Multidisciplinary International Journal of Research and Development

Volume: 01 | Issue: 02 | 2021 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

Towards a Secure Infrastructure for the IoT's Using Deep Learning

Muhammad Usman Arshad[1], Usama Jameel[2], Fawad Iqbal[3], Basharat Ali[4], and Natasha Khaliq[5]

[1,2,3,4] Software College, Northeastern University, Shenyang 110169, China

[5] Changchun University of Science and Technology, Changchun 130022, China

Email: [1]usmanarshad5051@outlook.com

Abstract— The Internet of Things has become a very important sector and has recognized to be a billion-dollar commerce. It is a large group of sensors and devices connected through wire or wireless and continuously shares data providing several benefits. Still, at the same time, the connectivity and its nature make it a target of cyber-attacks. These devices need to be secured. This paper proposes an intelligent model for securing IoT devices from such attacks. The authors used Gated Recurrent Unit (GRU) and Deep Neural Network (DNN) classifier, which has been trained and evaluated under the CICMAL2017 dataset. The performance of this model is assessed under all the standard evaluation metrics. The attained accuracy of our model is 99.3 %, with a precision of 99.7 %. Finally, to demonstrate the suggested model's efficacy, we compare it to alternative models.

Keywords— IoT, Deep Learning, Cyber-security, Threats, Malware.

I. INTRODUCTION

The Internet of Things (IoT), defined as a global network of networked gadgets with unique addresses, has seen tremendous expansion in modern years. The devices of IoT can be categorized into two categories: edge devices and gateway devices. The gateways devices have significantly greater resources than the edge devices. The edge devices are primarily low-power devices which duty is to collect the data and send it to the gateway [1]. These devices use different communication protocols along with sensing features. Because of the increasing growth of data in IoTs, IoT networks are the target of a large variety of assaults and threats [2]. Around eighty percent of cybersecurity specialists attempt to resolve at least one security issue each day, while sixty percent of professionals spend one hour or two a day dealing with network operations and security [3]. Cyber-physical systems have advanced at a breakneck pace in recent years because of the advances in computing and hardware technology. Such advancements resulted in the growth of numerous attacks, such as making the resource of the system unavailable, known as DoS attack. The authors of [4] discussed the replay and deception attacks along with the detection techniques of these attacks on the industrial level. Different security measures apply to different types of protocol-following devices that must be adhered to. According to multiple research surveys, internet sensors could be installed in vehicles, furniture, and plants by the end of 2025. To safeguard the entire IoT infrastructure, no integrated strategy has yet been devised. Traditional strategies of intrusion detection are used to defend the system from threats, and they work at the set-up level using IDS and IPS, Still, due to the heterogeneous and seamless nature of the devices of IoT, such security measures aren't enough to protect them from attacks. In automatic malware detection, deep learning plays a critical role. Deep Learning is one of the most extensively used research topics, and as a result of its growing popularity, it has gotten a lot of attention and sparked a lot of applications in threat detection [5].

Deep learning-based security solutions exhibit excellent efficiency and accuracy in the case of threat detection in IoT environments. That's why the authors aim to use GRU and DNN classifiers for effective threat detection to secure the IoT environment.

II. RELATED WORK

IoT is a networking environment in which physical items are incorporated into it in a method that they become dynamic members in this process. More than 46 billion devices of the IoT will be in operation by 2021, according to Juniper. This includes devices and sensors, as well as acutators, and represents a 200 percent growth over 2016 [6].

Certain real-time cyber security intrusion that are searched for by AV softwares are outlined in relation to the security difficulties faced in the IoT context. Numerous researches have used different techniques of deep learning for detecting threats and intrusions in IoT. In [7], the authors used a hybrid model of deep learning for threat detection in IoT by using a publicly available dataset for testing and training purposes.

The authors achieve very efficient detection accuracy with very low testing time. Recurrent neural network (RNN) techniques were utilized by the authors in [8] to recognize and categorize attacks. The performance of RNN-based techniques and non-RNN techniques was compared. The authors offer a self-learning system in [9] with the goal of identifying corrupted/ compromised devices in an IoT environment.

