumPy, Pandas, and Scikit-learn libraries. The learning rate significantly influences how the loss function changes across epochs, as a very low learning rate slows convergence while an excessively high learning rate may prevent reaching the optimal solution. Therefore, a decaying learning rate is preferred, allowing faster learning in early stages and finer adjustments in later stages of training.

Instead of just normal vs. attack traffic class, the categorical crossentropy considers more than two classes (DDoS, DoS, Reconnaissance, Normal, Theft). The labels are one-hot encoded. The output activation layer deployed the softmax activation (outputs a probability distribution across all classes) instead of a sigmoid activation (outputs a probability between 0 and 1) in binary crossentropy. The model's output shall be one neuron per class, all summing to 1 (probability distribution), instead of a single neuron with probability between [0,1].
The softmax activation function is described as follows:
For a given input vector z with n elements $[z_1,\ z_2,\ z_3, \dots, z_n]$, the softmax output for the i-th element is given as:

$$\sigma(z_i) = \frac{e^{z_i}}{\sum_{j=1}^{n} e^{z_j}} \quad (13)$$

where each z_i is the logit (raw output from the previous layer for class), the softmax function turns these logits into probabilities, so that their sum equals unity as follows:

$$\sum_{i=1}^{n}\sigma(z_i) = 1 \quad (14)$$

This is useful for multi-class classification problems, where the output represents a probability distribution across all classes.

The proposed models' performance was evaluated using accuracy, precision, recall, F1-score metrics as well as Receiver Operating Characteristic Area Under Curve (ROC-AUC). A

confusion matrix depicted in Figure 8 was also used to provide detailed class-wise performance analysis. To ensure robustness, both macro-average and weighted-average metrics were computed, enabling comprehensive evaluation across both majority and minority classes.

		Class 1	Class 2	Class 3	Class 4	Class 5
Actual Values	Class 1	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}
	Class 2	M_{21}	M_{22}	M_{23}	M_{24}	M_{25}
	Class 3	M_{31}	M_{32}	M_{33}	M_{34}	M_{35}
	Class 4	M_{41}	M_{42}	M_{43}	M_{44}	M_{45}
	Class 5	M_{51}	M_{52}	M_{53}	M_{54}	M_{55}

Predicted Values

Figure 8: Sample confusion matrix for evaluating models' performance

RESULTS AND DISCUSSION

This section presents the experimental results obtained from the implementation of the RNN and Bi-LSTM models for intrusion detection in Smart Grid AMI. The performance is analysed using training behaviour, overall evaluation metrics, and class-level performance.

Training Performance

Figures 9 and 10 show the training and validation curves for accuracy and loss metric for both RNN and Bi-LSTM models. Results indicate that both the RNN and Bi-LSTM models effectively learned from the pre-processed dataset, showing rapid convergence over 100 epochs with increasing training accuracy and decreasing loss. High validation performance indicated good generalization on test data, and the training curves confirmed that both models achieved strong performance before the end of training, demonstrating the suitability of the preprocessing approach and model architectures for the classification task.

