Low-rate DDoS attack Detection using Deep Learning for SDN-enabled IoT Networks

Abdussalam Ahmed Alashhab[1], Mohd Soperi Mohd Zahid[2], Amgad Muneer[3], Mujaheed Abdullahi[4]
Department of Computer and Information Science, Universiti Teknologi Petronas, Seri Iskandar, Malaysia[1, 2, 3, 4]
Faculty of Information Technology, Alasmarya Islamic University, Zliten, Libya[1]

***Abstract*—Software Defined Networks (SDN) can logically route traffic and utilize underutilized network resources, which has enabled the deployment of SDN-enabled Internet of Things (IoT) architecture in many industrial systems. SDN also removes bottlenecks and helps process IoT data efficiently without overloading the network. An SDN-based IoT in an evolving environment is vulnerable to various types of distributed denial of service (DDoS) attacks. Many research papers focus on high-rate DDoS attacks, while few address low-rate DDoS attacks in SDN-based IoT networks. There's a need to enhance the accuracy of LDDoS attack detection in SDN-based IoT networks and OpenFlow communication channel. In this paper, we propose LDDoS attack detection approach based on deep learning (DL) model that consists of an activation function of the Long-Short Term Memory (LSTM) to detect different types of LDDoS attacks in IoT networks by analyzing the characteristic values of different types of LDDoS attacks and natural traffic, improve the accuracy of LDDoS attack detection, and reduce the malicious traffic flow. The experiment result shows that the model achieved an accuracy of 98.88%. In addition, the model has been tested and validated using benchmark Edge IIoTset dataset which consist of cyber security attacks.**

***Keywords*—SDN; LDDoS attack; OpenFlow; Deep Learning; Long-Short Term Memory**

I. Introduction

Communication networks have significantly evolved, allowing users to connect with each other anytime, anywhere. The proliferation of various intelligent devices and applications is increasing demand and generating unprecedented traffic [1]. The increasing number of Internet-connected objects has made the IoT an increasingly important topic in recent years, and with the introduction of fifth-generation (5G) mobile networks, data traffic in communication networks is expected to increase by 20% in the next three years. The number of IoT devices will reach five billion by 2025 [2]. The exponential rise of the Internet of Things is driving the development of new advanced services with stricter criteria, including flexible administration and low latency. Emerging technologies such as SDN and Network Function Virtualization (NFV) are fundamental to the subsequent 5G mobile networks [3]. These technologies make the network more versatile in terms of hardware management and control, as more complex algorithms can be employed to administer the network and new features can be introduced with simple software updates. Traditional networks frequently require the deployment of vendor-specific hardware and proprietary software, and closed development, which hinder the introduction of new protocols and technologies in communication networks [4].

To achieve the integrated success that ensures the availability and high performance of advanced communications networks, advanced mechanisms must be developed to provide an adequate level of security to detect sophisticated cyberattacks. This is a significant challenge because IoT devices can handle sensitive data. Many low-cost commercial devices typically do not support robust security mechanisms, making them targets for various attacks. Although SDN can provide extensive functionality for IoT networks, network utilization efficiency has been improved. However, at the same time, SDN still faces many security challenges, such as DoS/DDoS attacks [5, 6], link failure [7, 8], switch data leakage [9], and other common attacks in traditional networks [10]. Distributed Denial of Services (DDoS) attacks is a security threat that has plagued the Internet for more than 20 years. It is becoming even more violent as the Internet evolves, such as with the development of IoT and 5G mobile networks. DDoS is a tremendously devastating attack that hackers frequently use to make numerous requests to a target and thwart the system's standard service. The DDoS attacks have developed from essential to high-rate traffic and sensible low-rate flows. As a result, a new evolution of DDoS attack called Low-rate DDoS (LDDoS) has recently emerged [11]. LDDoS attacks are described by low rapidity, persistence, and concealment, making them difficult to detect. The first problem with the current solutions is that the feature selection is not based on IoT networks, as it only relies on sampling the OpenFlow switches as features using the flow table. In this work, the traffic characteristics of IoT devices are targeted, and the features are sampled from the entire network traffic flows by the SDN controller. This improves the detection accuracy and achieves a precise detection effect. The second problem is that the current solutions have low detection accuracy if the type of network traffic varies. In this work, the LSTM activation function proposed to detect different types of LDDoS attacks by analyzing the characteristic values of different types of LDDoS attacks and natural traffic in IoT networks, so the characteristics are used to update the parameters. The sample is richer, which increases the detection rate, improves the accuracy of LDDoS attack detection, and reduces the flow of malicious traffic.

