A SOPHISTICATED TECHNIQUE FOR DETECTING THE INTRUSIONS ON NETWORKS OF SMART CONSUMER GADGETS

1 Katti. Jaya Krishna, 2 Ponduri Venkata Sai Divya,
1Associate Professor, Department of Master of Computer Applications,
QIS College of Engineering & Technology, Ongole, Andhra Pradesh, India
2PG Scholar, Department of Master of Computer Applications,
QIS College of Engineering & Technology, Ongole, Andhra Pradesh, India

Abstract: This project aims to tackle the cybersecurity challenges prevalent in smart CE networks, recognizing the inadequacy of conventional security measures. Additionally, it addresses the dynamic nature of IoT-enhanced CE networks, which demand adaptable security solutions. This project introduces a pioneering Intrusion Detection System (IDS) tailored for IoT-enabled smart Consumer Electronics (CE) networks. Furthermore, it emphasizes the need for an IDS that can seamlessly integrate into the evolving CE landscape, promoting user-friendly implementation. The IDS leverages Deep Learning techniques to precisely identify various attack types within the smart CE network. Moreover, it underlines the importance of real-time threat detection to prevent network vulnerabilities. Simulation results, utilizing the CICIDS-2018 dataset, substantiate the robustness and suitability of the proposed approach for safeguarding next-generation smart CE networks. Additionally, it highlights the significance of empirical validation in ensuring the reliability of the security system. And also, we enhanced the Intrusion Detection System (IDS) by incorporating a Convolutional Neural Network (CNN) and a hybrid model combining CNN with Long Short-Term Memory (LSTM). This hybrid approach strategically combines the strengths of both models, achieving remarkable accuracy and outperforming other algorithms with a perfect 100% accuracy rate.

Index terms *- Consumer Electronics, Cyber-Attacks, Deep learning, Internet of Things, Intrusion Detection System, Software-*

Detection System, Software-Defined Networking.

1. INTRODUCTION

The Internet of Things (IoT) is a network of devices embedded with software programs and sensors that utilize the Internet to communicate data. The amalgamation of IoT into traditional Consumer Electronics (CEs) has revolutionized it into next-generation CEs with higher connectivity and intelligence. 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. 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.

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. 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. Therefore, the traditional network design likewise struggles to adapt to the dynamic nature of modern applications. Moreover, the traditional static network infrastructure-based approaches need manual configuration and exclusive management of CE devices. Potentially, this results in inefficient use of all resources, which exposes systems to a variety of cyber-attacks. However, it is clear from the current literature that smart CE networks are subject to various subtle, cyber threats, including botnets, brute force, Denial-of-Service (DoS), Distributed Denial of Service (DDoS), and web attacks. The DDoS attack is identified as one of the most dangerous attacks on today's Internet. In DDoS, attackers use many compromised hosts to generate a lot of worthless traffic flow toward the target server, which causes servers to overload quickly by consuming their resources and making them unreachable to its user. Although DDoS attacks have been investigated for more than two decades, still it is the most compelling yet common attack approach in recent times.In this regard, Software-Defined

Networking (SDN) and Intrusion Detection System (IDS) can be considered the backbone for the next-generation smart CE network. An IDS is designed to detect threats and malicious behavior to defend the network against it. However, for timely detection, the conventional signature-based IDS must continuously be updated and have information tagged as signatures or patterns of prospective threats. Furthermore, it is unable to detect zero-day threats. Hence, Intelligent threat detection techniques should be developed to identify and counteract the most recent cyber threats in smart CE networks, which are constantly expanding with time. However, due to the specific service needs of smart CE (such as low latency, resource limitations, mobility, dispersion, and scalability), attack detection fundamentally differs from conventional approaches in such a network. Therefore, an adaptable, dynamic, well-timed, and cost-effective detection framework against various growing cyber threats is urgently needed for the CE networks.

