2022 25th International Symposium on Wireless Personal Multimedia Communications (WPMC) | 978-1-6654-7318-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/WPMC55625.2022.10014866

Smart LSTM-based IDS for Heterogeneous IoT (HetIoT)

Shalaka S. Mahadik[1], Pranav M. Pawar[2], Raja Muthalagu[3]
Birla Institute of Technology and Science Pilani, Dubai Campus, UAE[1,2,3]
p20200002@dubai.bits-pilani.ac.in[1], pranav@dubai.bits-pilani.ac.in[2], raja.m@dubai.bits-pilani.ac.in[3]

Neeli Rashmi Prasad[4]
TrustedMobi "VehicleAvatar Inc."
Mountain View, CA, USA
neeli.prasad@ieee.org

Dnyaeshwar Mantri[5]
Sinhgad Institute of Technology
Lonavala, India
dsmantri.sit@sinhgad.edu

***Abstract*—Distributed denial-of-service (DDoS) is the most formidable attack, and many researchers are focusing their attention on safeguarding the heterogeneous IoT (HetIoT) networks from it. The paper proposes a smart intrusion detection system (IDS) using long-short-term memory (LSTM), i.e., smart LSTM-based IDS for the HetIoT. The paper highlighted data preprocessing steps after thorough exploratory data analysis (EDA) and feature extraction using the principal component analysis (PCA) technique. The proposed smart LSTM-based IDS successfully identifies and mitigates the various DDoS attacks. The paper considers binary and multi-class classification (7-class and 13-class) of DDoS attacks for efficient detection of attacks. The performance of the proposed smart LSTM-based IDS is compared with two state-of-the-art deep learning approaches, and the results reveal that the proposed smart LSTM-based IDS outperforms it. The proposed LSTM-based IDS successfully identifies various DDoS attacks with an accuracy rate of 99.98% for binary classification, 98% for 7-classes, and 99.97% for 13-classes. The work also compares the individual accuracy of 7-classes and 13-classes with state-of-the-art work. Also, the proposed smart LSTM-based IDS is lightweight, simple, and less complex than the existing state-of-the-art work models.**

***Index Terms*—Heterogeneous IoT, Security, DDoS, IDS, Deep learning, Long-short-term memory.**

I. Introduction

Internet-of-things (IoT) has been gaining popularity for the past few decades despite challenges such as standardization, big data fusion, energy consumption, and many more. However, heterogeneity and security are the major challenging issues among them. The network architecture (e.g., WiFi, 3G/4G/5G, Mobile communication) of the IoT is intrinsically heterogeneous [1]. A recent statistical study [2] shows that IoT networks are more prone to various kinds of attacks because of their low-power, low-cost resources. Traditional security techniques cannot apply to this environment. Hence this paper mainly focuses on protecting such HetIoT networks.

DDoS is the most powerful and dangerous attack that has taken hold of HetIoT infrastructure. Cloudflare highlighted several real-time DDoS attack instances, including the 2016 Dyn attack, the GitHub DDoS attack in February 2018, and the AWS DDoS attack in February 2020 [3]. AWS reported an intruder hijacked the CLDAP protocol (connection-less lightweight directory access protocol) during the February 2020 DDoS attack. Each of these examples demonstrates that DDoS attacks are becoming extremely prevalent. Fig. 1 shows the annual report by Cisco estimating that the total number of DDoS attacks will double from 7.9 million in 2018 to around 15.4 million in 2023 [4].

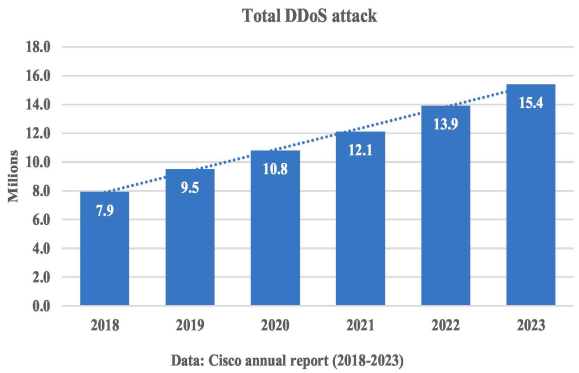

Fig. 1: Cicso analysis of DDoS attack history and prediction [4]

The literature survey shows that deep learning (DL) techniques gives promising result to safeguard the DDoS attack [1], [5]–[9]. Also, Fig. 2 shows that designing IDS using DL techniques gaining popularity over the past five years. The LSTM is a recurrent neural network (RNN) based DL technique. It removes long-term dependency issues in RNN and is a good solution for the vanishing gradient problem. Hence, more popular among the researchers [6], [11]–[14]. As a result, the paper is motivated to design an IDS to detect and classify the DDoS attack using a DL-based LSTM model to safeguard the HetIoT networks.