Therefore, this study proposes a DL-based method to detect LDDoS attacks for IoT network-based SDN. The method is based on the knowledge of the traffic of LDDoS

attacks from the IoT networks at the data layer of SDN architecture, including the network devices and the control plane belonging to the SDN controller. This paper makes the following contributions:

- Propose a Deep Learning-based LDDoS attack detection method for IoT networks based on SDN.
- Design and implement an LDDoS attack in an experimental SDN-based IoT environment that includes various IoT devices and OpenFlow messages managed by the SDN controller.
- Apply RNN as a supervised learning technique for the classification task and evaluate the performance of our method using various performance metrics.

The rest of this paper is organized as follows: Section II Related work. Section III presents Background on SDN, IoT, LDDoS, and Deep Learning. Section IV presents the LDDoS attack challenge. Section V describes our proposed model, analyzes and presents the results. Finally, the last section concludes this paper.

II. Related Work

LDDoS attack detection is critical to communications network infrastructure, especially for advanced technologies such as SDN, IoT, and 5G mobile networks [12]. Presently, researchers in academia and industry are developing detecting algorithms to defend against LDDoS attacks. At the current, attack detection approaches are divided into two types: There are both threshold and machine learning-based detection approaches. Threshold detection methods identify one or more traffic indicators, including traffic rate, packet delay, and maximum entropy. When real-time traffic measurements surpass a predetermined threshold, an attack can occur. The burst time is commonly employed as a detection threshold for LDDoS attacks. In the machine learning-based detection methods, a classifier is used to differentiate between abnormalities and regular traffic. In general, these approaches employ machine learning algorithms to construct a classification model containing the features of the attack behavior to detect the attack. For example, W. Zhijun et al. [13], described a protective strategy based on the dynamic deletion of traffic flow rules. They used the LDDoS attack technique on the SDN data layer to improve identification accuracy and provide numerous functionalities based on the Factorization Machine (FM). In [14], L. Yang and H. Zhao, created an SDN framework based on machine learning to identify and prevent LDDoS threats. For the system, they employed two aspects (traffic detection and flow table delivery). To detect the attack traffic, they employed the SVM algorithm and traffic attributes extracted from the flow table's statistical data.

In [15], K. M. Sudar and P. Deepalakshmi propose that their detection system uses four network flow parameters, including the length of the flow, the number of packets, the relative distribution of the packet interval, and the relative distribution of matched bytes. When the module detects an LDDoS attack, it adds information about the attack flow to the blocklist table and alerts the controller to remove a particular flow from the flow table by entering mitigation rules. However, the characteristics of the behavior of IoT networks based on SDN are different from the characteristics of the usual network based on SDN. For instance, IoT services have a stable temporal foundation and relatively consistent packet data volume, whereas SDNs separate information control and data forwarding. Therefore, attackers can leverage these new characteristics to launch LDDoS assaults that conceal themselves within normal data flows and are difficult to detect with conventional detection methods. For instance, attackers utilize compromised cameras to launch attacks, and the attack flow conceals itself among outgoing video flows. In this work, we solve the limitations of the current solutions, our method is based on sampling the traffic characteristics of IoT devices, and the characteristics are sampled from the entire network traffic flow by the SDN controller to improve the detection accuracy. In addition, we use the LSTM activation function to detect different types of LDDoS attacks by analyzing the characteristic values of different types of LDDoS attacks and natural traffic in IoT networks, so that the characteristics are used to update the parameters. The sample is richer, which increases the detection rate and improves the accuracy of LDDoS attack detection. Our proposed approach to detect LDDoS attacks using a DL-based model classifies traffic in several steps, which are explained in the Proposed Methodology Section.

III. Background on SDN, IoT, LDDoS, and Deep Learning

This section provides an overview of SDN model, IoT technology, LDDoS attack, and DL techniques; it also illustrates how LDDoS attacks in IoT network-based SDN cause bottlenecks.

A. Software-Defined Network

SDN is a proposed network model that avoids the limitations of existing network infrastructures, separating control data (control plane) from forwarding data (data plane) and breaking the vertical integration of network management using an SDN controller to control a network through a comprehensive view of all network devices, allowing easy control and flexibility in installing network devices from different vendors. Unlike traditional networks that are managed by multiple components, including specialized vendor software and switches that depend on vendor installation mechanisms, which complicates the management of IP networks and results in vendor solutions that often lack flexibility and scalability [16]. The SDN architecture, as shown in Fig. 1 contains three layers: The infrastructure layer, which contains the network devices, the control layer, which maintains the network, and the application layer, which executes the software on the network, are the three layers that make up the OSI model. At the infrastructure layer, network devices such as OpenFlow switches, IoT devices, gateways, etc. In the control plane, the network is logically managed centrally by the SDN controller, using the SDN data plane to make decisions that are made by the control plane in all network devices. The application layer includes network software and SDN applications that perform functions assigned to a network domain, IoT applications, and other

requirements such as cloud storage and client-server connectivity requirements [17].

