Indonesian Journal of Electrical Engineering and Computer Science
Vol. 38, No. 3, June 2025, pp. 1804~1818
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v38.i3.pp1804-1818

IoT based intrusion detection data analysis using deep learning models

Marwa Baich, Nawal Sael, Touria Hamim
Laboratory of Information Technology and Modeling, Faculty of Sciences, Ben M'Sik, Hassan II University of Casablanca, Casablanca, Morocco

Article Info

Article history:

Received May 17, 2024
Revised Nov 20, 2024
Accepted Nov 30, 2024

Keywords:

Cybersecurity
Deep learning
Internet of things
Intrusion detection system
UNSW-NB15
NSL-KDD

ABSTRACT

In both the academic and industrial domains, integration of the internet of things (IoT) is now universally accepted as a significant technical achievement. IoT offers a multitude of security issues despite its many advantages, such as protecting networks and devices, handling resource-constrained network scenarios, and controlling threats to IoT networks. This article gives a state-of-the-art analysis on the application of multiple deep learning (DL) algorithms in IoT intrusion detection systems (IDS), covering the years 2020 to 2024. Moreover, two popular network datasets, NSL-KDD and UNSW-NB15, are used for an experimental evaluation. The study thoroughly examines and assesses the advantages of well-known deep learning algorithms, including DNN, CNN, RNN, LSTM, and FFDNN. The study demonstrates the exceptional performance of the DNN approach on both datasets, with 99.14% accuracy in multiclass classification in NSL-KDD and 99.36% accuracy in binary classification. Furthermore, on UNSW-NB15, 82.26% of multiclass classifications and 93.96% of binary classifications with a 42-second minimum running time were achieved, along with an excellent performance in reducing false alarms at a rate of 2.19%.

Corresponding Author:

Marwa Baich
Laboratory of Information Technology and Modeling, Faculty of Sciences
Ben M'Sik, Hassan II University of Casablanca
Casablanca, Morocco
Email: marwa.baich-etu@etu.univh2c.ma

1. INTRODUCTION

The smart devices are becoming more and more commonplace in many daily activities due to the increasing prevalence of technology improvements in sensors, automatic item recognition, tracking, communication among interconnected devices, and integrated Internet services. Studies conducted by Cisco predict that the Internet of Things, it is projected that there will be approximately 75.3 billion devices that are actively linked by 2025 [1]. IoT technology differs from conventional Internet technologies in that it has the ability to facilitate data sharing across systems without requiring human intervention.

Acknowledging the crucial significance of cybersecurity becomes essential, especially as the IoT takes center stage as the driving force behind the ongoing industrial revolution and serves as the primary infrastructure for collecting real-time data [2]. It needs to be underlined that IoT-based intrusion detection research is extremely indispensable for enhancing security and privacy in such dynamic and networked environments. This will also provide the base for novel solutions and adaptive approaches toward effectively combating emerging threats and securing IoT networks. Installing a network intrusion detection system (NIDS) that can recognize both active and future assaults is essential for safeguarding the IoT network and the systems that are developed on it. When a breach is detected, an IDS can monitor the network activities

among the linked devices and generate an alert. While IDS are effective in traditional networks, creating an IDS for an IoT network poses a considerable challenge. This is primarily due to IoT network characteristics including the network's IDS agent nodes' constrained processing and storing capacities [3].

IDSes are available in various forms and employ different techniques to identify suspicious activities, including the ones listed below [4]: The purpose of a network intrusion detection system (NIDS) is to monitor all device traffic entering and leaving the network by strategically placing it inside.

The host intrusion detection system (HIDS) offers direct access to the company's internal network and the internet, functioning on all computers and devices linked to a network. The ability of HIDS to identify malicious traffic that a NIDS could have overlooked or suspicious network packets coming from inside the organization is one benefit it has over NIDS.

Signature-based intrusion detection system (SIDS) functions akin to antivirus software, monitoring every packet traversing the network and cross-referencing it with a database of attack signatures or recognized characteristics of potential threats. Constructing robust detection systems for the IoT necessitates extensive datasets for signature-based network IDS [5]. A network IDS architecture based on signatures has been introduced by Kasinathan *et al.* [6] and is specifically designed to identify denial-of-service (DoS) assaults in networks that use 6LoWPAN technology. Conversely, anomaly-based intrusion detection systems (AIDS) establish the parameters of network normalcy concerning ports, bandwidth, protocols, and other devices. To do this, network traffic is continuously monitored and contrasted with an established baseline. Anomaly-based detection techniques outperform signature-based techniques in terms of constraints, especially in the identification of new threats. To do this, they steer clear of specific fingerprints and traits and use a more comprehensive model to identify potential threats. Many NIDS used to secure IoT devices use anomaly-based techniques because of their lightweight nature.

Among other fields, computer vision, natural language processing, and bioinformatics use machine learning (ML) [7], [8] and deep learning (DL) [9], [10] techniques because of their exceptional analytical powers. These techniques are being included into an increasing number of edge/fog computing Internet of Things applications, as they show significant performance benefits over some traditional ML algorithms. IDS can improve network security by utilizing ML and DL to anticipate malicious activities and adjust to increasingly sophisticated attacks. Large amounts of data must be transmitted over the network for these applications, and it is interesting to observe that DL typically performs better than ML, especially when working with big datasets [11]. With minimal computer resources, deep learning can quickly analyze vast amounts of data and enable automatic security system alterations upon the discovery of malware or security breaches [12].

Enhancing intrusion detection systems (IDS) in the context of IoT requires careful consideration when choosing an appropriate deep learning technique [13], [14]. The best strategy can be found by evaluating different approaches to find the one that provides the maximum accuracy, then putting the chosen approach into practice. Using deep learning approaches, this research reduces the false alarm rate and improves detection accuracy, among other benefits. Improving IoT system security can guarantee a more robust IoT ecosystem and have far-reaching positive benefits on people's life, the economy, technology, and environment [15].

This research aims to perform a thorough analysis of the most advanced DL methods used in intrusion detection systems within the timeframe of 2020-2024. In addition to literature review and analysis, this paper develops an experiment aimed at exploring the potential of the most effective DL techniques in the field. Our study focuses on two most popular intrusion detection datasets: NSL-KDD and UNSW-NB15. We further improve our analysis by evaluating the models according to false alarm rate (FAR) and response time, going beyond the traditional comparison using the four widely used performance measures (accuracy, precision, recall, and F1-score). By addressing the significant issue of real-time processing in intrusion detection systems and false alarm rate analysis, this assessment extension seeks to deepen our understanding of the performance of DL models in this particular setting.

The rest of the paper is organized as follows: section 2, proposes a comprehensive analysis of various researches that have been developed to enhance the efficiency of IDS in the identification and mitigation of cyber risks. Variant factors such as datasets, methodologies, and prediction performances are discussed. Section 3 outlines the research methodology, encompassing details about the dataset, preprocessing steps, and the deep learning algorithms compared. It encompasses both binary-class and multi-class classification tasks, the evaluation metrics include accuracy, precision, recall, F1-score, Matthew’s correlation coefficient (MCC), execution time, and false alarm rate. Section 4 presents and analyzes the experimental results. It critically assesses how well the proposed models work, and Section 5 concludes the research and presents the next work.

2. STATE OF THE ARTS ANALYSIS

The literature has highlighted several approaches and algorithms for machine and deep learning-based intrusion detection. Therefore. This section delves into current methods and solutions grounded in deep learning approaches. These approaches are favored over traditional machine learning techniques owing to their outstanding performance, particularly when dealing with large datasets.

Utilizing the NSL-KDD dataset, a deep neural network (DNN) model with 200 hidden layers and a ReLU activation function was presented in [9] for intrusion detection. The entire dataset was preprocessed and normalized before the DNN was trained and tested on it. Metrics for accuracy and precision were used to assess the model's performance. By responding to dynamic threats, this DNN-based solution revealed an effective way to detect network anomalies and achieve up to 93% classification accuracy. An innovative IDS based on DNN was developed in response to the challenges posed by modern complex security-related networks and the proliferation of threats [10].