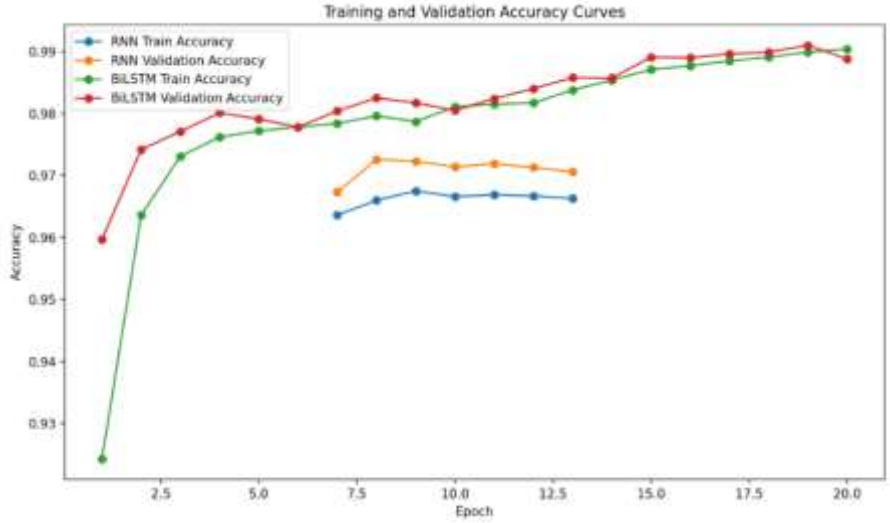


Figure 9: Training and validation accuracy curves for RNN and Bi-LSTM

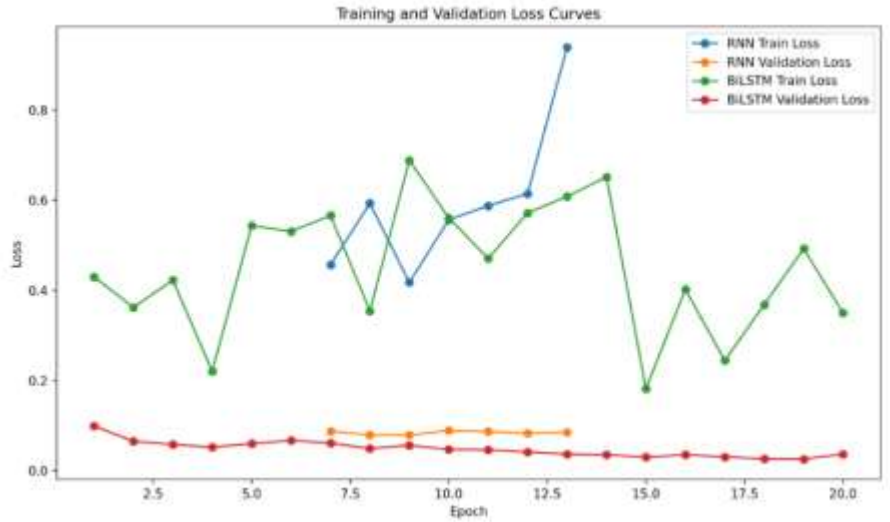


Figure 10: Training and validation loss curves for RNN and Bi-LSTM

Notably, the Bi-LSTM exhibited slightly faster convergence and more stable validation behaviour compared to the RNN, indicating improved learning efficiency. Table 1 presents the performance comparison of the RNN and Bi-LSTM models in terms of accuracy, macro precision, macro recall, macro F1-score, and ROC-AUC. Figures 11 and 12 shows the generated confusion matrices for RNN and Bi-LSTM models. Figure 13 visualizes the models' performance across all metrics while Figure 14 depicts their ROC-AUC report.

Table 1: Overall Performance of RNN and Bi-LSTM Models

Model	Accuracy	Macro Precision	Macro Recall	Macro F1-score	ROC-AUC
RNN	0.9729	0.6659	0.9655	0.7255	0.9986
Bi-LSTM	0.9912	0.8726	0.9782	0.9181	0.9996

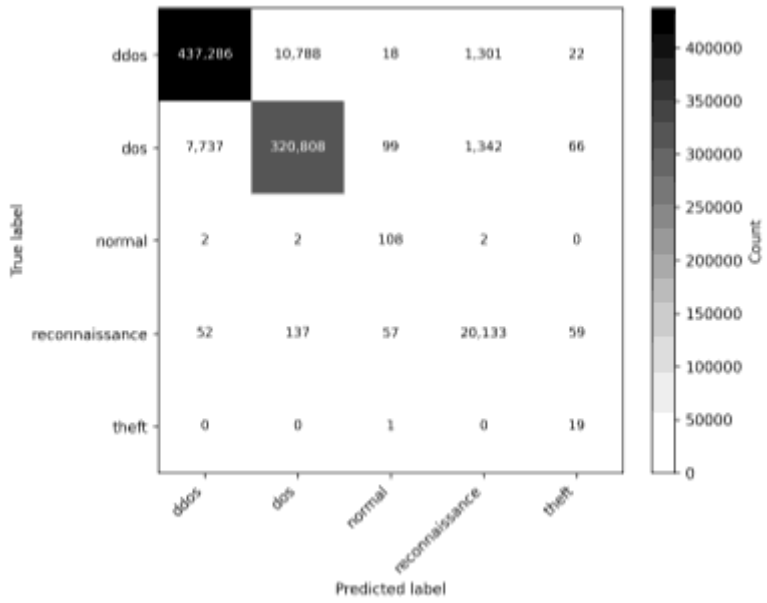


Figure 11: RNN confusion matrix

European Journal of Computer Science and Information Technology, 14(4),48-69, 2026
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

