Deep Learning Utilization for DDoS Attack Detection with Federated Learning: A Case Study on the CICDDoS2019 Dataset

Ayoub Alsarhan
Department of Data Science and Artificial Intelligence, Faculty of Information Technology, Al-Ahliyya Amman University, Jordan | Department of Information Technology, The Hashemite University, Zarqa, Jordan
ayoubm@hu.edu.jo (corresponding author)

Malek Barhoush
IT Department, Cybersecurity Program, IT&CS Faculty, Yarmouk University, Irbid, Jordan
malek@yu.edu.jo

Bashar Khassawneh
Department of Computer Science, Faculty of Information Technology, Amman Arab University, Amman, Jordan
b.khassawneh@aau.edu.jo

Malik Al-Essa
Computer Science Department, King Abdullah II School for Information Technology, University of Jordan, Jordan
m.alessa@ju.edu.jo

Mohammad Aljaidi
Department of Computer Science, Zarqa University, Zarqa, Jordan
mjaidi@zu.edu.jo

Qais Al-Na'amneh
Department of Cyber Security, Applied Science Private University, Jordan
q_naamneh@asu.edu.jo

Received: 16 August 2025 | Revised: 1 October 2025 | Accepted: 9 October 2025

 DOI: https://doi.org/10.48084/etasr.14119

ABSTRACT

Modern systems are highly susceptible to Distributed Denial of Service (DDoS) attacks, which often cause major service interruptions and financial losses. These attacks have become more frequent and sophisticated due to the unexpected explosion in the use of wireless technologies, making them more challenging to detect with traditional methods. In this paper we investigate the effective detection of DDoS attacks using deep learning, specifically within a federated learning architecture. The CICDDoS2019 dataset was used to train and evaluate the proposed intrusion detection scheme. Federated learning trains models on several dispersed servers or devices while maintaining local data, thereby preserving user privacy and enabling collaborative learning across clients. The results demonstrate that Federated Deep Learning (FDL) outperforms conventional machine learning algorithms such as Random Forest (RF), Support Vector Machines (SVM), and Recurrent Neural Networks (RNNs), achieving 98% detection accuracy. In addition, the proposed method improves recall and reduces false positives, making it ideal for real-time intrusion detection in dynamic environments.

Keywords-DDoS detection; deep learning; federated learning; IoT

I. INTRODUCTION

DDoS attacks pose a significant challenge to the advancement of the information technology sector and are becoming increasingly advanced and complex. Such attacks strive to flood the network and servers with enormous traffic and may cause serious service and financial losses [1, 2]. DDoS attacks attempt to exhaust system resources and significantly decrease service availability [3, 4]. Unfortunately, most security solutions that are available today cannot detect and prevent DDoS attacks in real time [5, 6]. The required detection systems that will make it possible to detect DDoS attacks in real-time have to be powerful enough to identify patterns of attack in huge and dynamic network data [7]. Wireless technology has become prolific, and this has led to an incredible increase in the number of DDoS attacks [8]. With the increasing levels of sophistication in DDoS attacks, the existing security mechanisms face a challenge to detect the attacks promptly and effectively [9, 10].

One interesting method to enhance DDoS attack detection is to combine the approaches of Deep Learning (DL) models with Federated Deep Learning (FDL) [11, 23]. FDL is a distributed data source technique that is used in real life situations without compromising user privacy [11, 13]. This paper considers the application of DL in detecting DDoS attacks, referencing it through the prism of FDL. The CICDDoS2019 dataset is used to train and test our model.

Several Machine Learning (ML) algorithms have been used to detect the DDoS attacks [14, 15], but they often involve the processing of data in a centralized location, raising concerns regarding data security. One potential solution to this challenge is FDL, a method that allows training the algorithm without sharing raw data. FDL is an ML method that involves many users (typically called the clients) jointly training models without sharing their local data [12]. Instead of transmitting the raw data to a central server, clients transmit changes to their local model (gradients), which are aggregated to optimize a global model. As a decentralized method, it not only enhances data privacy, but it also decreases the central server load. The contributions of this work include the following:

- This work introduces FDL as a novel approach for collaboratively training DL models across multiple platforms while preserving data privacy. FDL enables the aggregation of model updates from multiple clients (e.g., IoT devices, mobile phones, or edge nodes) to refine a global model under the coordination of a central server. By leveraging FDL, this work ensures privacy protection while enhancing the accuracy of attack detection, offering a valuable solution for privacy-preserving, and large-scale DDoS detection.
- An analysis of FDL's performance in detecting DDoS attacks is provided.
- An extensive evaluation is conducted using a recent dataset, demonstrating that the proposed approach outperforms traditional Intrusion Detection Systems (IDSs). The results show that the proposed FDL method produces higher classification accuracy, proving its efficiency and effectiveness in DDoS detection.