The overfitting problem is addressed by the suggested approach. The IDS efficiently keeps an eye on network traffic to spot both typical and unusual activity. Using the KDD99 dataset, experimental study showed an accuracy of up to 99.78%. A wireless intrusion detection system using a feed-forward deep neural network (FFDNN) and a wrapper-based feature extraction unit (WFEU) was suggested by Kasongo and Sun. [16]. The UNSW-NB15 and AWID datasets were used to examine the efficacy and efficiency of the WFEU-FFDNN model. The experimental findings on these different datasets showed that the accuracy for binary classification was 87.10% and 99.66%, and for multi-class classification it was 77.16% and 99.77%. In order to create an effective IDS, a deep neural network was utilized in [17] to identify and predict unanticipated cyberattacks in the context of the internet of medical things. To extract the high impact characteristics of the dataset, the proposed methodology combines classical principal component analysis (PCA) with the bio-inspired algorithm Grey-Wolf Optimizer. Hyperparameter selection techniques are used to preprocess, enhance, and fine-tune the network parameters. The suggested model has a smaller sample space than the classical DNN, which leads to faster training times. The hybrid -PCA-GWO performs better than the other two methods, as seen by its 99.9% accuracy, 95.4% sensitivity, and 100% specificity. Susilo *et al.* [18] go over a number of ML and DL techniques as well as common datasets for enhancing IoT security performance. Accuracy of the mitigation of attacks that happen on an IoT network could be improved using a deep learning model. Convolutional neural network (CNN) outperformed other superficial machine learning algorithms with an accuracy rate of 91.27%. M. Roopak *et al.* [19] designed an intrusion detection system by integrating the NSGA-II multi-objective optimization approach for data dimension reduction, specifically tailored for jumping genes. This system also incorporated a CNN with DL techniques, leveraging long short-term memory (LSTM) for attack identification. The experiment utilized the latest CISIDS2017 datasets on DDoS assaults, achieving an impressive accuracy of 99.03%. The authors of the study [20] used a four-layer DNN model to predict the test set and "normal" association rules to perform feature matching on the malicious traffic set in order to filter out the mistakenly classified normal traffic. This strategy aims to deliver an IDS with high accuracy and low false alarm rates; the detection method's accuracy using the NSL-KDD public dataset is 82.74%. A deep learning IDS that combines a deep neural network with a pretraining technique using a deep autoencoder (PTDAE) proposed by Unang *et al.* [21], they employed hyperparameter optimization and tested various models on NSL-KDD and CSE-CIC-ID2018 datasets. Among three feature extraction techniques (DAE, AE, SAE), DAE yielded the best results, with a recall rate and overall accuracy of 83.33% on the NSL-KDD dataset, the DAE+DNN model demonstrated impressive performance. A DL model comprising a specific feed-forward neural network was proposed by the authors in [22] as the basis for a network IDS design for the IoT. Using a dataset of actual network traffic, the efficacy of the binary and multi-class classification models has been assessed.

The results show how effective the recommended approach is. For multi-class classification, an approximate detection accuracy of 99.79% was achieved, and for binary classifier, 99.99%. Ullah and Mahmoud [23] employ a convolutional neural network to identify and categorize binary or multiclass. By employing this tactic, they generate four IoT datasets (IoT-DS-1, IoT-DS-2, BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, IoT-DS-2, and IoT-23) that are subsequently combined to increase the range of threat classifications. Through the utilization of 1D, 2D, and 3D convolutional neural network models, the authors are capable of effectively classifying an array of anomalies. The accuracy of the CNN1D model is 99.74%, the CNN2D model is 99.42%, and the CNN3D model is 99.03% across datasets, including BoT-IoT, MQTT-IoT-IDS2020, IoT-23, and IoT-DS-2. The application of deep learning and an identification model built on bidirectional LSTM is the main topic of the paper [24]. The system is tested on the KDDCUP-99 and UNSW-NB15 datasets. The model performed excellently in terms of accuracy, with 99% accuracy for both datasets. Employing a public dataset of MQTT assaults (MQTT-IoT-IDS2020), the authors of [25] demonstrated a DL based network IDS employing a convolutional and recurrent neural network combination (CNN-RNN-LSTM). The model's average accuracy in detecting MQTT assaults was 97.09%, with an F1-score of 98.33%. A strong framework for intrusion detection in IoT environment was created by the authors

in [26]. CNN, LSTM, and a hybrid CNN-LSTM model were applied in the suggested solution, which was created using the IoTID20 dataset assault, to classify intrusions. The proposed systems' accuracy, as determined by the experimental findings, was 98.2% for LSTM, 96.60% for CNN, and 98.80% for CNN-LSTM. The primary goal stated in reference [27] is to show the usage of a deep recurrent neural network (DRNN) in conjunction with decision trees, ridge classifiers, random forests, and k-nearest neighbors' algorithm (KNNs), which are examples of supervised machine learning models. Developing a robust intrusion detection system is the goal, in particular for the setting of the Internet of Medical Things (IoMT). Using NSL-KDD datasets, this intrusion detection system is engineered to efficiently detect and predict unknown cyberthreats. The study's results show an impressive accuracy rate of 96.08%.

Mahalakshmi *et al.* [28], an intrusion detection system has been crafted utilizing a convolutional neural network deep learning model, leveraging the UNSW-NB15 network intrusion public dataset. The outcome reveals a noteworthy accuracy of 93.5%, underscoring the robust efficacy of CNNs in the realm of intrusion detection. The research [29] presents a deep learning-based IDS designed for the IoT. It analyzes data from TCP/IP packets using hybrid rule-based feature selection. Utilizing NSL-KDD and UNSW-NB15, two well-known network datasets, the suggested approach is assessed. The NSL-KDD dataset yielded impressive findings, including a 1.0% false positive rate (FPR), 99.0% detection rate, and 99.0% accuracy. In the performance comparison, the UNSW-NB15 dataset shows similar results, with 98.9% of accuracy, 99.9% of detection rate, and 1.1% of FPR. The paper [30], emphasizes the security threats linked to IoT and the pivotal role of deep learning in detecting intrusions within IoT systems. It examines various deep learning-powered IoT intrusion detection systems. The results reveal that CNN achieved an 89% accuracy, while DNN attained 86% accuracy in binary classification. The approach outlined in [31], implements an IDS using Recursive Feature Elimination (RFE), DNN, and RNN models for classification. This approach achieves an accuracy rate of 94%, with DNN performing binary classification and RNN classifying different attack types. The efficacy of the system is confirmed using the NSL-KDD dataset, showcasing its suitability for offline IDS analysis. The authors in [32], presented CLSTMNet, a ground-breaking classification algorithm that was developed by fusing LSTM and CNN. They used the standard NSL-KDD datasets to develop and analyze their model, and they attained an outstanding accuracy of 99.28%. With the goal of efficiently finding unexpected attack patterns on networks.

A highly developed intrusion detection system is presented by Maithem *et al.* [33], this model conducts attack detection through binary and multiclass classifications by utilizing a deep neural network method. The system exhibits encouraging results, attaining remarkably elevated accuracy percentages of 99.98% in both binary and multiclass categorization. A CNN-based model for anomaly-based IDS was presented by Saba, Tanzila, et al in [34], the CNN-based model was employed to analyze IoT traffic with the aim of predicting potential intrusions and unusual traffic patterns, using the NID and BoT-IoT datasets, the model was trained and assessed, yielding accuracy rates of 99.51% and 95.55%, respectively. Vishwakarma and Kesswani [35] provided a real-time IDS based on deep neural networks that can detect malicious packets. Newly created benchmark NetFlow-based datasets (NF-UQ-NIDS datasets) were used to train the model, the accuracy of the suggested model was 93.02% for multiclass classification and 98.30% for binary classification. Sarhan *et al.* [36] investigate the effects of applying three feature extraction approaches, namely PCA, LDA and AE, on three deep learning models (DFF, CNN and RNN), as well as on three machine learning models (DT, LR and NB), applied to various datasets such as ToN-IoT, UNSW-NB15, CSE-CIC-IDS2018. Performance varies depending on the specific data and feature extraction techniques used. employing a recent IoT dataset (DS2OS), the authors in [37] investigated the impact of adversarial assaults on the deep learning and shallow machine learning models. The model can give detection accuracy above 99% against all forms of attacks, including adversarial attacks, according to simulation data.

