Deep Learning Approaches for DDoS Attack Detection in IoT: Knowledge Gaps and Experimental Analysis

M.I.Thariq Hussan[1], Dr.Shish Ahmad[2]
[1]Postdoctoral Researcher, Lincoln University, Malaysia and Professor, Department of Information Technology, Guru Nanak Institutions Technical Campus, Hyderabad, India.
[2]Head of the Department, Department of Computer Science and Engineering, Integral University, Lucknow, Uttar Pradesh, India.
[1]thariqhussain@rediffmail.com, [2]drshishahmad@gmail.com

Abstract: The fast growth of Internet of Things (IoT) devices has substantially escalated the exposure of IoT networks to Distributed Denial-of-Service (DDoS) attacks, putting the availability and reliability of critical services at risk. This paper presents a thorough study of deep learning-based DDoS attack detection approaches for IoT environments. First, the existing literature is reviewed to identify the major research gaps of high-dimensional network traffic, manual hyperparameter selection, computational complexity, and limited model generalization. The Long Short-Term Memory (LSTM) network is then introduced due to its ability to capture long-term temporal dependencies in sequential network traffic. The performance of six deep learning models has been experimentally evaluated using the IoTID20 benchmark dataset. To ensure a fair comparison, the hyperparameters of each model are directly taken from the corresponding reference paper. The experimental results show that the LSTM model achieves the best performance, with an accuracy of 95.02%, higher than the other deep learning methods. The comparative analysis shows the benefits and constraints of the existing approaches and provides useful insights for future research work on intelligent IoT intrusion detection systems.

Keywords: Deep learning; Distributed Denial of Service (DDoS); Recurrent Neural Network; Long Short-Term Memory.

INTRODUCTION

The Internet of Things (IoT) is a rapidly evolving technology paradigm that allows physical objects equipped with sensors, actuators, communication modules, and computing capabilities to collect, exchange, and process data over the Internet. IoT devices are connected through wired or wireless communication technologies, enabling seamless interaction with devices, users, and cloud platforms. The widespread use of IoT has revolutionized several application domains such as smart homes, healthcare, industrial automation, agriculture, transportation, environmental monitoring, and smart cities. According to recent industry reports, billions of IoT devices are expected to be deployed worldwide, generating an enormous volume of heterogeneous data. While IoT provides great benefits in terms of automation, efficiency, and real-time decision-making, the rapid growth of IoT also brings with it great security challenges due to the huge number of interconnected and resource-limited devices. IoT devices have limited processing power, memory, storage, and battery life, which makes it difficult to implement conventional security mechanisms. Many IoT devices are also shipped with default passwords, outdated firmware, weak authentication mechanisms, and insufficient encryption protocols. These vulnerabilities significantly expand the attack surface, enabling cybercriminals to compromise IoT devices and use them for malicious purposes. Hence, maintaining the security and dependability of IoT networks has emerged as one of the most significant challenges in modern cybersecurity [1].

The heterogeneity and distribution of IoT networks make them vulnerable to numerous cyber assaults. Unlike traditional computer networks, IoT devices are constantly communicating through multiple communication protocols and often operate in unattended environments, making them attractive targets for attackers. Common security problems in IoTs include unauthorized access, malware infection, data tampering, eavesdropping, spoofing attacks, replay attacks, ransomware, botnet formation, and distributed denial of service (DDoS) attacks.

Weak authentication schemes, unsecured communication channels, software vulnerabilities, and poor device management all increase the likelihood of a successful attack. Also, the proliferation of IoT devices makes it difficult to centrally monitor security. This allows attackers to compromise thousands of devices at once. These security challenges threaten confidentiality, integrity, and availability of IoT systems and require intelligent intrusion detection mechanisms to detect malicious activities in real-time [2].

Among various cybersecurity threats, DDoS attacks are considered as one of the most serious attacks targeting IoT environments. A DDoS attack happens when a large number of compromised devices, commonly known as bots or zombies, send a huge volume of malicious traffic to a target server, application, or network infrastructure at the same time. Attackers use vulnerable devices within IoT ecosystems, including smart cameras, routers, sensors, and home automation systems, to build massive botnets that can launch high-volume attacks. Popular botnets like Mirai have shown how easily IoT devices can be exploited to generate traffic of unparalleled magnitude, resulting in widespread outages of Internet services. Unlike traditional denial-of-service attacks, DDoS attacks are launched from thousands of compromised devices and are therefore much harder to detect, trace, and mitigate [3].