The remainder of this paper is organized as follows: Section II reviews the related work with a comparative study. Section

978-1-6654-7318-7/22/$31.00©2022 IEEE

Authorized licensed use limited to: Birla Inst of Technology and Science Pilani Dubai. Downloaded on November 17,2024 at 10:59:03 UTC from IEEE Xplore. Restrictions apply.

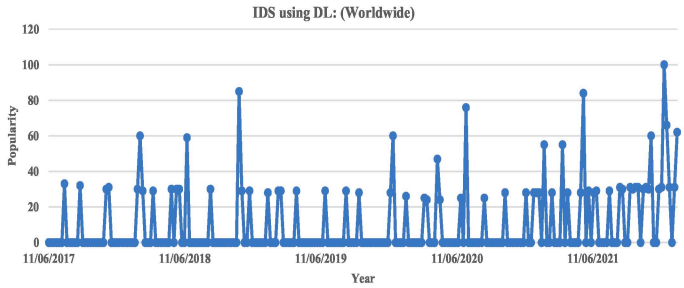

Fig. 2: Growth of IDS using DL technique (Google trends)

III presents the contribution of the paper, the description of a dataset used, PCA analysis, the proposed smart LSTM-based IDS methodology, and the network model. Section IV provides the details of the simulation environment and performance results with a discussion and summary of it, and Section V concludes the paper.

II. Related Work

The paper focuses solely on various DL-based models and the CICDDoS2019 dataset from 2020 to 2021. CICDDoS2019 is a DDoS evaluation dataset that is provided by the Canadian Institute for Cybersecurity (CIC) and the University of New Brunswick (UNB) [15], [16]. Table I describes the various existing state-of-the-art models (concerning model name, DL techniques used, binary or multi-class classification, models basic information and limitations) that use the DL technique to safeguard the HetIoT system against DDoS attacks. According to the literature survey, existing models consider either binary or multi-class classification but not both except model [8]. Even though the literature survey shows the model with good accuracy, it still fails to consider all recent DDoS attacks present in the CICDDoS2019 dataset. Furthermore, existing models are heavy and complex, with many layers and neurons; such models need high computing power and more processing time while training.

III. Smart LSTM-based IDS for HetIoT

The smart LSTM-based IDS block diagram in Fig. 3 clearly shows the necessary steps before training the model. Details of dataset (section III-B), PCA analysis (section III-C1) are highlighted in the next section. The LSTM model takes input in three-dimensional form; hence, data is reshaped from two-dimensional into three-dimensional form. Also, the LSTM-based IDS can be deployed at the network layer, as presented in Fig. 3. The LSTM-based IDS is lightweight, simple, and less complex; it requires less computing power to train-test the model. Hence the network admin can easily explore all the incoming flows, including DDoS attacks near the local data processing (such as edge devices) at a network layer.