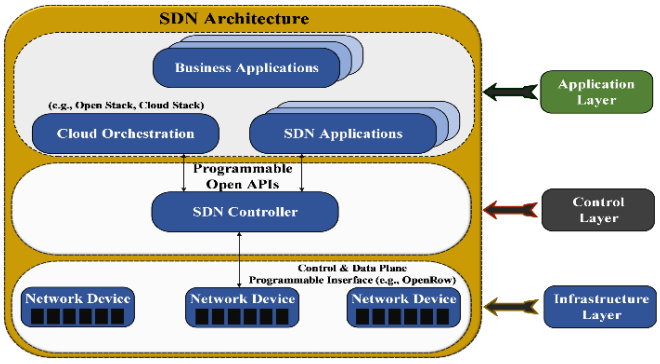

Fig. 1. Software Defined Networking Architecture.

B. Internet of Things (IoT)

The IoT is a computer term that conveys the idea of numerous physical items connected to the Internet and each device's capacity to recognize other devices. It's worth mentioning that the term "thing" on the Internet of Things refers to more than just inanimate items and tiny gadgets. A person wearing a heart rate monitor, a youngster carrying a tracker, a car outfitted with sensors, lighting systems in homes and retail centers, and so on are examples of "things.". In short, the term covers everything that could come to mind, and there are billions of connected objects in the Internet of Things network, which makes controlling and managing these devices a complex task [18]. Moreover, improving security in the IoT context has become a must [19]. The future IoT architecture must be secure enough to prevent the illegal activation of devices. Moreover, since most devices have limited resources, security techniques must be lightweight. In addition, verifying that data is up to date is critical. The lack of adequate security support in IoT can shake the confidence of IoT users and lead to the failure of the technology [20].

C. Low-Rate Distributed Denial of Service Attack

The LDDoS attack is a variant of a DDoS attack. Unlike a traditional flooding DDoS attack which requires a huge amount of resources to launch a successful attack by sending large data flows from infected hosts to the target element in the network [21]. LDDoS attack sends a small amount of malicious traffic, representing 20% or less of network traffic. Therefore, it does not show an apparent statistical anomaly to network monitors during the attack. LDDoS attack is hidden in the normal traffic flow and can perform a covert attack through slow traffic, so there is no obvious anomaly for network monitoring. Furthermore, [22], offers a thorough analysis of LDDoS attack detection techniques in software-defined networks. Currently, the most advanced detection methods for LDDoS attacks are mainly divided into three categories: Feature detection, frequency-domain detection, and time-domain detection. In feature detection, a feature dataset must be created. The feature record contains the features of the known LDDoS attack, and once the features of the LDDoS attack are detected, the LDDoS attack flow is evaluated. In frequency domain detection, the multifractal features of the data flow in the frequency domain are used, and the change conditions in the frequency domain are examined by methods such as spectral analysis, wavelet transform, etc., to detect the LDDoS attack. In time-domain detection, algorithms such as autocorrelation, etc., are used to determine whether the attack flow is present or not by comparing the calculated value with a static threshold [23].

D. Deep Learning

Deep Learning (DL) is a subfield of machine learning concerned with discovering ideas and algorithms that enable a computer to learn autonomously by stimulating human neurons. Deep Learning is a science that focuses on the development of methods to obtain a high level of abstraction by studying a huge data set including linear and nonlinear variables. Numerous disciplines, such as speech recognition, face recognition, computer vision, and natural language processing have made substantial, rapid, and applicable strides due to this field's discoveries. The system learns from massive amounts of data using multiple deep learning network architectures, including Recurrent Networks (RNNs) commonly used with text and continuous data, Convolutional Neural Networks (CNNs) guided by biological processes in the visual center, and others capable of extracting raw data features without human intervention. It can meet the high-performance rate by automatically finding the correlation of the raw data by training the model and displaying the results [24]. Moreover [25], provide a comprehensive review based on deep learning capability, approaches for IoT security. To address the current security and privacy issues such as intrusion detection systems (IDS) within IoT environment. Deep learning approaches generally contain a deep structure of hidden layers as shown in Fig. 2. It relies on abstractions and on automatic learning of features that provide facilities for modularization and transfer of learning.

The RNN method is utilized to choose the essential features and then provides the best data classification. As a result, we have used RNN as a supervised learning technique for network traffic classification to distinguish LDDoS traffic from regular traffic.

