JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 10 Issue 01
2025

Research Article
https://doi.org/10.56979/1001/2025/1169

Comparative Analysis of LSTM-Based Variant Models for Detecting Attacks in IoT Networks

Mosleh M. Abualhaj[1*], Hannan Adeel[2], Khalid Masood[3], Hama Soltani[4], Hadjir Zemmouri[5], Mohamed M. Reda Aly[6], Abdullah T. Elgammal[7], and Shahid Mehmood[8]

[1]Department of Networks and Cybersecurity, Al-Ahliyya Amman University, Amman, Jordan.
[2]Faculty of Artificial Intelligence and Cyber Security, Universiti Teknikal Malaysia Melaka, Melaka 76100, Malaysia.
[3]Faculty of Computer Science and IT, Minhaj University Lahore, Pakistan.
[4]Laboratory of Mathematics, Informatics and Systems (LAMIS), University of Tebessa, Tebessa, Algeria.
[5]MISC Laboratory, Abdelhamid Mehri University, Constantine, Algeria.
[6]Central Lab of Agriculture Expert Systems (CLAES), Agriculture Research Center (ARC), Giza, Egypt.
[7]Department of Mechanical Engineering, The British University in Egypt, El-Sherouk City, Egypt.
[8]Department of Computer Science, Bahria University, Lahore, 54000, Pakistan.
[*]Corresponding Author: Mosleh M. Abdullah. Email: m.abualhaj@ammanu.edu.jo

Received: September 08, 2025 **Accepted:** November 13, 2025

Abstract: Internet of Things (IoT) networks have established unparalleled connection possibilities and convenient features and have set new challenges associated with dubious security barriers and potential attacks. This study evaluates attack detection performance of LSTM-Based Variant models namely LSTM, DeepBiLSTM and BLSTM recurrent neural networks by bringing up experiment analysis of the IoT networks. We evaluate the three models using benchmark IoT dataset in terms of detection accuracy, precision, recall and F1 measure. The experiment results indicate that the three LSTM-based models, LSTM, BiLSTM, and DeepBiLSTM, demonstrate a high level of performance, regardless of the batch size (32, 64, 128, 256, and 512). DeepBiLSTM has a little better overall performance, which validates its soundness and suitability towards scale in detecting attacks in large IoT networks.

Keywords: Internet of Things; Recurrent Neural Network; Deep BLSTM; BLSTM; LSTM; IoT Attacks

1. Introduction

Digital transformation is reshaping multiple sectors, from empowering women in leadership through technology to improving workplace performance with gamified HR practices [1] [2]. It also supports sustainable decision-making in fintech and strengthens public trust through effective e-government services [3-4]. As these advancements expand, wireless communication technologies become essential for enabling seamless connectivity and real-time data exchange [5] [6]. Building on these capabilities, the Internet of Things (IoT) emerges as the next major evolution, providing intelligent integration across devices, systems, and services.

The Internet of Things (IoT) is described as a network of gadgets spread all over the world and able to organize activities, as well as information exchange, with their remoteness [7] [8]. This ecosystem has evolved to be a sophisticated environment with sophisticated medical technologies, the simplest health-monitoring gadgets, and daily smart-home devices. IoT systems are usually based on interdependent resources, i.e. processors, sensors and actuators, to gather data and relay it to server or to other machines to continue to be used [9] [11]. The growing possibilities to automate the activities, monitor systems, and conduct analytics have led to new possibilities to increase efficiency, optimize operations, and provide support in their decision-making to various industries [12] [13]. IoT applications currently cut across transportation, healthcare, agriculture, and manufacturing industries, and these applications illustrate the ability of this technology to enhance everyday life and remodel the ways we engage our environment [14] [15].

With the growing number of IoT devices that are connected to each other, the attackers have an increasing array of attack surfaces to target. In addition, the absence of definite security routines may allow malicious actors to have easy access to the information that is stored on the IoT devices or even have power in it [16] [17]. Data breaches and DDoS attacks are some of the threats that organizations face due to the poor security of the IoT systems [18] [19]. Another issue is that not every IoT technology and platform has security standards accepted by everyone. Consequently, it is vital to identify and curb attacks on IoT networks through relevant security mechanisms as early as possible [20] [21].

The reinforcement of the IoT network infrastructures is an urgent necessity because the high rate of the development of the interconnection of devices has increased the risk of security breach and data breach [22] [23]. Proper attack mitigation and early data protection strategies are important to reduce operational and financial costs. Development of effective security measures is of utmost importance to not only ensure that important assets are secured but also user confidence towards IoT-powered systems [24-26]. In a lot of situations, the vulnerabilities of IoT networks may interfere with critical services and give rise to serious security issues that were not typical of traditional data breaches. In turn, it would be necessary to sustain investment in efficient detection and prevention mechanisms to make the IoT networks resilient and safe to operate [27] [28].

Machine learning models exhibit great performance in content pattern identification and anomaly detection which is critical in the process of detecting unseen danger in big data [29] [30]. All these methods are becoming based on more sophisticated algorithms and models such as deep learning and neural networks to protect against new threats to security [31-33]. To implement machine learning to the full extent of IoT, it is necessary to analyze the data of various sources, such as user operations, device logs, and network traffic [34]. The use of these approaches will help to significantly increase the general security and resilience of IoT devices and networks. The objective of this paper is to critically analyze the behavior of three recurrent neural network (RNN) networks namely Deep Bidirectional Long Short-Term Memory (Deep Bi-LSTM), Bi-LSTM and LSTM with different batch sizes [35-37]. The results of the current research give an insight that can guide other researchers to adopt the most appropriate algorithm when undertaking intrusion detection exercises in the IoT environment.

In Section 2, the paper starts with a review of literature where the relevant researchers employ DL methods in detecting attacks on IoT. Section 3 provides an overview of the roles of LSMT, Bi-LSTM, and deep Bi-LSTM. In section 4, the ways of measuring the deep Bi-LSTM, Bi-LSTM, and LSTM are explained. In the meantime, the discussion and results are given in Section 5. Section 6 is the conclusion of the research work and offers future research directions.

2. Related works

The current section is a review of critical works applying deep learning techniques to identify IoT attacks. In [38] study, the authors offered a hybrid framework made of Convolutional Neural Network (CNN) and Convolutional LSTM (C-LSTM) models to detect anomalies in IoT networks. This integration is a mixture of geographical and time-related variables, which makes it reasonable in the case of limited resources, and time is of the essence when it comes to work with the large volume of data on IoT. CNN derives features out of the original data space and C-LSTM is a temporal specific feature deriver. The fusion model enhances parallelism training significantly and gets better results without necessarily having to have an excessively deep network. The researchers evaluated the proposed model based on the KDDCup-99 dataset. The results show that the fusion model makes better results compared to existing deep learning implementations on the accuracy, precision and recall on anomaly detection tasks in IoT settings, which points to the possible ability to improve the protocols used to secure the IoT.

In [39] study, the authors came up with an original method to detect botnet and malware cyber-attacks in IoT networks through a combination of LSTM and Generative Adversarial Networks (GANs). In this approach, LSTM models are used to identify complex relationships and connections between different network traffic features whereas GANs are used to identify traffic pattern anomalies. This unique strategy enables the models to evolve to unknown attack patterns which contribute to their effectiveness against new cyber threats. The authors use network traffic data of many IoT devices to train and evaluate their models, but they fail to provide any description of the used dataset. According to the study, the approaches used such as the LSTM and GAN-based are effective in the identification of botnet and virus attacks in the IoT networks. This will be an effective differentiator of benign and malicious communications and will develop more resilient and efficient security solutions that cater to IoT devices in a specific manner.