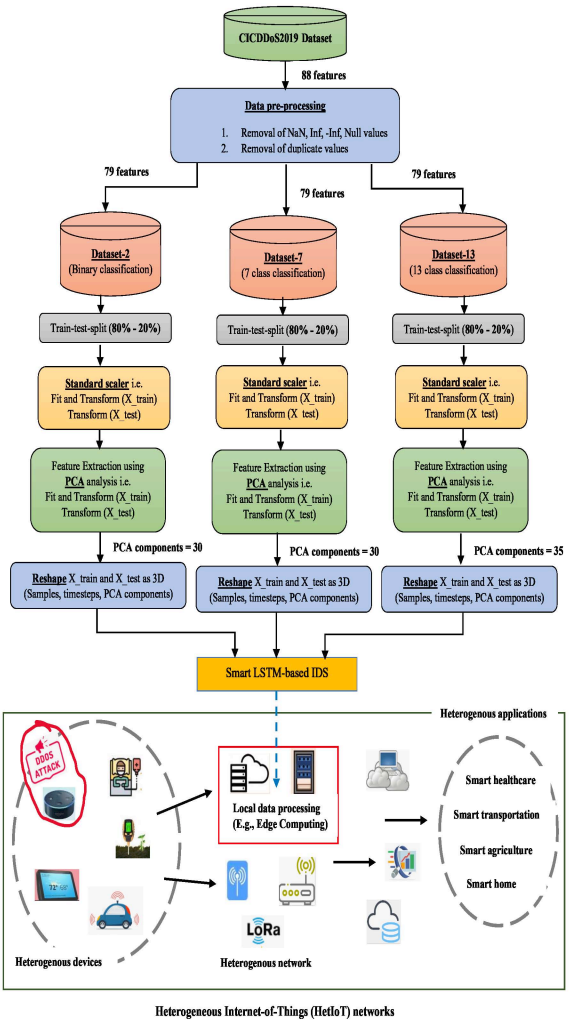

Fig. 3: Block diagram of Smart LSTM-based IDS for HetIoT.

A. Contributions

The main contributions of the paper are as follows: 1) Data pre-processing after doing thorough EDA [17] 2) Feature extraction using PCA technique 3) Smart deep learning-based LSTM model for detecting DDoS attack on HetIoT, i.e., Smart LSTM-based IDS. 4) The performance analysis with binary classification and multi-class classification (7-class and 13-class) using a popular and benchmark dataset, CICDDoS2019 [16]. The performance is evaluated using the parameter precision, recall, F1-score, and accuracy. 5) Smart LSTM-based IDS effectively identifies DDoS attacks for binary and multi-class (7-class and 13-class) classification with good accuracy, i.e., 99.98% for binary classification, 98% for 7-class classification, and 99.97% for 13-class classification. 6) The proposed smart LSTM-based IDS is lightweight, simple, and less complex in terms of the number of layers and neurons

Authorized licensed use limited to: Birla Inst of Technology and Science Pilani Dubai. Downloaded on November 17,2024 at 10:59:03 UTC from IEEE Xplore. Restrictions apply.

TABLE I: Comparative analysis of existing DL models

Year	Model name	DL technique	Accuracy (%)	Classification	Basic info	Limitation
2020	DDoSnet	RNN with AE	99	Binary	DDoS attack detection in SDN environment, AUC is 98.8, [18]	No multi-class classification
2020	Flowguard	LSTM	98.9	Binary	Edge defense technique against IoT DDoS attack identification, classification, and mitigation, [9]	More training time because of 1280 neurons, higher computational power is needed
2020	Cuda base LSTM	LSTM	99.6	Multi-class (4 class)	Achieve good accuracy against four types of DDoS attacks, [5]	All attacks are not focused, complex computation in terms of layers (i.e., 3 LSTM layer, 4 dense layer, 1 dropout)
2021	Stacked-LSTM	LSTM	99.55	Binary	Achieve good accuracy for binary classification using the 'portmap.csv'file, [10]	No multi-classification, heavy model with 1 input layer, 3 LSTM layer, 1 dense layer, and 1 output layer
2021	Composite framework for B5G	DNN	99.66	Multi-class (10 class)	Two separate DNN models combine to detect DDoS attacks, [6]	Heavy and complex structure with 2 DNN models, each model with 1 input layer, 7 hidden layers, 2 dropouts
2021	Hybrid approach	CuDNNLSTM and CuDNNGRU	99.74	Multi-class (8 class)	Achieve good accuracy using Cuda libraries against DDoS attacks, [7]	Heavy model (i.e. 2 CuDNNLSTM layer, 1 CuDNN GRU layer, 4 dense layer, 1 dropout)
2021	DL based IDS	LSTM	99.94	Binary	Three different models are proposed to protect agriculture 4.0 from DDoS attack, [8]	Complex structure with more layers
			94.99	Multi-class (7 class)		(5 LSTM,4 dropout,1 dense layer), 67,
			94.88	Multi-class (13 class)		300, 600, 300, 67 neurons each LSTM layer

used.