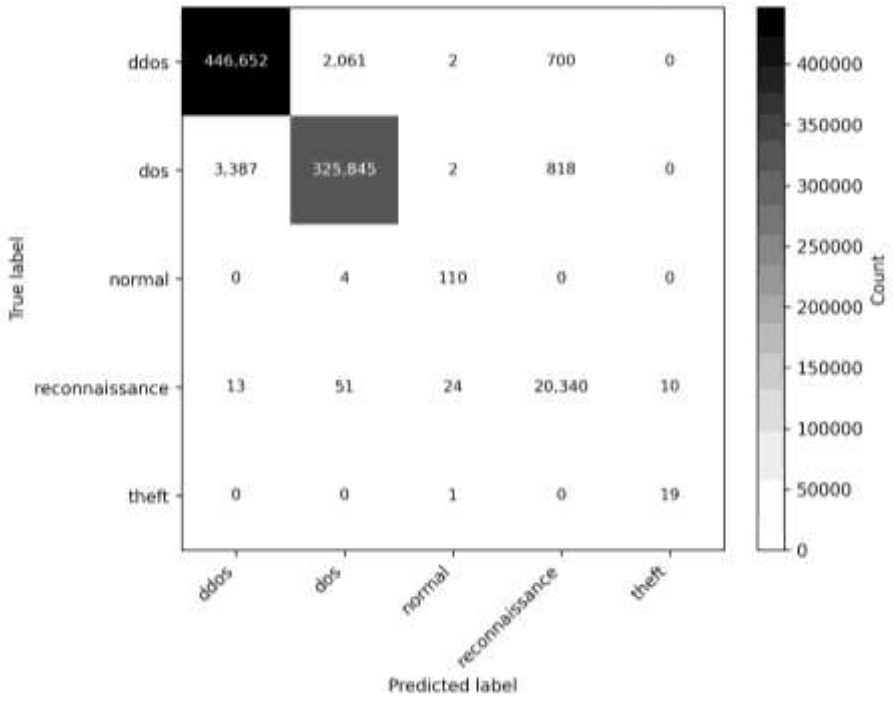
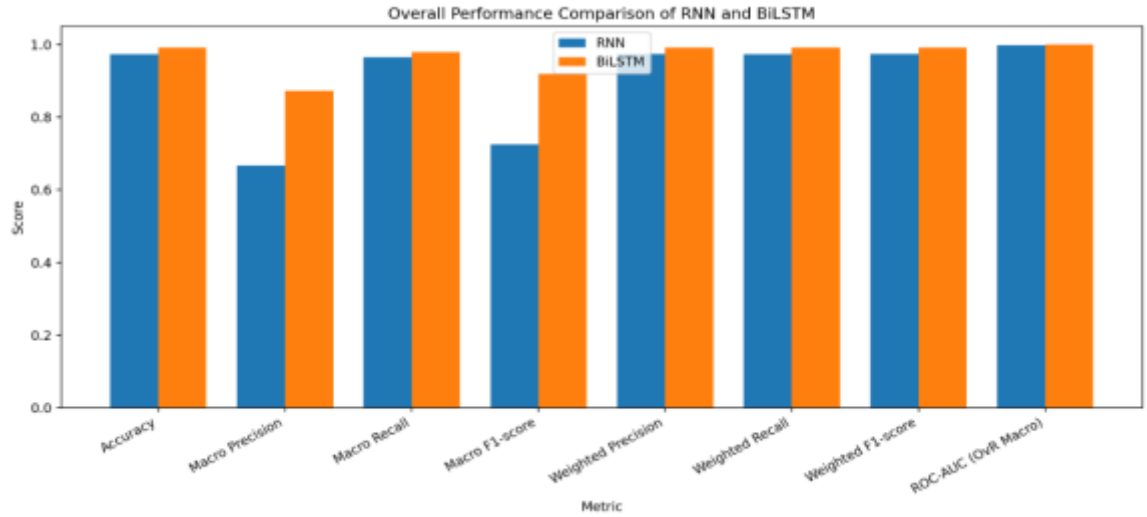


Figure 12: Bi-LSTM confusion matrix

Both models achieved strong performance across all metrics. However, the Bi-LSTM consistently outperformed the RNN. While the improvement in accuracy (+1.83%) appears modest, significant gains were observed in macro precision (+20.67%) and macro F1-score (+19.26%). These results indicate that the Bi-LSTM provides a more balanced classification



performance across all classes, particularly in handling class imbalance. The near-perfect ROC-AUC values for both models further confirm their strong discriminative capability.