2. LITERATURE SURVEY

Software defined networking (SDN) decouples the control plane from the data plane of forwarding devices. This separation provides several benefits, including the simplification of network management and control. However, due to a variety of reasons, such as budget constraints and fear of downtime, many organizations are reluctant to fully deploy SDN. Partially deploying SDN through the placement of a limited number of SDN devices among legacy (traditional) network devices, forms a so called hybrid SDN network. While hybrid SDN networks provide many of the benefits of SDN and have a wide range of applications, they also pose several challenges. These challenges have recently been addressed in a growing body of literature on hybrid SDN network structures and protocols. This paper presents a comprehensive up-to-date survey of the research and development in the field of hybrid SDN networks. We have organized the survey into five main categories, namely hybrid SDN network deployment strategies, controllers for hybrid SDN networks, protocols for hybrid SDN network management, traffic engineering mechanisms for hybrid SDN networks, as well as testing, verification, and security mechanisms for hybrid SDN networks. We thoroughly survey the existing hybrid SDN network studies according to this taxonomy and identify gaps and limitations in the existing body of research. Based on the

outcomes of the existing research studies as well as the identified gaps and limitations, we derive guidelines for future research on hybrid SDN networks.

As several home appliances, such as air conditioners, heaters, and refrigerators, were connecting to the Internet, they became targets of cyberattacks, which cause serious problems such as compromising safety and even harming users. We have proposed a method to detect such attacks based on user behavior. This method models user behavior as sequences of user events including operation of home IoT (Internet of Things) devices and other monitored activities. Considering users behave depending on the condition of the home such as time and temperature, our method learns event sequences for each condition. To mitigate the impact of events of other users in the home included in the monitored sequence, our method generates multiple event sequences by removing some events and learning the frequently observed sequences. For evaluation, we constructed an experimental network of home IoT devices and recorded time data for four users entering/leaving a room and operating devices. We obtained detection ratios exceeding 90% for anomalous operations with less than 10% of misdetections when our method observed event sequences related to the operation. In this article, we also discuss the effectiveness of our method by comparing with a method learning users' behavior by Hidden Markov Models.

The Internet of Things (IoT) has proven to be a billion-dollar industry. Despite offering numerous benefits, the prevalent nature of IoT makes it vulnerable and a possible target for the development of cyber-attacks. The diversity of the IoT, on the one hand, leads to the benefits of the integration of devices into a smart ecosystem, but the heterogeneous nature of the IoT makes it difficult to come up with a single security solution. However, the centralized intelligence and programmability of software-defined networks (SDNs) have made it possible to compose a single and effective security solution to cope with cyber threats and attacks. We present an SDN-enabled architecture leveraging hybrid deep learning detection algorithms for the efficient detection of cyber threats and attacks while considering the resource-constrained IoT devices so that no burden is placed on them. We use a state-of-the-art dataset, CICDDoS 2019, to train our algorithm. The results evaluated by this algorithm achieve high accuracy with a minimal false positive rate (FPR) and testing

time. We also perform 10-fold cross-validation, proving our results to be unbiased, and compare our results with current benchmark algorithms.

SDN is a pivotal technology that relies on the fundamental idea of decoupling control and data planes in the network. This property provides several advantages such as flexibility, simplification, and lower costs. However, it also brings several drawbacks that are largely induced by the centralized control paradigm. Security is one of the most significant challenges related to centralization. In that regard, DDoS attacks are particularly pertinent to the SDN environment. This article presents a concise survey on solutions against DDoS attacks in software-defined networks. Moreover, several mechanisms are analyzed, and a comparative classification is provided for rendering the current state of the art in the literature. This analysis will help researchers to address weaknesses of these solutions and thus mitigate such attacks using more effective defense mechanisms.

The paper " Intrusion detection systems: A cross-domain overview " addresses the Nowadays, network technologies are essential for transferring and storing various information of users, companies, and industries. However, the growth of the information transfer rate expands the attack surface, offering a rich environment to intruders. Intrusion detection systems (IDSs) are widespread systems able to passively or actively control intrusive activities in a defined host and network perimeter. Recently, different IDSs have been proposed by integrating various detection techniques, generic or adapted to a specific domain and to the nature of attacks operating on. The cybersecurity landscape deals with tremendous diverse event streams that exponentially increase the attack vectors. Event stream processing (ESP) methods appear to be solutions that leverage event streams to provide actionable insights and faster detection. In this paper, we briefly describe domains (as well as their vulnerabilities) on which recent papers were-based. We also survey standards for vulnerability assessment and attack classification. Afterwards, we carry out a classification of IDSs, evaluation metrics, and datasets. Next, we provide the technical details and an evaluation of the most recent work on IDS techniques and ESP approaches covering different dimensions (axes): domains, architectures, and local communication technologies. Finally, we discuss challenges and strategies to improve

IDS in terms of accuracy, performance, and robustness.