B. Dataset

CICDDoS2019 is a publicly available real-time benchmarking dataset that many researchers extensively use [16]. It contains 13 training and 7 testing separate CSV files. Each file has a type of DDoS attack such as domain name system (DNS), lightweight directory access protocol (LDAP), simple network management protocol (SNMP), simple service discovery protocol (SSDP), NETwork basic input-output system (NetBIOS), network time protocol (NTP), Microsoft SQL (MSSQL), user datagram protocol (UDP), UDP-lag, TFTP, WebDDoS, Syn, etc. The dataset contains more than 50 million samples, with 88 features for each sample. As part of the data pre-processing step using EDA, the paper examines all the features except Flow Id, Source IP, Destination IP, SimillarHTTP, Timestamp, Source port, Destination port, and Unnamed, which are non-informative or created inside the simulated environment [18]. The samples with NaN, Null, infinite values, and duplicates are removed to avoid over-fitting the model. Finally, 79 features and one target column are used to create the three separate datasets (Fig. 3), namely, Dataset-2 for binary classification, Dataset-7, and Dataset-13 for multi-class classification. The details of each datasets training and testing samples are provided in Table IV, V, VI.

C. Proposed methodology

1) PCA analysis: HetIoT applications generate a massive amount of data, which is hard to manage. PCA technique is a promising solution for dealing with such large amounts of data by reducing dimensionality [11], [19]. After doing EDA with a heatmap and Pearson correlation, it is observed that many redundant features are present in the dataset, namely dataset-2, dataset-7, and dataset-13. In order to capture valuable information with high variance, the PCA technique is adopted in the paper. This technique helps the proposed LSTM-based IDS reduce the complexity and increases computational efficiency by achieving high accuracy. The explained variance graph and cumulative explained variance graph help to visualize how much percent information, i.e., variance, each PCA component holds. The higher the variance, the more important the PCA component and the smaller the loss of information. Fig. 4 and 5 highlight both explained variance and cumulative explained variance graphs for each dataset. For Dataset-2 (Fig. 4), and Dataset-7 (Fig. 5), 1st PCA components hold maximum variance, followed by 2nd, 3rd, 4th, and continued up to 30. After that, variance is low; hence 30 PCA components are selected for both the datasets. Similarly, for Dataset-13, as shown in Fig. 6, the first three PCA components hold maximum variance and continue up to 35; hence, 35 PCA components are selected.

2) LSTM-based IDS model: The smart LSTM-based IDS implements 2-LSTM layers and 1-Dense layer as output layers to achieve good performance. The detailed LSTM-based IDS network structure with the layers, the neurons, and the activation function employed is shown in Fig. 7. The GridSearch hyperparameter settings [20] are used to decide the number of the neuron as 32 and 64 with activation

Authorized licensed use limited to: Birla Inst of Technology and Science Pilani Dubai. Downloaded on November 17,2024 at 10:59:03 UTC from IEEE Xplore. Restrictions apply.

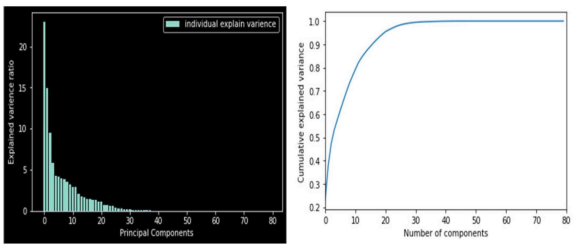

Fig. 4: Explained variance and Cumulative explained variance graph for Dataset-2.

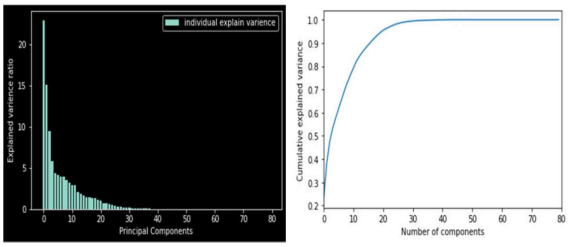

Fig. 5: Explained variance and Cumulative explained variance graph for Dataset-7.

function as 'ReLU (Rectified Linear Unit)'. The 'ReLU' is much faster when compared to other activation functions and helps achieve better accuracy; also, it removes the gradient descent problem that exists in RNN [21], [22]. The model applied 'sparse_categorical_crossentropy' as a loss function since target classes are integers, not one_hot encoded [23]. As mentioned in [13], 'RMSprop' as an optimizer with a default learning rate that gives better accuracy. The hyperparameter setting is highlighted in Table III.

IV. Results and Discussion

A. Simulation environment

The specification of the software and hardware set-up is provided in Table II. The hyperparameter settings are shown in Table III.