II. RELATED WORK

In [3], a hybrid classifier is proposed to detect DDoS attacks on the edge or switches of Software-Defined Network (SDN)-IoT. Nevertheless, several concerns have been identified. Firstly, it has an excessive load on data plane switches. Secondly, the model has not been tested using live SDN-IoT traffic. Thirdly, the dataset utilized in the research is outdated and lacks traces of IoT. Moreover, the research does not incorporate any of the mitigation strategies, noting that detection of attacks alone is not sufficient without mitigation strategies. Two methods were proposed in [4] for DDoS attack detection. The first proposed method uses a hybrid IDS to detect IoT-DoS attacks. The second method is based on DL, namely Long Short-Term Memory (LSTM). To avoid DDoS attacks within an SDN-IoT system, authors in [8] propose an ML-based detection and mitigation system. The control layer of the SDN in the proposed design is essential in securing the IoT network due to the implementation of a robust IDS that prevents intrusions. The IDS is enhanced with the use of a feature selection-based system categorization methodology, which enhances its resistance to DDoS attacks, making the whole system much more secure. Authors in [9] proposed the adapted (AMLSDM) structure. The AMLSDM framework suggests an SDN-enabled protection scheme of IoT which is efficient in detecting and countering DDoS attacks via a new ML classifying model. Examining the static features of the network traffic under inspection, the adaptive multilayer feedback structure of the framework within the context of ML algorithms enables the success of recognizing the DDoS attacks. Authors in [10] proposed a comprehensive framework of the SD-IoT. It is composed of an SD-IoT controller and SD-IoT switches that cooperate with the IOC gateway and IoT devices. Building off this framework, a DL-based method is integrated to enhance its detection capabilities. Authors in [7] propose a new DL-based technique that allows detecting DDoS attacks on IoT networks. The model examines the characteristic values of various DDoS attack types along with the minimum number of natural traffic. Authors in [14] propose a learning-based method to detect malicious traffic quickly in the controller and data planes. The experimental results stress the effectiveness of the suggested scheme to detect the low-rate DDoS attack traffic.

III. FEDERATED LEARNING FOR DETECTING DDOS ATTACKS IN IOT

DL models show exceptional performance in detecting complex patterns within network traffic that may indicate a DDoS attack. Artificial neural networks, especially Convolutional Neural Networks (CNNs) and RNNs have been successfully applied in various attack detection scenarios. CNN models are effective at detecting spatial patterns in network traffic. When applied to DDoS detection, CNNs can automatically extract features from traffic data and classify them as benign or malicious traffic. Since network traffic is often temporal in nature, RNNs (particularly LSTM networks) are effective in capturing time dependencies in the data, which are crucial for detecting slow and sophisticated DDoS attacks.

Instead of training a central model with data from all sources, FDL allows multiple clients to train a local model on their own traffic data and only share model updates. FDL is an ML paradigm that allows multiple clients (such as IoT devices, mobile phones, or edge nodes) to collaboratively train a model under the coordination of a central server [12]. Each client computes updates to the model locally based on its private data, and these updates are sent to the server. To refine the global model, the updates are aggregated by the server. This allows training DL models while preserving data privacy.

A. Federated Learning Algorithm

Let N denote the number of clients in the federated learning network. The global model θ^{t+1} is updated after every communication round t, where θ^{t+1} is an integer denoting the round number. Each client i has its own data set D_i, and the goal is to learn a global model θ that minimizes the global loss function $\mathcal{L}(\theta)$. $\mathcal{L}(\theta)$ is the sum of all clients' local loss functions. FDL is implemented for DL training by performing the following steps:

1) Local Model Update

To calculate model updates, every client i utilizes its local data D_i. For client i, the local modeling update is calculated by:

$$\theta_i^{t+1} = \theta^t - \eta \nabla_\theta \mathcal{L}_i(\theta^t, D_i) \quad (1)$$

where η is the learning rate and $\nabla_\theta \mathcal{L}_i(\theta^t, D_i)$ is the gradient of the local loss function $\mathcal{L}_i$ with respect to the model parameters θ^t at time t.