In [40], Conditional Tabular GAN (CTGAN) architecture is applied in the IDS architecture to identify in the real-time DDoS and Denial of Service (DoS) attacks in IoT networks. IDS can be trained to emulate real-world traffic by using a generator network, whereas a discriminator network is trained to differentiate innocuous and malicious behavior in the network. The system enhances the performance of various shallow and deep-learning classifiers in the detection models using the synthetic tabular data generated by CTGAN. The proposed method is tested on Bot-IoT dataset to identify the intrusions in IoT networks. This dataset contains several network traffic parameters, benign and malicious samples. The experimental results indicate the effectiveness of the system in detecting DDoS and DoS attacks in the IoT with high precision, recall, and detection accuracy and F1 measure.

The research paper in [41] introduces a Bi-LSTM-based network anomaly-detecting procedure and claims the existence of a strong performance because the model has the capability to reflect the temporal links between sequential data. The authors trained the model with optimal hyperparameters such as the optimizer, epochs, batch size, and training-testing split. Though less information about the NSL-KDD binary dataset is given, Bi-LSTM model attained an accuracy of 98.52%. The results in comparison and depending on the accuracy and F1-score indicate that the model is better than several available methods, which proves it to be effective in detecting network anomalies with high-precision.

LBDMIDS [42] is an IoT network IDS based on deep learning. To construct NIDS models, LBDMIDS employs some variations of LSTM models, including stacked LSTM and bidirectional LSTM. The reason for choosing the LSTM model is based on the capacity to deal with different input and output sequences and the model is adept at detecting familiar and unfamiliar threats. The two datasets UNSW-NB15 and BoT-IoT are used as training and validation datasets. Conversely, BoT-IoT data has a specific purpose of investigating the area of intrusion detection in the IoT network. LBDMIDS models are more effective than the traditional ML models and have comparable performance to those of DNNs. However, it is not stated in the research what specific performance indicators such as F1 score, accuracy, and recall are. However, LBDMIDS does have great potential in enhancing the intrusion detection abilities of IoT systems, offering resilience to most attack vectors.

In [43], the authors introduced a hybrid LSTM-GRU model, which was a combination of LSTM and Gated Recurrent Unit (GRU) architectures to enhance the system of detecting intrusion of IoT networks. The method employed PSO and GA as methods of carrying out feature selection processes. The CICIDS-2017 dataset is used to perform the analysis. As the findings of the research indicate, the LSTM-GRU combination leads to major improvements in attack detection, allowing network IDS to achieve the accuracy of 98.86 %. The suggested IDS system is effective since the trials conducted on the current alternatives demonstrate that it enhances the capabilities of the IoT intrusion detection.

In [44], the dual CNN-CNN method that deals with the process of choosing meaningful features along with the mechanism of detecting attacks in IoT networks is suggested. It uses two CNN models, the former being built with the purpose of identifying the key features of unprocessed network traffic data, and the latter being built with the use of these features to establish a robust detection infrastructure. Based on the BoT IoT 2020 dataset, the results reveal an outstanding performance of the method, whereby the method achieves a detection accuracy of 98.04%, precision of 98.09%, recall of 99.85%, and a false positive rate (FPR) of 1.93%.

In the article of [45], the authors present an optimized CNN-based intrusion detection system capable of detecting attacks on an IoT device. The proposed method is based on a combination of deep CNN (DCNN) and machine learning form a loss function that includes regularized ways of avoiding overfitting. The DCNN is evaluated using NSL-KDD dataset, which focuses on IoT devices. The model performance analysis is based on simulation testing on accuracy, precision, and recall F1 score measures and AUC. Table 1 presents a summary of related work.

The performance of LSTM-based variants (e.g. Bi-LSTM, stacked LSTM, hybrids of LSTM-GRUs and LSTM models augmented by GANs or optimization) in the detection of IoT attacks has always outpaced more traditional machine-learning algorithms, as per the reviewed literature listed in Table 1. Hybrid-based models such as CNN-LSTM or LSTM-GRU are demonstrated to be highly capacity models in accuracy rates to a rate of 98 and 99% in capturing time and space-based modelling on the recent datasets of IoT including BoT-IoT, UNSW-NB15 and CICIDS-2017. Besides, GAN-based LSTM models enhance the robustness of models through synthesizing data to balance class distribution, optimization algorithms (PSO, GA) enhance feature selection and detection. On balance, it can be concluded that the variants based on LSTM prove their superiority in the application of the anomaly detection of the IoT network, which proves the importance of the comparisons between the architectures that would be used to choose the most efficient way of intrusion detection.

Table 1. Summary of related work

Reference	Methodology	Dataset	Key Findings
[38]	Fusion model combining CNN and C-LSTM for anomaly detection in IoT networks.	KDDCup-99	Improved accuracy, precision, and recall. Enhanced parallelism without requiring a deep network.
[39]	LSTM and GAN-based approach for identifying botnet and malware cyber-attacks.	Unspecified IoT network traffic data	Effective differentiation between benign and malicious communications. Adapts to emerging threats.
[40]	IDS architecture uses Conditional Tabular GAN (CTGAN) to detect DDoS and DoS.	Bot-IoT	Enhanced detection performance using synthetic tabular data. High precision, recall, and F1-score.
[41]	Bi-LSTM model for network-based anomaly detection.	NSL-KDD (binary)	Achieved 98.52% anomaly detection accuracy. Outperforms traditional methods in accuracy and F1-score.
[42]	LBDMIDS IDS leveraging stacked and bidirectional LSTM models.	UNSW-NB15, BoT-IoT	It shows improved performance over ML approaches, which yields promising results for IoT intrusion detection.
[43]	Hybrid LSTM-GRU model with PSO and GA feature selection.	CICIDS-2017	Achieves 98.86% accuracy. Strengthens IoT intrusion detection compared to existing models.
[44]	Dual CNN approach for feature selection and attack detection.	BoT-IoT 2020	98.04% accuracy, 98.09% precision, 99.85% recall, and 1.93% FPR.

[45]	Optimized CNN-based IDS with deep CNN and ML techniques.	NSL-KDD	It uses a loss function to prevent overfitting. Evaluated with accuracy, precision, recall, F1-score, and AUC metrics.

3. Neural Network Architecture

3.1. Long short-term memory

A variant of RNN known as LSTM attempts to address the issue of diminishing gradients of standard RNNs. Ever since Hochreiter and Schmidhuber introduced LSTM in 1997, it has been praised in other fields, including natural language processing, and voice recognition. With the help of a memory unit, LSTM networks are highly efficient to trace long-term connections in sequential data. Deleting /saving data selectively over time is useful in a few situations. What enables them to be so exceptional in perception is a special attribute that they have and that it comes into handy in instances where they are aware of what preceded the past input which is paramount in making the right predictions. The gates are also used in the LSTM networks to further control the flow of data within the memory unit. These mechanisms allow the network to control the data amount stored or sent to the garbage at every period which is admission gate, ignoring and exit gate. This operation enables the network to analyze long sequences with greater accuracy and efficiency [36,46,47]. Many areas have also demonstrated the effectiveness and adaptability of the LSTM networks. The LSTM architecture is represented in Figure 1.