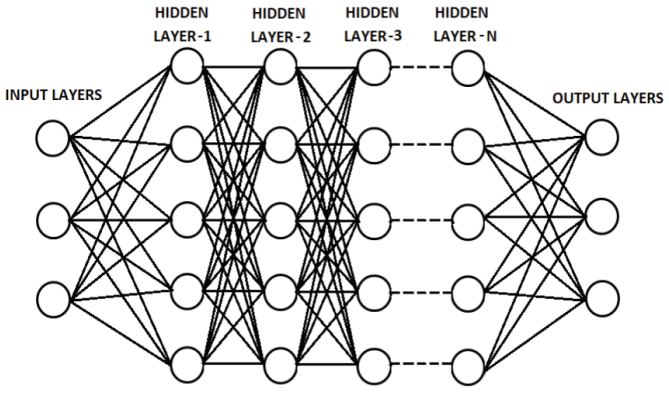

Fig. 2. Overview of Deep Learning Architecture.

IV. Proposed Methodology

A. SDN-based LDDoS Attack in IoT Networks

In SDN architecture, the infrastructure layer and its communication channel to the controller are most vulnerable to LDDoS threats in an SDN-based IoT network. The infrastructure layer consists of SDN forwarding devices, such as "OpenFlow switches, IoT gateways, and access points; the SDN device can be (re)configured for multiple reasons, including traffic separation, data path modification, and device virtualization". Forwarding rules are recorded in the flow table of a switch and govern the data forwarding path. The controller is accountable for receiving data forwarding requests and giving switch flow rules. SDN apps are responsible for starting data layer configuration instructions by calling controller-integrated functionalities. IoT gateways connect IoT devices using various protocols (WiFi, Bluetooth, ZigBee, etc.) and transmit the collected data to other network devices like switches and routers. Some IoT devices, such as WiFi-based cameras and sensors, can transfer data directly to other network devices by connecting to a WiFi access point without an IoT gateway [26].

In the SDN switches, the idle timeout for the input is the maximum amount of time the flow input can be mismatched. If there is no matching packet in the flow rule within this time, it is automatically discarded. Thus, an LDDoS attack can occur if the transmission rate remains constant and the inverse of the idle time is assured, as is the presence of the input flow and OpenFlow switch. The LDDoS attack target SDN switch, and control channel are seen in Fig. 3; when the capacity of the switch's flow table is complete, it can no longer install new flow rules and will not forward new packets. The number of low-rate attack flows grows in a linear fashion. If the attacker transmits 5 malicious packets during the first idle timeout interval, 10 flow rules are formed in the flow table at the same time. The attack packet is transmitted at regular intervals in the second idle timeout interval to ensure that the flow rules in the flow table do not disappear, but 5 attack packets are added concurrently. The flow table currently contains 20 flow bases. The flow rules will gradually increase as the attack continues until the flow table is saturated.

The data generated by IoT devices can be divided into two types: small data packets generated by sensors in vehicles, houses, etc., and large data packets generated by video display devices from surveillance cameras, among others. The infrastructure layer of the SDN presents these kinds of data packets as ordinary data flows. These two types of devices allow attackers to configure diverse LDDoS attack packets. Such as, they can utilize webcams to send high-volume malicious packets to overwhelm the target and, use IoT sensors to launch malicious volume packets to overwhelm the target or use a combination of both to launch a hybrid attack. For instant, attackers can utilize webcams to send large amounts of malicious traffic or IoT sensors to generate small amounts of malicious traffic, often using a combination of the two to launch a hybrid attack that floods the target. During this work, the model was developed to handle traffic from IoT devices that generate traffic and use traffic features to train and test the models to present the results presented in the next section.

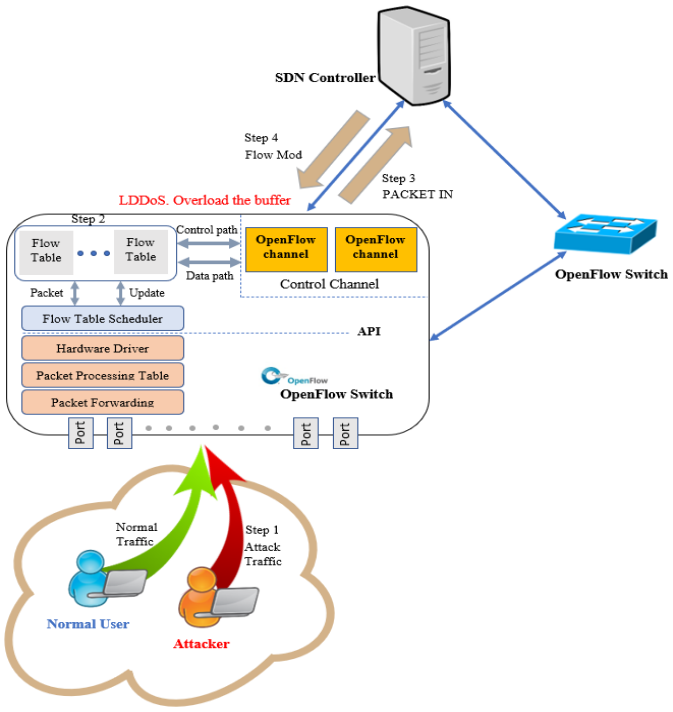

Fig. 3. LDDoS Attack Scenario Targeting SDN Switch and Control Channel.