2) Aggregation

Once all clients compute their local updates θ_i^{t+1}, the central server aggregates these updates to form the new global model. The aggregation step typically uses Federated Averaging (FedAvg), where the global model is updated as a weighted average of the local updates:

$$\theta^{t+1} = \sum_{i=1}^{N} \frac{n_i}{N} \theta_i^{t+1} \quad (2)$$

where n_i is the number of data points on client i and N is the total number of data points across all clients.

3) Repeat

The process is repeated across several communication rounds until the global model reaches convergence.

B. Deep Learning Models for Traffic Classification

DL models that classify traffic on network flows as benign or malicious can be trained to identify DDoS attacks. Features such as packet size, protocol type, and packet arrival rates can be used as input to the model. The goal is to use these features to identify unusual traffic patterns that may indicate a DDoS attack. In a federated learning setting, each client could represent a network node or an edge device with local traffic data. The model could be a CNN, LSTM network, or even transformers, depending on the data's characteristics.

Let the objective be to minimize the global loss function $\mathcal{L}(\theta)$, which measures the error between the predicted class (benign or malicious) and the true label of traffic instances:

$$L(\theta) = \frac{1}{|D|} \sum_{x_i \in D} \text{Loss}(f(x_i, \theta), y_i) \quad (3)$$

where x_i represents the input features of network traffic (e.g., packet size, arrival time, IP addresses), y_i is the true label of the traffic (benign or DDoS attack), $f(x_i, \theta)$ is the model's prediction for the input x_i, and Loss(.) is a loss function, commonly cross-entropy loss for classification tasks.

For a binary classification task (benign or DDoS attack), the loss function is computed as follows:

$$Loss(f(x_i, \theta), y_i) = -(y_i \log(f(x_i, \theta)) + (1 - y_i) \log(1 - f(x_i, \theta))) \quad (4)$$

Federated learning for DDoS attack detection involves decentralized data distribution, where data from each client D_i represent network traffic at different locations or times. This ensures the data are decentralized. The model architecture can incorporate convolutional and recurrent layers that can learn network traffic patterns both over time and space. Federated averaging enhances the global model and makes it more generalizable to all conditions within the network by averaging the updates of each of the clients. Due to the fact that the clients are not required to share their raw traffic data, federated learning in DDoS mitigation is beneficial since privacy is preserved in serious settings. It is also scalable and does not require central data storage. FDL training is conducted across different devices or geographies. Additionally, it is adaptable to local network conditions since federated learning has features that allow customization to different circumstances, significantly enhancing detection accuracy. Lastly, the methodology spares bandwidth and communication costs as the updates of the model are included independently.

C. Utilization and Preprocessing of the CICDDoS2019 Dataset for Deep Learning–Based DDoS Detection

To address the challenge of DDoS detection, the widely used CICDDoS2019 [16] dataset, consisting of 162,590 records with 88 features, was used to test and train the proposed scheme. The dataset provides traffic statistics labelled as benign and DDoS malicious. The dataset contains categories of features that enable training and testing. These categories include: timing-related data, flow statistics, and packet headers. The primary characteristics of the CICDDoS2019 dataset are:

- Diversity: For simulating actual attack patterns, the dataset has a variety of DDoS attack methods such as HTTP floods, UDP floods, DNS amplifications, etc.
- Granularity: It is suitable for ML since a flow is described using a set of variables such as packet size, flow duration, and source/destination IP.
- Realistic Traffic: For enabling the development of precise detection models, the dataset includes realistic traffic from legitimate users and attack traffic.

The dataset was split into a training set of 110,729 instances (≈70%) and a testing set of 47,456 instances (≈30%). It should be noted that the dataset is heavily biased toward DDoS traffic and does not include other attack types, reflecting its suitability for evaluating models focused specifically on DDoS detection.