3. METHODOLOGY

i) Proposed Work:

The project introduces an intelligent Intrusion Detection System (IDS) designed specifically for smart Consumer Electronics (CE) networks. It incorporates machine learning algorithms, including BiLSTM, GRU, DNN, CNN, and CNN + LSTM, to enhance security by identifying network attacks. Simulations conducted with the CICIDS-2018 dataset demonstrate its superior performance compared to existing solutions. And also, we have enhanced the Intrusion Detection System (IDS) by incorporating a Convolutional Neural Network (CNN) and a hybrid model combining CNN with Long Short-Term Memory (LSTM). This hybrid approach strategically combines the strengths of both models, achieving remarkable accuracy and outperforming other algorithms with a perfect 100% accuracy rate.

ii) System Architecture:

A DL-driven Intelligent framework for threat detection in the CE network is provided, incorporating Cu-BLSTM. A low cost, versatile, and powerful detection module is designed to detect threats across CE networks. Fig 1 depicts a comprehensive workflow of the proposed acquisition module. CuBiLSTM consists of two layers with 200 and 100 neurons. In addition, we added one dense layer with 30 neurons. The proposed work utilized Rely as 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-DNN consists of four dense layers with 100, 75, 50 and 30 neurons, respectively. Further, CuGRU comprises four layers of GRU with neurons of 500, 400, 300, and 100, respectively, with one dense layer of 03 neurons.

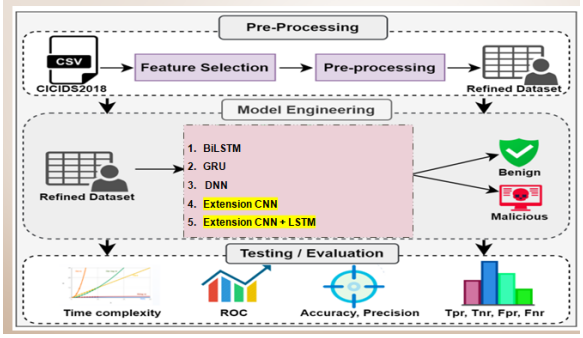
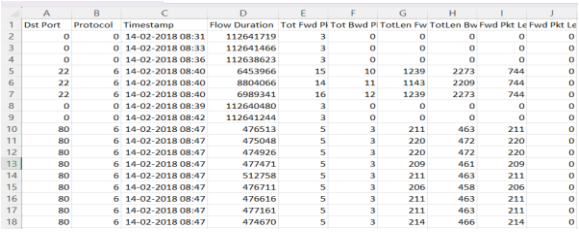


Fig 1 Proposed architecture

iii) Dataset collection:

The CICIDS2018 dataset, or the Canadian Institute for Cybersecurity Intrusion Detection System 2018 dataset, is a widely used dataset in the field of cybersecurity for evaluating intrusion detection systems. It's designed for assessing the effectiveness of intrusion detection and network traffic classification systems.



	A	B	C	D	E	F	G	H	I	J
1	Dst Port	Protocol	Timestamp	Flow Duration	Tot Fwd Pk	Tot Bwd Pk	TotLen Fw	TotLen Bw	Fwd Pkt Le	Fwd Pkt Le
2	0	0	14-02-2018 08:31	112641719	3	0	0	0	0	0
3	0	0	14-02-2018 08:33	112641466	3	0	0	0	0	0
4	0	0	14-02-2018 08:36	112638623	3	0	0	0	0	0
5	22	6	14-02-2018 08:40	6453966	15	10	1239	2273	744	0
6	22	6	14-02-2018 08:40	8804066	14	11	1143	2209	744	0
7	22	6	14-02-2018 08:40	6989341	16	12	1239	2273	744	0
8	0	0	14-02-2018 08:39	112640480	3	0	0	0	0	0
9	0	0	14-02-2018 08:42	112641244	3	0	0	0	0	0
10	80	6	14-02-2018 08:47	476513	5	3	211	463	211	0
11	80	6	14-02-2018 08:47	475048	5	3	220	472	220	0
12	80	6	14-02-2018 08:47	474926	5	3	220	472	220	0
13	80	6	14-02-2018 08:47	477471	5	3	209	461	209	0
14	80	6	14-02-2018 08:47	512758	5	3	211	463	211	0
15	80	6	14-02-2018 08:47	476711	5	3	206	458	206	0
16	80	6	14-02-2018 08:47	476616	5	3	211	463	211	0
17	80	6	14-02-2018 08:47	477161	5	3	211	463	211	0
18	80	6	14-02-2018 08:47	474670	5	3	214	466	214	0