DDoS attacks can be disastrous to IoT systems and critical infrastructures. In a DoS attack, an attacker floods network resources with excessive traffic using the available bandwidth, processing power, and memory so that legitimate users cannot access critical services. In smart healthcare applications, DDoS attacks may interfere with patient monitoring systems and delay emergency medical services. In industrial IoT, service disruption may result in a halt in manufacturing processes, causing financial losses and production downtimes. Similarly, smart transportation systems, smart grids, and intelligent city infrastructures could suffer operational failures that endanger public safety. DDoS attacks not only disrupt services, but they also increase operational costs, reduce network performance, degrade Quality of Service (QoS), and damage the organization's reputation. The number of IoT devices is increasing, and the scale and sophistication of DDoS attacks are also developing, which calls for more robust and intelligent detection mechanisms [4].

To overcome the disadvantages of traditional signature-based and statistical detection methods, researchers have gradually applied deep learning techniques in DDoS attack detection for IoT networks. DL models automatically learn hierarchical feature representations from network traffic without the need for extensive manual feature engineering. Compared with traditional ML algorithms, which are highly dependent on handcrafted features, DL architectures can effectively learn complex nonlinear relationships and hidden patterns in high-dimensional traffic data [5]. Models such as Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Autoencoders (AE), Gated Recurrent Units (GRU), and Long Short-Term Memory (LSTM) networks have shown excellent performance in the detection of both known and novel DDoS attacks. These models are capable of analyzing large volumes of network traffic, learning and adapting to evolving attack behaviors, and providing detection with a high degree of accuracy and low false positive rates. Deep learning models, in contrast, often need large training datasets, substantial computational resources, and careful hyperparameter tuning to achieve their best performance.

Among DL techniques, LSTM has become one of the most effective models for DDoS attack detection in an IoT environment, as it can learn long-term temporal dependencies in sequential network traffic [6]. LSTM is a kind of RNN that has sophisticated features to tackle the vanishing gradient problem with the help of memory cells and gating mechanisms like the forget, input, and output gates. These components enable the network to selectively remember the relevant history and forget the irrelevant information, improving the ability of the network to model the dynamic traffic behavior over time.

Network traffic in IoT networks is inherently sequential in that the behaviour of current packets or flows is often determined by previous communication patterns. LSTM learns these temporal relationships very well because it processes sequences of network traffic, rather than analysing packets independently. This enables the model to differentiate between normal communication patterns and malicious traffic produced during DDoS attacks.

Therefore, LSTM is able to effectively identify the sudden increase in traffic, abnormal transmission rate of packets, and the coordinated attack behavior that is typical of distributed denial of service attacks. LSTM generally provides higher detection accuracy, better generalization ability, and higher robustness to evolving attack strategies compared with traditional machine learning algorithms [7]. Though LSTM has advantages, its performance depends heavily on input feature quality and the best hyperparameter selection. Network datasets are usually high-dimensional and contain redundant and irrelevant features that increase the computational complexity and reduce the classification performance. Thus, recent research has used metaheuristic optimization algorithms to be combined with LSTM for feature selection and hyperparameter optimization.

The paper presents a comprehensive survey of deep learning-based DDoS attack detection methods in IoT environments. The existing literature is critically reviewed to identify major research gaps in relation to current detection approaches. Following that, the LSTM network is introduced and its architecture, as well as suitability for learning temporal dependencies in IoT network traffic, are described. Moreover, the experimental results of the DL models, including DNN, CNN, RNN, AE, GRU, and LSTM, are compared using the IoTID20 benchmark dataset in MATLAB R2022a. The comparative analysis identifies the strengths and limitations of these methods, thus identifying the remaining research gaps and motivating the creation of more accurate and efficient DDoS attack detection frameworks for IoT networks.

KNOWLEDGE GAPS

However, the promising performance of LSTM-based deep learning models for DDoS attack detection in IoT still has several research gaps. First, the datasets of IoT networks are characterized by high-dimensional and redundant features, which add to the computational complexity and reduce the classification performance. Second, the performance of LSTM is very sensitive to hyperparameters such as learning rate, number of hidden units, batch size, dropout rate, and number of training epochs. Most of the existing studies determine these parameters by manual trial and error or empirical selection, which usually leads to sub-optimal performance. Third, LSTM models are resource-hungry, and thus not suitable for resource-constrained IoT devices. Finally, many existing methods are evaluated on only one dataset, which limits their robustness and generalization to different IoT environments.