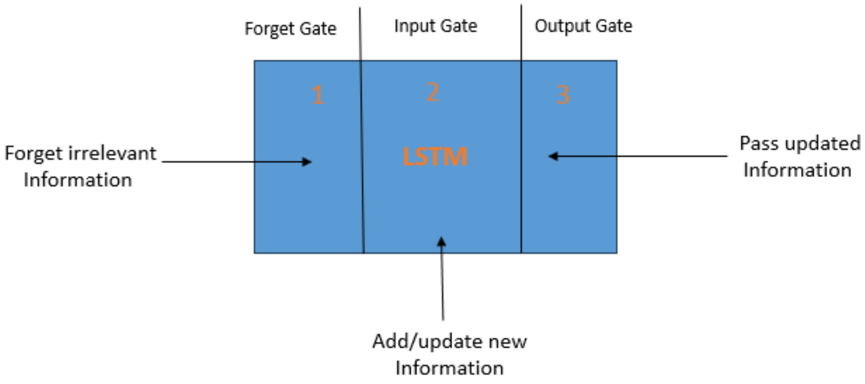


Figure 1. LSTM architecture

3.2. Bi-LSTM

The Bi-Directional-LMST uses the LSTM networks which are highly ranked in the discipline to process data both forward and backward. The sequencing is learned in the entirety by the network as it can understand the context of the step before and the step ahead. There are various applications of bidirectional long short-term memory, which include machine translation, sentiment analysis, and voice recognition. Dependencies in twin directions can be easily noted through bi-directional LSTM as it operates both ways. This is how to go with jobs where the order is very important. The skill of the Bi-Directional LSTMs to predict future occurrences is rather beneficial in those cases in which the forecasts or outcomes of future events play an important role [35] [48-49]. The Bi-Directional LSTM architecture is found in Figure 2.

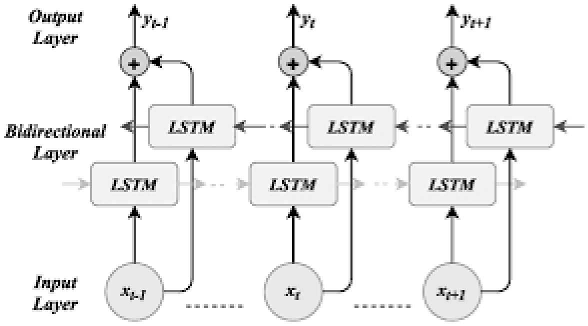


Figure 2. Bi-LSTM architecture

3.3. Deep Bi-LSTM

The study discovered that the models can be improved greatly by introducing additional layers of bidirectional LSTMs to networks. Finder understanding of the complex patterns and chain connection can be obtained through adding more layers to the network that will allow retrieving more detailed components and representations. Consequently, deep bi-directional LSTMs are good in a work that requires a comprehensive knowledge of the environment and accurate prediction. These frameworks have worked in several areas, and some of them include time series analysis and natural language processing. Deep bidirectional LSTMs are the best when it comes to predicting future events. Deep Bi-Directional LSTMs are also able to incorporate future and past information to capture long term dependencies and make more accurate predictions [50-52].

4. Methods

This section explains the methods used to conduct experimental analysis on LMST and its variants (Bi-LSTM, Deep Bi-LSTM). The dataset used to evaluate the capability of LSTM and Bi-LSTM, and Deep Bi-LSTM, data preprocessing, used deep learning algorithms architecture and evaluation metrics are explained in Section 4.1, Section 4.2, Section 4.3, and Section 4.4, respectively.

4.1. Dataset

In this study, the BoT-IoT dataset [16] would be used to test the methodology proposed. The BoT-IoT dataset is a CSV-based dataset that was created based on the network traffic analysis. It has a wider streaming and network capability which is intriguing. The types of attacks that can be found in the BoT-IoT dataset are Information theft, reconnaissance, DoS, and DDoS attacks. The dataset provides a comprehensive description of real-world attacks of IoT bots, which makes it suitable to evaluate the effectiveness of the proposed methodology. The inclusion of different types of attacks will help to evaluate the effectiveness of the methodology in a variety of situations. Besides this, annotated samples of normal network traffic are included in the dataset, which allows depending on anomalies and comparing them. This feature increases the usefulness of the dataset in building robust resilience intrusion detection architecture of IoT devices. The presence of common traffic traces, as well as different types of attacks, in the BoT-IoT data, makes it an all-valuable asset to not only security researchers but also to security practitioners. Table 2 presents the information on the distribution of the IoT-Botnet 2020.

Table 2. Distribution details of the used dataset

Category	Value
Number of normal rows	40073
Number of attack rows	585710
Total number of rows	625783
Total number of features	85

4.2. Data preprocessing

As the study aims to test LSTM variants models, it is important to make sure that the input data is appropriate and can be handled by deep learning models [53]. The existing structure of data underutilization does not suit deep learning models to the extent. As such, a job of preparing the dataset with several steps is applied. These steps are as follows:

- The data cleansing process entails determining and eliminating any errors, inconsistencies, or incorrect data in the data. This data should be cleaned up with the elimination of duplicating data, handling missing data and resolving formatting problems [54]. In the used dataset, all the missing values are eliminated.
- Data transformation entails transformation of categorical data into numerical data by means of one-hot or label encoding techniques. The utilized dataset contains seven categorical items namely: FlowID, SrcIP, DstIP, Timestamp, Label, Cat and SubCat. Values of features are given a unique integer as elements of that feature have different values. An example of data transformation of the source IP (Src_IP) feature is presented in Table 3 [55-56].

Table 3. Data transformation of source IP ('Src_IP') feature

Source IP	Assigned Value
192.168.0.13'	1
'222.160.179.132'	2
'192.168.0.16'	3
111.190.23.58	

- Data scaling is a method that is applied when the variables are to be standardized on the standard scale which can be beneficial. This may be by means of standardization or normalization. The extreme values that can influence the analysis may also be handled with the help of outlier detection and removal methods. The Min-Max normalization algorithm in the used dataset scales the values within a dataset so that they can be within a predefined range typically 0-1 [57] [58]. The following Equation is used to apply it:

$$x_{norm} = \frac{X \ \ -X_{min}}{X_{max}-X_{min}} \times 100\% \qquad (1)$$

Where**:**

- x represents the initial value of the feature.
- x_{min}represents the minimum value of the feature inside the dataset.
- x_{max}represents the highest value of the feature inside the dataset.

Lastly, it is vital to note that this study is focused on binary classification, where a clear distinction was made between normal and attack cases. Nonetheless, the dataset utilized in this research is multi-class which consists of the following categories: DDoS, DoS, Reconnaissance, Theft, and Normal. Consequently, all attack traffic is categorized with a value of 1, whereas normal one is categorized with 0.

4.3. LSTM, BiLSTM, and deep Bi-LSTM architectures

The architectures of LSTM, BiLSTM and Deep BiLSTM fix the information flow and capability of the model to feature long-term dependencies. These design options have a direct impact on the ability of each model to infer sequential data and produce the correct prediction, and influence the computational costs and training [59-60]. The architectures of the LSTM, BiLSTM, and Deep BiLSTM models are provided in Table 4, Table 5, and table 6 respectively, with the training parameters of the models summarized in Table 7. The parameters and structural designs used in the present study are the same as those ones, which are commonly reported in the literature, such as [61] and [62].