The authors used GRU classifier for this purpose. Some author authors used RF, SVM, LSTM, etc for intrusion detection. The authors of [10] aim to detect botnets by using LSTM classifies, which have been trained and tested on CVUT dataset.

The models of deep learning have been proven to have a very good output when it comes to securing the infrastructures of the Internet of things. The author's anomaly detection technique detected DDoS attacks with an accuracy of 87.35 % is presented in [11].

Further, it presents a DL-based codetection model in conjunction with Snort IDS for detecting IoT-based DDoS attacks. Finally, [12] generates a labeled behavioral data collection of IoT traffic, which includes both benign and malicious traffic.

The dataset for this traffic was generated from a network of 83 devices. From the above discussion, it has been observed that deep learning can show an important role in IDS for extraordinary accuracy for detection of threats and intrusions. A complete literature review is shown in Table 1.

III. METHODOLOGY

This section consists of the proposed methodology with dataset description and proposed detection technique.

Table 1: Existing Literature

Ref	Dataset	Model	Achievements	Limitations
7	CICIIDS2018	DNN-GRU	The authors achieved a good detection accuracy	The dataset is not explored properly
10	CVUT	LSTM	The model can detect botnets at the packet level	The dataset lacks supportive features of IoT
13	MovieLens 10m and 20m	CNN	The proposed methodology can detect the recommendation attack steadily and effectively	Imbalanced samples in the training set, Basic CNN Structure.
14	Data Collected from bitcoin Network	MLP	Achieved an accuracy of 87 %	The proposed method cannot detect the DDoS by imitating all of the features of the chunks formed when the attack happens
15	ICS datasets	DL-based cyber-attack detection method for ICS	The proposed technique outperformed conventional classifiers	Accuracy of the proposed method needs to be optimized, attack types along with locations need to be identified
16	Nine IoT attack detection Datasets	DTL-based approach (MMD-AE)	The proposed method significantly detects IoT Attacks, thus improving the accuracy	The proposed model requires added time for the training of the model.
17	NSL-KDD	Deep Model	Achieved a good accuracy	This dataset lack supportive features of IoT.
18	CTU13-ISOT	CNN-RNN	The model can detect botnets at the packet level	The detection accuracy is low, and time complexity is high
19	CVUT real-time traffic	LSTM	Achieved detection accuracy is good	Unable to determine if a sample is benign or malicious.

A. Proposed Model

The current research proposes a deep learning practice for the detection of malware in the environment of IoT.The proposed model is shown in Figure 1. We have tested and trained the proposed models, GRU and DNN. The Detection accuracy is improved due to a lower number of false positives. To acquire efficient findings, the try-outs were repeated up to 40 epochs with 64 batch size. After multiple experiments, these best parametric values were discovered. For the purposes of implementation, we used the Keras Python framework with TensorFlow as the backend. We have further used a graphical processing unit (GPU) for improved performance. In the proposed DL architecture, we have developed GRU and DNN models. GRU-DNN classifier was implemented for the training and testing of the model. A complete description of the model is shown in Table 2.