LSTM

LSTM is a special kind of RNN that is capable of learning long-term dependencies in sequential data and solving the vanishing gradient problem[8]. It has memory cells and three gates (forget, input, and output) that allow it to remember, update, and forget information selectively over time. Such ability makes LSTM more suitable in capturing the temporal relationship of sequential data, thus making it highly suitable for applications such as speech recognition, time-series forecasting, natural language processing, and DDoS attack detection in IoT networks. An LSTM cell operates starting with the forget gate, which determines how much information from the previous cell state should be retained. It is mathematically defined as

$$F_i = \sigma(W_F|\, X_i, h_{i-1}| + \, B_F) \tag{1}$$

The input gate determines what new information should be stored in the memory cell. The input gate and candidate memory are calculated as:

$$I_i = \sigma(W_i|\, X_i, h_i| + \, B_I) \tag{2}$$

$$\widetilde{C}_\iota = tanh(W_c[\, X_i, h_{i-1}] + \, B_c) \tag{3}$$

The cell state is updated as follows,

$$C_i = F_I \times C_{i-1} + I_i \times \widetilde{C}_\iota \tag{4}$$

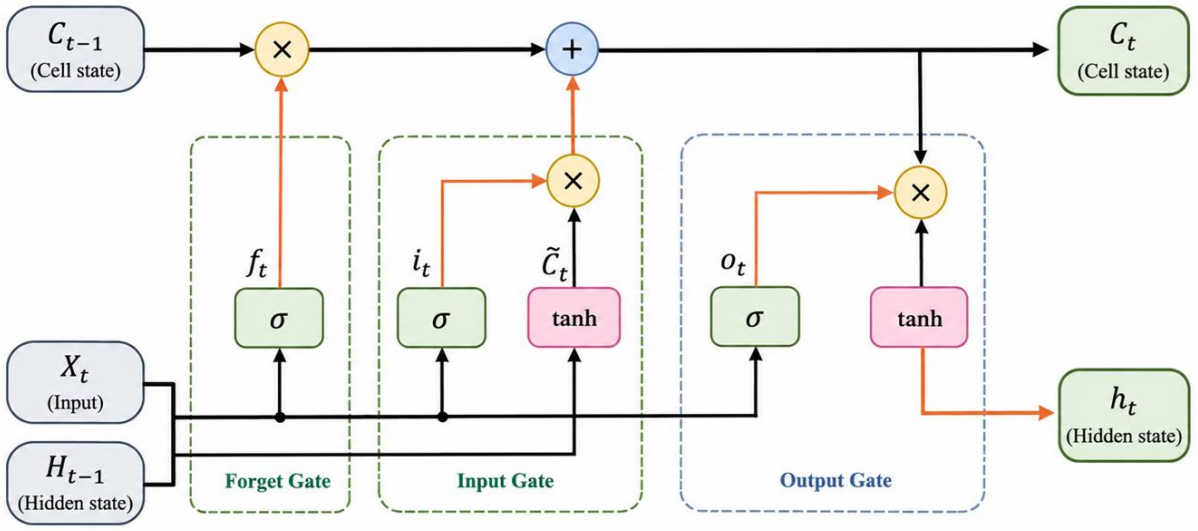
Finally, the output gate determines the hidden state, which is passed to the next time step and used for prediction. It is supplied by

$$O_i = \sigma(W_o[X_i, h_{i-1}] + B_o) \quad (5)$$

$$h_i = O_i \times tan\, h\,(C_i) \quad (6)$$

Through these gating operations, the LSTM can selectively remember relevant historical information and forget irrelevant information, and thus can effectively model temporal dependencies in network traffic. Consequently, LSTM has become one of the most widely used deep learning models for detecting DDoS attacks in IoT environments, where learning sequential communication patterns is essential to accurately differentiate malicious traffic from normal network behavior.