Table 4. LSTM architecture

Layer (type)	Features	Param #
lstm_7 (LSTM)	32	4352
dropout_1 (Dropout)	32	0
batch_normalization	32	128
dropout_2 (Dropout)	32	0
dense_8 (Dense)	(None, 2)	66
flatten_4 (Flatten)	(None, 2)	0
Total params:	4546	
Trainable params:	4482	
Non-trainable params:	64	

Table 5. Bi-LSTM architecture

Layer (type)	**Features**	Param #
bidirectional_7 (Bidirectional)	256	133,120
dense_9 (Dense)	64	16,448
dropout_3 (Dropout)	64	0
dense_10 (Dense)	2	130
flatten_5 (Flatten)	2	0
Total params:	149,698	
Trainable params:	149,698	
Non-trainable params:	0	

Table 6. Deep Bi-LSTM architecture

Layer (type)	**Output shape**	**Param #**
bidirectional_8 (Bidirectional)	(None, 74, 128)	33,792
bidirectional_9 (Bidirectional)	(None, 128)	98,816
dense_11 (Dense)	(None, 64)	8,256
dense_12 (Dense)	(None, 2)	130
flatten_6 (Flatten)	(None, 2)	0
Total params:	140,994	
Trainable params:	140,994	
Non-trainable params:	0	

Table 7. Parameters used in model architecture.

Parameter	**Value**
Overfitting Mechanism	Early Stopping (monitor=loss function, patience=3)
Optimizer	Adam
Loss Function	Sparse Categorical Cross-entropy
Learning Rate	0.1

The IoT-Botnet 2020 dataset is used to train the three models. Pareto 80/20 rule was used to divide the data set. This method involves the division of the data in terms of training and testing where 80 % will be used in the training and 20 % in testing. This approach can be useful in proving the ability of the trained models to apply to data that has not been seen before.

4.4. Evaluation Metrics

Deep BLSTM, BLSTM, and LSTM have been assessed through recognized metrics, including detection accuracy, False Positive Rate (FPR), precision, recall, and F1-measure [63,64,65,66]. The determination of these metrics is contingent upon the characteristics of the confusion metrics presented in Table 8, whereas Table 9 provides a detailed description of these characteristics [63-66].

Table 8. Attributes of the Confusion Matrix

		Predicted class	
		Attack	Normal
Actual Class	Attack	True-Positive	False-Negative
	Normal	False-Positive	True-Negative

Table 9. Description of Confusion Matrix Attributes

Term	**Description**

True-Positive (TP):	The incident is accurately categorized as an Attack.
False-Negative (FN):	The incident is inaccurately classified as a normal instance.
False-Positive (FP):	The incident is inaccurately categorized as an Attack.
True-Negative (TN)	This incident is accurately categorized as a regular instance.

The equations to calculate detection accuracy, FPR, precession, recall, and F1-measure are as follows [63-66]:

$$\boldsymbol{Accuracy\ rate = \frac{TP + TN}{TP + TN + FP + PN} \times 100\%} \qquad \boldsymbol{(2)}$$

$$\boldsymbol{False\ positive\ \ rate = \frac{FP}{FP + TN} \times 100\%} \qquad \boldsymbol{(3)}$$

$$\boldsymbol{Precession = \frac{TP}{TP + FP} \times 100\%} \qquad \boldsymbol{(4)}$$

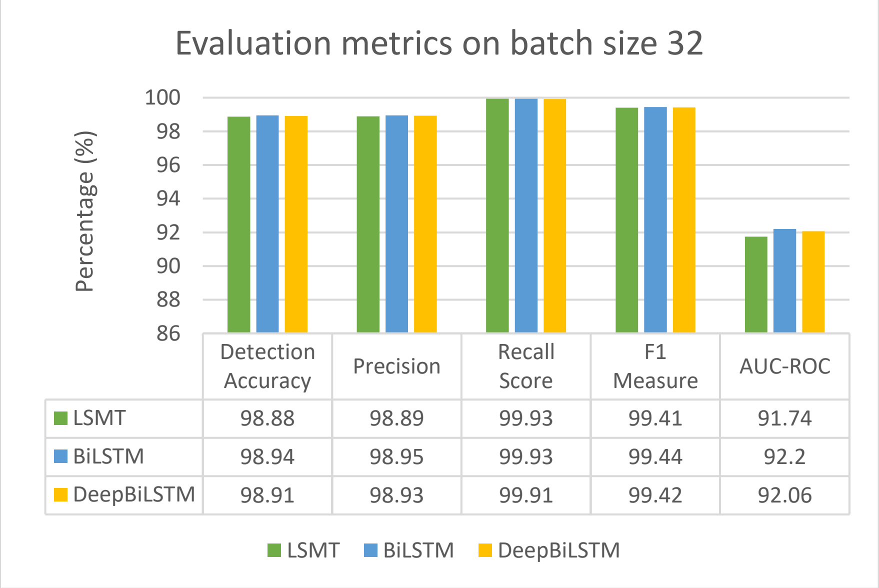
$$Recall\ = Detection\ Rate\ = \frac{TP}{TP + FN} \times 100\% \qquad (5)$$

$$F1 - measure\ \ = 2 * \frac{Precision * recal}{Precision + recall} \times 100\% \qquad (6)$$

5. Discussion and Results

In this sub-section, the metrics of the evaluation are used, which were described in Section 4.4 and apply them to the LSTM, BiLSTM, and Deep BiLSTM models and analyse their performances in depth. To study the influence of the variation of batch-size on generalization, convergence behavior and the overall dynamics of the model, we conducted experimental studies of the batch-sizes of 32, 64, 128, 256 and 512. The purpose of this comparison is to obtain more profound understanding of the effect of the batch size on the learning effectiveness and model performance. Because convergence stability, memory usage, and computational efficiency of deep learning models depend on batch size, cases of a proper choice are necessary during the training of deep learning models.

The experiments were carried out to determine a trade-off between computation cost and predictive performance. The analysis given points out significant issues in the training of LSTM-based models to detect threats in IoT networks. There are batch sizes of 32, 64, 128, 256, and 512 whose evaluation results are shown in Figure 3, 4, 5, 6 and 7, respectively.



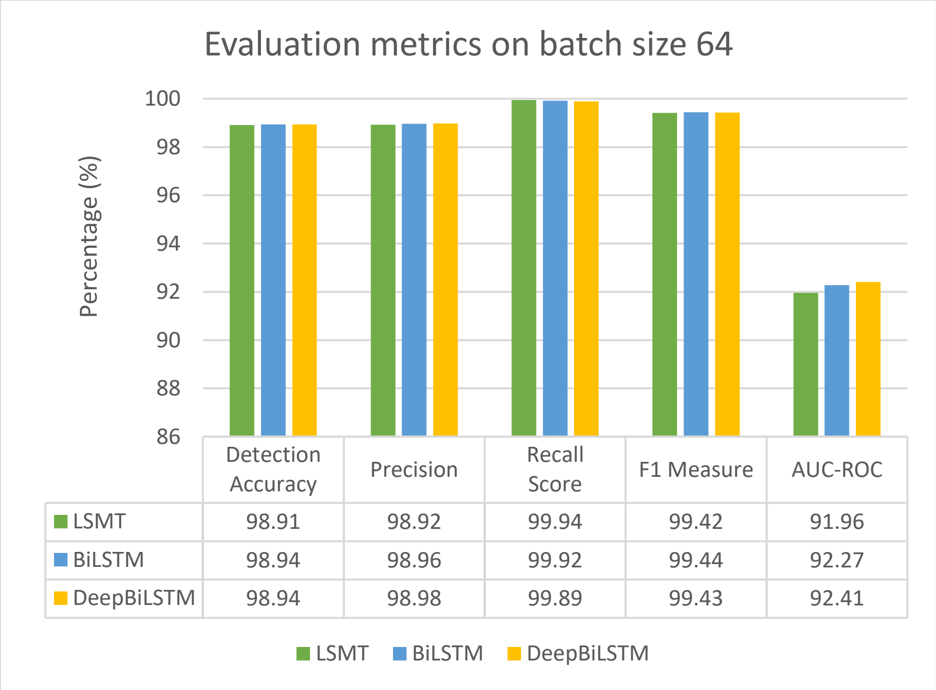
	Detection Accuracy	Precision	Recall Score	F1 Measure	AUC-ROC
🟩 LSMT	98.88	98.89	99.93	99.41	91.74
🟦 BiLSTM	98.94	98.95	99.93	99.44	92.2
🟨 DeepBiLSTM	98.91	98.93	99.91	99.42	92.06