Fig 2 NSL KDD dataset

The CICIDS2018 dataset is a valuable resource for cybersecurity research, specifically created to evaluate intrusion detection and network traffic classification systems. It provides labeled data for various cyber threats and attacks, making it crucial for assessing intrusion detection system effectiveness.

iv) Data Processing:

Data processing involves transforming raw data into valuable information for businesses. Generally, data scientists process data, which includes collecting, organizing, cleaning, verifying, analyzing, and converting it into readable formats such as graphs or documents. Data processing can be done using three methods i.e., manual, mechanical, and electronic. The aim is to increase the value of information and facilitate decision-making. This enables businesses to improve their operations and make timely strategic decisions. Automated data processing solutions, such as computer software programming, play a significant role in this. It can help turn large amounts of data, including big data, into meaningful insights for quality management and decision-making.

v) Feature selection:

Feature selection is the process of isolating the most consistent, non-redundant, and relevant features to use in model construction. Methodically reducing the size of datasets is important as the size and variety of datasets continue to grow. The main goal of feature selection is to improve

the performance of a predictive model and reduce the computational cost of modeling.

Feature selection, one of the main components of feature engineering, is the process of selecting the most important features to input in machine learning algorithms. Feature selection techniques are employed to reduce the number of input variables by eliminating redundant or irrelevant features and narrowing down the set of features to those most relevant to the machine learning model. The main benefits of performing feature selection in advance, rather than letting the machine learning model figure out which features are most important.

vi) Algorithms:

BiLSTM is a type of recurrent neural network (RNN) that processes sequential data in both forward and backward directions. It's utilized in the project for its ability to capture long-term dependencies in data, which is crucial for recognizing complex patterns and sequences in the context of intrusion detection within smart CE networks.

```
model1 = tf.keras.Sequential([
    tf.keras.layers.Embedding(100000, 64), # since it doesn't consider
    tf.keras.layers.Bidirectional(tf.keras.layers.LSTM(64)),
    tf.keras.layers.Dense(64, activation='relu'),
    tf.keras.layers.Dense(1, activation='sigmoid')
    # tf.keras.layers.Dense(1, activation='softmax') # loss too big
])
```

Fig 3 BILSTM

GRU is another variant of recurrent neural networks that is particularly efficient in modeling sequential data. In this project, GRU is chosen for its computational simplicity and effectiveness in capturing dependencies in the data. It provides a balance between model complexity and performance

```
model2 = tf.keras.Sequential([
    tf.keras.layers.Embedding(100000, 64), # since it doesn't c
    tf.keras.layers.GRU(64),
    tf.keras.layers.Dense(64, activation='relu'),
    tf.keras.layers.Dense(1, activation='sigmoid')
    # tf.keras.layers.Dense(1, activation='softmax') # loss too
])
```

Fig 4 GRU

A **Deep Neural Network** consists of multiple layers of interconnected neurons and is used to learn complex, hierarchical representations of data. DNNs are applied in the project for feature extraction and classification tasks, enabling the system to

understand the intricate relationships in network traffic data.

```
def nn():
    inputs = Input(name='inputs', shape=[X_train.shape[1],])
    layer = Dense(128, name='FC1')(inputs)
    layer = BatchNormalization(name='BC1')(layer)
    layer = Activation('relu', name='Activation1')(layer)
    layer = Dropout(0.3, name='Dropout1')(layer)
    layer = Dense(128, name='FC2')(layer)
    layer = BatchNormalization(name='BC2')(layer)
    layer = Activation('relu', name='Activation2')(layer)
    layer = Dropout(0.3, name='Dropout2')(layer)
    layer = Dense(128, name='FC3')(layer)
    layer = BatchNormalization(name='BC3')(layer)
    layer = Dropout(0.3, name='Dropout3')(layer)
    layer = Dense(1, name='OutLayer')(layer)
    layer = Activation('sigmoid', name='sigmoid')(layer)
    model = Model(inputs=inputs, outputs=layer)
    return model
```