The raw data of the CICDDoS2019 dataset require preprocessing before training the models. Data preprocessing involves removing columns with missing or incomplete data, as they can negatively impact model performance. Attributes like, Fwd Pkts/b Avg, Fwd Byts/b Avg, and Fwd Blk Rate Avg, which contain zero values in most records, were eliminated to ensure effective model training. Raw data preprocessing involves the following steps:

- Feature Selection: Choosing appropriate features enables describing network behavior precisely. These features include: flow duration, packet length, and traffic.
- Normalization: To enhance the training process, all features are scaled to a standard range. The min-max normalization method is applied to transform feature values into the range [0,1]. Normalization ensures that all features share a common scale, preventing extreme values from adversely affecting the performance of the deep learning model and improving its capability to detect intrusions effectively.
- Label Encoding: Assigning binary labels for attack and normal traffic to facilitate supervised learning.
- Data Splitting: The dataset was divided into training (70%) and testing sets (30%) to evaluate model performance.

IV. RESULTS AND DISCUSSION

Analysis of the resulting confusion matrix in Figure 1 indicates that the model achieves high detection performance, with the majority of attacks correctly classified while maintaining a low false-positive rate for benign traffic, demonstrating the model's reliability in distinguishing between normal and malicious network behavior.

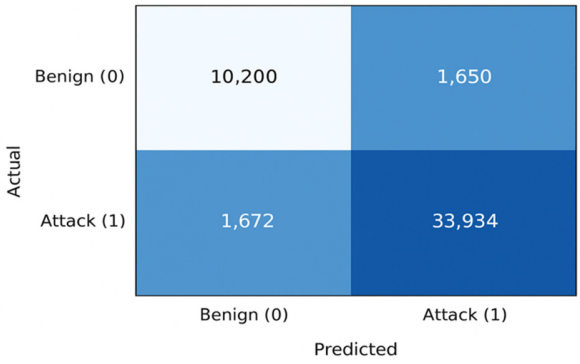

Fig. 1. Confusion matrix of the CIC-DDoS201.

The evaluation metrics employed to assess the classifier's performance are:

$$\text{Accuracy} = \frac{T_p+T_n}{T_p+F_p+T_n+F_n} \quad (5)$$

$$\text{Precision} = \frac{T_p}{T_p+F_p} \quad (6)$$

$$\text{Recall} = \frac{T_p}{T_p+F_n} \quad (7)$$

$$\text{F1-score} = \frac{2.\text{Recal.Precision}}{\text{Recal+Precision}} \quad (8)$$

where T_p is the number of True Positives, T_n is the number of True Negatives, F_p is the number of False Positives, and F_n is the number of False Negatives.

We evaluated the proposed approach (FDL) against SVM, RNN, and RF ML techniques. Figure 2 shows the accuracy of all considered methods. It can be seen that FDL achieves the highest accuracy at 98%, followed by RNN. It is notable that FDL performs better than the conventional classifiers. The uniqueness of the FDL approach lies in its ability to directly discover the hierarchy structures and extract complex features within raw data in an automatic way which is crucially important in the detection of complex DDoS behavior.

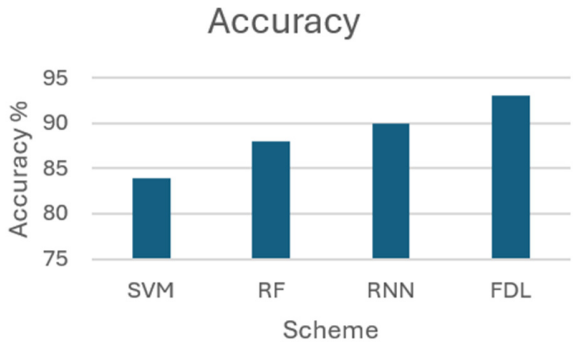

Fig. 2. Accuracy comparison.

One of the most critical parameters in detecting attacks is precision that measures the proportion between true positives and total positive predictions to minimize the number of false positives. Figure 3 shows that FDL outperforms the other classifiers in terms of precision. Due to the advanced feature extraction properties, FDL is able to detect DDoS attacks with high precision. It also reduces the risk of misclassification because it effectively identifies the subtle characteristics and complexity of DDoS attacks.