Figure 13: Comparative Performance of RNN and Bi-LSTM Across Evaluation Metrics

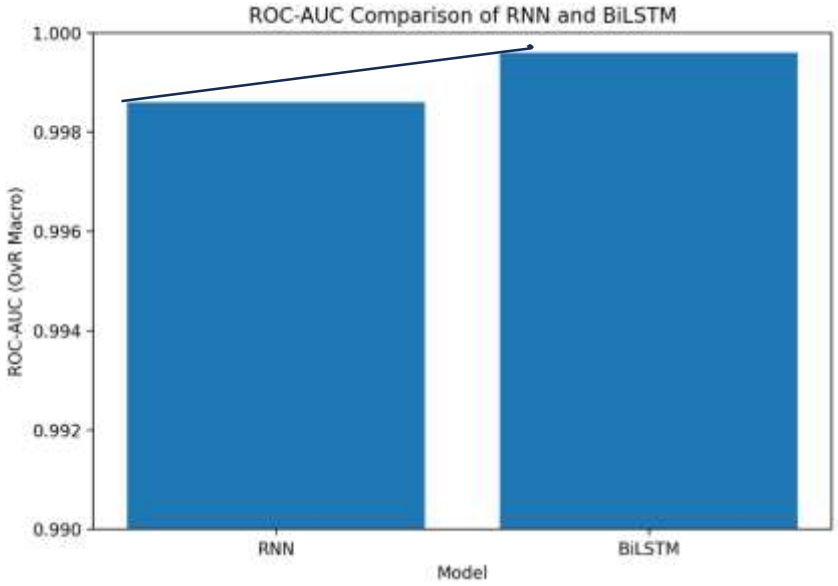


Figure 14: ROC-AUC Comparison of RNN and Bi-LSTM

Weighted Average Performance

To account for class imbalance, weighted average metrics were also evaluated, as shown in Table 2. Both models achieved high weighted scores, largely due to strong performance on dominant classes such as DoS and DDoS. Nevertheless, the Bi-LSTM maintained superior performance, confirming that its advantage is consistent across both balanced and imbalanced evaluations.

Table 2: Weighted Average Performance of RNN and Bi-LSTM

Model	Weighted Precision	Weighted Recall	Weighted F1-score
RNN	0.9735	0.9729	0.9731
Bi-LSTM	0.9913	0.9912	0.9912

Class-Level Performance Analysis

The class level performance shown in Table 3 shows that the RNN model achieved high performance on major classes such as DDoS, DoS, and Reconnaissance, with strong precision, recall, and F1-scores. Additionally, the model demonstrates consistently high recall across all classes, indicating strong sensitivity in detecting true attack instances. However, significant limitations were observed in minority classes. For example, the Normal class achieved high

recall (0.9474) but low precision (0.3816), while the Theft class recorded very low precision (0.1145) despite high recall (0.9500). This indicates that the RNN generated a high number of false positives, misclassifying many samples into minority classes.

Table 3: Class-Level Performance of the RNN Model

Class	Precision	Recall	F1-score	Support
DDoS	0.9825	0.9730	0.9777	449,415
DoS	0.9671	0.9720	0.9695	330,052
Normal	0.3816	0.9474	0.5441	114
Reconnaissance	0.8839	0.9851	0.9317	20,438
Theft	0.1145	0.9500	0.2043	20
Accuracy			0.9729	800,039
Macro Average	0.6659	0.9655	0.7255	800,039
Weighted Average	0.9735	0.9729	0.9731	800,039

The Bi-LSTM model achieved excellent performance across both major and minor classes. While maintaining high performance on dominant classes, it significantly improved classification balance for minority classes. For the Normal class, precision improved from 0.3816 to 0.7914 while maintaining high recall (0.9649), resulting in a substantial increase in F1-score. Similarly, for the Theft class, precision improved from 0.1145 to 0.6552, with recall remaining high (0.9500), leading to a major improvement in F1-score. These results demonstrate that the Bi-LSTM effectively reduces false positives while preserving strong detection capability, making it more reliable for real-world intrusion detection scenarios.