Iftikhar, Saman, *et al.* [38], employs machine learning algorithms and a deep learning technique to intelligently identify anomalies or potentially harmful activities within IoT, by using the recent UNSW-NB15 dataset, the research accomplishes an accuracy of 93% in binary classification by employing LSTM. In order to improve attack detection accuracy, the study [39] attempts to develop a novel hybrid IDS model using DL models, notably CNN and LSTM, with the NSL-Botnet dataset, the suggested model achieves 99.4% accuracy in binary classification, and with UNSW-NB15, it obtains 93% accuracy. For other classification measures, it achieves 82% accuracy with UNSW-NB15 and 92% accuracy with NSL-Botnet. DL was used by Sharma et al. [40] to develop an anomaly-based IDS for IoT networks. To get rid of strongly correlated features, they used a deep neural network using filter-based feature selection. The model, fine-tuned with various parameters, achieved 84% accuracy on the UNSW-NB15 dataset, which includes four attack classes. To address class imbalance, a generative adversarial network (GAN) was employed, boosting accuracy to 91%. To differentiate and accurately identify network traffic data, ensuring equipment safety and the smooth operation of the industrial internet of things (IIoT), a network IDS classification model (NIDS-CNN-LSTM) is established in reference [41]. This model, based on DL, is specifically designed for the IIoT. Training of the model involves utilizing the classic KDD CUP99, NSL-KDD and UNSW-NB15 datasets. It's interesting

to note that the model uses the NSL-KDD dataset to achieve 99% accuracy for binary and multiclass classification. To ascertain whether network traffic indicated a hostile attack, six models were created in [42], CNN + RNN, CNN + LSTM, CNN, DNN, RNN, and LSTM, by employing the CSE-CIC-IDS2018 dataset and standard evaluation criteria, the models demonstrated classification accuracies of over 98% for both multi and binary data.

A proposed architecture for an IDS is designed in [43] and combines three different recurrent neural networks: LSTM, gated recurrent unit (GRU), and Simple RNN. To evaluate this kind of IDS model's efficacy, benchmarks from the UNSW-NB15 and NSL-KDD datasets are employed. Each dataset's feature space has been enhanced using an XGBoost-based method. The NSL-KDD dataset yielded a Total Accuracy Rate of 86.93% for XGBoost-LSTM, while the UNSW-NB15 dataset yielded a TAC of 78.40% for XGBoost-GRU. Three deep learning architecture models were offered by the research in [44]: CNN, a CNN + LSTM hybrid, and LSTM. In the UNSW-NB15 and X-IIoTID datasets, the hybrid CNN + LSTM model performed well, achieving multi-class classification accuracy of 92.9% and binary classification accuracy of 93.21%. The technique proposed in [45], such as RNN, LSTM-RNN, and DNN, was applied with the datasets KDD'99, NSL-KDD, and UNSW-NB15 for their evaluation. Remarkably, the RNN and DNN models posted higher performance for the KDD'99 and NSL-KDD datasets. However, these techniques could not provide significant results for the UNSW-NB15 dataset. The RNN and DNN techniques showed high accuracy based on the overall performance analysis. It could achieve a detection rate of 98% for both the KDD'99 and NSL-KDD datasets in the binary and multiclass classification. Morshedi *et al.* [46] propose an advanced intrusion detection method for IoT networks. Their model utilizes the CICIDS2017 dataset and integrates LSTM architecture with dense transition layers to effectively capture both temporal and spatial dependencies in network traffic. The model demonstrates exceptional performance, achieving an accuracy of 99.7% in detecting cyberattacks such as distributed denial of service (DDoS), port scans, and botnet activity. In the study [47], a hybrid DL method called AttackNet—a CNN-GRU model—is proposed for the purpose of detecting different types of botnet attacks in the context of the IoT. An analysis of AttackNet, our suggested model's scalability.

The security dataset "detection of IoT botnet attacks N_BaIoT" is used to train and test the model. With an accuracy of 95.75% and a validation loss of 0.0063 at a 0.001 learning rate, the model outperforms current DL techniques. To identify DDoS attacks, a unique IDS for smart agriculture was created in [48]. In order to discover important characteristics of DDoS attacks, the system preprocesses data using normalization and label encoding. It then uses a fused CNN and Bi-GRU model with an attention mechanism. The wild horse optimization (WHO) technique is used to further increase the model's classification accuracy. The IDS demonstrated great accuracy, on the ToN-IoT (99.71%) and APA-DDoS-attack (99.35%) datasets. Racherla *et al.* [49] introduces Deep-IDS, an effective IDS utilizing DL designed specifically for IoT networks. In order to identify various cyberattacks, a 64-unit LSTM network is utilized, which was educated on the CIC-IDS2017 dataset. Deep-IDS achieves a detection rate of 96.8% and an accuracy of 97.67% at a 70% DR-FAR threshold, along with precision, recall, and F1-score of 97.67%, 98.17%, and 97.91%. The system quickly and efficiently ensures the security of IoT nodes and networks by detecting and eliminating threats in just 1.49 seconds.

According to this state-of-the-art, research projects addressing security and privacy issues in IoT networks have primarily focused on developing IDS based on several deep learning frameworks. This related works investigation informs us that a number of public datasets, such as NSL-KDD, CICIDS2017, CSE-CIC-IDS2018, UNSW-NB15, BoT-IoT, and others, are employed to evaluate intrusion detection models' effectiveness.

The UNSW-NB15 and NSL-KDD datasets are broadly recognized as the datasets that are most frequently used in intrusion detection. Their popularity stems from several factors. Firstly, they are publicly available and widely adopted by the research community. Secondly, these datasets are frequently utilized because new intrusion detection algorithms often require benchmarking against established ones.

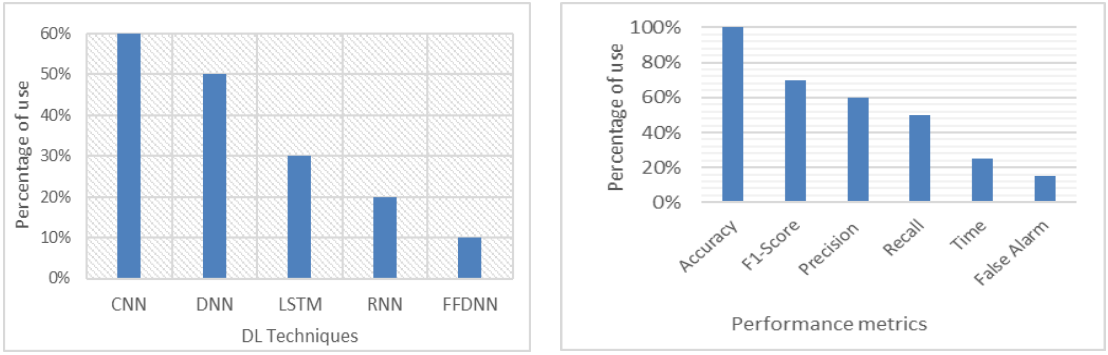
Figure 1 highlights the percentage distribution of deep learning models and Performance Metrics employed in intrusion detection. In Figure 1(a), CNN, RNN, DNN, and LSTM to be the most employed DL techniques within intrusion detection. This has shown how common and popular these DL methods are with researchers and practitioners in the intrusion detection domain.

The CNN technique demonstrated exceptional performance in [23], achieving an accuracy of 99.98%, precision of 99.96%, recall of 99.95%, and an F1-Score of 99% in binary classification. The CNN method achieved accuracy of 99.94%, 99.92%, and 99.92% for precision, recall, and F1-Score, respectively, for multiclass classification. The DNN technique yielded an accuracy of 99.9% in binary classification, according to the authors in [17].

Figure 1(b) shows the percentage utilization of each metric in the works evaluated, with accuracy emerging as the most common metric (100%) in this case. This observation suggests that many researchers

accord particular importance to this metric when evaluating the performance of their DL models, while highlighting the less frequent use of time (25%) and false alarm rate (15%). Indeed, it is crucial to note that depending solely on accuracy may not always offer a complete and accurate evaluation of model performance.