B. LDDOS Attack Detection Method

The embodiment of the LDDoS attack detection method is based on RNN Deep Learning, which is used to effectively detect various types of LDDoS attacks for SDN-enabled IoT networks. The proposed method was tested using a comprehensive, realistic cybersecurity dataset for IoT and IIoT applications called Edge-IIoTset, which machine learning-based systems can use to detect intrusions. The Edge-IIoTset dataset is divided into several layers, including the IoT perception layer, the IIoT layer, the software-defined network layer and the network function virtualization layer. These layers leverage new emerging technologies that address the key requirements of IoT and IIoT applications, such as the ONOS SDN controller, Things Board IoT platform, and OPNFV platform. IoT data is generated from more than 10 different IoT devices, such as low-cost ultrasonic sensors, water level detection sensors, Ph sensors, soil moisture sensors, heart rate sensors, flame sensors, and digital temperature sensors for temperature and humidity, etc. In the Edge-IIoTset dataset, various attacks including DDoS attacks were identified and analyzed and extracted their features from various sources including alerts, system resources, logs and network traffic [27].

The sampling data were divided into training (70%) and testing (30%). Learning algorithms learn from current datasets and make informed decisions. The proposed detection method contains six main steps: data collection, data pre-processing, training, and testing data, model evaluation, model Prediction, and decision making. As illustrated in Fig. 4, multiple independent processes make up the proposed detection

method overall. The proposed method is based on Recurrent Neural Networks (RNN), where the model consists of an activation function of the LSTM layer to take time-series data as input and learn how to value time, each step of the method is explained as follows.

- Data collection: The datasets have been collected from Edge-IIoT and consist of cybersecurity attacks, which include DoS/DDoS. In these attack categories, the attackers tend to deny the services of legitimate users, either solely or in a distributed fashion. We look at the four most common methods: the TCP SYN Flood, the UDP Flood, the HTTP Flood, and the ICMP Flood. Also, the quality and variety of legitimate entries in a dataset are important for building a profile of how a system normally works. Additionally, malicious entries are essential for security solutions to recognize not only the precise attack patterns but also to identify new ones.

- Data pre-processing: Any machine learning approach requires exploratory data analysis and data observations, so we first create a data collection that can be fed to any classifier. The procedures involve dealing with the missing data, Colum, which was missing value from Edge-IIoT datasets. Our data reprocessing procedures include converting row data into a clean dataset and removing the missing data (column) that was missing from the Edge-IIoT datasets. Second, the phase will unify the engineering steps required to determine the data feature type among the datasets. The data set included categorical datasets as well as numerical data. It was normalized using min-max data normalization as shown in Eq. 1.

$$\mathbf{x}_i' = \frac{\mathbf{x}_i - min\,\mathbf{x}_i}{max\,\mathbf{x}_i - min\,\mathbf{x}_i} \quad (1)$$

- LSTM model training: The datasets have been split into training 70% and testing 30%. The proposed LSTM model which has been calculated for 30 epochs using training and validation of Edge-IIoT datasets. The model parameter and calculation in percentage is an interpretable way to determine the model performance. The LSTM model has been optimized using Adam optimizer with a learning rate 0.03. The dropout method with a probability of 0.5 has been used to prevent the model from over fitting. Therefore, the proposed LSTM model attempts to sequence-dependent behaviour such as LDDoS attacks detection in network traffic known as IDS. This is performed by feeding back the output of a neural network layer at time T to the input of some layer at time T + 1. Moreover, we used deep learning solution based on LSTM for LDDoS attack detection in SDN enabled IoT networks due to its high efficiency of network data flow.

- Evaluation Metrics: accuracy (ACC) has been used for evaluation measure in this research. The classification models can be evaluated on a variety of parameters, including their accuracy. It depicts its single-class accuracy measurement. Accuracy will also be given by the total number of predictions made by the primary performance metric used in the behaviour recognition domain that measures different values predicted by a trained model and observed values from the environment. Furthermore, the authors used accuracy for practical decisions and accuracy for model result outcomes in decision-making after training. The accuracy of the proposed LSTM model was determined using Eq. 2.

$$\text{Accuracy} = \frac{(\text{tp} + \text{tn})}{(\text{tp} + \text{fp} + \text{tn} + \text{fn})} \quad (2)$$

where *tp* means true positive, *tn* is a true negative, *fp* denotes false positive, and *fn* is a false negative.