Figure 3. Evaluation metrics on a batch size 32

All batch sizes (32, 64, 128, 256, and 512) display a high rate of detection ([98.8%-99.0%), high level of precision, and near-perfect recall values ([99.9%) that assumes the LSTM, BiLSTM and DeepBiLSTM models are efficient in detecting attack instances with minimal occurrence of false negatives. DeepBiLSTM typically outperforms LSTM and BiLSTM in the vast majority of the settings, and especially at larger batch sizes, it has the highest F1-scores and the most predictive stability.

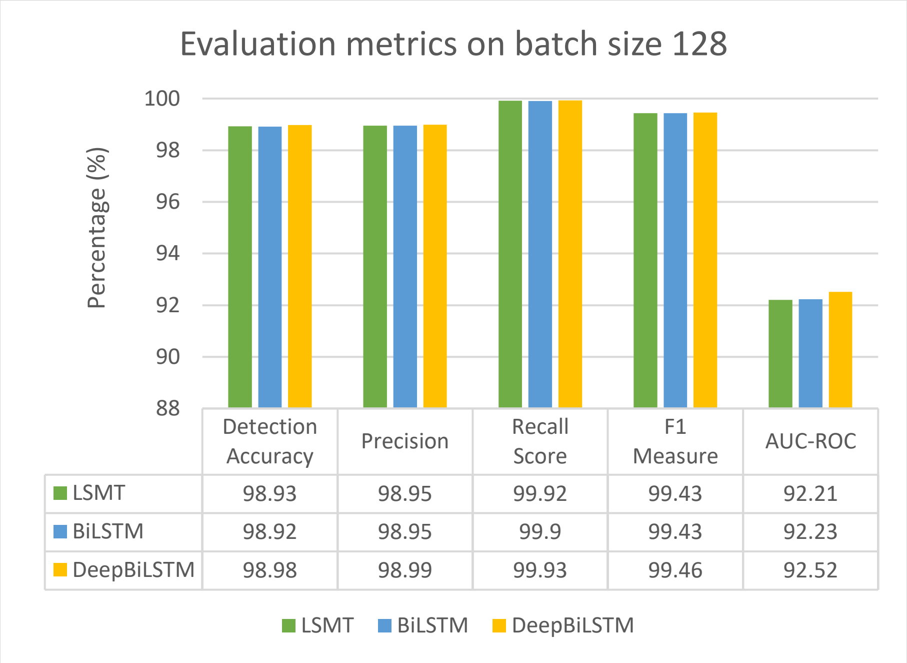
Whereas AUC-ROC values continue to maintain a 92% range with smaller batch sizes, the values are significantly stronger with larger batch sizes, particularly with DeepBiLSTM in which discriminatory strength is seen to be stronger between attack and benign traffic. The stability in performance is independent of configuration and indicates that the batch size does not significantly affect the detection ability, and the models are stable and can be scaled to process large IoT data.

The consistency in these findings in configurations poses that the batch size does not have a great impact on detection and the implication is that these models are scalable and can receive large volumes of IoT properly. In general, the obtained comparative outcomes support the research aims by showing that the three architectures are all relevant to the detection of IoT attacks, but Deep Bi-LMST demonstrates a better robustness, generalization ability and discrimination capacity, especially in large-scale setting. This provides the basis for research objectives in terms of the differences in robustness, generalization and discrimination capability of LSTM-based variants.



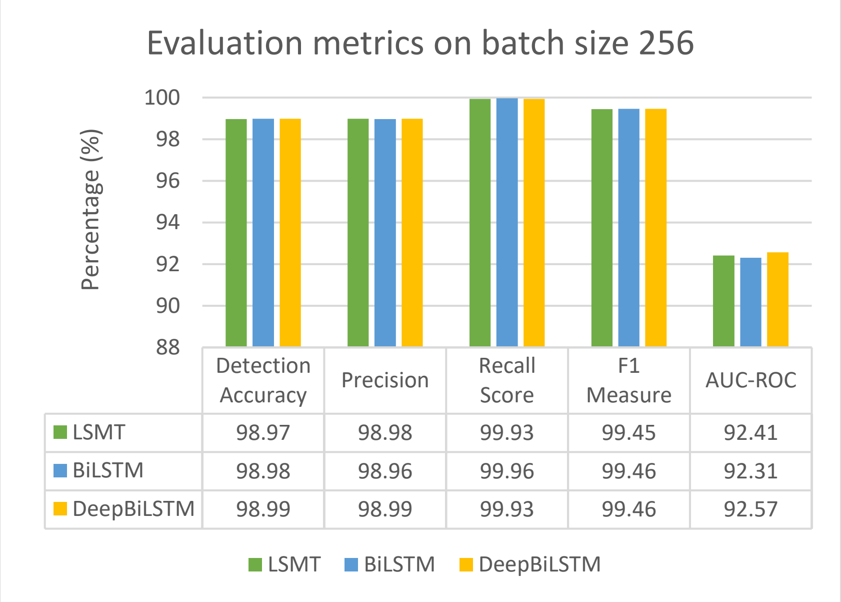
	Detection Accuracy	Precision	Recall Score	F1 Measure	AUC-ROC
🟩 LSMT	98.91	98.92	99.94	99.42	91.96
🟦 BiLSTM	98.94	98.96	99.92	99.44	92.27
🟨 DeepBiLSTM	98.94	98.98	99.89	99.43	92.41

Figure 4. Evaluation metrics on a batch size 64



	Detection Accuracy	Precision	Recall Score	F1 Measure	AUC-ROC
🟩 LSMT	98.93	98.95	99.92	99.43	92.21
🟦 BiLSTM	98.92	98.95	99.9	99.43	92.23
🟨 DeepBiLSTM	98.98	98.99	99.93	99.46	92.52

Figure 5. Evaluation metrics on batch size 128



	Detection Accuracy	Precision	Recall Score	F1 Measure	AUC-ROC
🟩 LSMT	98.97	98.98	99.93	99.45	92.41
🟦 BiLSTM	98.98	98.96	99.96	99.46	92.31
🟨 DeepBiLSTM	98.99	98.99	99.93	99.46	92.57