As a result, it is imperative to include extra evaluation measures. When evaluating intrusion detection algorithms, authors often overlook to take factors like false alarms and detection times into account. However, detection time is an important metric to consider in intrusion detection because a quick response to intrusions can significantly reduce potential damages. Similarly, managing false alarms is crucial to prevent operator fatigue and ensure that the alerts issued by the system are relevant.



(a) (b)

Figure 1. Percentage distribution of (a) deep learning models and (b) performance metrics

In our pursuit of enhancing the application of DL in internet of things intrusion detection systems, we compare the most commonly used deep learning techniques. Additionally, we will assess leading datasets used for training and testing IDS models in IoT environments. Standard performance metrics such as accuracy, precision, recall, F1-score and Matthews correlation coefficient (MCC) will be used, as well as metrics such as detection time and false alarm rate which are also very important in this context. The goal of this comparative experiment is to provide insight into the strengths and limitations of different DL techniques in IoT intrusion detection, as well as the impact of dataset selection on model performance. These findings will help advance IDS research and facilitate informed decision-making when deploying security solutions for IoT environments. We propose in the next sections a comparative experiment to further enhance the analysis in this research.

3. RESEARCH METHOD

Even though various models have been suggested for intrusion detection and show strong performance, it is still difficult to identify the most effective DL techniques for this purpose. This is because numerous studies must consider processing time and false alarm rate, which are crucial factors in intrusion detection. It is important to consider this during assessments since the continuous improvement of fraudsters' tactics and the integration of new data into systems increase the overall cost. In order to increase the efficacy and dependability of fraud detection systems, it's also critical to achieve a balance between precisely identifying fraudulent activity and limiting disruptions to legal transactions. This can be achieved by lowering the false alarm rate.

By adding the significant issue of real-time processing in intrusion detection systems and false alarm rate analysis, this assessment extension seeks to deepen our understanding of the performance of DL models in this particular setting. To address these challenges, we investigate the performance of different DL models for intrusion detection, using the NSL-KDD and UNSW-NB15 datasets as benchmarks. Figure 2 illustrates the experimental process, which includes data pre-processing, model training and testing, and evaluation metrics. Below is a more detailed explanation of the experimental setup, including the methods, tools, procedures, and data analysis.

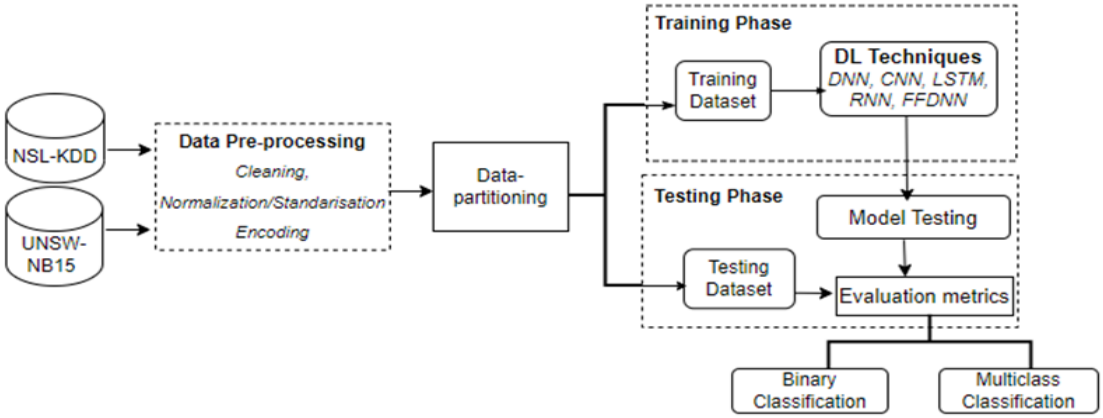


Figure 2. Methodology diagram

3.1. Datasets used

The NSL-KDD dataset [50]: the NSL-KDD dataset was chosen for its enhanced features over the older KDD99 dataset. It contains 41 attributes representing network activity, with over 125,000 entries and four main attack types (DoS, Probe, R2L, U2R). We selected this dataset due to its accessibility and its continued use in network-based IDS research. However, despite its improvements, the dataset still has some limitations (e.g., not fully representative of modern network traffic).

UNSW-NB15 [50], this dataset was selected for its larger and more diverse dataset (over 2 million records), representing a wider range of modern cyber-attacks. It provides a more realistic network traffic scenario than NSL-KDD and includes nine attack types, offering a broader evaluation of the models' capabilities. UNSW-NB15 has been extensively used for network behavior analysis.

3.2. Data preprocessing

The right data preprocessing steps play a vital role in building the effective intrusion detection system. Preprocessing ensures good data quality, thereby ensuring its interpretation and analysis by the deep learning models. It is a multi-step process involving data cleaning, normalization, encoding categorical features, and assignment of labels. These processes help in the transformation of raw datasets into structured formats for training and evaluation.

- Cleaning and normalization: we employed data cleaning techniques to eliminate noise and incomplete records. Normalization was applied to scale numerical attributes, while categorical features were processed through one-hot encoding. For binary classification, labels were given integer values, where 0 represented benign samples and 1 represented attack samples. In the case of multiclass classification, benign samples were assigned 0, while attacks were categorized into distinct classes ranging from 1 to 4 for NSL-KDD (DoS (1), probe (2), R2L (3) and U2R (4)), and 1 to 9 for UNSW-NB15 (generic (1), exploits (2), Fuzzers (3), DoS (4), reconnaissance (5), analysis (6), backdoor (7), shellcode (8), worms (9)).
- Data partitioning: after preprocessing, the datasets were split into two sets: 70% for training and 30% for testing. This split allows for a robust evaluation of model performance across both binary and multiclass classification scenarios.

3.3. Deep learning models

The most popular methods for intrusion detection through deep learning from state-of-the-art literature are RNNs, CNNs, DNNs, LSTMs, and FFDNNs. RNNs find favor in modeling temporal sequences and are thus applicable to intrusion detection, which operates on time-related data. CNNs are good at spatial feature extraction and hence are applicable to intrusion detection with structured data. DNNs are versatile and applied in different intrusion detection contexts. LSTMs are therefore important in applications where the understanding of context over a long period is required, due to their capability to handle long-term dependencies. As for FFDNNs, they are relatively straightforward and direct; the emphasis is on efficient forward information propagation for classification.

Various parameters are employed to assess the efficacy of DL models. Although most of these parameters share identical values between models, such as the Adam optimizer, the ReLU activation function, and the loss function, distinctions appear in some cases as explained in Tables 1 and 2.

Table 1. DL model parameters with NSL-KDD dataset

DL	Binary classification	Multiclass classification
RNN	Neuron= (64,2), Maxpooling2D (2,2), epochs=10 and batch size=500	Neuron= (64,5), MaxPooling1D(pool_size=2), epochs=10 and batch size=500
CNN	Neuron= (32,2), MaxPooling1D(pool_size=2), epochs=10 and batch size=500	Neuron=(124,5), MaxPooling1D(pool_size=2),epochs=10 and batch size=500
DNN	Neuron= (40,40,40,2), epochs=100 and batch size=500	Neuron= (50,50,5), epochs=100 and batch size=500
LSTM	Neuron= (64,2), epochs=5 and batch size=500	Neuron= (32,5), epochs=3 and batch size=500
FFDNN	Neuron= (64,64,2), epochs=100and batch size=500	Neuron= (100,100,100,5), epochs=50 and batch size=500

Table 2. DL model parameters with UNSW-NB15 dataset

DL	Binary classification	Multiclass classification
RNN	Neuron= (64,64,2), epochs=20 and batch size=64	Neuron= (100,100,10), epochs=5 and batch size=500
CNN	Neuron= (32,64,2), MaxPooling2D (2,2), epochs=10 and batch size=32	Neuron=(32,32,10),MaxPooling1D(pool_size=2),epochs=10 and batch size=500
DNN	Neuron= (100,200,100,200,2), epochs=30 and batch size=500	Neuron= (100,200,100,10), epochs=100 and batch size=500
LSTM	Neuron= (64,64,2), epochs=10 and batch size=500	Neuron= (32,32,10), epochs=30 and batch size=500
FFDNN	Neuron= (128,64,2), epochs=10 and batch size=32	Neuron= (164,128,64,10), Dropout Layer1=0.01, DropoutLayer2=0.01, DropoutLayer2=0.5, epochs=100 and batch size=1000

3.4. Training and testing process

The testing set (30%) was used to assess the models' performance after they had been trained using the training set (70% of the data). This data division is essential in ensuring that the models are not overfitting to the training data and are generalizing well to new samples. The training lasted for several epochs so that the models would have adequate opportunities to learn iteratively while being able to continuously refine their knowledge about patterns within the training data. The batch size was set in consideration of the characteristics of the data set and the particular deep learning model being used (see Tables 1 and 2).

