An Intelligent Intrusion Detection System For Smart Consumers

Mr .P. Muthyalu, Associate Professor, Department of CSE, Narayana Engineering College Gudur.

P. Phani Datta, Department of CSE, Narayana Engineering College, Gudur.

Abstract: The technological advancements of Internet of Things (IoT) has revolutionized traditional Consumer Electronics (CE) into next-generation CE with higher connectivity and intel ligence. This connectivity among sensors, actuators, appliances, and other consumer devices enables improved data availability, and provides automatic control in CE network. However, due to the diversity, decentralization, and increase in the number of CE devices the data traffic has increased exponentially. Moreover, the traditional static network infrastructure-based approaches need manual configuration and exclusive management of CE devices. Motivated from the aforementioned challenges, this article presents a novel Software-Defined Networking (SDN) orchestrated Deep Learning (DL) approach to design an intelligent Intrusion Detection System (IDS) for smart CE network. In this approach, we have first considered SDN architecture as a promising solution that enables reconfiguration over static network infrastructure and handles the distributed architecture of smart CE network by separating the control planes and data planes. Second, an DL-based IDS using Cuda-enabled Bidirectional Long Short-Term Memory (Cu-BLSTM) is designed to identify different attack types in the smart CE network. The simulations results based on CICIDS-2018 dataset support the validation of the proposed approach over some recent state-of the-art security solutions and confirms it a phenomenal choice for next-generation smart CE network.

Keywords: Consumer Electronics, Cyber-Attacks, Deep learning, Internet of Things, Intrusion Detection System, Software-Defined Networking

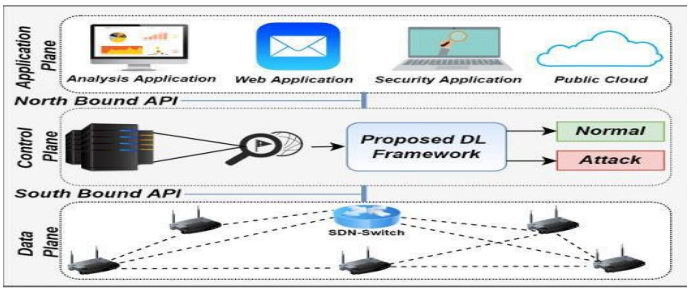
INTRODUCTION

The Internet of Things (IoT) is a network of devices embedded with software programs and sensors that utilizetheInternettocommunicatedata.TheamalgamationofIoTintotraditionalConsumerElectronics (CEs) has revolutionized it into next-generation CEs with higher connectivity and intel ligence. This improved data availability and automatic control in the CE network are made possible by the connectivity of sensors, actuators, appliances, and other consumer devices [1]. Nevertheless, CE devices connections are now remotely accessed anytime, anywhere in the world with the utilization of computing devices, including laptops, smartphones, and smartwatches, regardless of the network to which they are connected. These smart devices can be used in various fields, including smart homes [2]. The CE devices have significantly evolved in the last decade. According to a recent study, the CE segment might reach 2,873.1m users by 2025 while the Average Revenue Per User (ARPU) is expected to amount to US 317.10 billion [3]. Today, every device may create and share data online, contributing to the CE expansion. The traditional internet architecture is a complex system with a multitude of network components, i.e., routers, middleboxes,

switches, and several layers, etc. due to decentralization [4]. Therefore, the traditional network design likewise struggles to adapt to the dynamic nature of modern applications.

RELATEDWORK

The CE is characterized by the integration of physical things into a network in a way that makes them active participants in corporate operations. These objects might include everything from network gear to sensors to home and healthcare products. CE is made up of a range of devices that can be wireless or wired and can be used in several places and networks. According to a recent Juniper report, more than 46 billion IoT devices were in operation by 2021. This includes sensors, actuators, and gadgets and represents a 200% growth over 2016 [11]. In any changing computer and network paradigm, IoT becomes an integral part of it. IoT transformation is growing exponentially, leading to significant growth in terms of revenue and automation. Because these devices are created to satisfy the individual demands of users, it is difficult to find a solution that works for everyone [12]. With security being a key concern right now, determining the security of these devices is difficult. These products are too diverse to be compared to a single procedure.

