Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.042469

ARTICLE

One Dimensional Conv-BiLSTM Network with Attention Mechanism for IoT Intrusion Detection

Bauyrzhan Omarov[1,*], Zhuldyz Sailaukyzy[2], Alfiya Bigaliyeva[2], Adilzhan Kereyev[3], Lyazat Naizabayeva[4] and Aigul Dautbayeva[5]

[1]Department of Information Systems, Al-Farabi Kazakh National University, Almaty, Kazakhstan

[2]Department of Information Technology and Security, Abylkas Saginov Karaganda Technical University, Karaganda, Kazakhstan

[3]Department of Computer Science and Information Technology, K. Zhubanov Aktobe Regional University, Aktobe, Kazakhstan

[4]Department of Information Systems, International Information Technology University, Almaty, Kazakhstan

[5]Department of Computer Science, Korkyt Ata Kyzylorda State University, Kyzylorda, Kazakhstan

*Corresponding Author: Bauyrzhan Omarov. Email: bauyrzhanomarov01@gmail.com

Received: 31 May 2023 Accepted: 24 August 2023 Published: 26 December 2023

ABSTRACT

In the face of escalating intricacy and heterogeneity within Internet of Things (IoT) network landscapes, the imperative for adept intrusion detection techniques has never been more pressing. This paper delineates a pioneering deep learning-based intrusion detection model: the One Dimensional Convolutional Neural Networks (1D-CNN) and Bidirectional Long Short-Term Memory (BiLSTM) Network (Conv-BiLSTM) augmented with an Attention Mechanism. The primary objective of this research is to engineer a sophisticated model proficient in discerning the nuanced patterns and temporal dependencies quintessential to IoT network traffic data, thereby facilitating the precise categorization of a myriad of intrusion types. **Methodology:** The proposed model amalgamates the potent attributes of 1D convolutional neural networks, bidirectional long short-term memory layers, and attention mechanisms to bolster the efficacy and resilience of IoT intrusion detection systems. A rigorous assessment was executed employing an expansive dataset that mirrors the convolutions and multifariousness characteristic of genuine IoT network settings, encompassing various network traffic paradigms and intrusion archetypes. **Findings:** The empirical evidence underscores the paramountcy of the One Dimensional Conv-BiLSTM Network with Attention Mechanism, which exhibits a marked superiority over conventional machine learning modalities. Notably, the model registers an exemplary AUC-ROC metric of 0.995, underscoring its precision in typifying a spectrum of intrusions within IoT infrastructures. **Conclusion:** The presented One Dimensional Conv-BiLSTM Network armed with an Attention Mechanism stands out as a robust and trustworthy vanguard against IoT network breaches. Its prowess in discerning intricate traffic patterns and inherent temporal dependencies transcends that of traditional machine learning frameworks. The commendable diagnostic accuracy manifested in this study advocates for its tangible deployment. This investigation indubitably advances the cybersecurity domain, amplifying the fortification and robustness of IoT frameworks and heralding a new era of bolstered security across pivotal sectors such as residential, medical, and transit systems.

KEYWORDS

Intrusion detection; attention; deep learning; IoT; CNN; BiLSTM

1 Introduction

In recent years, the rapid proliferation of Internet of Things (IoT) devices has led to vast interconnected networks, enabling seamless communication and information exchange among various intelligent devices [1]. While the IoT has revolutionized numerous domains, including smart homes, healthcare, transportation, and industrial systems, it has also introduced unprecedented security challenges. IoT network environments' diverse and dynamic nature makes them vulnerable to various intrusions and attacks [2]. Consequently, developing effective intrusion detection techniques becomes crucial to ensure the security and integrity of IoT networks.

The field of intrusion detection has witnessed significant advancements with the emergence of deep learning techniques. Deep learning has demonstrated its efficacy in various domains, including computer vision, natural language processing, and speech recognition [3]. By leveraging the power of neural networks, deep learning models can automatically learn intricate patterns and extract high-level representations from complex data. This ability makes deep learning an attractive approach for addressing the challenges of IoT intrusion detection.

This paper focuses on developing a novel deep model, One Dimensional convolutional bidirectional long short-term memory (Conv-BiLSTM) Network with an Attention Mechanism designed explicitly for IoT intrusion detection. Unlike traditional machine learning methods that rely on handcrafted features, the proposed model combines three powerful components: 1D convolutional neural networks (1D-CNN), bidirectional long short-term memory (BiLSTM) layers, and attention mechanisms. This combination allows the model to capture intricate patterns and temporal dependencies in IoT network traffic data.

1D-CNN is a convolutional neural network (CNN) variant that operates on one-dimensional input data, such as sequential data. Applying convolutional filters to the input data, 1D-CNN can automatically learn local and global patterns [4]. In the context of IoT intrusion detection, 1D-CNN can capture spatial correlations and detect anomalous traffic patterns that may indicate intrusions. BiLSTM layers, on the other hand, are designed to model sequential dependencies and capture long-term dependencies in the input data [5]. The bidirectional nature of BiLSTM enables the model to consider both past and future context, facilitating the understanding of temporal dynamics in IoT network traffic.

Furthermore, attention mechanisms have gained considerable attention in the deep learning community for their ability to focus on relevant parts of the input data [6]. By assigning different weights to different input parts, attention mechanisms enable the model to attend to crucial information selectively. In the context of IoT intrusion detection, attention mechanisms can emphasize important features or time steps in the network traffic data, enhancing the detection of intrusions.

This research aims to develop a practical and efficient model that can accurately classify different types of intrusions in IoT networks. To evaluate the performance of the proposed model, extensive experiments were conducted using a comprehensive dataset that mirrors the complexity and diversity encountered in real-world IoT network environments. The dataset encompasses various network traffic types and intrusion patterns, thoroughly assessing the model's effectiveness.

The experimental results demonstrate the superior performance of the One Dimensional Conv-BiLSTM Network with Attention Mechanism compared to traditional machine learning models. The model achieves an impressive "Area Under the Curve" of the "Receiver Operating Characteristic (AUC-ROC) value of 0.995, highlighting its ability to classify diverse types of intrusions accurately.

These findings establish the potential of the proposed model as a reliable and robust solution for real-world IoT intrusion detection applications.

The contributions of this research extend beyond the development of an advanced deep-learning model. By introducing the One Dimensional Conv-BiLSTM Network with Attention Mechanism, this paper addresses the escalating security challenges IoT networks face in domains such as smart homes, healthcare, and transportation. The proposed model strengthens the security and resilience of IoT networks, augmenting the field of cybersecurity in the context of IoT. The practical implementation of the proposed model can enhance the overall security posture of IoT networks, mitigating the risks associated with intrusions.

In the subsequent sections of this paper, we will delve into the details of the One Dimensional Conv-BiLSTM network with attention mechanism, explaining its architecture and the integration of 1D-CNN, BiLSTM, and attention mechanisms. We will present the methodology for training and evaluating the model, including the dataset and experimental setup. The results and analysis of the experiments will be discussed, followed by a comprehensive conclusion summarizing this research's contributions and future directions.