3.5. Evaluation metrics

In this work, the accurate and misclassified outcomes predicted by the experimental model were assessed using seven criteria. Accuracy, is a statistic that assesses the overall accuracy of model predictions, by dividing the total number of examples in the dataset by the number of correctly categorized instances (1). The precision measure computes the percentage of accurately detected incursions, or true positive predictions, relative to the total number of anticipated positive cases (2). Recall measures the percentage of real attack samples that the model properly recognizes (3). By incorporating both precision and recall, the F1-score, being a harmonic measure of both metrics, provides a balanced and comprehensive evaluation of model performance (4). The Matthews correlation coefficient (MCC) provides a fair evaluation of the model's efficacy by accounting for the four outcomes of binary classification: true positives, true negatives, false positives, and false negatives (5). The fraction of negative cases that the model incorrectly classifies as positive is measured by the false alarm rate (FAR), often referred to as the false positive rate (FPR) (6).

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

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

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

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

$$MCC = \frac{\text{TN}\times\text{TP}-\text{FN}\times\text{FP}}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \quad (5)$$

$$FAR = \frac{\text{FP}}{\text{FP+TN}} \quad (6)$$

At the same time, response time is becoming an increasingly relevant metric, especially in real-time scenarios. Evaluating the time, it takes for a model to generate predictions can be just as important as raw accuracy, especially when quick decisions are needed. For an in-depth comparison of the performance of intrusion detection models, it is recommended to incorporate false positives, thereby highlighting the model's ability to minimize false alarms, as well as consider response time to evaluate the operational efficiency in real-time environments. This approach offers a more holistic and pragmatic view of the models' capabilities in real security contexts.

4. RESULTS AND DISCUSSION

For binary classes and multiclass scenarios, we performed two different comparisons. We assessed algorithm performances in each instance by utilizing particular measures like accuracy, recall, F1-score, MCC, false alarm and execution time, in order to ascertain the efficacy of every model's in various categorization scenarios.

4.1. Binary classes

In this experiment, we conducted a performance comparison of five DL algorithms (DNN, CNN, LSTM, RNN, FFDNN) for binary classification on the NSL-KDD and UNSW-NB15 datasets. The target variable had two classes: normal and attack.

The results in Table 3 indicate that all five deep learning algorithms achieved relatively high accuracy in classifying instances as normal or attack. The DNN algorithm attained the highest performance, achieving an accuracy of 99.36%, precision of 99.34% and better performance in terms of false alarm minimization (0.60%), and low execution time of 150 seconds, followed by FFDNN with 99.34% accuracy, RNN with 99.04%, CNN with 97.32% and LSTM with 90.86%.

In Table 4, All models perform relatively well, with DNN leading in accuracy with 93.96% with minimal running time, followed by CNN with 93.72% and a precision of 95.60% and the longest response time (609 seconds) which may be a critical factor in real-time applications, while LSTM is slightly behind at 92.86%. and RNN performs the best in terms of minimizing false alarms (6.77%). FFDNN attains a balanced recall (94.61%), F1 score (94.95%), good accuracy (93.58%) and precision (95.28%). The model sustains a decent response time of 203 seconds while maintaining a comparatively low false alarm rate of 8.24%. DNN is notable for its effectiveness in reaction time and classification accuracy.

Table 3. Binary classification results on the NSL-KDD dataset

DL	Accuracy	Precision	Recall	F1-score	MCC	FAR	Time (s)
RNN	0.9904	0.9876	0.9923	0.9899	0.9807	0.0095	773
CNN	0.9732	0.9716	0.9724	0.9720	0.9463	0.0247	75.92
DNN	**0.9936**	**0.9934**	**0.9932**	**0.9933**	**0.9872**	**0.0060**	**150**
LSTM	0.9086	0.9466	0.8575	0.8998	0.8196	0.0443	447
FFDNN	0.9934	0.9937	0.9926	0.9931	0.9869	0.0057	216

Table 4. Binary classification results on the UNSW-NB15 dataset

DL	Accuracy	Precision	Recall	F1-score	MCC	FAR	Time (s)
RNN	0.9329	0.9603	0.9334	0.9466	0.8571	0.0677	383.89
CNN	0.9372	0.9560	0.9450	0.9505	0.8649	0.076	609
DNN	**0.9396**	**0.9527**	**0.9525**	**0.9526**	**0.8694**	**0.083**	**42.19**
LSTM	0.9286	0.9487	0.9388	0.9437	0.8463	0.089	232.56
FFDNN	0.9358	0.9528	0.9461	0.9495	0.8615	0.0824	203

Learning curves offer a dynamic perspective that helps comprehend the path leading to these performance levels, whereas the final metrics may provide a static assessment of the model's performance. As shown in Figure 3, we examined loss and accuracy curves to evaluate the performance of the DNN model on both the NSL-KDD and UNSW-NB15 datasets in binary classification. In Figure 3(a), we observe the loss and accuracy curves for the DNN model applied to the NSL-KDD dataset, where the model converges quickly, with similar training and validation results. Notably, there is no significant change between the training and validation loss curves, which indicates effective learning. Figure 3(b) illustrates the DNN model's performance on the UNSW-NB15 dataset, it is clear that while the model does a good job learning the training set, it finds it difficult to sustain its performance on the validation set. The zigzag pattern in the

validation curve suggests that the problem could be caused by overfitting or by the intrinsic variability in the validation data.

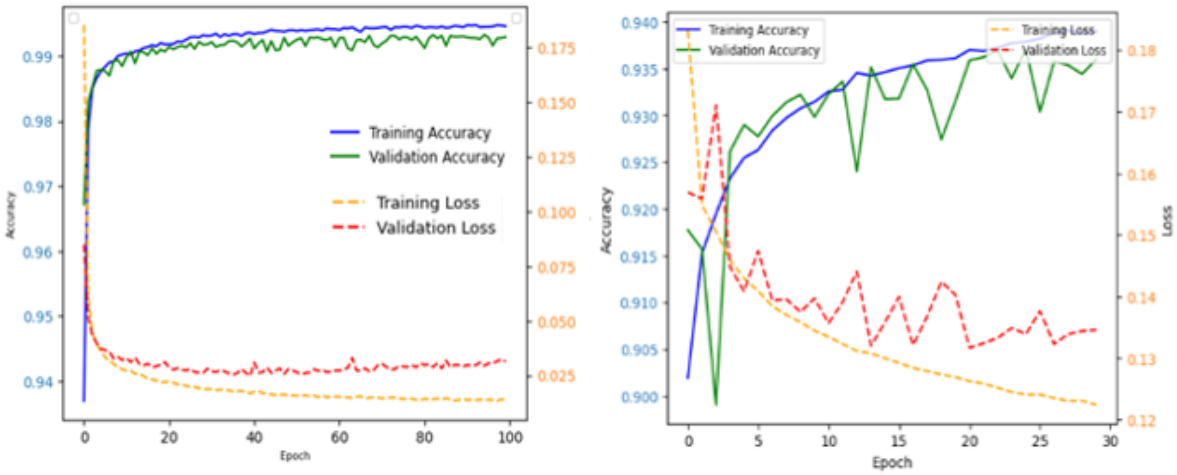


Figure 3. Loss and accuracy curves of (a) DNN model for NSL-KDD and (b) DNN model for UNSW-NB15 in binary classification

4.2. Multi-classes experiment

The results of the DL models in multi-class classification involving 10 classes (Normal, Generic, Exploits, Fuzzers, DoS, Reconnaissance, Analysis, Backdoor, Shellcode, Worms) for the UNSW-NB15 dataset and 5 classes (Normal, DOS, Probe, R2L, and U2R) for the NSL-KDD dataset are presented in detail in Tables 5 and 6 of the second experiment. A variety of metrics are used to assess each model, such as false alarm rate, execution time, accuracy, precision, recall, F1-score, and Matthews correlation coefficient (MCC).