$$\text{Precision} = \frac{\text{tp}}{(\text{tp} + \text{fp})}, \quad (3)$$

$$\text{Recall} = \frac{\text{tp}}{(\text{tp} + \text{fn})}, \quad (4)$$

$$\text{F-measure} = \frac{2 \times \text{precision} \times \text{recall}}{\text{recision} + \text{recall}}, \quad (5)$$

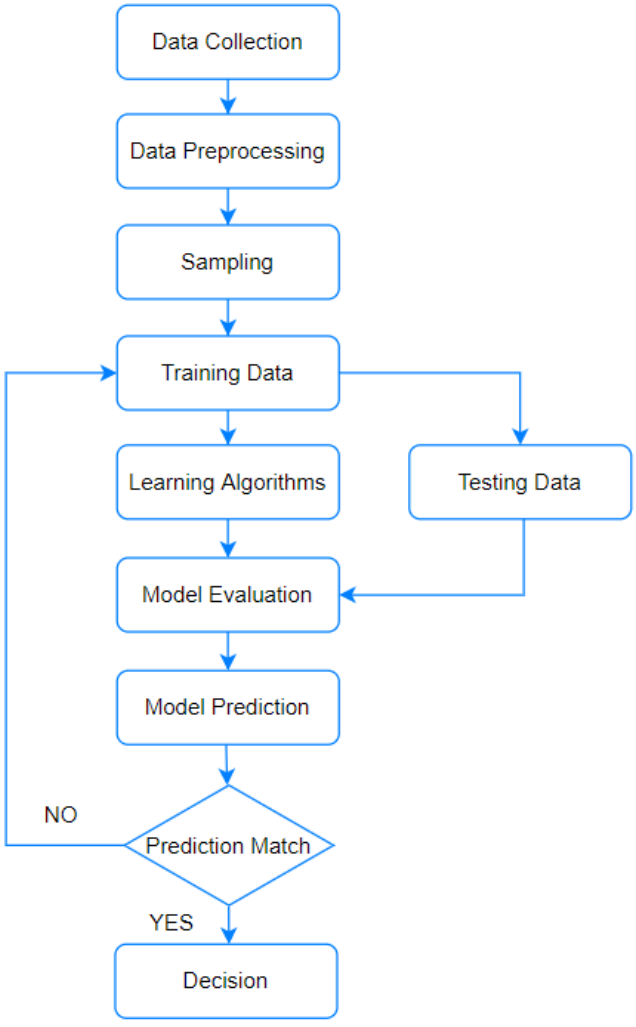

Fig. 4. Flowchart of Proposed Method.

V. Results and Discussion

According to training and validation data from industrial Edge-IIoTset datasets in Fig. 5, the proposed RNN model's accuracy has been calculated over 30 iterations. The model parameter and percentage calculation are an easy-to-understand way to measure the model's effectiveness. As the result indicate training accuracy is 98.88%, this result can be used for LDDoS attacks prediction and decision, which determines that there is a significant increase after iterations with fluctuation.

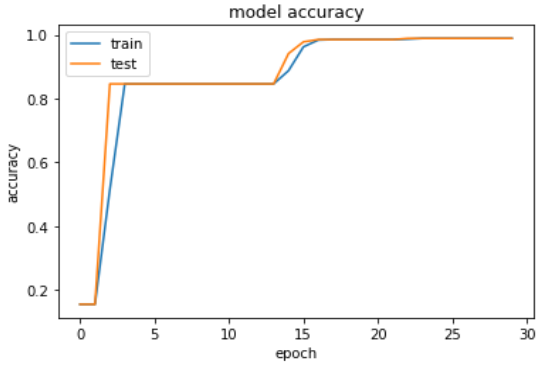

Fig. 5. Training and Validation of Accuracy Performance for 30 Epochs.

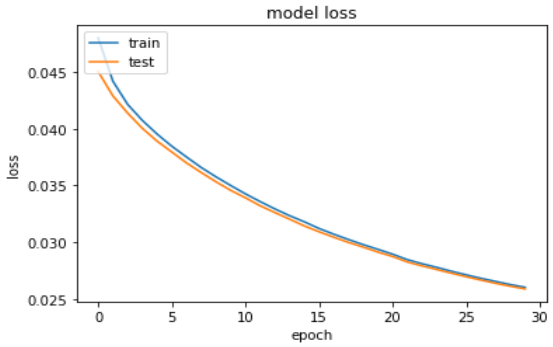

Fig. 6. Training and Validation of Loss Performance for 30 Epochs.

Fig. 6 shows the model's loss performance was also calculated for 30 epochs using training and validation datasets from the industrial Edge-IIoTset dataset. Adding to this, the authors' contribution results show better performance against LDDoS attacks with high accuracy, which was significantly improved after training and testing. Furthermore, the loss parameter calculates training and validation to interpret how the model performance of input datasets. The loss did not increase significantly after iterations but rather decreased. The final loss validation performance was 0.25.