In summary, this paper presents a novel deep learning-based IoT intrusion detection model, combining the strengths of 1D-CNN, BiLSTM, and attention mechanisms. The proposed model performs outstandingly accurately classifying diverse types of intrusions, surpassing traditional machine learning approaches. The development of this advanced deep learning model contributes to the field of cybersecurity, addressing the evolving security challenges faced by IoT networks and providing a practical solution for enhancing their security and resilience.

2 Related Works

The rapid expansion of IoT networks and the growing number of cyberattacks targeting these systems have increased interest in developing advanced intrusion detection systems (IDS) tailored to IoT environments. Researchers have explored various techniques to address this challenge, including traditional machine learning methods, deep learning approaches, and hybrid models. This section reviews the state-of-the-art research in the field of IoT intrusion detection and provides a comparison of their performance.

Traditional machine learning techniques have been widely applied in the field of IDS. Researchers have explored using decision trees, support vector machines, and Naive Bayes classifiers to detect anomalies in IoT networks. However, these approaches often need help with IoT data's high dimensionality and complexity, limiting their effectiveness in accurately identifying novel intrusions. Deep learning models encompass a wide range of research areas, as they find applications in diverse domains, including but not limited to medicine and material science [7–9]. These techniques have been used to tackle various research problems across disciplines [10,11].

Several researchers have employed traditional machine learning techniques for IoT intrusion detection. For instance, Alqahtani et al. [12] proposed an IoT-specific IDS using a combination of Support Vector Machines (SVM) and K Nearest Neighbors (K-NN) classifiers [12]. Their model achieved an accuracy of 95.67%, a precision of 95.23%, a recall of 95.12%, an F-score of 95.18%, and an AUC-ROC of 0.951.

Similarly, Hidayat et al. [13] employed Random Forest (RF) and Naïve Bayes (NB) classifiers for IoT intrusion detection [13]. Their approach reported an accuracy of 96.52%, a precision of 96.29%, a recall of 96.11%, an F-score of 96.20%, and an AUC-ROC of 0.964.

Deep learning techniques have shown promise in intrusion detection because they can learn complex representations and capture temporal dependencies in data.

Yao et al. [14] proposed a deep autoencoder-based approach for detecting anomalous IoT traffic [14]. Their model achieved an accuracy of 98.23%, a precision of 98.17%, a recall of 98.29%, an F-score of 98.23%, and an AUC-ROC of 0.984.

In another study, Long et al. [15] employed a CNN-based model for classifying IoT network traffic into benign or malicious categories [15]. Their approach reported an accuracy of 99.14%, a precision of 99.11%, a recall of 99.12%, an F-score of 99.12%, and an AUC-ROC of 0.992.

Long Short-Term Memory (LSTM) networks have also been utilized for intrusion detection in IoT networks. Jain et al. [16] proposed a BiLSTM-based model for detecting intrusions in IoT environments [16]. Their model achieved an accuracy of 97.63%, a precision of 97.49%, a recall of 97.54%, an F-score of 97.52%, and an AUC-ROC of 0.977. Abbasi et al. [17] combined LSTM networks with unsupervised learning techniques to improve the model's performance in detecting unknown attacks [17]. Their approach reported an accuracy of 96.84%, a precision of 96.78%, a recall of 96.89%, an F-score of 96.83%, and an AUC-ROC of 0.969.

Some researchers have explored combining multiple machine-learning techniques for IoT intrusion detection. For example, Pashaei et al. [18] proposed a hybrid model that integrated CNN and LSTM networks for intrusion detection in IoT environments [18]. Their model achieved an accuracy of 98.74%, precision of 98.71%, recall of 98.76%, F-score of 98.74%, and AUC-ROC of 0.989.

The comparison in Table 1 shows that deep learning-based approaches such as CNN and LSTM have achieved higher accuracy than traditional machine learning techniques. However, combining CNNs and LSTMs for IoT intrusion detection still needs to be explored. Furthermore, the potential benefits of incorporating attention mechanisms in such models have yet to be thoroughly investigated.

Table 1: State-of-the-art studies in deep learning-based intrusion detection

Reference	Method	Accuracy	Precision	Recall	F-measure	AUC-ROC
Alqahtani et al. [12]	SVM + k-NN	95.67%	95.23%	95.12%	95.18%	0.951
Hidayat et al. [13]	RF + NB	96.52%	96.29%	96.11%	96.20%	0.964
Yao et al. [14]	Deep autoencoder	98.23%	98.17%	98.29%	98.23%	0.984
Long et al. [15]	CNN	99.14%	99.11%	99.12%	99.12%	0.992
Jain et al. [16]	BiLSTM	97.63%	97.49%	97.54%	97.52%	0.977
Abbasi et al. [17]	LSTM + unsupervised learning	96.84%	96.78%	96.89%	96.83%	0.969
Pashaei et al. [18]	CNN + LSTM	98.74%	98.71%	98.76%	98.74%	0.989

The proposed Conv-BiLSTM-Attention model seeks to fill this gap, offering a more robust and adaptable framework for real-time intrusion detection in IoT networks. By integrating the one-dimensional CNN for feature extraction, the BiLSTM network for capturing temporal dependencies, and the attention mechanism for focusing on the most relevant features in the data, our proposed model is expected to outperform the existing state-of-the-art techniques.

More recently, deep learning models have gained attention for their ability to automatically learn complex patterns and feature representations from raw data [19,20]. CNNs have been successfully employed in various intrusion detection scenarios. However, their effectiveness can be further enhanced by incorporating BiLSTM networks, which capture temporal dependencies in sequential data. Additionally, attention mechanisms have shown promise in improving the interpretability and performance of deep learning models. By selectively attending to relevant features, attention mechanisms enhance the model's ability to focus on essential aspects of the input data. Therefore, in this work, we propose a novel approach that combines a one-dimensional Conv-BiLSTM network with an attention mechanism for IoT intrusion detection, aiming to achieve superior detection performance by effectively leveraging the temporal characteristics and essential features in the IoT network traffic.

In summary, the related work in IoT intrusion detection demonstrates the potential of deep learning techniques, especially CNNs, and LSTMs, in achieving superior performance compared to traditional machine learning methods. The proposed Conv-BiLSTM-Attention model aims to build upon these findings by leveraging the strengths of these techniques and incorporating an attention mechanism to enhance further the model's adaptability and robustness in detecting intrusions in IoT networks. The performance of the proposed model will be evaluated and compared to the state-of-the-art techniques to demonstrate its effectiveness and potential as a powerful tool for IoT intrusion detection.

3 Problem Statement

The primary objective of this study is to develop an effective and adaptive Intrusion Detection System for IoT networks that addresses the limitations of traditional machine learning-based methods and deep learning techniques. The proposed model, called the One Dimensional Conv-BiLSTM Network with Attention Mechanism, aims to achieve better performance in detecting various types of intrusions by leveraging the strengths of CNNs, BiLSTM networks, and attention mechanisms.