Table 5. Multiclass classification results on the NSL-KDD dataset

DL	Accuracy	Precision	Recall	F1-score	MCC	FAR	Time (s)
RNN	0.9626	0.9626	0.9626	0.9626	0.9374	0.0084	264
CNN	0.9787	0.9787	0.9787	0.9787	0.9646	0.0052	269
DNN	0.9914	0.9914	0.9914	0.9914	0.9858	0.0021	143
LSTM	0.9250	0.9250	0.9250	0.9250	0.8742	0.0132	593
FFDNN	**0.9916**	**0.9916**	**0.9916**	**0.9916**	**0.9860**	**0.0020**	**87**

By examining the results shown in Table 5, we can determine how well each model performs in comparison to the others. To be more precise, the FFDNN model realized an F1-score of 0.9916 along with accuracy, precision, and recall. At 87 seconds of execution time and a low false alarm of 0.2%, the FFDNN model showcases a robust capability to accurately predict different classes.

Table 6. Multiclass classification results on the UNSW-NB15 dataset

DL	Accuracy	Precision	Recall	F1-score	MCC	FAR	Time (s)
RNN	0.8090	0.7942	0.8090	0.7754	0.6435	0.0245	790
CNN	0.7968	0.7772	0.7968	0.7703	0.7375	0.0255	290
DNN	0.8226	0.8179	0.8226	0.8093	0.7695	0.0219	286
LSTM	0.8031	0.7908	0.8031	0.7810	0.7464	0.0243	167
FFDNN	**0.8212**	**0.8189**	**0.8212**	**0.7942**	**0.770**	**0.0227**	**98.7**

In Table 6, FFDNN shows the highest accuracy at 82.12% and precision at 81.89% with a shorter execution time (98.7s), DNN demonstrate competitiveness in terms of both accuracy and various performance metrics., exhibiting high accuracy (82.26%) and relatively low false positive rates (2.19%). But it needs more execution time (286s). While CNN demonstrates an accuracy of 79.68%. There's a notable

disparity in execution times across models. RNN requires the longest time at 790 seconds, while LSTM and FFDNN have considerably shorter execution time at 167 and 98.7 seconds, respectively. The FAR values of DNN and FFDNN are the lowest, demonstrating their resilience against the misleading acceptance of illegal attempts. All models do a good job in this regard, although DNN and FFDNN outperform RNN, LSTM, and CNN in terms of their capacity to reduce false alarms. This implies that DNN and FFDNN may be more dependable in preventing false positive predictions, which is especially important in applications like anomaly detection systems or security where reducing false alarms is a top concern.

The Figure 4 shows the loss and accuracy curves of the FFDNN model for both the NSL-KDD and UNSW-NB15 datasets in multi-class classification, the Figure 4(a) show a steady decline with each epoch, and while there is a tiny gap, it indicates only slight differences in performance, suggesting efficient generalization to new, untested data without overfitting, it is clear that the model does a good job learning the training set, it finds it difficult to sustain its performance on the validation set. Figure 4(b) shows the performance on the UNSW-NB15 dataset, where a noticeable gap between training and validation loss suggests a slight overfitting tendency, likely due to variability in the validation data. This disparity is shown to be marginally larger when compared to the NSL-KDD dataset's application of the DNN and FFDNN models. Despite the discrepancy between the training and validation curves on UNSW-NB15 compared to NSL-KDD, the models show good overall performance on both datasets.

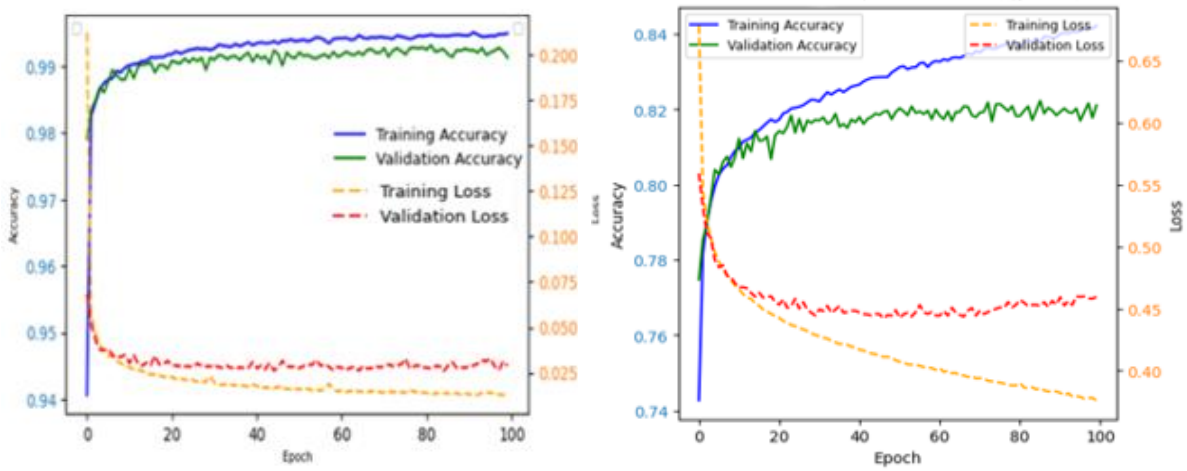


Figure 4. Loss and accuracy curves of FFDNN model for (a) NSL-KDD and (b) FFDNN model for UNSW-NB15 in multi-class classification

4.3. Result analysis and discussion

This research assesses different deep learning algorithms such as RNN, DNN, CNN, LSTM, and FFDNN in binary and multi-class classification scenarios with the NSL-KDD and UNSW-NB15 datasets. Apart from standard performance metrics like precision, recall, F1-score, and accuracy, the research also includes unique measurements such as the false alarm rate (FAR) and response time, tackling the issues linked to real-time processing in IDS. The main objective is to improve comprehension of DL model effectiveness in a real-life intrusion detection scenario while considering practical limitations.

Our study confirms that deep neural network (DNN) models are highly effective for intrusion detection. Specifically, DNNs demonstrated impressive accuracy in binary classification, with 99.36% on the NSL-KDD dataset and 93.96% on the UNSW-NB15 dataset, as well as a low-rate false alarms (0.60% and 8.3% respectively). They also displayed the quickest detecting time. In terms of accuracy for multiclass classification, FFDNN performed competitively in both datasets (99.16% and 82.12%, respectively). Moreover, the FFDNN was unique in that it had the shortest detection time. These findings demonstrate how well DNN models—especially FFDNN—perform in internet of things scenarios for intrusion detection. A comparison has been done for both classification types, as shown in Table 7.

Table 7. Performance comparison between the proposed techniques and State-of-the-Art methods on the NSL-KDD Dataset

	Acc. In Binary	Acc. In multi-class
Proposed DNN	99.36%	99.14%
Proposed FFDNN	99.34%	99.16%
DNN [20]	82.74%	77.03%

Our model achieves 93.96% accuracy in binary classification and 82.26% accuracy in multiclass classification with 10 classes on the UNSW-NB15 dataset, using DNN technique revealing that it still needs more improvement compared to [29]. Certainly, the second dataset (UNSW-NB15) presents different challenges compared to the first dataset (NSL-KDD), which might explain the need for further improvements despite surpassing most existing models such as [30], [40], [45].

Utilizing real datasets is essential for accurately depicting the intricacy and variety of real-world attacks in IoT environments. They enable the training of models that are not just stronger but also more indicative of the risks faced in real-life scenarios.

It is crucial to take into account factors like response time and false positives. Response time is crucial for real-time systems, where each and every second is critical. Reducing false positives is essential to prevent unnecessary alerts that may erode confidence in the detection system.

Ultimately, it is crucial to optimize energy use and running time for IoT devices, which frequently have limited resources. A successful detection system needs to find a middle ground between accuracy in detecting and practical factors such as energy efficiency and speed of operation. Blending these dimensions is essential in creating intrusion detection systems that are suitable for IoT settings.