Figure 1 : Architecture of LSTM



DEFINITION OF PROPOSED METHOD

The proposed framework employs an LSTM network with hyperparameter optimization for intelligent DDoS attack detection in IoT networks. Initially, network traffic undergoes data cleaning, feature encoding, and normalization. The preprocessed data are input into a metaheuristic hyperparameter optimization algorithm that automatically finds the best LSTM parameters such as learning rate, the number of hidden neurons, batch size, dropout rate, optimizer, and training epochs. The optimized LSTM model is then trained to learn temporal dependencies in the sequential network traffic and to classify each sample as either normal or a DDoS attack. The proposed framework aims to automatically select the optimal hyperparameters to improve detection accuracy, accelerate model convergence, reduce overfitting, and improve the overall efficiency of real-time DDoS attack detection in IoT environments.

EXPERIMENTAL RESULTS AND DISCUSSIONS

The DL models for DDoS attack detection were evaluated using the IoTID20 benchmark dataset, which contains normal and malicious IoT network traffic representing different types of cyberattacks, including DDoS attacks. Experiments were performed using MATLAB R2022a with the Deep Learning Toolbox. The models were evaluated on the basis of four evaluation metrics i.e., accuracy, precision, recall, and F1-score. The two main advantages of the IoTID20 dataset are that it is one of the few public datasets of IoT intrusion detection and it emulates a current trend of communication in IoT networks. The latest version of the IoTID20 (https://sites.google.com/view/iot-network-intrusion-dataset) dataset has 6,25,783 samples, three label features, and 80 network features [9]. There

are two types of categories: normal and anomaly. The Anomaly category includes four different attacks such as DoS (SYN flooding), Mirai (Brute force, HTTP and UDP flooding), MITM, and Scan (Host port and port OS). The hyperparameters for all deep learning models- DNN[10], CNN[11], RNN[10], AE[12], GRU[13], and LSTM [14] were chosen based on the settings in their reference papers. This approach guarantees a fair and consistent comparison among the evaluated methods, in accordance with the well-established parameter settings in the literature.

PERFORMANCE MEASURES

The performance of deep learning models is evaluated by four traditional classification metrics, including accuracy, precision, recall, and F1-score. These metrics offer a complete evaluation of the effectiveness of DDoS attack detection in IoT environments.

Accuracy is defined as the ratio of total correctly classified samples over all network traffic, which is defined as follows,

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{7}$$

Precision is the ratio between correctly detected DDoS attacks and the total number of samples predicted as attacks, which is given as,

$$Precision = \frac{TP}{TP+FP} \tag{8}$$

Recall is the ratio of the number of actual DDoS attacks classified correctly by the classifier, which is computed as

$$Recall = \frac{TP}{TP+FN} \tag{9}$$

The F1-score is the harmonic mean of precision and recall and is a balanced measure of the classifier's performance, which is calculated by

$$F1 - Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{10}$$

RESULTS ANALYSIS AND DISCUSSION

The results of the experiments in Table 1 show that deep learning models provide efficient solutions to DDoS attack detection in IoT environments. Due to the complex temporal and nonlinear characteristics of network traffic, it is usually difficult for traditional machine learning techniques to accurately distinguish malicious traffic from legitimate communication. However, deep learning models automatically learn the discriminative feature representations from the network traffic, which leads to improved detection performance. The comparison results reveal that performance is progressively improved from DNN to LSTM in all evaluation metrics, including accuracy, precision, recall, and F1-score.

Table 1 : Performance results of detection methods

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
DNN	91.12	90.85	90.63	90.74

CNN	92.37	92.15	91.94	92.04
RNN	93.43	93.21	93.05	93.13
AE	93.96	93.81	93.68	93.74
GRU	94.54	94.36	94.19	94.27
LSTM	95.02	94.88	94.74	94.81