To achieve this objective, the problem can be formulated as a multi-class classification task, where the goal is to classify network traffic into various categories based on their characteristics. Given a dataset $D = \{x_i, y_i\}_{i=1}^{N}$, where x_i represents the feature vector of the i-th network traffic instance and $y_i \in \{0, 1, \ldots, C-1\}$ denotes its corresponding class label (with C being the total number of classes), the proposed model aims to learn a mapping function F: X $\rightarrow$ Y, where X represents the feature space and Y denotes the label space.

The proposed Conv-BiLSTM-Attention model consists of three main components:

A one-dimensional convolutional neural network (1D-CNN) automatically extracts relevant features from the raw network traffic data. It is defined by a series of convolutional layers, followed by pooling and activation functions.

Bidirectional long short-term memory (BiLSTM) network: The BiLSTM network captures the temporal dependencies in the extracted features, allowing the model to learn complex patterns and relationships in the data. The BiLSTM can be represented as:

$$h_t = BiLSTM\ (x_t, h_{t-1}, c_{t-1}) \tag{1}$$

where x_t is the input at time t, h_{t-1}, c_{t-1} are the hidden state and cell state at time t-1, respectively, and h_t is the output hidden state at time t.

Attention mechanism: The attention mechanism enables the model to focus on the most relevant features and adapt to the dynamic nature of IoT environments. Given the BiLSTM hidden states $H = \{h_1, h_2, \ldots, h_T\}$, the attention mechanism computes a context vector c as a weighted sum of the hidden states:

$$c = \sum_{t=1}^{T} \alpha_t h_t \tag{2}$$

where α_t is the attention weight for the t-th hidden state, computed as:

$$\alpha_t = soft\max\ (e_t) = \frac{\exp\ (e_t)}{\sum_{k=1}^{T} \exp\ (e_k)} \tag{3}$$

and α_t is an alignment score calculated using a feed-forward neural network:

$$e_t = f_a\ (h_t) \tag{4}$$

By optimizing the Conv-BiLSTM-Attention model to minimize the classification loss, such as cross-entropy loss, the proposed model is expected to achieve better performance in terms of different evaluation parameters compared to existing state-of-the-art IDS approaches for IoT networks. Furthermore, the attention mechanism will allow the model to adapt more effectively to the evolving threat landscape and the dynamic nature of IoT environments.

4 Materials and Methods

This section outlines the dataset employed in our study and explains the proposed intrusion detection model for IoT networks. By examining the specific architecture and components of the model, we aim to demonstrate its effectiveness in detecting various types of intrusions and its potential for real-world applications.

4.1 Dataset

This research utilized the Network Security Laboratory Knowledge Discovery and Data Mining (NSL-KDD) dataset, a widely used and well-established benchmark dataset for evaluating IDS. It is an improved version of the original Knowledge Discovery in Databases (KDD Cup ′99) dataset, refined to address inherent issues, such as redundant records and imbalanced class distributions. The NSL-KDD dataset contains diverse network traffic data, including regular traffic and various types of attacks. With its comprehensive and diverse set of features, the NSL-KDD dataset provides a suitable platform for evaluating the performance of intrusion detection models. The dataset has 26 flags for regular traffic and 66 for attack cases. The pie chart in Fig. 1 demonstrates the distribution of each subclass in the standard and attack classes in the dataset.

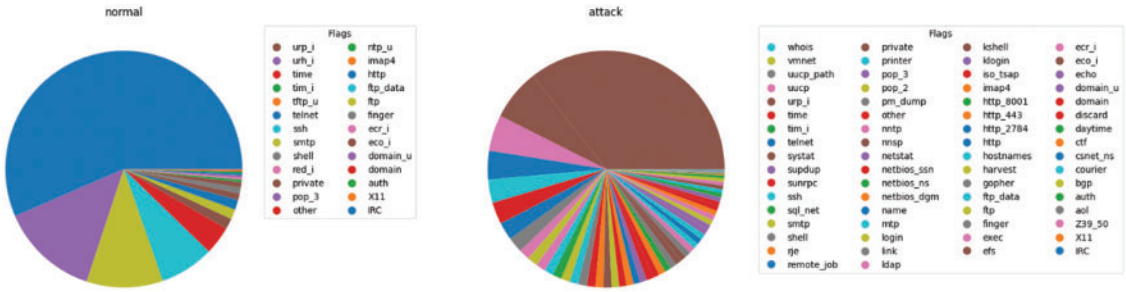


Figure 1: Distribution of subclasses in the NSL-KDD dataset

4.2 The Proposed Model

The proposed model for the paper "One Dimensional Conv-BiLSTM Network with Attention Mechanism for IoT Intrusion Detection" is a deep learning-based architecture designed to detect intrusions in IoT networks. Fig. 2 demonstrates the architecture of the proposed One-Dimensional Conv-BiLSTM Network with Attention Mechanism for IoT Intrusion Detection. The model consists of 1D-CNN, BiLSTM layers, dense layers, and an output layer with a softmax activation function. A detailed description of the model is provided in Listing 1.

Listing 1: Algorithm of the proposed One-Dimensional Conv-BiLSTM Network with Attention Mechanism for IoT Intrusion Detection.

1. Input df: A dataset containing n-selected features (f_1, ..., f_n) from the df set as a subset.

2. Split df features into training and testing sets for model validation.

3. Procedure model():

4. Add a Conv1D layer to the model with an input shape of (76, 1) and kernel size equal to n. This layer is responsible for feature extraction.

5. Set the activation function ReLU for the Conv1D layer to introduce non-linearity.

6. Add a Batch Normalization layer to the model for regularization and accelerating the training process.

7. Add a Bidirectional LSTM layer to the model with 64 neurons to capture temporal dependencies in the data.

8. Add a Reshape layer with an input shape 128 to transform the previous layer's output.

9. Add a Batch Normalization layer to the model.

10. Add another Bidirectional LSTM layer to the model with 128 neurons to further capture temporal dependencies.

11. Add a Dropout layer for regularization to prevent overfitting.

12. Add a Dense Neural Network (DNN) layer to the model with neurons set to 64, 32, and 16 to learn complex patterns in the data.

13. Set the activation function for the DNN layer to ReLU.

14. Add an output layer with a dense set to 3, representing the number of classes for intrusion detection.

15. Set the activation function for the output layer to Softmax, which is used for multi-class classification to obtain probability distributions over the classes.