5. CONCLUSION

This research explores intrusion detection systems, examining commonly used methods such as DNN, CNN, RNN, LSTM, and FFDNN on NSL-KDD and UNSW-NB15 datasets by introducing a wider array of performance indicators, surpassing traditional metrics like accuracy, precision, and recall. In particular, the inclusion of FAR and response time as key metrics is crucial for IoT environments, where both minimizing false alarms and ensuring rapid threat detection are essential. DNN is the best performer in the NSL-KDD dataset, with an amazing 99.36% accuracy in binary classification. Not only does DNN perform exceptionally well in terms of accuracy, but it also has a low false alarm rate—0.6%. FFDNN continues to demonstrate its superiority for multiclass classification in NSL-KDD, attaining an astounding 99.16% accuracy rate with very low false alarms (0.20%). This highlights the superiority of FFDNN in multiclass classification and the competence of DNN in binary classification on the NSL-KDD dataset. Contrastingly, in the UNSW-NB15 dataset, DNN demonstrates strength with a 93.96% accuracy in binary classification, and with an astoundingly low-rate false alarm of 2.19%. In multiclass classification, DNN performed well as well, with an accuracy of 82.26% and a low false alarm rate of 2.19%. These findings demonstrate DNN's efficacy in the UNSW-NB15 dataset, highlighting its accuracy and efficiency in lowering false alarms, especially in binary classification and multiclass scenarios. Our upcoming goal is to investigate models that are appropriate for edge networks due to the growing trend of edge computing and the need to enhance intrusion detection capabilities in distributed systems.

FUNDING INFORMATION

No funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Marwa Baich	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓
Nawal Sael		✓		✓		✓		✓	✓	✓	✓	✓		
Touria Hamim	✓	✓	✓	✓		✓				✓	✓		✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

No conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, M.B, upon reasonable request.

REFERENCES

[1] R. Dodda, V. Gaddam, J. R. Prasad and B. V. S. Rao., "The evolution of internet of things (IoT) and its impact on existing technology," *International Journal of Science Technology and Engineering*, vol. 2, pp. 96-103, 2016.

[2] J. Pacheco and S. Hariri, "IoT Security Framework for Smart Cyber Infrastructures," *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W)*, Augsburg, Germany, 2016, pp. 242-247, doi: 10.1109/FAS-W.2016.58.

[3] I. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," *2015 IEEE Symposium on Computers and Communication (ISCC)*, Larnaca, Cyprus, 2015, pp. 180-187, doi: 10.1109/ISCC.2015.7405513.

[4] E. Gyamfi and A. Jurcut, "Intrusion detection in internet of things systems: a review on design approaches leveraging multi-access edge computing, machine learning, and datasets," *Sensors*, vol. 22, no. 10, p. 3744, 2022, doi: 10.3390/s22103744.

[5] H. Zhengbing, L. Zhitang and W. Junqi, "A novel network intrusion detection system (NIDS) based on signatures search of data mining," *First International Workshop on Knowledge Discovery and Data Mining (WKDD 2008)*, Adelaide, SA, Australia, 2008, pp. 10-16, doi: 10.1109/WKDD.2008.48.

[6] P. Kasinathan, C. Pastrone, M. A. Spirito and M. Vinkovits, "Denial-of-service detection in 6LoWPAN based internet of things," *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Lyon, France, 2013, pp. 600-607, doi: 10.1109/WiMOB.2013.6673419.

[7] A. Shaver, Z. Liu, N. Thapa, K. Roy, B. Gokaraju and X. Yuan, "Anomaly based intrusion detection for iot with machine learning," *2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*, Washington DC, DC, USA, 2020, pp. 1-6, doi: 10.1109/AIPR50011.2020.9425199.

[8] S. Mittal, A. K. Mishra, V. Tripathi, P. Singh and P. Pandey, "A comparative analysis of supervised machine learning models for smart intrusion detection in IoT network," *2023 3rd Asian Conference on Innovation in Technology (ASIANCON)*, Ravet IN, India, 2023, pp. 1-6, doi: 10.1109/ASIANCON58793.2023.10270377.

[9] Liu, Zhiqiang *et al*., "Deep learning approach for IDS: using DNN for network anomaly detection." *Fourth International Congress on Information and Communication Technology: ICICT 2019, London, Volume 1*. Springer Singapore, 2020.

[10] S. Ahmad, F. Arif, Z. Zabeehullah and N. Iltaf, "Novel approach using deep learning for intrusion detection and classification of the network traffic," *2020 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA)*, Tunis, Tunisia, 2020, pp. 1-6, doi: 10.1109/CIVEMSA48639.2020.9132744.

[11] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: a deep learning–based intrusion detection framework for securing IoT," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, p. e3803, 2022, doi: 10.1002/ett.3803.

[12] X. Wang, Y. Zhao, and F. Pourpanah, "Recent advances in deep learning," *International Journal of Machine Learning and Cybernetics*, vol. 11, pp. 747-750, 2020, doi: 10.1007/s13042-020-01096-5.

[13] T. Khan, R. Sarkar, and A. F. Mollah, "Deep learning approaches to scene text detection: A comprehensive review," *Artificial Intelligence Review*, vol. 54, pp. 3239-3298, 2021, doi: 10.1007/s10462-020-09930-6.

[14] L. Aversano, M. L. Bernardi, M. Cimitile, and R. Pecori, "A systematic review on deep learning approaches for IoT security," *Computer Science Review*, vol. 40, p. 100389, 2021, doi: 10.1016/j.cosrev.2021.100389.

[15] A. M. Banaamah and I. Ahmad, "Intrusion detection in IoT using deep learning," *Sensors*, vol. 22, no. 21, p. 8417, 2022, doi: 10.3390/s22218417.

[16] S. M. Kasongo and Y. Sun, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system," *Computers & Security*, vol. 92, p. 101752, 2020, doi: 10.1016/j.cose.2020.101752.

[17] S. Priya R. M., *et al.*, "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Computer Communications*., vol. 160, pp. 139–149, 2020, doi: 10.1016/j.comcom.2020.05.048.

[18] B. Susilo and R. F. Sari, "Intrusion detection in IoT networks using deep learning algorithm," *Information*, vol. 11, no. 5, p. 279, 2020, doi: 10.3390/info11050279.

[19] M. Roopak, G. Y. Tian and J. Chambers, "An intrusion detection system against DDoS attacks in IoT networks," *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2020, pp. 0562-0567, doi: 10.1109/CCWC47524.2020.9031206.

[20] M. Gao *et al*., "Malicious network traffic detection based on deep neural networks and association analysis," *Sensors*, vol. 20, no. 5, p. 1452, 2020, doi: 10.3390/s20051452.

[21] Y. N. Kunang, S. Nurmaini, D. Stiawan, and B. Y. Suprapto, "Attack classification of an intrusion detection system using deep learning and hyperparameter optimization," *Journal of Information Security and Applications*, vol. 58, Mar. 2021, doi: 10.1016/j.jisa.2021.102804.

[22] M. Ge, N. F. Syed, X. Fu, Z. Baig, and A. Robles-Kelly, "Towards a deep learning-driven intrusion detection approach for Internet of Things," *Computer Networks*, vol. 186, pp. 1–15, Feb. 2021, doi: 10.1016/j.comnet.2020.107784.

[23] I. Ullah and Q. H. Mahmoud, "Design and development of a deep learning-based model for anomaly detection in IoT networks," *IEEE Access*, vol. 9, pp. 103906–103926, 2021, doi: 10.1109/ACCESS.2021.3094024.

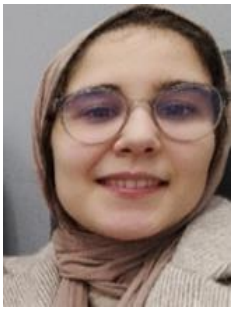
[24] T. S. Pooja and P. Shrinivasacharya, "Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 448–454, 2021, doi: 10.1016/j.gltp.2021.08.017.

[25] F. Mosaiyebzadeh, L. G. Araujo Rodriguez, D. Macêdo Batista and R. Hirata, "A network intrusion detection system using deep learning against MQTT attacks in IoT," *2021 IEEE Latin-American Conference on Communications (LATINCOM)*, Santo Domingo, Dominican Republic, 2021, pp. 1-6, doi: 10.1109/LATINCOM53176.2021.9647850.