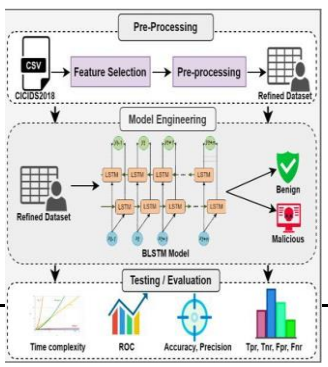


METHODOLOGY

A Network Model

SDN is considered as a well-established method for building integrated networks in recent years. Its architecture separates the data planes and control planes, allowing simplicity and f lexibility. Furthermore, in traditional networks, each router in the network can only perceive the network's local state. The lack of a full overview of the whole network makes it challenging to construct a potentially powerful defensive mechanism against cyber threats. SDN, on the other hand, pro vides a global network perspective and centralized control ca pabilities, making network statistics easier to obtain. In SDN, the control plane manages routing choices, data transfers, and traffic monitoring via application techniques.The data plane in corporates many CE devices, such as intelligent devices,

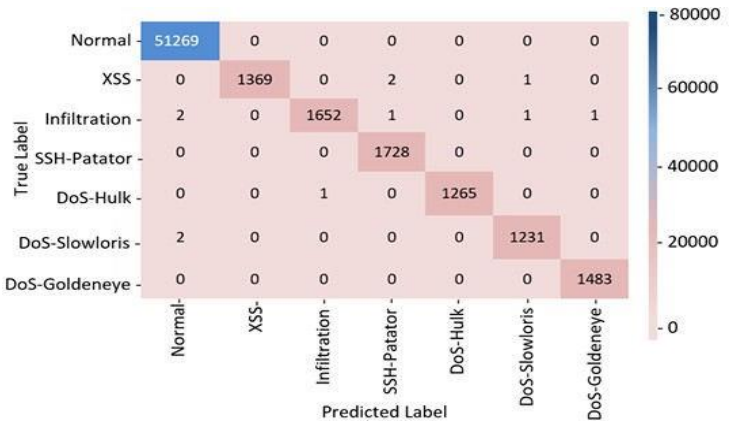
Proposed DL-driven BLSTM-based framework



The proposed acquisition module. Cu of two layers with 200 and 100 neurons. In addition, we added one dense layer with 30 neurons. The proposed work utilized Reluas the activation function (AF) for all levels except the output layer. SoftMax, on the other hand, is employed in the output layer.The Categorical Cross entropy (CC-E) is used as a loss function (LF). Tests are run up to 10 epochs with 64 batch sizes to acquire effective findings. We utilized Cuda-enabled versions for GPU processing for an enhanced performance. Furthermore, the authors used the Keras framework, which is the foundation for Python TensorFlow. Cuda is a GPU-enhanced library that enables repeated readings, resulting in quicker multiplication of matrices. Moreover, we have used Cu-DNN and Cu-GRU as comparison models that have been trained and evaluated in the same environment. Cu-DNNconsistsoffourdenselayerswith100,75,50and30 neurons, respectively. Further, Cu GRU comprises four layers of GRU with neurons of 500,400, 300,and 100,respectively,with one dense layer of 03 neurons.

Cu-BLSTM

The proposed work used the Cu-BLSTM model for effective and timely threat detection in smart CE networks. An Artificial Neural Network (ANN) type called Recurrent Neural Networks (RNN) offers much promise for learning from earlier time steps. RNN utilizes Back Propagation Through Time to constantly learn from previous time steps. Standard RNN cannot perform better when time steps overlap. The RNN employs feedback loops and links hidden units to preserve information over time. It can take consecutive inputs of any length and produce fixed-length outputs because of such features, The back-propagation causes error signals to disappear or explode, causing weights to fluctuate, resulting in poor system performance and gradient vanishing problems. Analysts focused on Long-Short-Term Memory (LSTM), as LSTM blocks can save information for a long time. RNN with LSTM blocks was designed to solve this issue. However, to address the short comings of the LSTM model, researchers improved it and is known as BLSTM. By traversing time steps both forward and backward, BLSTM makes the best use of the data. To generate two layers side by side, the architecture copies the first recurrent network. The input is sent to the first layer in its original form, while the second layer receives a copy that has been reversed.