A. Evaluation of Performance

Table I shows the model evaluation measures where the method obtains an accuracy of 98.88% and precision, recall, f1-score of 0.9746, 0.9657, 0.9691, respectively. The obtained performance of the method utilized in this research is presented in Fig. 7, where the model shows a good performance in term of the accuracy and the F1-score.

B. Evaluation Metrics

This section emphasizes o the proposed method performance comparing to the state-of-the-art methods. The proposed LSTM model performance in this work was benchmarked and compared with the related literature contributions with the available performance measures shown in Table II. Our proposed method shows an improvement in the network attack detection accuracy and surpassed other methods exist in the literature review. the proposed method performance outperformed the suggested methods by authors in [13], and authors in [14], as well as the introduced model in the work in [15]. Table II summarize the comparison with related work.

TABLE I. Evaluation Measures of the Model

Accuracy	Loss rate	Precision	Recall	F1-score
98.88%	0.25	0.9746	0.9657	0.9691

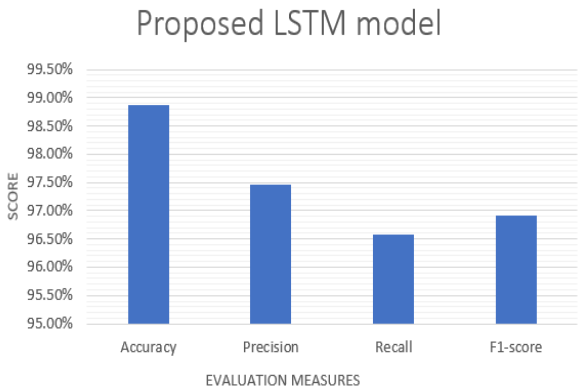

Fig. 7. Results Summary of the Attack Detection using LSTM.

TABLE II. Comparison of Proposed Method Performance with the Related Literature Contributions

References	Year	Layer Location	Classifier/ Method	Dataset	SDN Controller	Network-based	Detection Results
[13]	2019	Data layer	FM	NSL-KDD, CAIDA	Ryu	Traditional wired Network	95.8%
[14]	2021	Control Layer	GBDT, GBDT-LR	Custom	Ryu	Traditional wired Network	96%
[15]	2022	Control Layer and Data Layer	SVM,DT,NB	CIC	POX	Traditional wired Network	93%
Proposed Method	2022	Control Layer and Data Layer	RNN-LSTM	Edge-IIoTset	Ryu	IoT Network	98.8%

VI. Conclusion

To conclude, despite the fact that SDN removes bottlenecks and helps handle IoT data efficiently without overloading the network. However, in an evolving environment, SDN-based IoT is vulnerable to various types of distributed denial of service (DDoS) attacks. Traditional DDoS attack detection methods only allow detection of high-rate DDoS attacks; there are problems with low detection accuracy and poor scalability in the case of low-rate DDoS attacks. Our proposed method based on RNN enables detection that targets various LDDoS attacks in the network and more finely divides the types of LDDoS attacks. Meanwhile, for each type of LDDoS attack, the feature types that are significantly different from the normal data flow are identified by the analysis, and the relevant features of the attack can be described using the feature set. Therefore, the proposed detection model can detect various types of LDDoS attacks with high accuracy, output classification results for detection, improve the extensibility of a detection system, and increase the rate of malicious data flow reduction. According to the analysis of the tests performed, our LSTM model has achieved better results in classifying LDDoS attacks because it achieves a fast training time and the results were measured based on accuracy. The accuracy is 98.8% after the training and validation of the model. Finally, one of the future research directions is to implement bio-inspired metaheuristic optimization techniques and investigates their significance performance in obtaining the optimal hyper-parameters and architecture of DNNs with massive-scale data. The other research direction will be exploring deep reinforcement learning in detecting low-rate DDoS attack in IoT networks.

References

[1] A. Sivanathan et al., "Classifying IoT devices in smart environments using network traffic characteristics," IEEE Transactions on Mobile Computing, vol. 18, no. 8, pp. 1745-1759, 2018.

[2] Ericsson, "Ericsson Mobility Report," 2019. [Online]. Available: https://www.ericsson.com/assets/local/reports-papers/mobility-report/documents/2019/emr-november-2019.pdf

[3] C. Bouras, P. Ntarzanos, and A. Papazois, "Cost modeling for SDN/NFV based mobile 5G networks," in 2016 8th international congress on ultra modern telecommunications and control systems and workshops (ICUMT), 2016: IEEE, pp. 56-61.

[4] R. Amin, M. Reisslein, and N. Shah, "Hybrid SDN networks: A survey of existing approaches," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3259-3306, 2018.