Figure 6. Evaluation of metrics on batch size 256

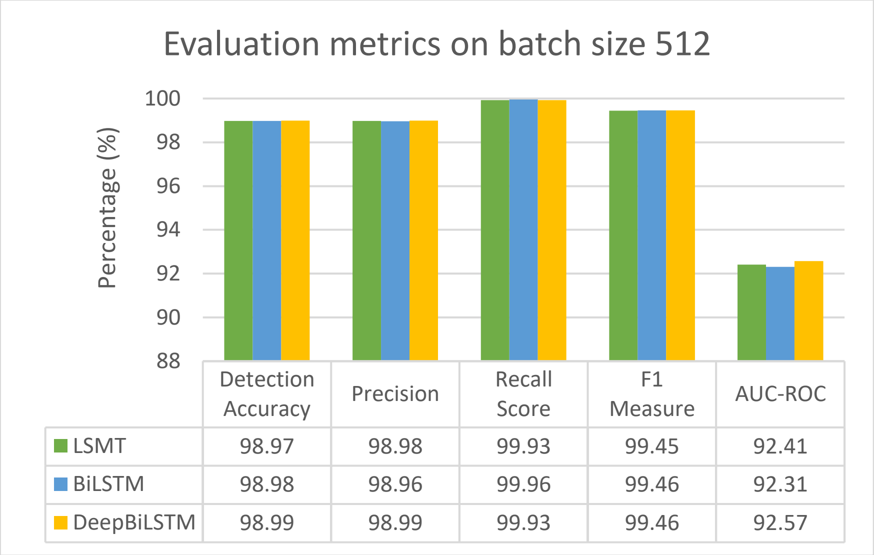


Figure 7. Evaluation metrics on batch size 512

6. Conclusion

The results of this paper have proven the applicability of deep learning models in the detection of attack in IoT settings and create a large possibility of using deep learning technologies to improve cybersecurity in the IoT networks. Based on the IoT-BoTnet 2020 dataset, the three recurrent neural network architectures, namely LSTM, BiLSTM, and Deep BiLSTM, were compared to each other following the main performance measures, such as accuracy, precision, recall, F1-score, and AUC-ROC. The three models were found to be highly effective in the intrusion-detection work which means that they can be used in protecting the IoT networks. Further studies on the scalability and robustness of these models under the influence of more complicated and diverse IoT data are required. It is desirable to include more attack scenarios with varying conditions of a network to have a more comprehensive insight into the strength and flexibility of each model. As well, these deep learning techniques need to be made more transparent and practical in the real-world setting by enhancing their model interpretability. Future research can also look at how the performance of RNN-based intrusion detection systems is impacted by the feature-selection methods.

References

1. A. Y. Areiqat, “Empowering women through digital transformation: Case studies in enhancing gender equality in business leadership,” in Business Development via AI and Digitalization, A. Hamdan and A. Harraf, Eds., Cham, Switzerland: Springer, 2024, pp. 1087–1092, doi: 10.1007/978-3-031-62106-2_82.
2. A. Al Sarayreh, R. J. Kutieshat, R. M. I. Almajali, S. I. Mohammad, A. A. Al-Tit, and M. Y. Abo Keir et al., “Examining the effects of gamified human resource management on job performance of IT startups,” in Frontiers of Human Centricity in the Artificial Intelligence-Driven Society 5.0 (Studies in Systems, Decision and Control, vol. 226), S. Reyad and A. Hannoon, Eds., Cham, Switzerland: Springer, 2024, pp. 203–216, doi: 10.1007/978-3-031-73545-5_18.
3. A. A. Alsmadi, I. A. Abu-AlSondos, K. I. Al-Daoud, and S. H. Aldulaimi, “Sustainable decision-making in fintech: Impact on sustainable development,” in Proc. 2024 Int. Conf. Decision Aid Sciences and Applications (DASA), Manama, Bahrain, Dec. 11–12, 2024, pp. 2165–2172, doi: 10.1109/DASA63652.2024.10836533.
4. S. A. Khattab, I. Shaar, L. Al Abbadi, A. Y. Kalbouneh, and W. B. Alhyasat, “The relationship between e-government effectiveness and e-government use: The mediating effect of online trust and the moderating effect of habit,” Journal of Theoretical and Applied Information Technology, vol. 102, no. 9, pp. 3917–3936, May 2024
5. R. Almajdoubah and O. Hasan, “Time and wavelength diversity schemes for transdermal optical wireless links,” International Journal of Electrical and Computer Engineering (IJECE), vol. 14, no. 6, pp. 6423–6432, Dec. 2024, doi: 10.11591/ijece.v14i6.pp6423-6432.
6. A. M. Ali, H. Abu Owida, and A. Al-Qerem, “Spectrum Serenade: OPNET Expedition Unveiling WLAN 802.11e Performance Evaluation,” in Proceedings of FTC 2024 (or relevant conference proceedings), 2024.
7. Iskandarani, M. Z. (2024, November). Communication analysis of wireless sensor networks with mobility function. In 2024 4th International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) (pp. 1-6). IEEE.
8. AlHija, M. A., Alqudah, H. J., & Dar-Othman, H. (2024). Uncovering botnets in IoT sensor networks: A hybrid self-organizing maps approach. Indonesian Journal of Electrical Engineering and Computer Science, 34(3), 1840-1857.
9. Ghazal, T. M., Hasan, M. K., Hassan, R., Safie, N., Abualhaj, M. M., & Ahmad, M. (2026). A prognosis-centric evaluation model for wearable sensor inputs in digital health intelligence. Biomedical Signal Processing and Control, 112, 108740.
10. Iskandarani, M. Z. (2024, October). Effect of Transmission Range and Grid Dimensions on Route Cost in WSN Using TABU Search Algorithm. In 2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE) (pp. 1-6). IEEE.
11. Alkhawatrah, M., AlAyyad, M., & Korostynska, O. (2025). Balanced inter-relay charging buffer-aided IOT networks. EURASIP Journal on Wireless Communications and Networking, 2025(1), 88.
12. Ali, A. M., Al-Qerem, A., Owida, H. A., & Abu-Khadrah, A. (2025, June). Comparative Performance Evaluation of WLAN 802.11 ac vs. 802.11 n for VoIP and HTTP Applications Using OPNET. In Intelligent Computing-Proceedings of the Computing Conference (pp. 391-405). Cham: Springer Nature Switzerland.
13. Alja'afreh, S. S., Altakhaineh, A. T., Al-shamaileh, M. H., Matarneh, A. M., Daoud, O. R., & Al-Khawaldah, M. (2024, April). A Dual-Port, and Single-Element Planar Inverted-F Antenna for Current 4G/5G Portable Applications. In 2024 21st International Multi-Conference on Systems, Signals & Devices (SSD) (pp. 750-754). IEEE.
14. Ali, A. M., & Hassan, M. R. (2024, March). Exceptional Mixed Real-Time Service Performance by Unleashing the Potential of 802.11 WLAN Technologies. In Future of Information and Communication Conference (pp. 246-267). Cham: Springer Nature Switzerland.
15. Awais, Z., Hussain, M., Elshenawy, A., Arsalan, A., Anwar, M., Habib, M. A., ... & Ahmad, M. (2025). ISCC: Intelligent Semantic Caching and Control for NDN-Enabled Industrial IoT Networks. IEEE Access.
16. Y. A. Maz, M. Anbar, S. Manickam, and M. M. Abualhaj, “Transfer Learning Approach for Detecting Keylogging Attack on the Internet of Things,” in Proc. 2024 4th Int. Conf. Emerging Smart Technol. Appl. (eSmarTA), Sana’a, Yemen, Aug. 2024, pp. 97–104, doi: 10.1109/eSmarTA62850.2024.10638915.
17. K. S. Pokkuluri, A. Kumar, K. K. S. Gautam, P. Deshmukh, P. G., and L. Abualigah, “Collaborative Intelligence for IoT: Decentralized Net Security and Confidentiality,” Journal of Intelligent Systems and Internet of Things, vol. 13, no. 2, pp. 202–211, 2024, doi: 10.54216/JISIoT.130216.
18. O. E. Elejla, M. Anbar, B. Belaton, and B. O. Alijla, “Flow-based IDS for ICMPv6-based DDoS Attacks Detection,”

Arabian Journal for Science and Engineering, vol. 43, no. 12, pp. 7757–7775, Mar. 2018, doi: 10.1007/s13369-018-3149-7.