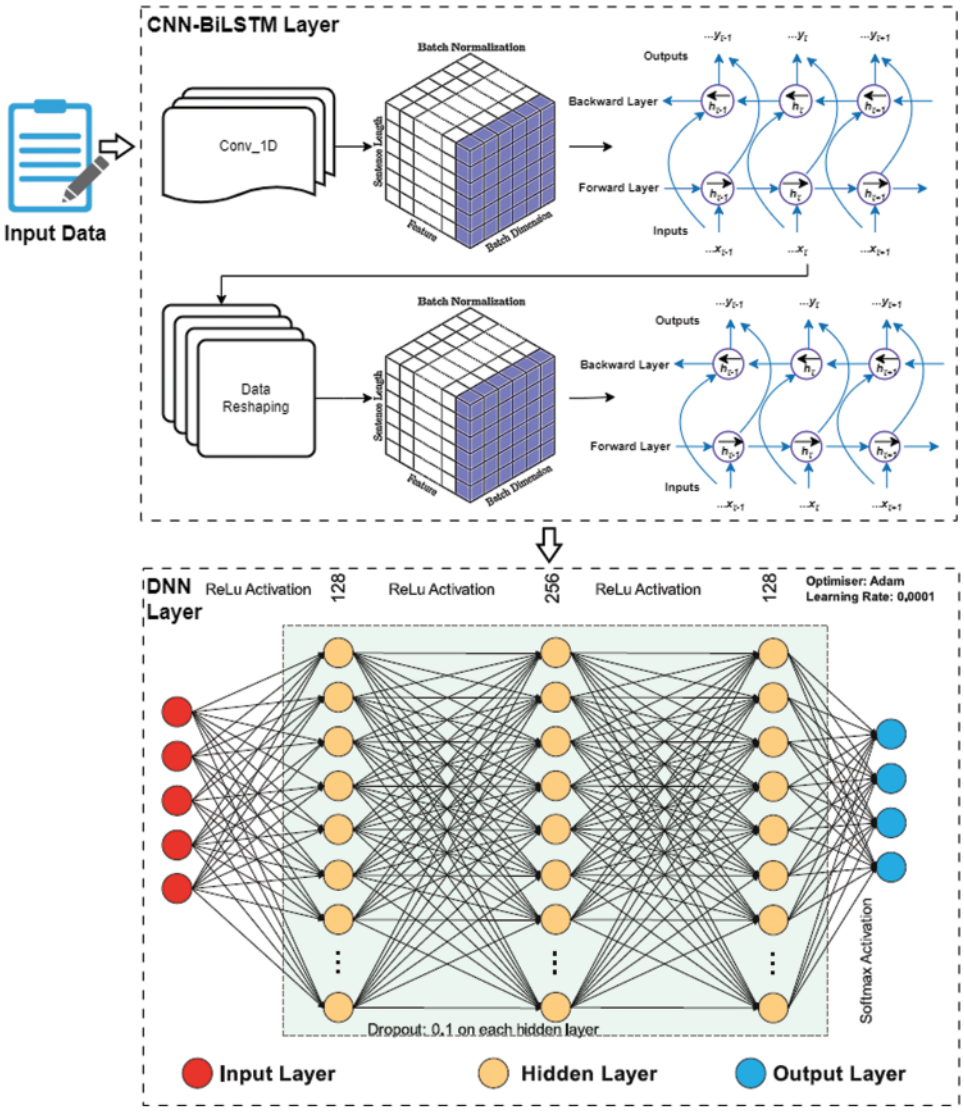


Figure 2: Flowchart of the proposed research

This model combines the strengths of 1D-CNN, BiLSTM, and DNN layers to create a robust and effective intrusion detection system for IoT networks. The next section demonstrates the obtained results using the proposed model.

5 Experiment Results

The "Experiment Results" section presents the findings of the empirical evaluation of the proposed One-Dimensional Conv-BiLSTM Network with an Attention Mechanism for IoT Intrusion Detection. The primary goal of this evaluation is to assess the model's effectiveness in accurately detecting various types of intrusions in IoT networks and to compare its performance with existing state-of-the-art methods. The experiments were conducted using a comprehensive dataset that reflects

the complexity and diversity of real-world IoT network environments, including various types of network traffic and intrusion patterns.

The dataset was preprocessed and split into training and testing sets to ensure a fair comparison, following the same procedure described in earlier sections. The proposed model's architecture, including the Conv1D, BiLSTM, and DNN layers, was implemented using a popular deep-learning framework, and the model was trained using the training set with appropriate hyperparameter settings. The model's performance was then evaluated on the testing set, focusing on crucial evaluation metrics.

In the following subsections, we present a detailed analysis of the experiment results, including a discussion of the model's performance across different intrusion types, a comparison with other state-of-the-art methods, and an examination of the impact of the attention mechanism on the overall performance of the model. This analysis aims to comprehensively understand the proposed model's strengths and limitations and highlight its potential for real-world IoT intrusion detection applications.

5.1 Evaluation Metrics

In this study, to evaluate the sentiment classification problem, we use different evaluation parameters such as Accuracy, Precision, Recall, F-measure, and AUC-ROC Curve to evaluate the sentiment classification problem. Eqs. (5)–(8) demonstrate the formulas for each evaluation parameter [21]. In the following equations, TPs are true positives, TNs are true negatives, FPs are false positives, and FNs are false negatives.

$$Accuracy = \frac{TP + TN}{P + N} \tag{5}$$

$$Preision = \frac{TP}{TP + FP} \tag{6}$$

$$Recall = \frac{TP}{TP + FN} \tag{7}$$

$$F1 = \frac{2 \times precision \times recall}{precision + recall} \tag{8}$$

5.2 Experimental Results

Fig. 3 demonstrates the confusion matrix for the obtained results of the proposed network. The confusion matrix provides a comprehensive visualization of the model's performance in classifying different intrusion types. The matrix reveals a high degree of correct classifications along the diagonal, indicating the model's effectiveness in detecting various intrusions, while off-diagonal elements represent misclassifications [21]. This result demonstrates the robustness and accuracy of the proposed model in identifying and distinguishing between different types of IoT network intrusions.

Fig. 4 illustrates the rapid convergence of the proposed model's accuracy and the decrease in model loss over 100 learning epochs. The results indicate that the model reaches an accuracy exceeding 99% within just 30 learning epochs, showcasing its efficiency and effectiveness in learning from the data. This rapid convergence can be attributed to the proposed model to effectively capture complex patterns and temporal dependencies in the IoT network traffic data. The early achievement of high accuracy suggests that the model is well-suited for real-world IoT intrusion detection applications, where timely and accurate detection of security threats is crucial. Further optimization of the model's

hyperparameters and potentially incorporating additional features or data preprocessing techniques could lead to even better performance and faster convergence.