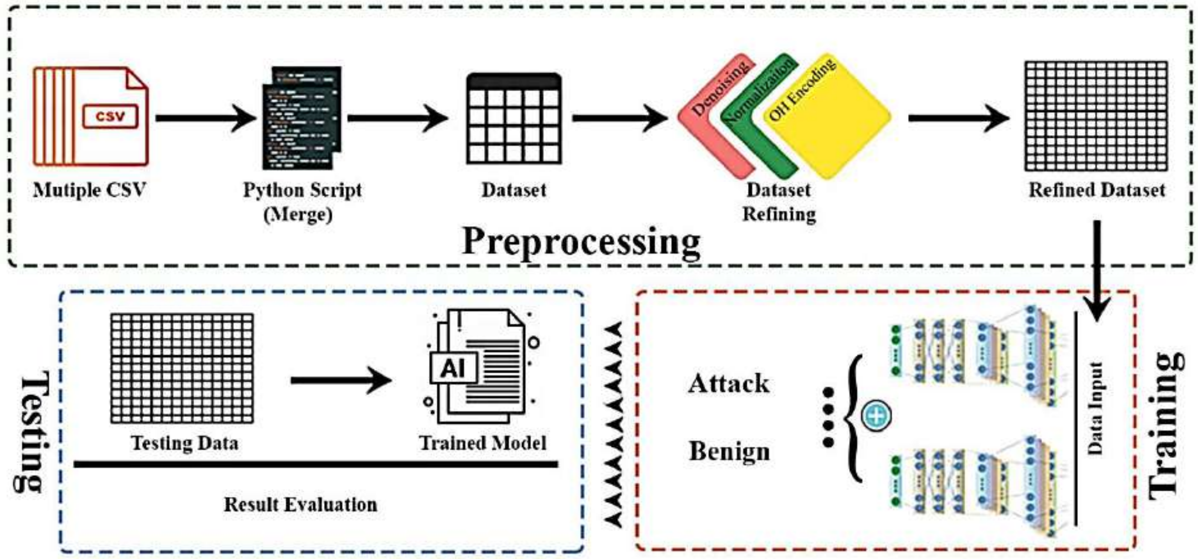

Figure 1: Proposed detection scheme

Table 2: Proposed Model Description

Algorithm	Layers	Optimizer	Neurons	AF	LF	Epochs	Batch-Size
GRU	GRU (1)	Admax	100	Relu	CC-E	40	64
	Dropout		0.3				
	Dense (3)		200,100,50				
	Output (1)		07	Softmax			
DNN	DNN (1)	Admax	100	Relu	CC-E	40	64
	Dropout		0.3				
	Dense (3)		200,100,50				
	Output (1)		07	Softmax			

B. Dataset

Selecting an appropriate dataset is the most important part of the research journey. As the accuracy of the results totally rely on the nature of the dataset, its features, and wholeness. For this research, the dataset utilized is provided by CICMAL17. The dataset comprises multiple output classes, i.e., Adware, Ransomware, etc. All these different classes have been successfully identified in the confusion matrix of the implementation results. Complete detail of the dataset is given in Table 3 below.

C. Feature Scaling

There are multiple features that have been extracted from the dataset by using python. The extracted features of the dataset are shown in Table 3. The dataset contains a rich feature set consisting of more than 80 features. MinMaxScaler function is used that is also known as normalization function, and it transforms all the values in the range between (0 to 1) formula as shown in the equation below:

$$X_{new} = \frac{X_i - \min(X)}{\max(x) - \min(x)} \qquad (1)$$

Table3. Dataset Details

Category	Type
Ransomware	PornDroid, pletor, charger family, wannaLocker, jisut
Adware	Feiwo, koodus, selfmite, gooligan, kemoge
Scareware	AVpass, faketaobao, penetho, fakejoboffer
SMS Malware	Zsone, jifake, fakeinst, biige

IV. RESULTS & DISCUSSION

This section comprises the experimentation results and the discussion. In order to assess the model's performance, all of the standard evaluation metrics have been followed, e.g., accuracy, recall, F1-score, Confusion metric, TPR, TNR etc.