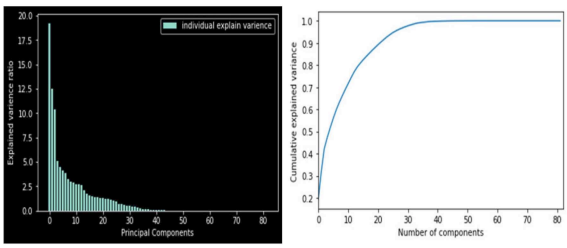

Fig. 6: Explained variance and Cumulative explained variance graph for Dataset-13.

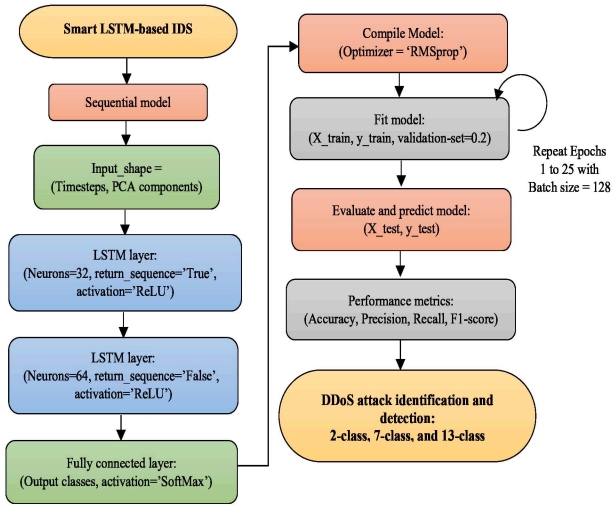

Fig. 7: LSTM-based IDS structure.

TABLE II: Simulation set-up

Software specification:	
Software tool	Spyder 5.0.1 IDE
Programming language	Python 3.8, Sklearn library, Matplotlib 3.5
API tool	Keras on TensorFlow 2.7.0
Hardware specification:	
Processor i7-10750H CPU @ 2.60GHz, 16GB RAM,	
Windows 10 64-bit OS, dedicated 4GB NVIDIA GEFORCE GTX 1650Ti	

The standard performance metrics such as accuracy, precision, recall, and F1-score are used to evaluate the LSTM-based IDS performance [14]. Fig. 3 shows that all steps are the same for all three datasets beginning with data pre-processing and ending with PCA component computation. A 20% validation set is included in the training set to ensure that all results are unbiased.

TABLE III: Hyperparameter settings

Hyperparameter settings	Value
Learning rate	0.001
Optimizer	RMSprop
Activation function	Relu
Classification function	SoftMax
Batch Size	128
Epoch	25
Loss function	Sparse_categorical_crossentrophy

B. Binary classification

Binary classification is performed using Dataset-2. The training and testing sample details are given in Table IV.

TABLE IV: Details of Dataset-2

Sr.no	Attacks name	Total sample	Training sample	Testing sample
1	Benign	5,565	4,452	1,113
2	DDoS attack	1,864,694	1,491,755	372,939
		1,870,259	1,496,207	374,052

Authorized licensed use limited to: Birla Inst of Technology and Science Pilani Dubai. Downloaded on November 17,2024 at 10:59:03 UTC from IEEE Xplore. Restrictions apply.

The performance of the LSTM-based IDS is examined with the state-of-the-art model[[8] as shown in Fig. 8. The LSTM-based IDS achieves a 99.98% accuracy, whereas the state-of-the-art model [8] achieves 99.94% accuracy. The comparative performance accuracy in detecting DDoS attacks and benign flow shows slight improvement using the LSTM-based IDS compared to the state-of-the-art model [8].

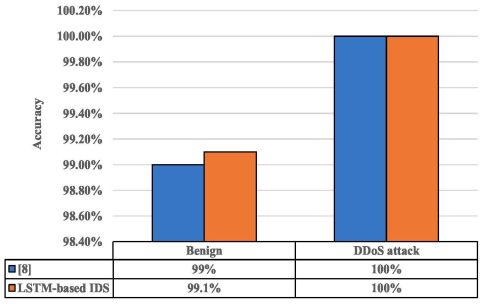

Fig. 8: Performance result for Binary classification

C. 7-class classification

Dataset-7 is used for 7-class classification. The training and testing sample of individual DDoS attacks are detailed in Table V.