[26] H. Alkahtani and T. H. H. Aldhyani, "Intrusion detection system to advance Internet of Things infrastructure-based deep learning algorithms," *Complexity*, vol. 2021, pp. 1–18, 2021, doi: 10.1155/2021/5579851.

[27] Y. K. Saheed and M. O. Arowolo, "Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms," *IEEE Access*, vol. 9, pp. 161546–161554, 2021, doi: 10.1109/ACCESS.2021.3128837.
[28] G. Mahalakshmi *et al.*, "Intrusion detection system using convolutional neural network on UNSW NB15 dataset," in *Advances in Parallel Computing Technologies and Applications*, *IOS Press*, 2021, pp. 1–8, doi: 10.3233/APC210116.
[29] J. B. Awotunde, C. Chakraborty, and A. E. Adeniyi, "Intrusion detection in industrial internet of things network-based on deep learning model with rule-based feature selection," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–17, 2021, doi: 10.1155/2021/7154587.
[30] J. Jose and D. V. Jose, "Performance analysis of deep learning algorithms for intrusion detection in IoT," *2021 International Conference on Communication, Control and Information Sciences (ICCISc)*, 2021, doi: 10.1109/ICCISc52257.2021.9484979.
[31] B. Mohammed and E. K. Gbashi, "Intrusion detection system for NSL-KDD dataset based on deep learning and recursive feature elimination," *Engineering and Technology Journal* vol. 39, no. 7, pp. 1069–1079, 2021.
[32] A. S. Ahmed and Z. Albayrak, "CLSTMNet: A deep learning model for intrusion detection," *Journal of Physics: Conference Series*, vol. 1973, no. 1, 2021, doi: 10.1088/1742-6596/1973/1/012244.
[33] M. Maithem and G. A. Al-Sultany, "Network intrusion detection system using deep neural networks," *Journal of Physics: Conference Series*, vol. 1804, no. 1, 2021, doi: 10.1088/1742-6596/1804/1/012138.
[34] T. Saba, A. Rehman, T. Sadad, H. Kolivand and S. Ali Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Computers and Electrical Engineering*, vol. 99, p. 107810, 2022, doi: 10.1016/j.compeleceng.2022.107810.
[35] M. Vishwakarma and N. Kesswani, "DIDS: A deep neural network based real-time intrusion detection system for IoT," *Decision Analytics Journal*, vol. 5, p. 100142, 2022, doi: 10.1016/j.dajour.2022.100142.
[36] M. Sarhan, S. Layeghy, N. Moustafa, M. Gallagher and Ma. Portmann, "Feature extraction for machine learning-based intrusion detection in IoT networks," *Digital Communications and Networks*, vol. 10, no. 1, pp. 205-216, 2024, doi: 10.1016/j.dcan.2022.08.012.
[37] Md. M. Rashid, J. Kamruzzaman, M. M. Hassan, T. Imam, S. Wibowo, S. Gordon and G. Fortino, "Adversarial training for deep learning-based cyberattack detection in IoT-based smart city applications," *Computers & Security*, vol. 120, p. 102783, 2022, doi: 10.1016/j.cose.2022.102783.
[38] S. Iftikhar, D. Khan, D. Al-Madani, K. M. Ali Alheeti and K. Fatima, "An intelligent detection of malicious intrusions in IoT based on machine learning and deep learning techniques," *Computer Science*, vol. 30, no. 3, p. 90, 2022, doi: 10.56415/csjm.v30.16.
[39] S. Jain, P. M. Pawar, and R. Muthalagu, "Hybrid intelligent intrusion detection system for Internet of Things," *Telematics and Informatics Reports*, vol. 8, 2022, doi: 10.1016/j.teler.2022.100030.
[40] B. Sharma, L. Sharma, C. Lal and S. Roy, "Anomaly based network intrusion detection for IoT attacks using deep learning technique," *Computers and Electrical Engineering*, vol. 107, p. 108626, 2023, doi: 10.1016/j.compeleceng.2023.108626.
[41] J. Du, K. Yang, Y. Hu and L. Jiang, "NIDS-CNNLSTM: network intrusion detection classification model based on deep learning," in *IEEE Access*, vol. 11, pp. 24808-24821, 2023, doi: 10.1109/ACCESS.2023.3254915.
[42] Y.-C. Wang, Y.-C. Houng, H.-X. Chen, and S.-M. Tseng, "Network anomaly intrusion detection based on deep learning approach," *Sensors*, vol. 23, no. 4, p. 2171, 2023, doi: 10.3390/s23042171.
[43] S. M. Kasongo, "A deep learning technique for intrusion detection system using a recurrent neural networks based framework," *Computer Communications*, vol. 199, pp. 113–125, 2023, doi: 10.1016/j.comcom.2022.12.010.
[44] H. C. Altunay and Z. Albayrak, "A hybrid CNN+ LSTM-based intrusion detection system for industrial IoT networks," *Engineering Science and Technology, an International Journal*, vol. 38, p. 101322, 2023, doi: 10.1016/j.jestch.2022.101322.
[45] A. K. Silivery, R. M. Rao Kovvur, R. Solleti, LK. Suresh Kumar and B. Madhu, "A model for multi-attack classification to improve intrusion detection performance using deep learning approaches," *Measurement: Sensors*, vol. 100924, 2023, doi: 10.1016/j.measen.2023.100924.
[46] R. Morshedi, S. M. Matinkhah, and M. T. Sadeghi, "Intrusion detection for IoT network security with deep learning," *Journal of AI and Data Mining*, vol. 12, no. 1, pp. 37–55, 2024, doi: 10.22044/jadm.2023.13539.2471.
[47] H. Nandanwar and R. Katarya, "Deep learning enabled intrusion detection system for industrial IoT environment," *Expert Systems with Applications*, vol. 249, p. 123808, 2024, doi: 10.1016/j.eswa.2024.123808.
[48] K. Kethineni and G. Pradeepini, "Intrusion detection in Internet of Things-based smart farming using hybrid deep learning framework," *Cluster Computing*, vol. 27, no. 2, pp. 1719–1732, 2024, doi: 10.21203/rs.3.rs-2498495/v1.
[49] S. Racherla, P. Sripathi, N. Faruqui, M. Alamgir Kabir, M. Whaiduzzaman and S. Aziz Shah, "Deep-IDS: A real-time intrusion detector for IoT nodes using deep learning," in *IEEE Access*, vol. 12, pp. 63584-63597, 2024, doi: 10.1109/ACCESS.2024.3396461.
[50] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," *2015 Military Communications and Information Systems Conference (MilCIS)*, Canberra, ACT, Australia, 2015, pp. 1-6, doi: 10.1109/MilCIS.2015.7348942.

BIOGRAPHIES OF AUTHORS



Marwa Baich received the engineer degree in information science and engineering from Faculty of Sciences Ben M'Sick, Hassan II University of Casablanca, Morocco, in 2017. Currently she is preparing her Ph.D. in Computer Science. Her research areas are artificial intelligence, deep learning, machine learning, and Internet of Things. She can be contacted at email: baich.marwaa@gmail.com.

Nawal Sael received the engineering degree in software engineering from ENSIAS, Morocco, in 2002. She has been a Teacher-Researcher, since 2012, an Authorized Professor, since 2014, and a professor of higher education with the Department of Mathematics and Computer Science, Faculty of Sciences Ben M'Sick, Hassan II University of Casablanca, Casablanca, since 2020. Her research interests include data mining, educational data mining, machine learning, deep learning, and the Internet of Things. She can be contacted at email: saelnawal@hotmail.com.

Touria Hamim earned her Bachelor's degree in Engineering from the National School of Applied Sciences of El-Jadida in 2017. Following her passion for computer sciences, Touria pursued a Ph.D. in Computer Sciences at Hassan II University, Casablanca, Faculty of Sciences Ben M'sik, which she successfully completed in 2021. Currently, Touria holds a key position as a responsible data scientist in a prominent telecommunications company, where she applies her expertise in machine learning, big data, and other advanced data science techniques to solve industry-specific challenges. She can be contacted at email: hamimxtouria@gmail.com.