Table 4: Class-Level Performance of the Bi-LSTM Model

Class	Precision	Recall	F1-score	Support
DDoS	0.9924	0.9939	0.9931	449,415
DoS	0.9935	0.9873	0.9904	330,052
Normal	0.7914	0.9649	0.8696	114
Reconnaissance	0.9306	0.9952	0.9618	20,438
Theft	0.6552	0.9500	0.7755	20
Accuracy			0.9912	800,039
Macro Average	0.8726	0.9782	0.9181	800,039
Weighted Average	0.9913	0.9912	0.9912	800,039

Comparative Discussion and Study Limitations

A direct comparison between the two models, shown in Table 5, highlights the advantages of the Bi-LSTM architecture. The most significant improvements are observed in macro precision and F1-score, which are critical for evaluating balanced multiclass performance. These gains indicate that the Bi-LSTM produces more reliable and consistent predictions across all traffic categories. The superior performance of the Bi-LSTM can be attributed to its bidirectional learning capability, which enables it to capture both past and future contextual dependencies in network traffic sequences. This is particularly important in intrusion detection, where attack patterns often evolve.

Table 5: Performance Improvement of Bi-LSTM over RNN

Metric	RNN	Bi-LSTM	Improvement
Accuracy	0.9729	0.9912	+0.0183
Macro Precision	0.6659	0.8726	+0.2067
Macro Recall	0.9655	0.9782	+0.0127
Macro F1-score	0.7255	0.9181	+0.1926
ROC-AUC	0.9986	0.9996	+0.0010

The results confirm that deep learning models are highly effective for intrusion detection in Smart Grid AMI environments. While both RNN and Bi-LSTM achieve high accuracy and strong detection capability, the Bi-LSTM provides a more robust and balanced classification performance. In particular, the ability of the Bi-LSTM to significantly improve precision in minority classes highlights its suitability for real-world deployment, where reducing false alarms is critical. The findings also emphasise the importance of temporal context in modelling network traffic behaviour. The proposed Bi-LSTM-based intrusion detection system demonstrates strong potential for enhancing cybersecurity in smart grid infrastructures.

One of the limitations of this study is the observed class imbalance in the dataset, where DDoS and DoS classes dominate the dataset, whereas the Normal and Theft classes contain only a very small number of samples. Consequently, the developed RNN and Bi-LSTM models may become biased toward the majority classes, leading to lower detection performance for minority (rare) attacks despite achieving high overall accuracy. Future research will employ data balancing techniques such as the Synthetic Minority Over-sampling Technique (SMOTE), Adaptive Synthetic Sampling (ADASYN), or Generative Adversarial Networks (GANs) to generate realistic minority-class samples. Additionally, under-sampling of the majority classes or hybrid sampling methods could be investigated to obtain a more balanced training dataset. Another promising direction is the use of ensemble learning techniques, including Random Forest, XGBoost, or LightGBM, which have demonstrated improved robustness when

handling imbalanced cybersecurity datasets. Although the present study places emphasis on class-specific metrics such as precision, recall, and F1-score, future evaluations should emphasize on metrics such as Matthews Correlation Coefficient (MCC) and Area Under the Precision-Recall Curve (AUPRC), on a larger and more balanced dataset, to provide a more comprehensive assessment of intrusion detection performance.

CONCLUSION

This work presented a DL-based intrusion detection framework for cyber-attack detection in smart grids AMI. The proposed approach utilized RNN and Bi-LSTM models to perform multiclass classification of network traffic using the BoT-IoT dataset. A robust preprocessing pipeline was developed to improve data quality and ensure effective feature representation for sequence-based learning. The experimental results demonstrated that both models are capable of achieving high detection performance; however, the Bi-LSTM model consistently outperformed the RNN across all evaluation metrics. RNNs analyze temporal patterns in smart meter and network traffic data to detect anomalies, learn normal system behaviour, identify cyber-attacks such as DoS, DDoS, reconnaissance, and data theft, and support real-time threat monitoring and early warning mechanisms. Bi-LSTM leverages past and future context to improve detection accuracy, captures long-term dependencies, identifies sophisticated cyber-attacks and subtle anomalies, and enhances classification performance in dynamic smart grid environments.