TABLE V: Details of Dataset-7

Sr.no	Attacks name	Total sample	Training sample	Testing sample
1	Benign	5,665	4,532	1,133
2	DrDoS_LDAP	191,598	153,278	38,320
3	DrDoS_MSSQL	578,714	462,971	115,743
4	DrDoS_NetBIOS	365,667	292,534	73,133
5	Syn	489,318	391,454	97,864
6	DrDoS_UDP	386,606	309,285	77,321
7	UDP-Lag	171	137	34
		2,017,739	1,614,191	403,548

The performance of the LSTM-based IDS is assessed with the state-of-the-art model [8] as shown in Fig. 9. The LSTM-based IDS detects UDP attacks with an accuracy of 100%, MSSQL with 98%, and UDP-lag with an accuracy of 18%. The number of samples used for UDP-lag is less (171 samples). Still, the data preprocessing steps and features extracted using the PCA technique help the LSTM-based IDS appropriately learn and detect the attack with a precision of 50% and an accuracy of 18%. However, the state-of-the-art model [8] fails to detect UDP-lag attack; UDP and MSSQL attack detection accuracy is 71%, 94% respectively. The comparative performance accuracy in detecting six individual DDoS attacks and benign flow shows good improvement using the LSTM-based IDS compared to the state-of-the-art model [8].

D. 13-class classification

Dataset-13 is used for 13-class classification. The training and testing sample of individual DDoS attacks are detailed in Table VI.

The performance of the LSTM-based IDS is examined with the state-of-the-art model [8] as shown in Fig. 10. The LSTM-based IDS accurately predicts LDAP, MSSQL, NetBIOS, Syn, UDP, UDP-lag, TFTP, NTP, SSDP, SNMP, and DNS with an

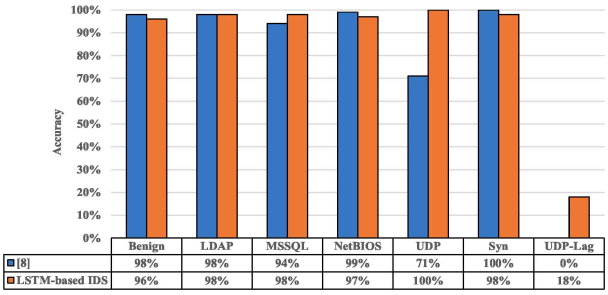

Fig. 9: Performance result for 7-class classification

TABLE VI: Details of Dataset-13

Sr.no	Attacks name	Total sample	Training sample	Testing sample
1	Benign	31,880	25,504	6,376
2	DrDoS_LDAP	60,000	48,000	12,000
3	DrDoS_MSSQL	60,000	48,000	12,000
4	DrDoS_NetBIOS	60,000	48,000	12,000
5	Syn	60,000	48,000	12,000
6	DrDoS_UDP	60,000	48,000	12,000
7	UDP-Lag	60,000	48,000	12,000
8	TFTP	60,000	48,000	12,000
9	WebDDoS	439	351	88
10	DrDoS_NTP	60,000	48,000	12,000
11	DrDoS_SSDP	60,000	48,000	12,000
12	DrDoS_SNMP	60,000	48,000	12,000
13	DrDoS_DNS	60,000	48,000	12,000
		692,319	553,855	138,464

accuracy rate 100% whereas WebDDoS attack achieves 97% accuracy. The comparative performance accuracy in detecting 12 DDoS attacks and benign flow demonstrates that the LSTM-based IDS outperforms the state-of-the-art model [8].

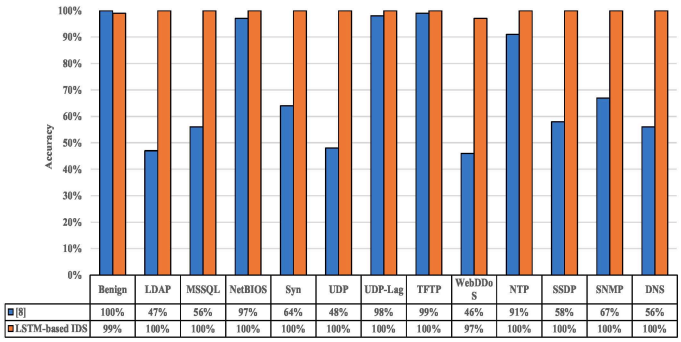

Fig. 10: Performance result for 13-class classification

E. Summary of results

The comparative summary of the overall accuracy with the state-of-the-art model [8] and [9] is shown in Fig. 11. The LSTM-based IDS outperforms as compared with the state-of-the-art models. The LSTM-based IDS shows 99.98% accuracy for Binary classification, 98% accuracy for 7-class and 99.97% accuracy for 13-class classification, which is higher as compared with the state-of-the-art model discussed in [8] and [9]. The data pre-processing steps, PCA techniques,