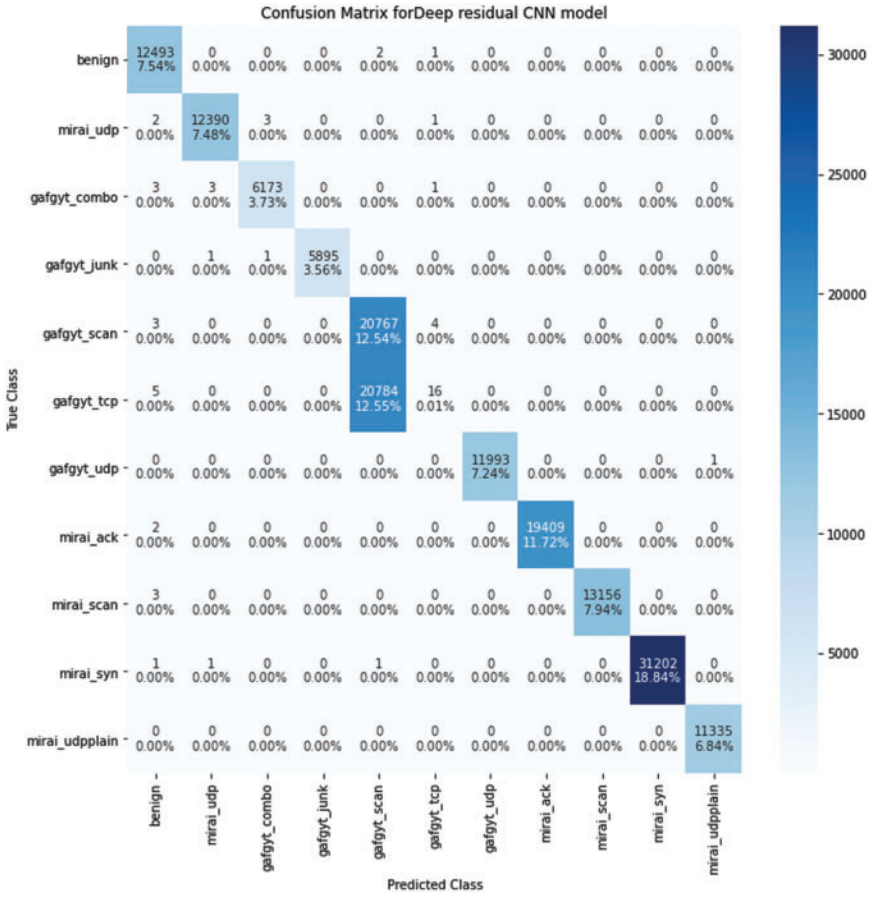
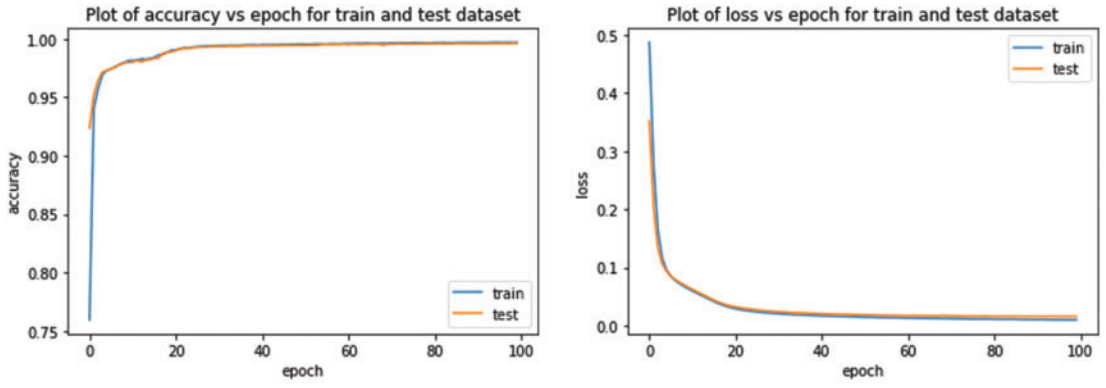


Figure 3: Confusion matrix in classifying different intrusion types



(a) Model accuracy (b) Model loss

Figure 4: The proposed model accuracy and loss for intrusion classification

Fig. 5 demonstrates the AUC-ROC curves of the proposed One-Dimensional Conv-BiLSTM Network with an Attention Mechanism for classifying different types of attacks. The results indicate that the model performs exceptionally well in detecting various intrusions, with ROC values ranging from 0.94 to 1.00. This high performance can be attributed to the combined strengths of the Conv1D, BiLSTM layers, and the attention mechanism, which effectively capture the complex patterns and temporal dependencies in the IoT network traffic data. These results validate the proposed model's efficacy and suggest that it holds significant promise for real-world IoT intrusion detection applications, particularly in detecting a wide range of attack types with high accuracy and precision.

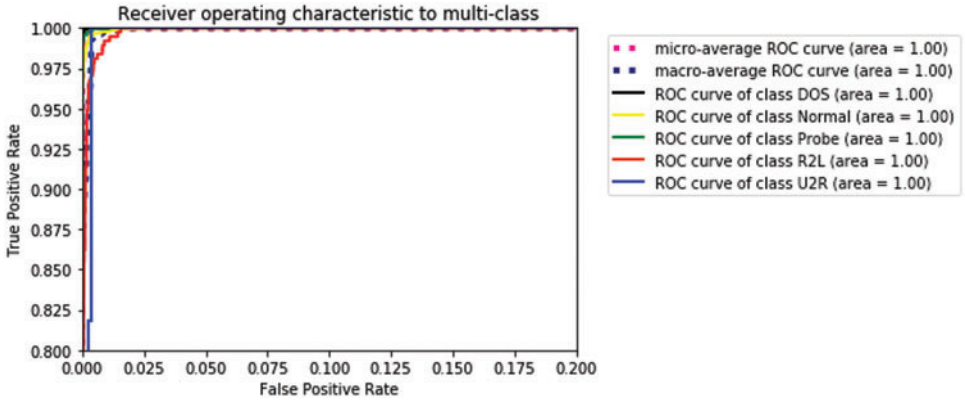


Figure 5: ROC-AUC curve for intrusion classification

Fig. 6 presents the confusion matrix for the binary classification task, which focuses on distinguishing between attack and non-attack instances in the IoT network traffic data. The matrix highlights the model's ability to accurately identify both instances, demonstrating a solid performance in positive and negative classifications. This result underscores the performance of the proposed model in detecting potential threats while maintaining a low false positive rate. Consequently, the model's performance in binary classification lends further support to its applicability in real-world IoT environments, where accurate and timely identification of attacks is crucial for ensuring the security and reliability of the network.

To compare the proposed model with machine learning techniques, we applied different machine learning models to this problem. Fig. 7 compares eight traditional machine-learning algorithms for intrusion detection problems. The results show that machine learning techniques' accuracy is at most 80%. The decision tree algorithm achieves the highest recall rate, with 78%. The maximum precision rate achieved is 98%. These results indicate that traditional machine learning methods yield low IoT network intrusion detection performance.

Fig. 8 compares the AUC-ROC curves of the proposed One Dimensional Conv-BiLSTM Network with Attention Mechanism with those of traditional machine learning models in detecting IoT network intrusions. The results reveal that the Gaussian Naive Bayes (NB) [22] model needs to address the problem effectively. In contrast, the performance of other models, such as K-Nearest Neighbors (KNN) [23] and Random Forest Classifier [24], varies with AUC-ROC values ranging from 0.84 to 0.91, respectively. In contrast, the proposed deep learning-based model significantly outperforms these traditional approaches, achieving an impressive AUC-ROC value of 0.995.