In particular, the Bi-LSTM showed substantial improvements in macro precision and F1-score, indicating more balanced and reliable classification across all traffic classes. Furthermore, the model significantly reduced false positives in minority classes such as Normal and Theft, which is critical for real-world deployment where false alarms can undermine system reliability. The superior performance of the Bi-LSTM can be attributed to its ability to capture bidirectional temporal dependencies in network traffic, enabling better modeling of complex and evolving attack patterns. These results confirm the effectiveness of deep learning, particularly bidirectional recurrent architectures, in addressing the challenges of intrusion detection in smart grid environments. Future work will focus on improving real-time deployment capabilities, exploring hybrid and attention-based deep learning models, and evaluating the proposed framework on additional real-world smart grid datasets to further enhance generalization and scalability.

Acknowledgement

The authors are grateful to Tertiary Education Trust Fund (TETFund), Nigeria for funding this research and the Management of the University of Uyo for creating a conducive environment for research.

REFERENCES

Abdullah, A. A., El-Den, B. M., Abo-Al-Ez, K. M., & Hassan, T. M. (2023). Security management for an advanced metering infrastructure (AMI) system of smart electrical grids. Applied Sciences, 13(15). https://doi.org/10.3390/app13158990

Abiramasundari, S., & Ramaswamy, V. (2025). Distributed denial-of-service (DDOS) attack detection using supervised machine learning algorithms. Scientific reports, 15(1), 13098. https://doi.org/10.1038/s41598-024-84879-y

Acharya, R., Al Sardy, L., Muhammad, M., & German, R. (2026). ADVIS-G: An Adversarially Defended Intrusion Detection System for Smart Grids Using Deep Learning. KI-Künstliche Intelligenz, 1-23. https://doi.org/10.1007/s13218-026-00905-3

Adeshina, M. A., Ogunleye, A. M., Suleiman, H. O., Yakub, A. O., Same, N. N., Suleiman, Z. A., & Huh, J.-S. (2024). From Potential to Power: Advancing Nigeria's Energy Sector through Renewable Integration and Policy Reform. Sustainability, 16(20), 8803. https://doi.org/10.3390/su16208803

Adua, A. M., Alabi, I. I., Araga, A. I., Sabo, A., Shehu, M. A., Danshehu, B. G., ... & Abubakar, N. (2025). Factors Affecting the Power Outage in Nigeria (A Case Study of Kainji Hydro Power Station). Int. J. Innov. Math. Stat. Energy Policies, 13, 107-141. https://doi.org/10.5281/zenodo.17614603

Ali, M. H., Jaber, M. M., Abd, S. K., Rehman, A., Awan, M. J., Damaševičius, R., & Bahaj, S. A. (2022). Threat Analysis and Distributed Denial of Service (DDoS) Attack Recognition in the Internet of Things (IoT). Electronics, 11(3), 494. https://doi.org/10.3390/electronics11030494

Alnasser, O., Al Muhtadi, J., Saleem, K., & Shrestha, S. (2025). Signature and anomaly based intrusion detection system for secure IoTs and V2G communication. Alexandria Engineering Journal, 125, 424-440. https://doi.org/10.1016/j.aej.2025.03.068

Apaydin, H., Feizi, H., Sattari, M. T., Colak, M. S., Shamshirband, S., & Chau, K.-W. (2020). Comparative Analysis of Recurrent Neural Network Architectures for Reservoir Inflow Forecasting. Water, 12(5), 1500. https://doi.org/10.3390/w12051500

Chui, K. T., Gupta, B. B., Chaurasia, P., Arya, V., Almomani, A., & Alhalabi, W. (2023). Three-stage data generation algorithm for multiclass network intrusion detection with highly imbalanced dataset. International Journal of Intelligent Networks, 4, 202-210. https://doi.org/10.1016/j.ijin.2023.08.001

Ciaburro, G. and Venkateswaran, B. (2017). Neural Networks with R: SMART Models Using CNN, RNN, Deep Learning, and Artificial Intelligence Principles; Packt Publishing Ltd.: Birmingham, UK, 2017.

Cui, Z.; Member, S.; Ke, R.; Member, S.; Wang, Y. Deep Stacked Bidirectional and Unidirectional LSTM Recurrent Neural Network for Network-wide Traffic Speed Prediction. In Proceedings of the UrbComp 2017: The 6th International Workshop on Urban Computing, Halifax, NS, Canada, 14 August 2017; 2017; pp. 1–12.