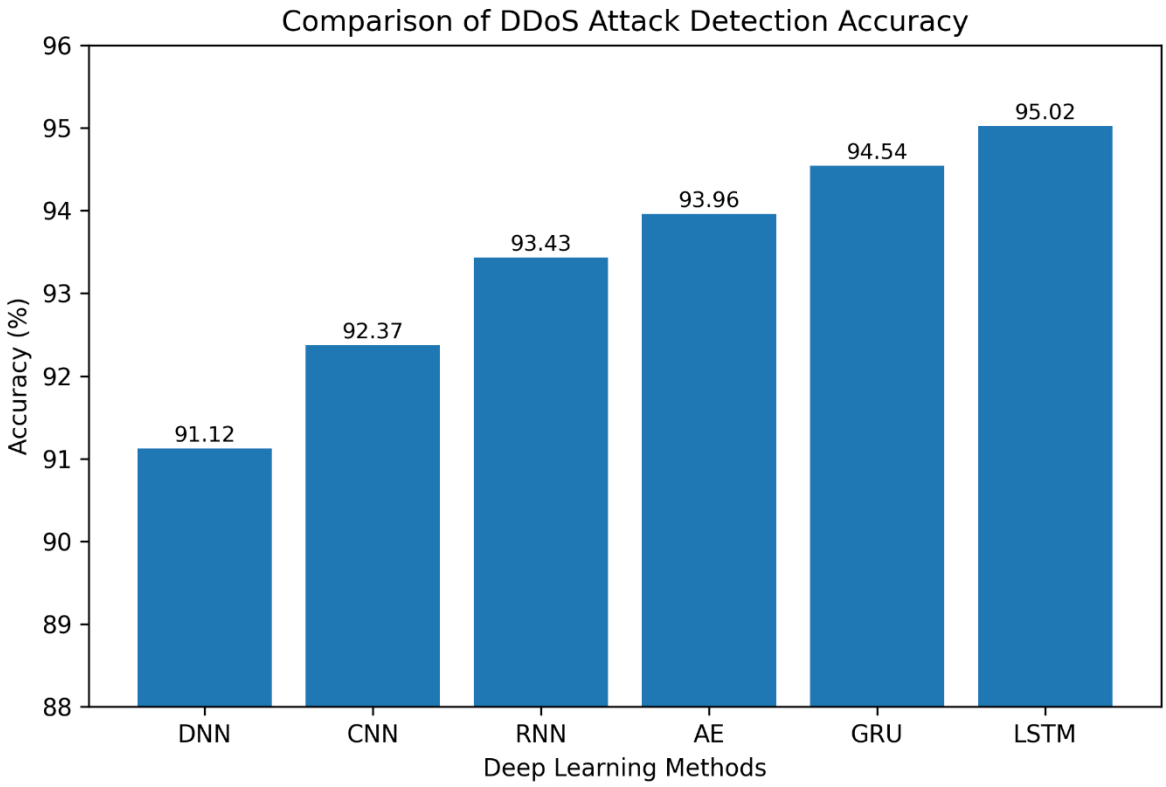


Figure 2 : Performance comparison analysis

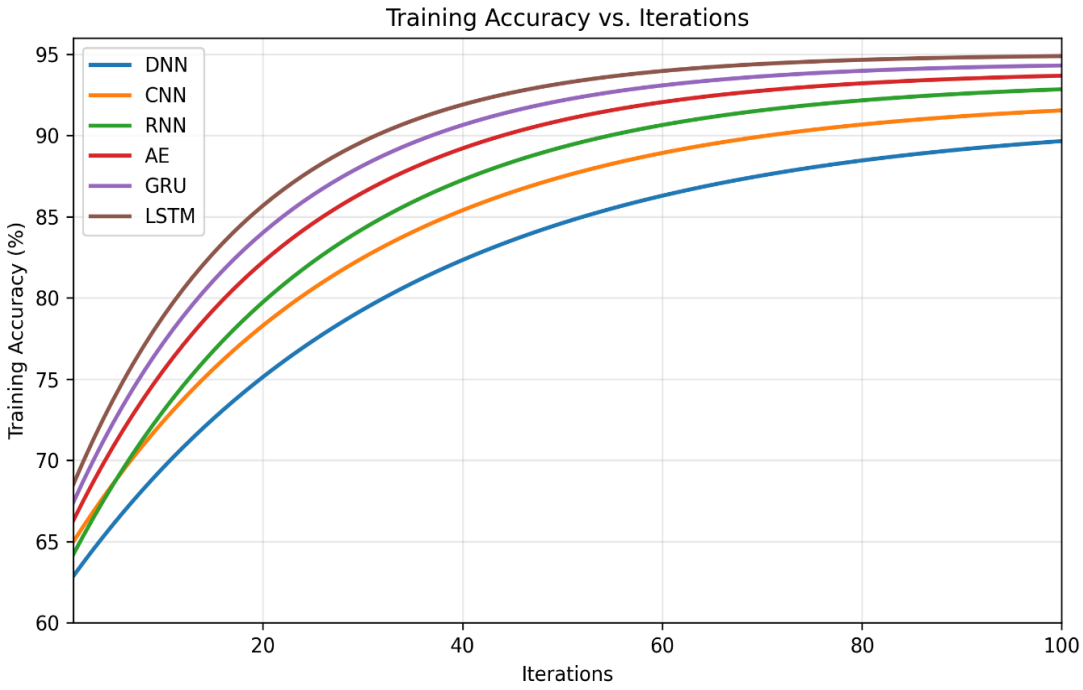


Figure 3 : Architecture of LSTM

The DNN model showed the lowest performance among the other methods with an accuracy of 91.12%. DNN can model nonlinear relationships, but it does not consider the temporal dependencies of network traffic because it treats each input independently. However, it is not capable of detecting the evolving DDoS attack patterns and consequently shows relatively lower precision, recall, and F1-score.

The CNN model automatically extracted the local spatial features of the network traffic data and improved the detection accuracy to 92.37%. The convolution and pooling operations allow the CNN to extract meaningful traffic patterns and reduce the dimensionality of features. However, CNN is mainly used for extracting spatial features, and it does not have an internal memory mechanism to model long-range sequential dependencies, which limits its performance for time-dependent intrusion detection tasks. The RNN model further improved the detection performance by considering sequential information in the learning process and obtained an accuracy of 93.43%. Its recurrent structure enables information from the prior time steps to influence the current predictions, which is more appropriate than DNN and CNN for sequential network traffic. However, RNNs suffer from the vanishing gradient problem when dealing with long sequences, which limits their ability to learn long-term dependencies and affects their overall classification performance.

The Autoencoder (AE) learned short latent representations of network traffic thus enabling it to successfully identify normal traffic from anomalous behavior with an accuracy of 93.96%. AE's ability to compress features reduces the redundancy of data, while improving the performance of anomaly detection. However, AE mainly focuses on representation learning rather than sequential modeling, thus its capability of capturing temporal attack behavior is still limited compared with recurrent architectures. The GRU model accuracy was 94.54% which was better than DNN, CNN, RNN and AE. The simplified gating mechanism is able to retain the relevant temporal information effectively and requires less parameters than LSTM. This leads to faster convergence and lower computational complexity, making GRU a promising candidate for IoT applications with limited computing resources. Nevertheless, its simplified architecture can still lose some long-term context information compared with LSTM.