Fig 5 DNN

CNNs are designed for processing grid-like data, such as images or network traffic data in this case. They are employed to automatically extract relevant features from raw data, allowing the system to recognize spatial patterns, anomalies, and threats in the network traffic

```
verbose, epoch, batch_size = 1, 100, 2
activationFunction='relu'

def CNN():

    cnnmodel = Sequential()
    cnnmodel.add(Conv1D(filters=128, kernel_size=2, activation='relu',input_shape=(X_train.shape[1],X_t
    cnnmodel.add(MaxPooling1D(pool_size=2))
    cnnmodel.add(Dropout(rate=0.2))
    cnnmodel.add(Flatten())
    cnnmodel.add(Dense(2, activation='softmax'))
    cnnmodel.compile(optimizer='adam', loss='categorical_crossentropy',metrics=['accuracy'])
    cnnmodel.summary()
    return cnnmodel

cnnmodel = CNN()
```

Fig 6 CNN

The fusion of **CNN and LSTM** is used to leverage the strengths of both architectures. CNNs excel at feature extraction from raw data, while LSTMs capture sequential dependencies. In the project, this combination is applied to enhance the system's ability to detect attacks by simultaneously considering spatial and temporal aspects of network traffic data, thus improving overall accuracy and reliability.

```
import tensorflow as tf
tf.keras.backend.clear_session()

model_en = tf.keras.models.Sequential([tf.keras.layers.Conv1D(filters=64,kernel_size=5,strides=1,paddi
    tf.keras.layers.MaxPooling1D(pool_size=2, strides=1, padding="valid"),
    tf.keras.layers.Conv1D(filters=32, kernel_size=3, strides=1, padding="causal", activation="relu"),
    tf.keras.layers.MaxPooling1D(pool_size=2, strides=1, padding="valid"),
    tf.keras.layers.LSTM(128, return_sequences=True),
    tf.keras.layers.Flatten(),
    tf.keras.layers.Dense(128, activation="relu"),
    tf.keras.layers.Dropout(0.2),
    tf.keras.layers.Dense(32, activation="relu"),
    tf.keras.layers.Dropout(0.1),
    tf.keras.layers.Dense(2)
])

lr_schedule = tf.keras.optimizers.schedules.ExponentialDecay(5e-4,
                                                             decay_steps=1000000,
                                                             decay_rate=0.98,
                                                             staircase=False)

model_en.compile(loss=tf.keras.losses.MeanSquaredError(),
                 optimizer=tf.keras.optimizers.SGD(learning_rate=lr_schedule, momentum=0.8),
                 metrics=['acc'])
model_en.summary()
```

Fig 7 CNN + LSTM

4. EXPERIMENTAL RESULTS

Precision: Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the formula to calculate the precision is given by:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

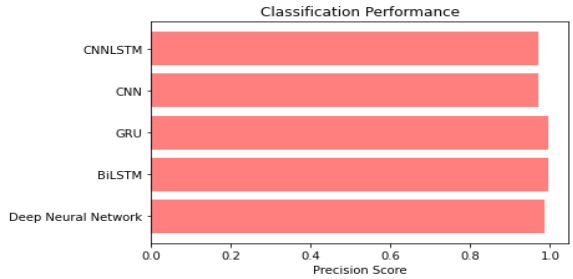


Fig 8 Precision comparison graph

Recall: Recall is a metric in machine learning that measures the ability of a model to identify all relevant instances of a particular class. It is the ratio of correctly predicted positive observations to the total actual positives, providing insights into a model's completeness in capturing instances of a given class.

$$Recall = \frac{TP}{TP + FN}$$

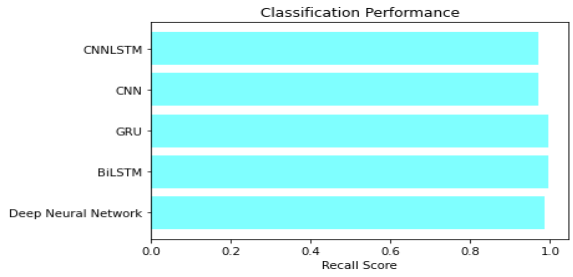


Fig 9 Recall comparison graph

Accuracy: Accuracy is the proportion of correct predictions in a classification task, measuring the overall correctness of a model's predictions.