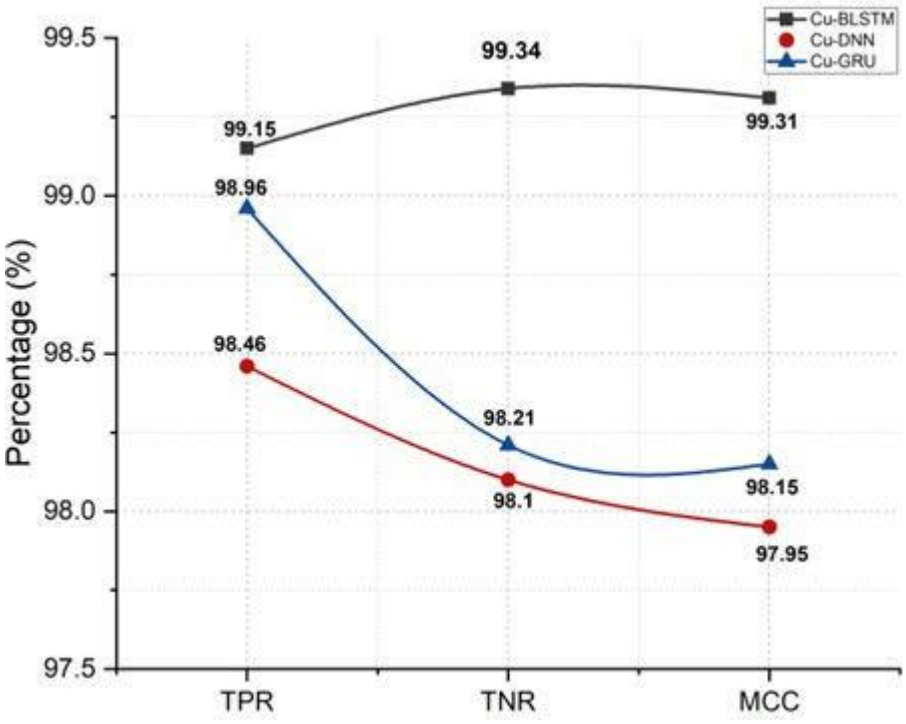


Confusion matrix of Cu-BLSTM

Result and Discussion

This scientific study employed 10-fold cross-validation, and the findings are displayed in Table II to explicitly demonstrate unbiased outcomes. For a better understanding, each fold's results are shown in this section. The confusion matrix depicts the model's performance in the test dataset. Data that is binary or multi-category. It is advantageous to assess the receiver's operational element's accuracy, precision, memory, and curve (ROC). The confusion matrix of the proposed model is depicted . The figure is evident that the proposed model identifies all five classes properly. Further, the ROC curve corrects the given data so that positive and negative positive values may be compared. The extent of segregation is mostly determined by the success of various class division issues, as demonstrated by the ROC. The ROC curve structure is located between the TP and FP levels. depicts the ROC of the proposed Cu-BLSTM model, demonstrating the efficiency of the proposed model. The authors further provided the ACC, PN, RL, and FS of the CU-BLSTM model along with the baseline techniques. The detection accuracy reveals the Cu-BLSTM efficiency and performance. Fig 5 depicts the ACC, PN, RL, and FS of all three models. The proposed model achieved 99.57% ACC with 99.62% PN. Further, the proposed model is having FS and RL of 99.23% and 99.39% respectively. The figure is evident that the proposed Cu-BLSTM model outclassed the baseline models. We have further provided the per-class accuracy of all three models in Table III respectively. Other performance assessment methodologies , such as FP rate,FOrate,FDrate,andFNratearealsostudiedtoproperlyevaluatetheproposedmodel.Fig6demonstrates that our proposed model has values of 0.0033, 0.0022, 0.0033, and 0.0029 percent for the FP rate, FN rate, FD rate, and FO rate. Furthermore, Cu-GRU outperforms Cu-DNN in terms of such metrics. For a thorough assessment, we have further calculated the TPR, TNR, and MCC. These values are obtained using the uncertainty matrix .

Parameter	Models	1	2	3	4	5	6	7	8	9	10
ACC (%)	BLSTM	99.43	99.41	99.63	99.52	99.74	99.67	99.80	99.46	99.49	99.56
	DNN	98.59	98.53	98.90	99.21	98.81	99.1	98.81	99.42	99.23	98.86
	GRU	98.59	98.81	99.10	99.42	99.26	99.29	99.12	98.89	98.82	98.33
RL (%)	BLSTM	99.90	99.89	99.21	99.18	99.23	99.85	99.12	99.14	99.10	99.16
	DNN	98.59	98.52	98.43	98.52	98.21	98.30	99.14	99.65	99.14	99.16
	GRU	98.94	99.25	99.03	99.17	99.15	98.99	99.21	98.96	98.90	97.56
PN (%)	BLSTM	99.82	99.65	99.51	99.62	99.23	99.46	99.69	99.83	99.89	99.91
	DNN	98.95	99.25	98.31	98.23	98.29	98.56	98.64	98.79	99.25	99.65
	GRU	98.89	99.05	98.59	99.10	99.21	99.35	99.26	99.19	99.14	99.29
FS (%)	BLSTM	99.20	99.28	99.15	98.81	99.14	99.29	99.05	99.56	99.21	99.69
	DNN	98.69	98.51	98.56	98.86	99.12	98.87	98.64	98.93	99.12	98.71
	GRU	98.72	98.83	98.97	99.15	99.49	99.11	98.98	98.96	98.89	98.34



Overall TPR, TNR and MCC of Cu-BLSTM against baseline models.