19. Mosleh, A., Ahmad, A., Mohammad, O., Yousef, A., Mahran, A., & Mohammad, A. (2022). A paradigm for DoS attack disclosure using machine learning techniques. International Journal of Advanced Computer Science and Applications, 13(3).
20. A. Aldhaheri, F. Alwahedi, M. A. Ferrag, and A. Battah, "Deep learning for cyber threat detection in IoT networks: A review," Internet of Things and Cyber-Physical Systems, vol. 4, pp. 110–128, 2024, doi: 10.1016/j.iotcps.2023.09.003.
21. Abualhaj, M. M., Al-Khatib, S. N., Alsharaiah, M. A., & Hiari, M. O. (2024). Performance Comparison of Whale and Harris Hawks Optimizers with Network Intrusion Prevention Systems. Journal of Applied Data Sciences, 5(4), 1530-1538.
22. Ghazal, T. M., Hasan, M. K., Raju, K. N., Khan, M. A., Alshamayleh, A., Bhatt, M. W., & Ahmad, M. (2025). Data Space Privacy Model with Federated Learning Technique for Securing IoT Communications in Autonomous Marine Vehicles. Journal of Intelligent & Robotic Systems, 111(3), 84.
23. Y. A. Maz, M. Anbar, S. Manickam, M. M. Abualhaj, Sultan Ahmed Almalki, and Basim Ahmad Alabsi, “Transfer Learning-Based Approach with an Ensemble Classifier for Detecting Keylogging Attack on the Internet of Things,” Computers, materials & continua/Computers, materials & continua (Print), vol. 0, no. 0, pp. 1–10, Jan. 2025, doi: https://doi.org/10.32604/cmc.2025.068257.
24. Shorman, A. R., Alzubi, M., Almseidin, M., & Rateb, R. (2025). Adaptive Intrusion Detection for IoT Networks using Artificial Immune System Techniques: A Comparative Study. Journal of Robotics and Control (JRC), 6(2), 570-582.
25. Anbar, M., Abdullah, R., Saad, R. M., Alomari, E., & Alsaleem, S. (2016). Review of security vulnerabilities in the IPv6 neighbor discovery protocol. In Information Science and Applications (ICISA) 2016 (pp. 603-612). Singapore: Springer Singapore.
26. Mosleh M. Abualhaj, Sumaya N. Al-Khatib, Mahran Al-Zyoud, Iyas Qaddara, Mohammad O. Hiari, and Sultan Mesfer A. Aldossary, “Enhanced Network Communication Security Through Hybrid Dragonfly-Bat Feature Selection for Intrusion Detection," Journal of Communications, vol. 20, no. 5, pp. 607-618, 2025. Doi: 10.12720/jcm.20.5.607-618
27. Abu-Khadrah, A., AlMutairi, M. A., Hassan, M. R., & Ali, A. M. (2025, February). Enhancing IoT Security and Malware Detection Based on Machine Learning. In International Congress on Information and Communication Technology (pp. 561-571). Singapore: Springer Nature Singapore.
28. Anbar, M., Abdullah, R., Hasbullah, I. H., Chong, Y. W., & Elejla, O. E. (2016, December). Comparative performance analysis of classification algorithms for intrusion detection system. In 2016 14th annual conference on privacy, security and trust (PST) (pp. 282-288). IEEE.
29. Adawy, M., Abualese, H., El-Omari, N. K. T., & Alawadhi, A. (2024). Human-Robot Interaction (HRI) using Machine Learning (ML): a Survey and Taxonomy. International Journal of Advances in Soft Computing & Its Applications, 16(3).
30. M. M. Abualhaj, S. N. Al-Khatib, A. A. Abu-Shareha, O. Almomani, H. Al-Mimi, A. Al-Allawee, M. Sh. Daoud, and M. Anbar, “Spam Detection Boosted by Firefly-Based Feature Selection and Optimized Classifiers,” International Journal of Advances in Soft Computing and Its Applications (IJASCA), vol. 17, no. 3, pp. 1–19, 2025, doi: 10.15849/IJASCA.251130.01.
31. Owida, H. A., Al-Nabulsi, J., Al Hawamdeh, N., Abuowaida, S., Salah, Z., & Elsoud, E. A. (2024, November). Deep Learning-Based Kidney Disease Classification Using ResNet50: Enhancing Diagnostic Accuracy. In 2024 Second Jordanian International Biomedical Engineering Conference (JIBEC) (pp. 126-129). IEEE.
32. Sharma, C., Singh, G., Muttum, P. S., & Mahajan, S. (2024). CNN-FastText Multi-Input (CFMI) Neural Networks for Social Media Clickbait Classification. Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science), 17(6), 13-24.
33. Akram, N., Irfan, R., Al-Shamayleh, A. S., Kousar, A., Qaddos, A., Imran, M., & Akhunzada, A. (2024). Online recruitment fraud (ORF) detection using deep learning approaches. IEEE Access.
34. Ramaiah, M., Chandrasekaran, V., Chand, V., Vasudevan, A., & Ibrahim, S. (2024). Enhanced phishing detection: an ensemble stacking model with DT-RFECV and SMOTE. Applied Mathematics, 18(6), 1481-1493.
35. Vasudevan, A., Gandhimathi, K., Mohammad, S. I., Harsavarthini, M., Raja, N., & Hui, E. E. (2024). Predictive Maintenance for Vehicle Performance using Bidirectional LSTM. Appl. Math, 18(6), 1469-1479.
36. Iskandarani, M. Z. (2024). Application of Correlated Long-short Term Memory Algorithms for Intelligent Management

of Sensors (IMS LSTM). International Journal of Intelligent Engineering & Systems, 17(6).