Diana, L., Dini, P., & Paolini, D. (2025). Overview on Intrusion Detection Systems for Computers Networking Security. Computers, 14(3), 87. https://doi.org/10.3390/computers14030087

Hassan, N., Miah, A. S. M., & Shin, J. (2024). A Deep Bidirectional LSTM Model Enhanced by Transfer-Learning-Based Feature Extraction for Dynamic Human Activity Recognition. Applied Sciences, 14(2), 603. https://doi.org/10.3390/app14020603

Jablaoui, R., & Liouane, N. (2025). Network security based combined CNN-RNN models for IoT intrusion detection system. Peer-to-peer Networking and Applications, 18(3), 129. https://doi.org/10.1007/s12083-025-01944-7

Khalifa, S., Marie, M., & Mohamed, W. (2026). An Optimized Deep Learning Approach for Multiclass Anomaly Detection. Information, 17(2), 183. https://doi.org/10.3390/info17020183Koukouvinos, K. G., Koukouvinos, G. K., Chalkiadakis, P., Kaminaris, S. D., Orfanos, V. A., & Rimpas, D. (2025). Evaluating the Performance of Smart Meters: Insights into Energy Management, Dynamic Pricing and Consumer Behavior. Applied Sciences, 15(2), 960. https://doi.org/10.3390/app15020960.

Kratzert, F., Klotz, D., Brenner, C., Schulz, K. and Herrnegger, M. (2018). Rainfall–runoff modelling using Long
Short-Term Memory (LSTM) networks. Hydrol. Earth Syst. Sci. 2018, 22, 6005–6022.

Krichen, M., & Mihoub, A. (2025). Long Short-Term Memory Networks: A Comprehensive Survey. AI, 6(9), 215. https://doi.org/10.3390/ai6090215

Kumar, L. K. S., Nethi, S. R., Uyyala, R., Vurubindi, P., Narahari, S. C., Das, A. K., K, V. B., & Alenazi, M. J. F. (2026). Anomaly-based intrusion detection on benchmark datasets for network security: a comprehensive evaluation. Scientific reports, 16(1), 8507. https://doi.org/10.1038/s41598-026-38317-w

Mienye, I. D., Swart, T. G., & Obaido, G. (2024). Recurrent Neural Networks: A Comprehensive Review of Architectures, Variants, and Applications. Information, 15(9), 517. https://doi.org/10.3390/info15090517

Panda, D. K. and Das, S. (2021). Smart grid architecture model for control, optimization and data analytics of future power networks with more renewable energy, Journal of Cleaner Production, Volume 301, 2021, 126877, https://doi.org/10.1016/j.jclepro.2021.126877.

Paul, B., Sarker, A., Abhi, S. H., Das, S. K., Ali, M. F., Islam, M. M., ... & Saqib, N. (2024). Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies. Heliyon, 10(19). https://doi.org/10.1016/j.heliyon.2024.e37980

Qian, H., Zhang, X., Zhang, C., & Jiang, C. (2023). A novel cyber intrusion detection model based on improved hybrid sampling. Transactions of the Institute of Measurement and Control, 45(15), 2903-2913. https://doi.org/10.1177/01423312231158422

Ravindran, V. K., Ojha, S. S., & Kamboj, A. (2025). A comparative analysis of signature-based and anomaly-based intrusion detection systems. International Journal of Latest Technology in Engineering, Management & Applied Science, 14(5), 209-214. https://doi.org/10.51583/IJLTEMAS.2025.140500026

Szczepaniuk, E. K., & Szczepaniuk, H. (2025). Cybersecurity of Smart Grids: Requirements, Threats, and Countermeasures. Energies, 18(18), 5017. https://doi.org/10.3390/en18185017

Tayebi, M., & El Kafhali, S. (2025). Performance analysis of recurrent neural networks for intrusion detection systems in Industrial-Internet of Things. Franklin Open, 12. https://doi.org/10.1016/j.fraope.2025.100310

Wei, T., Li, H., & Miao, J. (2025). Integration and Development Path of Smart Grid Technology: Technology-Driven, Policy Framework and Application Challenges. Processes, 13(8), 2428. https://doi.org/10.3390/pr13082428.

Witten, I., Frank, E., Hall, M. and Pal, C. (2016). Data Mining. In Practical Machine Learning Tools and Techniques, 4th ed.; Elsevier: Amsterdam, The Netherlands.

Zhang, X. Y., Guo, P., Kuenzel, S., & Yin, C. (2024). Ethical considerations in advanced metering infrastructure integration: A systematic review. Energy Strategy Reviews, 56, 101571. https://doi.org/10.1016/j.esr.2024.101571