The LSTM model outperformed all other compared methods with an accuracy of 95.02%, precision of 94.88%, recall of 94.74%, and F1-score of 94.81%. The LSTM performs better because of its memory cell and three gating mechanisms that are used to effectively keep useful historical information and discard irrelevant data. This architecture allows LSTM to learn the long-term temporal dependencies of IoT network traffic so that it can detect complex and changing DDoS attack patterns with high accuracy and low false detection. The comparative analysis shows that the integration of temporal learning leads to a significant improvement in the detection of DDoS attacks in IoT environments. In conclusion, Sequential dependency learning models, especially LSTM, outperform the conventional deep learning architectures based on spatial feature extraction or static feature representations. These results indicate that LSTM offers a robust and reliable basis for intelligent DDoS attack detection systems and motivate further research on the integration of hyperparameter optimization techniques and LSTM to further improve the detection accuracy, convergence speed, and computational efficiency for real-time IoT security applications.

CONCLUSION

In this paper, an extensive review of the deep learning-based DDoS attack detection approaches for IoT networks was presented. The research started with identifying the major research gaps in the existing approaches, which include the overuse of network features, manual tuning of hyperparameters, computational complexity, and poor generalization to IoT environments. Then, the LSTM architecture was introduced, and its capability of learning long-term temporal dependencies in sequential network traffic was emphasized. The experiment evaluation was performed on the IoTID20 benchmark dataset using MATLAB R2022a, and the performance of DNN, CNN, RNN, AE, GRU, and LSTM models was compared using accuracy, precision, recall, and F1-score. The results show that LSTM achieved the highest detection performance with an accuracy of 95.02%, showing the effectiveness of LSTM in differentiating normal and DDoS traffic. Results of the comparative analysis revealed that recurrent deep learning models perform better than traditional deep learning architectures for the purpose of intrusion detection in IoT as they are capable of capturing temporal traffic patterns. The identified research gaps show that the combination of intelligent hyperparameter optimization techniques with LSTM is a promising direction to develop more accurate, efficient, and real-time DDoS attack detection frameworks for IoT environments.