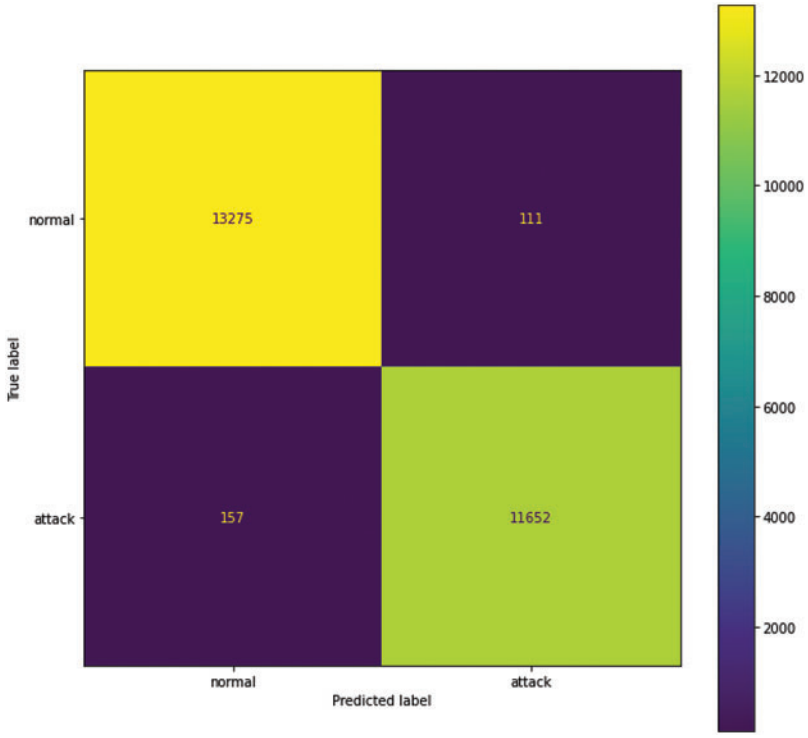


Figure 6: Confusion matrix for attack and non-attack categorization

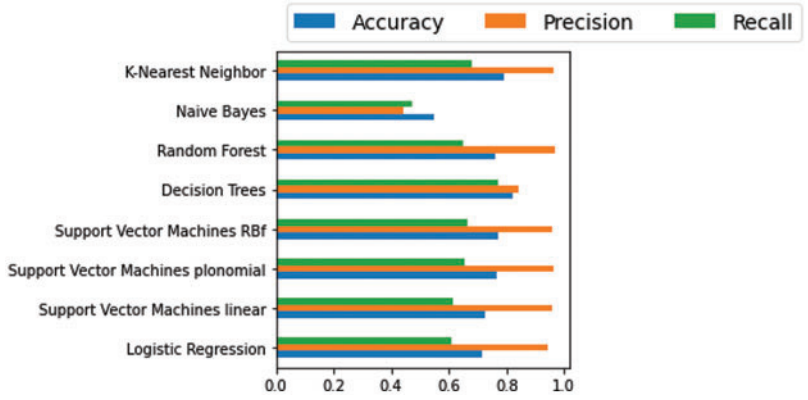
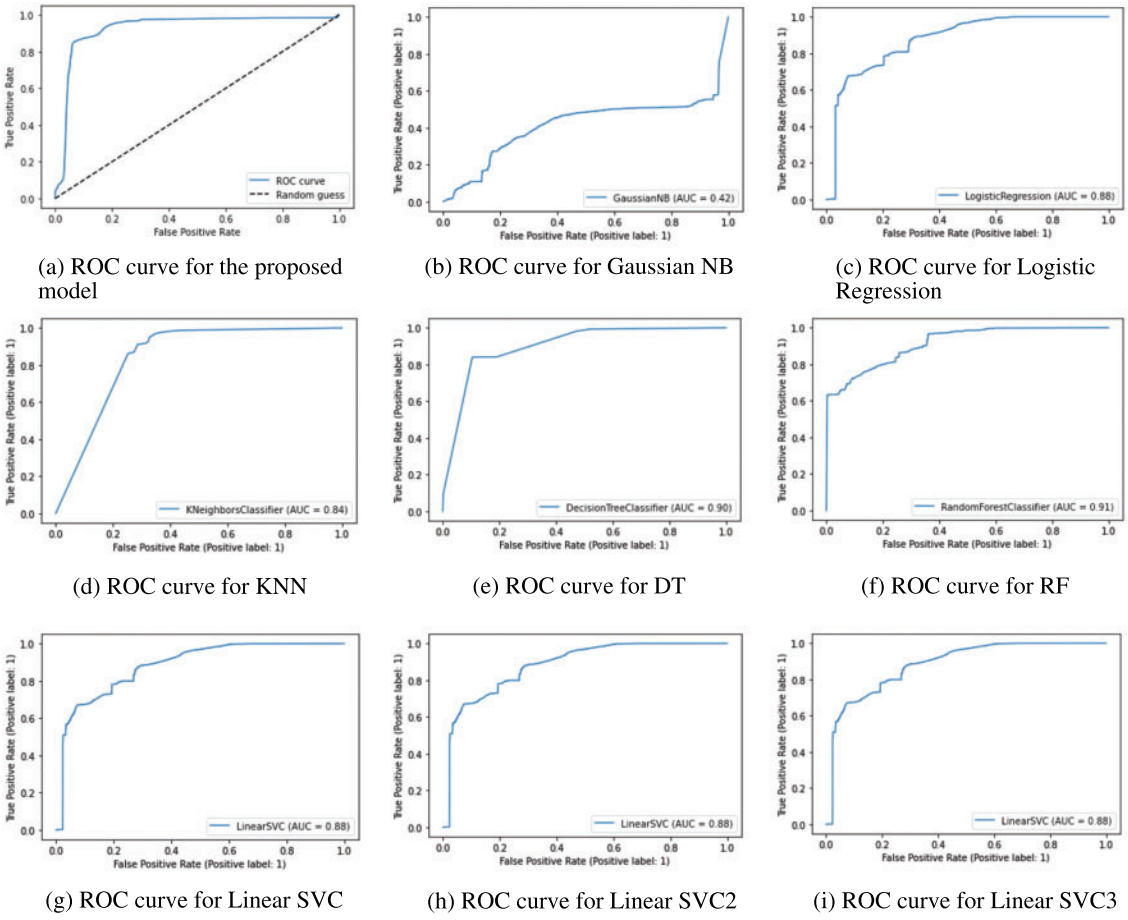


Figure 7: Evaluating different machine learning models based on their performance outcomes

This superior performance can be attributed to the inherent capabilities of the Conv1D and BiLSTM layers, along with the attention mechanism, in capturing complex patterns and temporal dependencies within the IoT network traffic data. The results highlight the advantages of employing advanced deep learning techniques for intrusion detection tasks in IoT environments, as they provide greater accuracy and effectiveness in detecting various attacks compared to traditional machine learning models. Consequently, the proposed model demonstrates its potential as a reliable and robust solution for real-world IoT intrusion detection applications, ensuring the security and resilience of IoT networks.