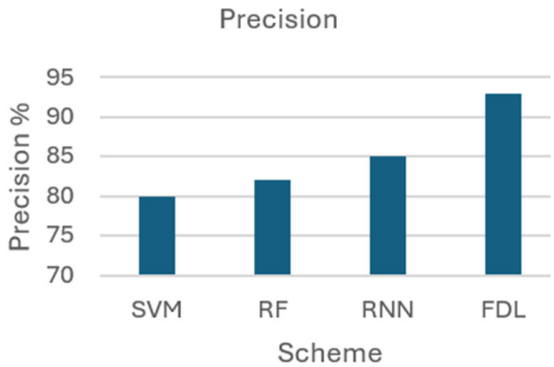

Fig. 3. Precision comparison.

Recall is critical in DDoS detection as failure to recognize genuine attacks may lead to severe security breaches. Figure 4 shows that the FDL model excels in detecting DDoS attacks in term of recall. Although RNN, SVM, and RF may be competitive models, the DL technique is more effective than

the former three since it can recognize complex patterns and correlations in large datasets, which results in a more sturdy and reliable detection capacity.

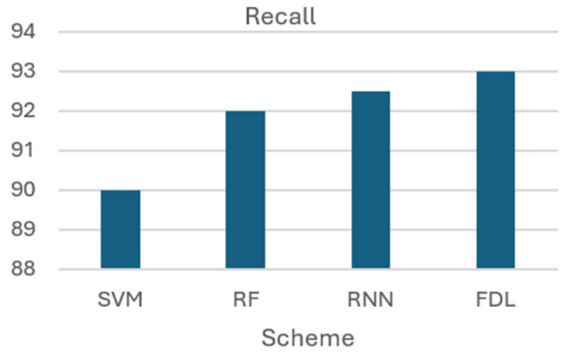

Fig. 4. Recall comparison.

In term of F1-score, Figure 5 illustrates that the FDL model again outperforms the others. F1-score is an essential parameter when assessing the overall performance of the model. The FDL model has a higher F1-score, with the benefit of having fewer false positives (high precision), and identifying a higher percentage of real DDoS attacks (high recall). The FDL technique is superior and effective as a detection system in comparison to the other models due to its competence in detecting complex patterns in the data.

The results indicate that an IDS can effectively detect DDoS attacks through the federated learning model when conditioned on the basis of real-time response. The technology of federated learning also promotes the collaborative security approach, which allows multiple agents to enhance the model while ensuring the security of their data confidentiality.

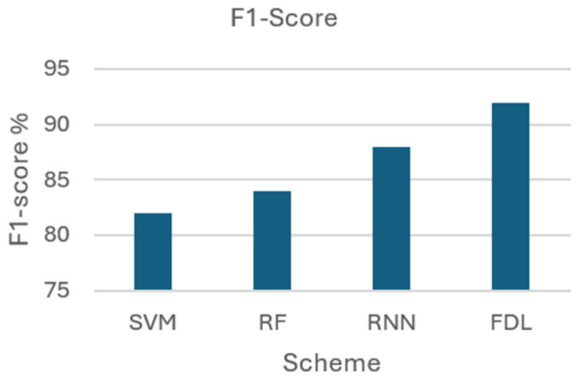

Fig. 5. Comparison of F-measure across the detection schemes.

V. CONCLUSION

In this paper, we introduced and evaluated the FDL model for DoS attack detection and compared it to more traditional machine learning algorithms. The findings indicate that the proposed model outperforms the other classifiers in several crucial aspects like accuracy, precision, recall, and F1-score.

The fact that FDL has minimal false positives and retains high positive rates is crucial for real time attacks detection. As compared to the traditional approaches, FDL is a consistent and stable detection system. The joint improvement of the model is also feasible due to the federated learning integration where different groups are able to alter the system without the loss of data privacy.

Overall, the FDL approach is an effective method for timely and accurately recognizing DDoS attacks. Nevertheless, much needs to be done to address the flexibility and the effectiveness of DDoS detection systems where it remains burdensome to remain centered on the augmentation of federated learning techniques such as model consolidation tech and client selection plans.

REFERENCES

[1] A. Alnatsheh *et al.*, "Machine Learning-Based Approach for Detecting DDoS Attack in SDN," in *2023 2nd International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI)*, Zarqa, Jordan, Sep. 2023, pp. 1–5, https://doi.org/10.1109/EICEEAI60672.2023.10590313.