CONCLUSION

In this article, to protect consumer electronics network, we proposed an intelligent intrusion detection system based on software-defined networking-orchestrated deep learning approach. Specifically, software-defined networking architecture was integrated with consumer electronics network to handle its distributed architecture and heterogeneous consumer electronic devices. Then, an IDS based on cuda-enabled bidirectional long short-term memory was proposed and deployed at control plane to enhance threat detection mechanism. We proved the effectiveness of the proposed IDS in terms of accuracy, precision and speed efficiency through experimental evaluation on the CICIDS-2018dataset.We also compared the performance of the proposed IDS against some recent state-of-the art technique. In the future we aim to train the model on different datasets further improve intrusion detect in in such networks. Finally, we endorse DL-based Intelligent models for efficient threat detection in next-generation smart consumer electronic networks.

REFERENCES

[1]C.K.Wu,C.-T.Cheng,Y.Uwate,G.Chen,S.MumtazandK.F.Tsang(2022),"State-of-the-Artand Research Opportunities for Next Generation Consumer Electronics," in IEEE Transactions on Consumer Electronics, doi: 10.1109/TCE.2022.3232478.

[2] R. Amin, M. Reisslein, and N. Shah, "Hybrid SDN networks: A survey of existing approaches, IEE Commun. Surveys Tuts., vol. 20, no. 4, pp.32593306, 4th Quart., 2018.

[3] Statista. (2022, July 28). Consumer Electronics. In Statista, Electronics. Retrieved 14:57, July 28, 2022, from https://www.statista.com/outlook/dmo/ecommerce/electronics/consumer-electronics/worldwide

[4] Al Razib, M., Javeed, D., Khan, M. T., Alkanhel, R., & Muthanna, M. S.A. (2022). Cyber Threats Detection in Smart Environments Using SDN-Enabled DNN-LSTM Hybrid Framework. IEEE Access, 10, 53015-53026.

[5] Yamauchi, M., Ohsita, Y., Murata, M., Ueda, K., & Kato, Y. (2020).Anomaly detection in smart home operation from user behaviors and home conditions. IEEE Transactions on Consumer Electronics, 66(2),183-192.

[6] 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.

[7] K. Kalkan, G. Gur, and F. Alagoz, "Defense mechanisms against ddosattacks in sdn environment", IEEE Communications Magazine, vol. 55,no. 9, pp. 175–179, 2017.

[8] L. N. Tidjon, M. Frappier, and A. Mammar, "Intrusion detection systems: A cross-domain overview," IEEE Communications Surveys &Tutorials, 2019.

[9] Prabhakar, G. A., Basel, B., Dutta, A., & Rao, C. V. R. (2023). Multi-channel CNN-BLSTM Architecture for Speech Emotion Recognition System by Fusion of Magnitude and Phase Spectral Features using DCCA for Consumer Applications. IEEE Transactions on Consumer Electronics.

[10] R. Kumar, P. Kumar, A. Kumar, A. A. Franklin and A. Jolfaei,"Blockchain and Deep Learning for Cyber Threat-Hunting in Software-Defined Industrial IoT," 2022 IEEE International Conference on Communications Workshops (ICC Workshops), 2022, pp. 776-781, doi: 10.1109/ICCWorkshops53468.2022.9814706.

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

[12] Saurabh, Kumar, et al. "LBDMIDS: LSTM Based Deep Learning Model for Intrusion Detection Systems for IoT Networks." 2022 IEEE WorldAI IoT Congress (AIIoT). IEEE, 2022.

[13] Jindal, Anish, et al. "SeDaTiVe: SDN-enabled deep learning architecture for network traffic control in vehicular cyber-physical systems." IEEE network 32.6 (2018): 66-73.

[14] S. Khorsandroo, A. G. S´anchez, A. S. Tosun, J. Arco, and R. Doriguzzi-Corin, "Hybrid SDN evolution: A

comprehensive survey of the state-of-the-art," Comput. Netw., vol. 192, Jun. 2021, Art. no. 107981.

[15] Ren, Xiaodong, et al. "Adaptive recovery mechanism for SDN con-trollers in Edge-Cloud supported FinTech applications." IEEE Internet of Things Journal (2021).

[16] J. Cui, M. Wang, Y. Luo, and H. Zhong, "DDoS detection and defense mechanism based on cognitive-inspired computing in SDN," Future Gener. Comput. Syst., vol. 97, pp. 275283, Aug. 2019.

[17] X.-H. Nguyen, X.-D. Nguyen, H.-H. Huynh and K.-H. Le, "Real guard: A lightweight network intrusion detection system for IoT gateways",Sensors, vol. 22, no. 2, pp. 432, Jan. 2022.

[18] Otoum, Y., Liu, D., & Nayak, A. (2022). DL-IDS: a deep learning–based intrusion detection framework for securing IoT. Transactions on Emerging Telecommunications Technologies, 33(3), e3803.[19] R. Ahmad, I. Alsmadi, W. Alhamdani et al., "A comprehensive deep learning benchmark for IoT IDS," vol. 114, pp. 102588, 2022.