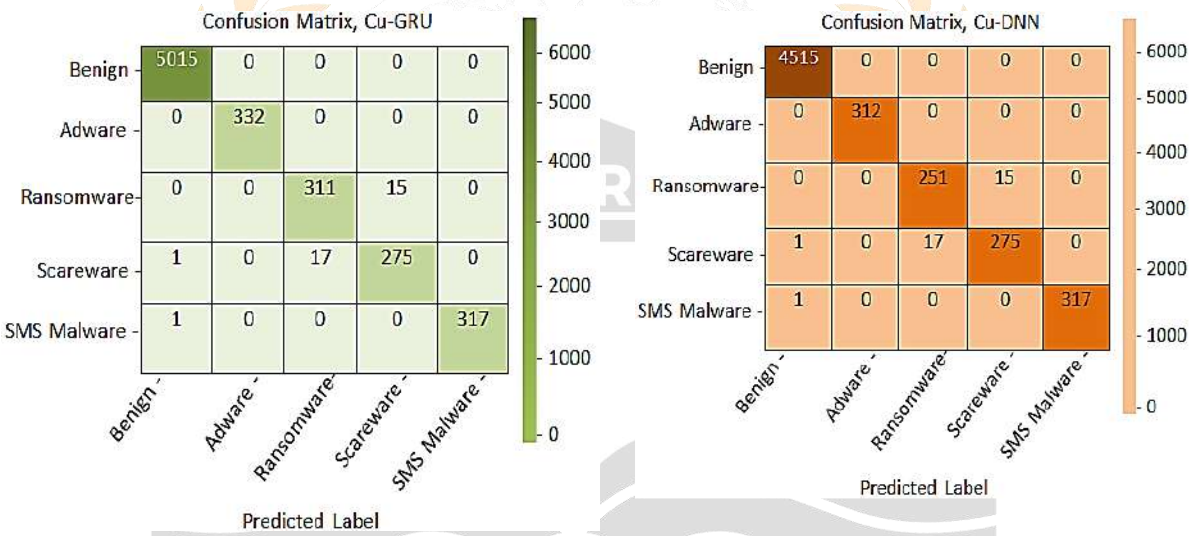

Figure 2: Confusion Metrics

The confusion matrix is mostly used to classify objects. It depicts whether the planned output will consist of five or six classes. It is represented by a quadrilateral structure with rows and columns; hence, rows are the genuine classes of the images, while columns are the derived classes. The confusion metrics of the proposed models are shown in figure 2. For a systematic assessment, the projected work depicts the detection accuracy of the classifiers. The result clearly illustrates that the projected model has a 99.30 percent accuracy, which is significantly superior than the other model. The accuracy was determined by applying the GRU and DNN algorithms to the dataset in order to train the threat detection algorithm. Our proposed model is quite efficient, as evidenced by the achieved accuracy. It further means that it is 99.30 % accurate in terms of threat detection. The precision of the proposed model is 99.70 %. However, the DNN

Volume: 01 | Issue: 02 | 2021 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

achieved a precision of 96.80 %. Further, the F1 –score and recall of the GRU model is 99.20 % and 99.47 %, respectively. The accuracy, precision, etc., is shown in figure 3.

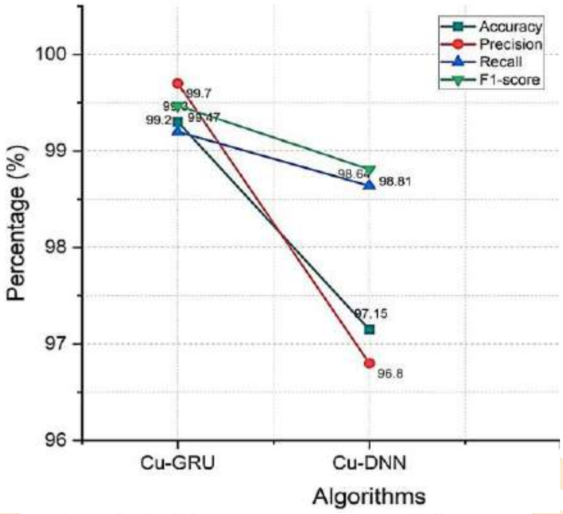

Figure 3: Accuracy, precision of the models

False discover rate (FDR), False positive rate (FPR), False negative rate (FNR), and False omission rate (FOR) are some of the evaluation metrics that are measured in the proposed study for a better estimation. Figure 4 demonstrates that our results had a Fpr of only 0.0035 percent, a Fnr of only 0.0023 percent, and FDR and FOR of only 0.028 and 0.0049 percent, respectively.