Authorized licensed use limited to: Birla Inst of Technology and Science Pilani Dubai. Downloaded on November 17,2024 at 10:59:03 UTC from IEEE Xplore. Restrictions apply.

and hyperparameter settings such as *RMSprop* optimizer and *Relu* activation function contribute to a smoother and faster LSTM-based IDS training and testing process. As a result, the LSTM-based IDS excels and outperforms in terms of individual DDoS attack accuracy and overall accuracy. In addition, the LSTM-based IDS two-LSTM layer, followed by a one-dense layer as the output layer, is lightweight, simple, and less complex. The state-of-the-art model [9] includes a one-input layer, a one-LSTM layer with neuron 1280, and an output layer. Another state-of-the-art model [8] includes five-LSTM layer, four-dropout layer, and one-dense layer as on output with neurons 67, 300, 600, 300, 67.

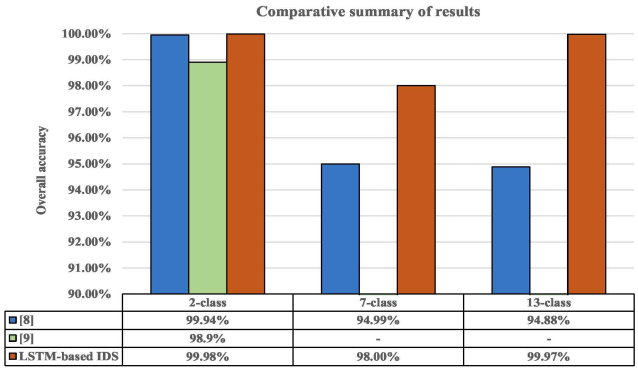

Fig. 11: Comparative summary with state-of-the art model

V. Conclusions

The paper proposed smart LSTM-based IDS for HetIoT networks to safeguard against various DDoS attacks. The data pre-processing step using EDA, Feature extraction using PCA techniques help the LSTM-based IDS perform well and achieve better accuracy compared to the state-of-the-art models. Also, the overall performance of the LSTM-based IDS is good when compared with the existing state-of-the-art models. The smart LSTM-based model is lightweight, simple, and less complex compared to the state-of-the-art models. The proposed LSTM-based HetIoT model shows 99.98% accuracy for Binary classification, 98% accuracy for 7-class, and 99.97% accuracy for 13-class classification. In future work, will concentrate on real-time implementation of the model on a hardware test-bed and also explore the application of reinforcement learning for DDoS detection.

References

[1] T. Qiu, N. Chen, K. Li, M. Atiquzzaman, W. Zhao (2018), "How Can Heterogeneous Internet of Things build our Future A survey", IEEE Communications Surveys & Tutorials, vol.20(3), pp.2011–2027.

[2] SCOTT IKEDA, IoT-Based DDoS Attacks Are Growing and Making Use of Common Vulnerabilities [Online]. Available: https://www.cpomagazine.com/cyber-security/iot-based-ddos-attacks-are-growing-and-making-use-of-common-vulnerabilities/. [Accessed: 25-Mar-2020].

[3] Cloudfare-Famous DDoS attack [Online]. Available: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/.

[4] Cicsco DDoS Annual Report (white paper) [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. [Accessed: 9-MAR-2020].

[5] Badamasi UM, Khaliq S, Babalola O, et al, "A Deep Learning based approach for DDoS attack Detection in IoT-enabled Smart environments", International Journal of Computer Networks and Commu. Security, vol. 8(10), pp.93–99, (2020).

[6] Amaizu GC, Nwakanma CI, Bhardwaj S, et al, "Composite and Efficient DDoS attack Detection framework for B5G networks", Computer Networks, Elsevier, vol. 188:107, pp.871, (2021).

[7] Javeed D, Gao T, Khan MT, "SDN-enabled Hybrid DL-driven framework for the Detection of Emerging Cyber Threats in IoT", Electronics, MDPI, vol. 10(8), pp.918, (2021).