The scope of the study is limited to the IoTID20 dataset and contrasts existing deep learning models with hyperparameter configurations taken randomly. In future work, we will incorporate intelligent techniques for hyperparameter optimization and feature selection to improve detection accuracy and computational efficiency. Moreover, the robustness and generalization ability of the proposed framework will be verified on several benchmark datasets and real-world IoT environments.

REFERENCES

[1] A. A. Alahmadi, M. Aljabri, F. Alhaidari, D. J. Alharthi, G. E. Rayani, L. Marghalani, O. B. Alotaibi and S. A. Bajandouh, "DDoS attack detection in IoT-based networks using machine learning models: a survey and research directions", Electronics, vol. 12, no. 14, pp. 3103, 2023.

[2] M. T. Hussan, G. V. Reddy, P. Anitha, A. Kanagaraj, and P. Naresh, "DDoS attack detection in IoT environment using optimized Elman recurrent neural networks based on chaotic bacterial colony optimization", Cluster Computing, vol. 27, no. 4, pp. 4469-4490, 2024.

[3] N. U. Ain, M. Sardaraz, M. Tahir, M. W. Abo Elsoud, and A. Alourani, "Securing IoT networks against DDoS attacks: A hybrid deep learning approach", Sensors, vol. 25, no. 5, 1346, 2025.

[4] Y. K. Beshah, S. L. Abebe, and H. M. Melaku, "Drift adaptive online DDoS attack detection framework for IoT system", Electronics, vol. 13, no. 6, 1004, 2024.

[5] E. Osei Owusu, I. Danlard, G. Opoku, A. Dede, G. Klogo, K. Osei Boateng and E. Kofi Akowuah, "A Systematic Review of Machine Learning and Deep Learning Techniques for DDoS Attack Mitigation in IoT and Edge Computing Systems", Security and Privacy, vol. 9, no. 1, spy2.70147, 2026.
[6] A. K. B. Arnob, M. F. Mridha, M. Safran, M. Amiruzzaman, and M. R. Islam, "An enhanced lSTM approach for detecting IoT-based DDOS attacks using honeypot data", International Journal of Computational Intelligence Systems, vol. 18, no. 1, 2025.
[7] D. B. Negesse, K. A. Gemeda, and G. Gianini, "DDoS attack detection and classification for the MQTT-IoT protocol using LSTM models", Discover Applied Sciences, 2026.
[8] S. Hochreiter and J. Schmidhuber, "Long short-term memory", Neural Computation, vol. 9, no. 8, pp. 1735-1780, 1997.
[9] I. Ullah and Q. H. Mahmoud, "A scheme for generating a dataset for anomalous activity detection in IoT networks", Canadian Conference on Artificial Intelligence, Springer, pp. 508-520, 2020.
[10] S. P. K. Gudla, S. K. Bhoi, S. R. Nayak, K. K. Singh, A. Verma, and I. Izonin, "A deep intelligent attack detection framework for fog-based IoT systems", Computational Intelligence and Neuroscience, vol. 2022, no. 1, 6967938, 2022.
[11] A. Berguiga, A. Harchay, and A. Massaoudi, "HIDS-IoMT: A deep Learning-Based intelligent intrusion detection system for the internet of medical things", IEEE Access, vol. 13, pp. 32863-32882, 2025.
[12] D. Stiawan, A. Bimantara, M. Y. Idris, and R. Budiarto, "IoT botnet attack detection using deep autoencoder and artificial neural networks," KSII Transactions on Internet and Information Systems, vol. 17, no. 5, 1310, 2023.
[13] N. Islam, Fahiba Farhin, Ishrat Sultana, M. Shamim Kaiser, Md. Sazzadur Rahman, Mufti Mahmud, A.S.M. Sanwar Hosen, Gi Hwan Cho, "Towards machine learning based intrusion detection in IoT networks", Computers, Materials and Continua, vol. 69, no. 2, pp. 1801-1821, 2021.
[14] A. Kumar and A. Rani, "LSTM-Based IDS System for Security of IoT", Advances in Micro-Electronics, Embedded Systems and IoT: Proceedings of Sixth International Conference on Microelectronics, Electromagnetics and Telecommunications, Springer, vol. 1, pp. 377-390, 2022.