The Matthews correlation coefficient (MCC) is a further reliable arithmetical rate that produces a high score only if the prediction is correct in all of the four areas of the confusion matrix. (TPR, FNR, TNR, and FPR). The TPR, TNR, and MCC were calculated using an uncertainty matrix. The values of the Tpr, Tnr, and Mcc of the models are clearly seen in Figure 5. The proposed model achieved the values of 99.33, 99.13, and 98.03 percent.

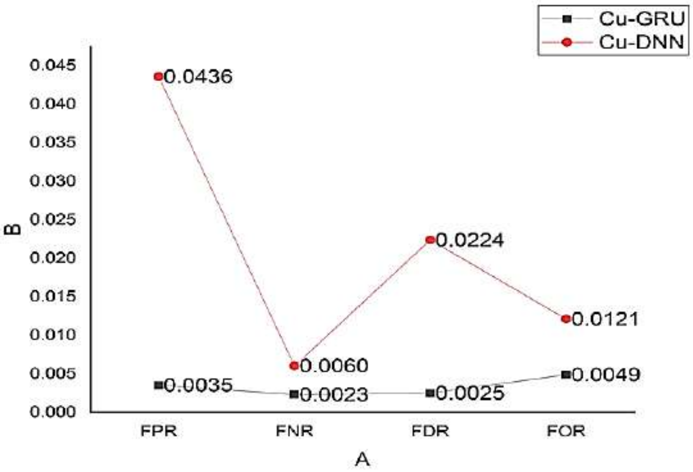

Figure 4: FPR, FNR FDR of the models

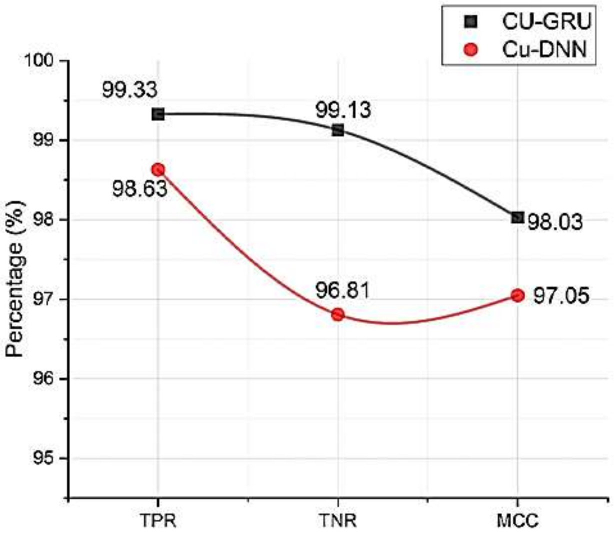

Figure 5: TPR, TNR and MCC

V. CONCLUSION

The widespread connectivity and the heterogeneous nature of the IoT devices make them a target of numerous cyber-threats, and thus IoT necessitates a dependable, versatile, and secure infrastructure. The authors present a flexible and reliable model to protect the IoT environment and its devices from sophisticated threats, i.e., DoS, botnets, adware, and other malware. Deep learning has attracted the attention of the entire globe as a result of its advancement. In this research work, we have used two state-of-the-art classifiers, i.e., GRU and DNN, for the purpose of experimentation. The power of the GPU and the CPU have been used for testing purposes for improved performance. The architecture presented is both cost-effective and scalable. The proposed framewrok attained an accuracy of 99.30 percent 99.33 percent of TPR. The output validates the effectiveness of our projected model. In the future, the authors hope to leverage a variety of datasets and deep learning techniques to detect malware in IoT environments.

REFERENCES

[1] Khan, Tahir Ullah. "Internet of Things (IOT) systems and its security challenges." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 8.12 (2019).

[2] Al Shorman, A.; Faris, H.; Aljarah, I. Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection. J. Ambient. Intell. Humaniz. Comput. 2019, 11, 2809–2825.