[8] Ferrag M.A., Shu L., Djallel H., Choo K.-K.R., "Deep Learning-Based Intrusion Detection for Distributed Denial of Service Attack in Agriculture 4.0", Electronics, MDPI, vol. 10, pp.1257–1283, (2021). DOI: 10.3390/electronics10111257.

[9] Jia Y, Zhong F, Alrawais A, et al, "Flowguard: An intelligent Edge Defense Mechanism against IoT DDoS attacks", IEEE Internet of Things Journal, IEEE, vol.7(10), pp.9552–9562, (2020).

[10] Meenakshi, K. Kumar and S. Behal, "Distributed Denial of Service Attack Detection using Deep Learning Approaches ", In: 2021 8th International Conf. on Computing for Sustainable Global Development (INDIACom), IEEE, pp. 491–495 (2021).

[11] Laghrissi, F., Douzi, S., Douzi, K. et al, "Intrusion Detection Systems using Long Short-Term Memory (LSTM)", Journal of Big Data, Springer, vol.8, pp.65, (2021). DOI:10.1186/s40537-021-00448-4.

[12] Rohith Gandhi, A Look at Gradient Descent and RMSprop Optimizers [Online]. Available: https://towardsdatascience.com/a-look-at-gradientdescent-and-rmsprop-optimizers-f77d483ef08b. [Accessed: 05-Nov-2019].

[13] M. D. Hossain, H. Ochiai, D. Fall and Y. Kadobayashi, "LSTM-based Network Attack Detection: Performance Comparison by Hyper-parameter Values Tuning", In: 2020 7th IEEE International Conf. on Cyber Security and Cloud Computing (CSCloud), pp.62–69, (2020) DOI: 10.1109/CSCloud-EdgeCom49738.2020.00020.

[14] Gaur V, Kumar R, "Analysis of Machine Learning Classifiers for Early Detection of DDoS Attacks on IoT Devices", Arabian Journal for Science and Engineering, Springer, pp.1–22, (2021).

[15] Sharafaldin I, Lashkari AH, Hakak S, et al, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy", In: 2019 International Carnahan Conf. on Security Technology (ICCST), IEEE, pp.1–8, (2019).

[16] CICDDoS2019 Dataset [Online]. Available: https://www.unb.ca/cic/datasets/ddos-2019.html. [Accessed: 2019].

[17] Prasad Patil, Exploratory Data Analysis (EDA) [Online]. Available: https://towardsdatascience.com/exploratory-data-analysis-8fc1cb20fd15/. [Accessed: 23-MAR-2018].

[18] Elsayed, M. S., Le Khac, N. A., Dev, S. & Jurcut, A. D., "DDoSnet A Deeplearning Model for Detecting Network Attacks", In: IEEE 21st International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), IEEE, pp.391–396, (2020).

[19] Aditya sharma, Principal Component Analysis (PCA) [Online]. Available: https://www.datacamp.com/tutorial/principal-component-analysis-in-python, [Accessed: 1-Jan-2020].

[20] Jason Brownlee, Hyperparameter Optimization With Random Search and Grid Search [Online]. Available: https://machinelearningmastery.com/hyperparameter-optimization-with-random-search-and-grid-search/, [Accessed: 19-Sep-2020].

[21] Divyang Goswami, Comparison of Sigmoid, Tanh and ReLU Activation Functions [Online]. Available: https://www.aitude.com/comparison-of-sigmoid-tanh-and-relu-activation-functions/. [Accessed: 19-Aug-2020].

[22] Devrim Akgun, Selman Hizal, Unal Cavusoglu, "A new DDoS attacks Intrusion Detection Model based on Deep Learning for Cybersecurity", Computers & Security, Elsevier, Vol.118, pp.102748, (2022), ISSN 0167-4048, DOI: 10.1016/j.cose.2022.102748.

[23] Christian Versloot, How-to-use-sparse-categorical-crossentropy-in-keras [Online]. Available: https://github.com/christianversloot/machine-learning-papers/blob/main/how-to-use-sparse-categorical-crossentropy-in-keras.md, [Accessed: 01-Feb-2020].

Authorized licensed use limited to: Birla Inst of Technology and Science Pilani Dubai. Downloaded on November 17,2024 at 10:59:03 UTC from IEEE Xplore. Restrictions apply.