[5] A. A. Alashhab, M. S. M. Zahid, A. A. Barka, and A. M. Albaboh, "Experimenting and evaluating the impact of DoS attacks on different SDN controllers," in 2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA, 2021: IEEE, pp. 722-727.

[6] L. F. Eliyan and R. Di Pietro, "DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges," Future Generation Computer Systems, vol. 122, pp. 149-171, 2021.

[7] M. Y. Daha, M. S. M. Zahid, B. Isyaku, and A. A. Alashhab, "Cdra: A community detection based routing algorithm for link failure recovery in software defined networks," International Journal of Advanced Computer Science and Applications, vol. 12, no. 11, 2021.

[8] M. Y. Daha, M. S. M. Zahid, A. Alashhab, and S. U. Hassan, "Comparative Analysis of Community Detection Methods for Link Failure Recovery in Software Defined Networks," in 2021 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), 2021: IEEE, pp. 157-162.

[9] A. H. Shamsan and A. R. Faridi, "Security Issues and Challenges in SDN," in International Conference on Advances in Cyber Security, 2021: Springer, pp. 515-535.

[10] A. N. Alhaj and N. Dutta, "Analysis of security attacks in SDN network: A comprehensive survey," Contemporary Issues in Communication, Cloud and Big Data Analytics, pp. 27-37, 2022.

[11] S. Sambangi, L. Gondi, and S. Aljawarneh, "A Feature Similarity Machine Learning Model for DDoS Attack Detection in Modern Network Environments for Industry 4.0," Computers and Electrical Engineering, vol. 100, p. 107955, 2022.

[12] H. Chen, C. Meng, Z. Shan, Z. Fu, and B. K. Bhargava, "A novel Low-rate Denial of Service attack detection approach in ZigBee wireless sensor network by combining Hilbert-Huang Transformation and Trust Evaluation," IEEE Access, vol. 7, pp. 32853-32866, 2019.

[13] W. Zhijun, X. Qing, W. Jingjie, Y. Meng, and L. Liang, "Low-rate DDoS attack detection based on factorization machine in software defined network," IEEE Access, vol. 8, pp. 17404-17418, 2020.

[14] L. Yang and H. Zhao, "DDoS attack identification and defense using SDN based on machine learning method," in 2018 15th international symposium on pervasive systems, algorithms and networks (I-SPAN), 2018: IEEE, pp. 174-178.

[15] K. M. Sudar and P. Deepalakshmi, "Flow-Based Detection and Mitigation of Low-Rate DDOS Attack in SDN Environment Using Machine Learning Techniques," in IoT and Analytics for Sensor Networks: Springer, 2022, pp. 193-205.

[16] D. Kumar and J. Thakur, "Handling Security Issues in Software-defined Networks (SDNs) Using Machine Learning," in Computational Vision and Bio-Inspired Computing: Springer, 2022, pp. 263-277.

[17] D. B. Rawat and S. R. Reddy, "Software defined networking architecture, security and energy efficiency: A survey," IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 325-346, 2016.

[18] Y. Lu and L. Da Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2103-2115, 2018.

[19] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions," Mobile Networks and Applications, pp. 1-17, 2022.

[20] R. F. Ali, A. Muneer, P. Dominic, S. M. Taib, and E. A. Ghaleb, "Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review," in International Conference on Advances in Cyber Security, 2021: Springer, pp. 128-154.

[21] Z. Li, H. Jin, D. Zou, and B. Yuan, "Exploring new opportunities to defeat low-rate DDoS attack in container-based cloud environment," IEEE Transactions on Parallel and Distributed Systems, vol. 31, no. 3, pp. 695-706, 2019.

[22] A. A. Alashhab, M. S. M. Zahid, M. A. Azim, M. Y. Daha, B. Isyaku, and S. Ali, "A Survey of Low Rate DDoS Detection Techniques Based on Machine Learning in Software-Defined Networks," Symmetry, vol. 14, no. 8, p. 1563, 2022. [Online]. Available: https://www.mdpi.com/2073-8994/14/8/1563.

[23] T. A. Pascoal, I. E. Fonseca, and V. Nigam, "Slow denial-of-service attacks on software defined networks," Computer Networks, vol. 173, p. 107223, 2020.

[24] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," nature, vol. 521, no. 7553, pp. 436-444, 2015.

[25] M. Abdullahi et al., "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," Electronics, vol. 11, no. 2, p. 198, 2022.

[26] D. C. Y. Vargas and C. E. P. Salvador, "Smart IoT gateway for heterogeneous devices interoperability," IEEE Latin America Transactions, vol. 14, no. 8, pp. 3900-3906, 2016.

[27] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," IEEE Access, vol. 10, pp. 40281-40306, 2022.