[3] Ferdowsi, A.; Saad, W. Deep Learning for Signal Authentication and Security in Massive Internet-of-Things Systems. IEEE Trans. Commun. 2019, 67, 1371–1387.

[4] Bhunia, S.S.G.M. Dynamic attack detection and mitigation in IoT using SDN. In Proceedings of the 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 22–24 November 2017; pp. 1–6.

[5] Javeed, D., Gao, T., & Khan, M. T. (2021). SDN-Enabled Hybrid DL-Driven Framework for the Detection of Emerging Cyber Threats in IoT. Electronics, 10(8), 918. URL: https://www.mdpi.com/2079-9292/10/8/918/pdf

[6] Ojo, M.; Adami, D.; Giordano, S. A SDN-IoT architecture with NFV implementation. In Proceedings of the IEEE Globecom Workshops (GC Wkshps), Washington, DC, USA, 4–8 December 2016; pp. 1–6.

[7] Javeed D, Gao T, Khan MT, Ahmad I. A Hybrid Deep Learning-Driven SDN Enabled Mechanism for Secure Communication in Internet of Things (IoT). Sensors. 2021 Jan;21(14):4884.

[8] Vinayakumar, R.; Soman, K.P.; Poornachandran, P. Evaluation of Recurrent Neural Network and its Variants for Intrusion Detection System (IDS). Int. J. Inf. Syst. Model. Des. 2017, 8, 43–63.

[9] Nguyen, T.D.; Marchal, S.; Miettinen, M.; Fereidooni, H.; Asokan, N.; Sadeghi, A.-R. DÏoT: A Federated Self-Learning Anomaly Detection System for IoT. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019; pp. 756–767.

[10] Torres, P.; Garcia, C.C.S.; Garino, C.G. An analysis of recurrent neural networks for botnet detection behavior. In Proceedings of the 2016 IEEE Biennial Congress of Argentina (ARGENCON), Buenos Aires, Argentina, 15–17 June 2016; pp. 1–6.

[11] Ujjan, R.M.A.; Pervez, Z.; Dahal, K.; Bashir, A.K.; Mumtaz, R.; González, J. Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN. Future Gener. Comput. Syst. 2020, 111, 763–779.

[12] Ujjan, R.M.A.; Pervez, Z.; Dahal, K.; Bashir, A.K.; Mumtaz, R.; González, J. Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN. Future Gener. Comput. Syst. 2020, 111, 763–779. URL: https://www.sciencedirect.com/science/article/pii/S0167739X19318333

[13] Zhou Q, Wu J, Duan L. Recommendation attack detection based on deep learning. Journal of Information Security and Applications. 2020 Jun 1;52:102493.

[14] U. Baek, S. Ji, J. T. Park, M. Lee, J. Park and M. Kim, ”DDoS Attack Detection on Bitcoin Ecosystem using Deep-Learning,” 2019 20th Asia- Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 2019, pp. 1-4, doi: 10.23919/APNOMS.2019.8892837.

[15] Al-Abassi A, Karimipour H, Dehghantanha A, Parizi RM. An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System. IEEE Access. 2020 May 4;8:83965-73.

[16] Vu L, Nguyen QU, Nguyen DN, Hoang DT, Dutkiewicz E. Deep Transfer Learning for IoT Attack Detection. IEEE Access. 2020 Jun 8;8:107335-44.

[17] A. A. Diro and N. Chilamkurti, “Distributed attack detection scheme using deep learning approach for internet of things,” Future Generation Computer Systems, vol. 82, pp. 761–768, 2018.

[18] Pekta¸s, A.; Acarman, T. Botnet detection based on network flow summary and deep learning. Int. J. Netw. Manag. 2018, 28, e2039.

[19] Javeed D, Badamasi UM, Iqbal T, Umar A, Ndubuisi CO. Threat Detection using Machine/Deep Learning in IOT Environments. International Journal of Computer Networks and Communications Security. 2020 Aug 1;8(8):59-65. [Google Scholar]