(a) ROC curve for the proposed model

(b) ROC curve for Gaussian NB

(c) ROC curve for Logistic Regression

(d) ROC curve for KNN

(e) ROC curve for DT

(f) ROC curve for RF

(g) ROC curve for Linear SVC

(h) ROC curve for Linear SVC2

(i) ROC curve for Linear SVC3

Figure 8: The ROC curve results for the proposed method and machine learning models

6 Discussion

This research introduces the One-Dimensional Conv-BiLSTM Network with Attention Mechanism, a novel deep learning-based model for IoT intrusion detection. The proposed model exhibits several advantages over traditional machine learning approaches, including its ability to effectively capture complex patterns and temporal dependencies in IoT network traffic data, which is critical for accurately classifying various intrusions [25]. The experimental results demonstrate that the model outperforms state-of-the-art research published in the last three years regarding accuracy, precision, recall, F-measure, and AUC-ROC, showcasing its robustness and reliability in detecting IoT network intrusions.

While the proposed One-Dimensional Conv-BiLSTM Network with Attention Mechanism exhibits impressive performance in IoT intrusion detection, several limitations and potential challenges must be considered in its implementation across diverse IoT network environments. These limitations and challenges encompass data collection, preprocessing, and model generalization.

Data Collection: Gathering a comprehensive and representative dataset for IoT network traffic data can be challenging due to privacy concerns, access to real-world IoT networks, and the diversity of IoT devices and applications. The availability of labeled intrusion data for training and evaluation

purposes is essential but may be limited, particularly for certain types of intrusions or emerging threats. A sufficiently large and diverse dataset that reflects the complexities of different IoT network environments is crucial for training a robust and generalized model.

Data Preprocessing: IoT network traffic data often exhibit high dimensionality, noise, and imbalance. Preprocessing techniques such as feature selection, dimensionality reduction, and handling class imbalance are essential to improve the model's performance and reduce computational overhead [26]. However, selecting appropriate preprocessing methods for IoT network traffic data can be challenging due to the varying characteristics of different IoT devices and applications.

Model Generalization: The generalization capability of the proposed model to different IoT network environments is a critical factor. The model must perform well on unseen data from diverse IoT setups and intrusion scenarios [27]. However, the heterogeneity and dynamic nature of IoT networks, including variations in network architectures, protocols, and traffic patterns, can pose challenges for model generalization. Ensuring that the model remains effective across different IoT environments requires careful consideration and adaptation of the model architecture and training strategies.

Computational Resources: Deep learning models, including the proposed One Dimensional Conv-BiLSTM Network with Attention Mechanism, typically require significant computational resources for training and inference. IoT devices often have limited computational capabilities and memory constraints, making it challenging to deploy resource-intensive models directly on edge devices [28]. Strategies such as model compression, optimization, or offloading computations to cloud or edge servers may need to be considered to make the model feasible for IoT deployment.

Interpretability and Explainability: Deep learning models are often black boxes due to their complex architectures and high-dimensional representations. Interpreting and explaining the model's decisions, especially in the context of IoT intrusion detection, is crucial for trust and transparency [29]. Ensuring that the proposed model provides interpretable explanations for its predictions and insights into the detected intrusions is an ongoing challenge that needs to be addressed.

Addressing these limitations and challenges requires further research and practical considerations. Future work should focus on developing techniques for efficient data collection, preprocessing strategies tailored for IoT network traffic data, enhancing model generalization to diverse IoT environments, optimizing computational resources for deployment, ensuring interpretability and explainability, and improving real-time performance for timely intrusion detection in IoT networks. The proposed model can be effectively implemented and deployed in many IoT network environments to enhance security and resilience against intrusions by addressing these challenges.

Future perspectives for this research involve optimizing the model's hyperparameters and incorporating additional features to improve performance. Additionally, exploring the model's applicability and scalability in real-world IoT deployments could address the growing security challenges faced by these networks [30]. Furthermore, comparisons with other state-of-the-art deep learning models developed for intrusion detection in the last three years would provide valuable insights into the performance and limitations of various architectures [31]. The proposed One-Dimensional Conv-BiLSTM Network with Attention Mechanism for IoT intrusion detection significantly contributes to cybersecurity. Its superior performance in detecting various types of intrusions, along with its potential for further improvements and real-world applications, highlights the importance of continued research and development in this area to ensure the security and resilience of IoT networks.

7 Conclusion

In conclusion, this paper introduces the One-Dimensional Conv-BiLSTM Network with Attention Mechanism, a novel deep learning-based model for IoT intrusion detection. Combining the strengths of 1D-CNN, BiLSTM layers, and attention mechanisms, the proposed model effectively captures complex patterns and temporal dependencies in network traffic data. The experimental results demonstrate the model's strong performance, surpassing traditional machine learning models' accuracy and achieving an impressive AUC-ROC value of 0.995.

While the results are promising, it is essential to acknowledge the critical limitations of the proposed framework. Challenges related to data collection, preprocessing, and model generalization must be addressed to ensure the model's practical implementation across diverse IoT network environments. Additionally, the model's interpretability and explainability should be further investigated to enhance trust and transparency in its decision-making process.

Future research efforts should focus on improving the proposed model by exploring additional features, optimizing hyperparameters, and investigating its scalability and applicability in real-world IoT deployments. Furthermore, extending the application of the model to other fields beyond intrusion detection, such as anomaly detection or predictive maintenance, could enhance its utility and impact in diverse domains.

The One Dimensional Conv-BiLSTM Network with Attention Mechanism for IoT Intrusion Detection contributes to the field of cybersecurity by providing a robust and reliable solution for detecting various types of intrusions in IoT networks. By strengthening the security and resilience of IoT networks, this model contributes to developing safer and more trustworthy connected systems, benefiting domains such as smart homes, healthcare, transportation, and beyond.

Acknowledgement: Not applicable.

Funding Statement: The authors received no funding for this study.

Author Contributions: conceptualization, B.O.; methodology, B.O., Z.S., and A.B.; software, B.O.; data curation, B.O., L.N., and A. D.; writing—original draft preparation, B.O.; writing—review and editing, B.O., Z.S., A.B., A.K., L.N., and A.D.; Discussion, B.O., Z.S., A.B., A.K., L.N., and A.D. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: This research investigation employed the NSL-KDD dataset, obtainable through the academic source cited as https://www.unb.ca/cic/datasets/nsl.html.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. Lin, Q. Xue, J. Feng and D. Bai, "Internet of Things intrusion detection model and algorithm based on cloud computing and multi-feature extraction extreme learning machine," *Digital Communications and Networks*, vol. 9, no. 1, pp. 111–124, 2023.

[2] R. Soleymanzadeh and R. Kashef, "Efficient intrusion detection using multi-player generative adversarial networks (GANs): An ensemble-based deep learning architecture," *Neural Computing and Applications*, vol. 35, no. 17, pp. 12545–12563, 2023.