[2] A. Sanmorino, L. Marnisah, and H. D. Kesuma, "Detection of DDoS Attacks using Fine-Tuned Multi-Layer Perceptron Models," *Engineering, Technology & Applied Science Research*, vol. 14, no. 5, pp. 16444–16449, Oct. 2024, https://doi.org/10.48084/etasr.8362.

[3] P. Chauhan and M. Atulkar, "A Framework for DDoS Attack Detection in SDN-Based IoT Using Hybrid Classifier," in *Machine Learning, Image Processing, Network Security and Data Sciences*, Singapore, 2023, pp. 889–900, https://doi.org/10.1007/978-981-19-5868-7_67.

[4] M. Shurman, R. Khrais, and A. Yateem, "DoS and DDoS Attack Detection Using Deep Learning and IDS," *The International Arab Journal of Information Technology*, vol. 17, no. 4A, pp. 655–661, Jul. 2020, https://doi.org/10.34028/iajit/17/4A/10.

[5] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting DDoS attacks: a systematic review," *Soft Computing*, vol. 27, no. 18, pp. 13039–13075, Sep. 2023, https://doi.org/10.1007/s00500-021-06608-1.

[6] H. M. Belachew, M. Y. Beyene, A. B. Desta, B. T. Alemu, S. S. Musa, and A. J. Muhammed, "Design a Robust DDoS Attack Detection and Mitigation Scheme in SDN-Edge-IoT by Leveraging Machine Learning," *IEEE Access*, vol. 13, pp. 10194–10214, 2025, https://doi.org/10.1109/ACCESS.2025.3526692.

[7] A. A. Alashhab, M. S. M. Zahid, A. Muneer, and M. Abdullahi, "Low-rate DDoS attack Detection using Deep Learning for SDN-enabled IoT Networks," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 13, no. 11, Nov. 2022, https://doi.org/10.14569/IJACSA.2022.0131141.

[8] K. J and A. L. R. P. J, "Mitigate Volumetric DDoS Attack using Machine Learning Algorithm in SDN based IoT Network Environment," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 14, no. 1, Jan. 2023, https://doi.org/10.14569/IJACSA.2023.0140161.

[9] M. Aslam *et al.*, "Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT," *Sensors*, vol. 22, no. 7, Mar. 2022, https://doi.org/10.3390/s22072697.

[10] J. Wang, Y. Liu, W. Su, and H. Feng, "A DDoS attack detection based on deep learning in software-defined Internet of things," in *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, Victoria, BC, Canada, Aug. 2020, pp. 1–5, https://doi.org/10.1109/VTC2020-Fall49728.2020.9348652.

[11] R. Doriguzzi-Corin and D. Siracusa, "FLAD: Adaptive Federated Learning for DDoS attack detection," *Computers & Security*, vol. 137, Feb. 2024, Art. no. 103597, https://doi.org/10.1016/j.cose.2023.103597.

[12] Y.-C. Lee, W.-C. Chien, Y.-C. Chang, Y.-C. Lee, W.-C. Chien, and Y.-C. Chang, "FedDB: A Federated Learning Approach Using DBSCAN for DDoS Attack Detection," *Applied Sciences*, vol. 14, no. 22, Nov. 2024, https://doi.org/10.3390/app142210236.

[13] Y. Alhasawi and S. Alghamdi, "Federated Learning for Decentralized DDoS Attack Detection in IoT Networks," *IEEE Access*, vol. 12, pp. 42357–42368, 2024, https://doi.org/10.1109/ACCESS.2024.3378727.

[14] H. Cheng, J. Liu, T. Xu, B. Ren, J. Mao, and W. Zhang, "Machine learning based low-rate DDoS attack detection for SDN enabled IoT networks," *International Journal of Sensor Networks*, vol. 34, no. 1, pp. 56–69, Jan. 2020, https://doi.org/10.1504/IJSNET.2020.109720.

[15] A. Alsarhan *et al.*, "Optimizing Cyber Threat Detection in IoT: A Study of Artificial Bee Colony (ABC)-Based Hyperparameter Tuning for Machine Learning," *Technologies*, vol. 12, no. 10, Sep. 2024, Art. no. 181, https://doi.org/10.3390/technologies12100181.

[16] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCST)*, Chennai, India, Jul. 2019, pp. 1–8, https://doi.org/10.1109/CCST.2019.8888419.