37. Ali, A. M., Nashwan, S., Al-Qerem, A., Aldweesh, A., Alauthman, M., Elgamal, Z., & Almomani, A. (2024, February). CNNs in Crop Care: A Comparative Analysis of Tomato Disease Detection Models. In 2024 2nd International Conference on Cyber Resilience (ICCR) (pp. 1-5). IEEE.
38. C. Li et al., "An Anomaly Detection Approach Based on Integrated LSTM for IoT Big Data," Security and Communication Networks, vol. 2023, 2023.
39. P. Kaushik, "Unleashing the power of multi-agent deep learning: Cyber-attack detection in IoT," International Journal for Global Academic \& Scientific Research, vol. 2, no. 2, pp. 15–29, 2023.
40. B. A. Alabsi, M. Anbar, and S. D. A. Rihan, "Conditional Tabular Generative Adversarial Based Intrusion Detection System for Detecting DDoS and DoS Attacks on the Internet of Things Networks," Sensors, vol. 23, no. 12, p. 5644, 2023.
41. T. Acharya, A. Annamalai, and M. F. Chouikha, "Efficacy of Bidirectional LSTM Model for Network-Based Anomaly Detection," in 2023 IEEE 13th Symposium on Computer Applications \& Industrial Electronics (ISCAIE), 2023, pp. 336–341.
42. K. Saurabh et al., "LBDMIDS: LSTM Based Deep Learning Model for Intrusion Detection Systems for IoT Networks," in 2022 IEEE World AI IoT Congress (AIIoT), 2022, pp. 753–759.
43. M. S. Al-kahtani, Z. Mehmood, T. Sadad, I. Zada, G. Ali, and M. ElAffendi, "Intrusion detection in the Internet of Things using fusion of GRU-LSTM deep learning model," Intelligent Automation \& Soft Computing, vol. 37, no. 2, 2023.
44. B. A. Alabsi, M. Anbar, and S. D. A. Rihan, "CNN-CNN: Dual Convolutional Neural Network Approach for Feature Selection and Attack Detection on Internet of Things Networks," Sensors, vol. 23, no. 14, p. 6507, 2023.
45. W. D. C. Y. T. W. Y. S. T. L. Y. L. Jie Yin Yuxuan Shi, "Internet of Things Intrusion Detection System Based on Convolutional Neural Network," Computers, Materials \& Continua, vol. 75, no. 1, pp. 2119–2135, 2023, doi: 10.32604/cmc.2023.035077.
46. Hiari, M., Alraba'nah, Y., & Qaddara, I. (2025). A Deep Learning-Based Intrusion Detection System using Refined LSTM for DoS Attack Detection. Engineering, Technology & Applied Science Research, 15(4), 25627-25633.
47. Alraba'nah, Y., Al-Sharaeh, S., & Al Hindi, G. (2025). Enhancing Intrusion Detection Using Hybrid Long Short-Term Memory and XGBoost. Journal of Soft Computing and Data Mining, 6(1), 247-261.
48. Vasudevan, A., Albinaa, T. A., Mohammad, S. I., Sharmila, E., Raja, N., Soon, E. E. H., ... & Al-Adwan, A. S. (2024). Bidirectional LSTM for electronic product recommendation. Appl. Math. Inf. Sci., 18(6), 1443-1453.
49. Agrawal, N. M., Cheitanya, H. B., Rai, A. K., & Mahajan, S. (2024). Bidirectional LSTM for Heart Arrhythmia Detection. Integrating Metaheuristics in Computer Vision for Real-World Optimization Problems, 243-251.
50. Alasadi, A. A. I., Manjula, S., Smerat, A., Govindu, K., Sivakumar, G., & Sahasranamam, V. (2025). Mathematically Modified Deep Learning Model Assisted Handwritten Digit Recognition for Intelligent Document Processing Systems.
51. Tarek, R., Elshenawy, A., Assadwy, M. I., & Madkour, M. A. (2025). Automated Diagnosis of Dental Diseases Using Deep Learning on Radiographic Images. SN Computer Science, 6(6), 751.
52. J. Sinha and M. Manollas, "Efficient Deep CNN-BiLSTM Model for Network Intrusion Detection," in Proceedings of the 2020 3rd International Conference on Artificial Intelligence and Pattern Recognition, New York, NY, USA: ACM, Jun. 2020, pp. 223–231. doi: 10.1145/3430199.3430224.
53. J. Burdack, F. Horst, S. Giesselbach, I. Hassan, S. Daffner, and W. I. Schöllhorn, "Systematic Comparison of the Influence of Different Data Preprocessing Methods on the Performance of Gait Classifications Using Machine Learning," Front Bioeng Biotechnol, vol. 8, Apr. 2020, doi: 10.3389/fbioe.2020.00260.
54. Hassan, M., & Arabiat, A. (2024). An evaluation of multiple classifiers for traffic congestion prediction in Jordan. Indonesian Journal of Electrical Engineering and Computer Science, 36(1), 461-468.
55. Al-Mimi, H., Hamad, N. A., Abualhaj, M. M., Daoud, M. S., Al-Dahoud, A., & Rasmi, M. (2023). An Enhanced Intrusion Detection System for Protecting HTTP Services from Attacks. International Journal of Advances in Soft Computing & Its Applications, 15(3).
56. Al-Mimi, H., Hamad, N. A., Abualhaj, M. M., Al-Khatib, S. N., & Hiari, M. O. (2023). Improved intrusion detection system to alleviate attacks on DNS service. Journal of Computer Science, 19(12), 1549-1560.
57. R. Alabdallat, M. Abualhaj, and A. Abu-Shareha, “Enhanced Multiclass Android Malware Detection Using a Modified Dwarf Mongoose Algorithm”, International Journal of Analysis and Applications, vol. 23, pp. 1–23, Jan. 2025, doi:

https://doi.org/10.28924/2291-8639-23-2025-0.

58. Mosleh M. Abualhaj, Sumaya N. Al-Khatib, Ahmad A. Abu-Shareha, Abdallah Hyassat, and Mohammad Sh. Daoud, "Smart Firewall for Phishing Detection Powered by Bio-Inspired Algorithms," Journal of Advances in Information Technology, Vol. 16, No. 11, pp. 1529-1539, 2025. doi: 10.12720/jait.16.11.1529-1539
59. Y. Sanjalawe, S. Fraihat, S. Al-E'mari, M. M. Abualhaj, S. Makhadmeh, and E. Alzubi, "Smart load balancing in cloud computing: Integrating feature selection with advanced deep learning models," PLOS One, vol. 20, no. 9, Sep. 2025, Art. no. e0329765. DOI: 10.1371/journal.pone.0329765.
60. Al-Nabulsi, J., Ahmad, M. A. S., Hasaneiah, B., & AlZoubi, F. (2024, November). Diagnosis of Knee Osteoarthritis Using Bioimpedance & Deep Learning. In 2024 Second Jordanian International Biomedical Engineering Conference (JIBEC) (pp. 1-5). IEEE.
61. C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet Detection in the Internet of Things using Deep Learning Approaches," in 2018 International Joint Conference on Neural Networks (IJCNN), IEEE, Jul. 2018, pp. 1–8. doi: 10.1109/IJCNN.2018.8489489.
62. B. Roy and H. Cheung, "A Deep Learning Approach for Intrusion Detection in Internet of Things using Bi-Directional Long Short-Term Memory Recurrent Neural Network," in 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), IEEE, Nov. 2018, pp. 1–6. doi: 10.1109/ATNAC.2018.8615294.
63. R. Alabdallat, M. Abualhaj, and A. Abu-Shareha, "Android Malware Detection Using a Modified Dwarf Mongoose Algorithm," International Journal of Intelligent Engineering and Systems, vol. 18, no. 8, 2025, Art. no. ijies2025.0930.21. DOI: 10.22266/ijies2025.0930.21.
64. Abualhaj, M. M., Al-Khatib, S. N., Alsharaiah, M. A., & Hiari, M. O. (2024). Performance Comparison of Whale and Harris Hawks Optimizers with Network Intrusion Prevention Systems. Journal of Applied Data Sciences, 5(4), 1530-1538.
65. Ibrahim, A., Gatzoulis, C., Eid, M. M., Rizk, F. H., Abualigah, L., & El-kenawy, E. S. M. (2024, July). Regression Models for Predicting Gamified Educational Outcomes. In 2024 International Telecommunications Conference (ITC-Egypt) (pp. 537-542). IEEE.
66. Al-Ghraibah, A., Al-Abbas, A., Kmainasi, M. B., Mustafa, I. E., & Brmo, K. (2024, November). Automated Detection of Lung Cancer Levels Based on Patient's Lifestyle Information. In 2024 Second Jordanian International Biomedical Engineering Conference (JIBEC) (pp. 22-27). IEEE.