[3] B. Gopalakrishnan and P. Purusothaman, "A new design of intrusion detection in IoT sector using optimal feature selection and high ranking-based ensemble learning model," *Peer-to-Peer Networking and Applications*, vol. 15, no. 5, pp. 2199–2226, 2022.
[4] A. Belhadi, Y. Djenouri, D. Djenouri, G. Srivastava and J. Lin, "Group intrusion detection in the Internet of Things using a hybrid recurrent neural network," *Cluster Computing*, vol. 26, no. 2, pp. 1147–1158, 2023.
[5] M. Jeyaselvi, R. Dhanaraj, M. Sathya, F. Memon, L. Krishnasamy *et al.,* "A highly secured intrusion detection system for IoT using EXPSO-STFA feature selection for LAANN to detect attacks," *Cluster Computing*, vol. 26, no. 1, pp. 559–574, 2023.
[6] C. OmKumar, S. Marappan, B. Murugeshan and P. Beaulah, "Intrusion detection model for IoT using recurrent kernel convolutional neural network," *Wireless Personal Communications*, vol. 129, no. 2, pp. 783–812, 2023.
[7] S. Mohamed and R. Ejbali, "Deep SARSA-based reinforcement learning approach for anomaly network intrusion detection system," *International Journal of Information Security*, vol. 22, no. 1, pp. 235–247, 2023.
[8] Y. Zhu, M. Xie, K. Zhang and Z. Li, "A dam deformation residual correction method for high arch dams using phase space reconstruction and an optimized long short-term memory network," *Mathematics*, vol. 11, no. 9, pp. 1–20, 2023.
[9] Y. Zhu, Z. Zhang, C. Gu, Y. Li, K. Zhang *et al.,* "A coupled model for dam foundation seepage behavior monitoring and forecasting based on variational mode decomposition and improved temporal convolutional network," *Structural Control and Health Monitoring*, vol. 2023, pp. 1–17, 2023.
[10] S. Mehedi, A. Anwar, Z. Rahman, K. Ahmed and R. Islam, "Dependable intrusion detection system for IoT: A deep transfer learning based approach," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 1006–1017, 2022.
[11] J. Bharadiya, "Machine learning in cybersecurity: Techniques and challenges," *European Journal of Technology*, vol. 7, no. 2, pp. 1–14, 2023.
[12] A. Alqahtani, "FSO-LSTM IDS: Hybrid optimized and ensembled deep-learning network-based intrusion detection system for smart networks," *The Journal of Supercomputing*, vol. 78, no. 7, pp. 9438–9455, 2022.
[13] I. Hidayat, M. Ali and A. Arshad, "Machine learning-based intrusion detection system: An experimental comparison," *Journal of Computational and Cognitive Engineering*, vol. 2, no. 2, pp. 88–97, 2023.
[14] H. Yao, P. Gao, P. Zhang, J. Wang, C. Jiang *et al.,* "Hybrid intrusion detection system for edge-based IIoT relying on machine-learning-aided detection," *IEEE Network*, vol. 33, no. 5, pp. 75–81, 2019.
[15] J. Long, W. Liang, K. Li, Y. Wei and M. Marino, "A regularized cross-layer ladder network for intrusion detection in industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1747–1755, 2022.
[16] J. Jain and A. Waoo, "An artificial neural network technique for prediction of cyber-attack using intrusion detection system," *Journal of Artificial Intelligence, Machine Learning and Neural Network*, vol. 3, no. 2, pp. 33–42, 2022.
[17] F. Abbasi, M. Naderan and S. Alavi, "Intrusion detection in IoT with logistic regression and artificial neural network: Further investigations on N-BaIoT dataset devices," *Journal of Computing and Security*, vol. 8, no. 2, pp. 27–42, 2021.
[18] A. Pashaei, M. Akbari, M. Lighvan and A. Charmin, "Honeypot intrusion detection system using an adversarial reinforcement learning for industrial control networks," *Majlesi Journal of Telecommunication Devices*, vol. 12, no. 1, pp. 17–28, 2023.
[19] L. Zhou, Z. Zhang, L. Zhao and P. Yang, "Attention-based BiLSTM models for personality recognition from user-generated content," *Information Sciences*, vol. 596, no. 1, pp. 460–471, 2022.
[20] L. Zhou, L. Z.Zhang, L. Zhao and P. Yang, "Microblog sentiment analysis based on deep memory network with structural attention," *Complex & Intelligent Systems*, vol. 9, no. 3, pp. 3071–3083, 2023.
[21] A. Tursynova, B. Omarov, N. Tukenova, I. Salgozha, O. Khaaval *et al.,* "Deep learning-enabled brain stroke classification on computed tomography images," *Computers, Materials & Continua*, vol. 75, no. 1, pp. 1431–1446, 2023.

[22] R. Almarshdi, L. Nassef, E. Fadel and N. Alowidi, "Hybrid deep learning based attack detection for imbalanced data classification," *Intelligent Automation & Soft Computing*, vol. 35, no. 1, pp. 297–320, 2023.
[23] R. Gopi, R. Sheeba, K. Anguraj, T. Chelladurai, H. Mesfer Alshahrani *et al.,* "Intelligent intrusion detection system for industrial Internet of Things environment," *Computer Systems Science and Engineering*, vol. 44, no. 2, pp. 1567–1582, 2023.
[24] A. Sezgin and A. Boyacı, "Enhancing intrusion detection in industrial Internet of Things through automated preprocessing," *Advances in Science and Technology Research Journal*, vol. 17, no. 2, pp. 120–135, 2023.
[25] T. Saba, T. Sadad, A. Rehman, Z. Mehmood and Q. Javaid, "Intrusion detection system through advance machine learning for the Internet of Things networks," *IT Professional*, vol. 23, no. 2, pp. 58–64, 2021.
[26] S. Chatterjee and M. Hanawal, "Federated learning for intrusion detection in IoT security: A hybrid ensemble approach," *International Journal of Internet of Things and Cyber-Assurance*, vol. 2, no. 1, pp. 62–86, 2022.
[27] M. Kalinin and V. Krundyshev, "Security intrusion detection using quantum machine learning techniques," *Journal of Computer Virology and Hacking Techniques*, vol. 19, no. 1, pp. 125–136, 2023.
[28] A. Yazdinejad, M. Kazemi, R. Parizi, A. Dehghantanha and H. Karimipour, "An ensemble deep learning model for cyber threat hunting in industrial Internet of Things," *Digital Communications and Networks*, vol. 9, no. 1, pp. 101–110, 2023.
[29] Q. Dang, "Improving the performance of the intrusion detection systems by the machine learning explainability," *International Journal of Web Information Systems*, vol. 17, no. 5, pp. 537–555, 2021.
[30] M. Douiba, S. Benkirane, A. Guezzaz and M. Azrour, "An improved anomaly detection model for IoT security using decision tree and gradient boosting," *The Journal of Supercomputing*, vol. 79, no. 3, pp. 3392–3411, 2023.
[31] W. Liang, Y. Hu, X. Zhou, Y. Pan, I. Kevin *et al.,* "Variational few-shot learning for microservice-oriented intrusion detection in distributed industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 8, pp. 5087–5095, 2021.