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$

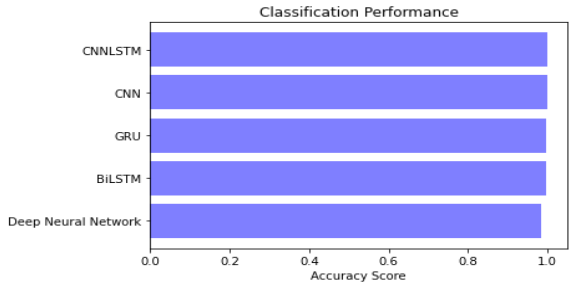


Fig 10 Accuracy graph

F1 Score: The F1 Score is the harmonic mean of precision and recall, offering a balanced measure that considers both false positives and false negatives, making it suitable for imbalanced datasets.

$$\text{F1 Score} = 2 * \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} * 100$$

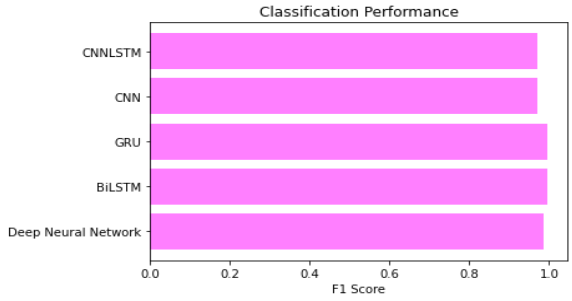


Fig 11 F1Score

ML Model	Accuracy	F1-score	Recall	Precision
DNN	0.985	0.985	0.985	0.985
BiLSTM	0.996	0.996	0.996	0.996
GRU	0.996	0.996	0.996	0.996
Extension CNN	1.000	0.972	0.971	0.971
Extension CNN + LSTM	1.000	0.972	0.971	0.971

Fig. 12: Results

CONCLUSION

The project effectively bolsters intrusion detection capabilities within smart Consumer Electronics (CE) networks, with a specific focus on countering Distributed Denial-of-Service (DDoS) attacks and proactively addressing emerging cyber threats. The selection of the algorithm with the highest accuracy among the four under consideration served as the basis for deploying the Intrusion Detection System (IDS) in this study, ensuring the robustness of the security measures. This project substantiates the efficacy of the IDS by utilizing the CICIDS-2018 dataset, demonstrating its superior performance through meticulous comparisons with contemporary intrusion detection techniques. The hybrid CNN and LSTM model's 100 % accuracy, user-friendly interface, and adaptability to Smart Consumer Electronics Networks make it a compelling and robust choice for real-world deployment, significantly advancing the security of interconnected devices. To meet the evolving challenges in safeguarding smart consumer electronics networks, the project advocates the adoption of deep learning-based intelligent models for efficient and adaptive threat detection, thereby fortifying the security landscape.

5. FUTURE SCOPE

In the future, the project can focus on training the intrusion detection system on diverse datasets, exposing it to a wider range of attack scenarios and patterns. This will enhance the system's accuracy and effectiveness in identifying and mitigating various types of cyber threats in smart CE networks. Exploring the incorporation of advanced machine learning techniques and algorithms to improve the system's overall performance. This will allow for more efficient and precise detection of security breaches in smart CE networks. Future work will involve the development of real-time response mechanisms, ensuring that the intrusion detection system can promptly detect and mitigate threats, thereby safeguarding smart CE networks effectively. The project can be investigated by the integration of anomaly detection techniques and behavioral analysis, further enhancing the system's ability to identify previously unknown attacks, making it more robust in securing smart CE networks.

REFERENCES

[1] C. K. Wu, C. -T. Cheng, Y. Uwate, G. Chen, S. Mumtaz and K. F. Tsang (2022), ”State-of-the-Art and Research

Opportunities for NextGeneration 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, IEEE 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/consumerelectronics/worldwide

[4] Al Razib, M., Javeed, D., Khan, M. T., Alkanhel, R., & Muthanna, M. S. A. (2022). Cyber Threats Detection in Smart Environments Using SDNEnabled 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 DLdriven 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 ddos attacks 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). Multichannel 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 SoftwareDefined 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 World AI 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. Sanchez, A. S. Tosun, J. Arco, and R. Doriguzzi- ´ Corin, “Hybrid SDN evolution: A comprehensive survey of the state-ofthe-art,” Comput. Netw., vol. 192, Jun. 2021, Art. no. 107981.

[15] Ren, Xiaodong, et al. ”Adaptive recovery mechanism for SDN controllers 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,”Realguard: 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.

[20] N. Moustafa, E. Adi, B. Turnbull, and J. Hu, “A new threat intelligence scheme for safeguarding industry 4.0 systems,” IEEE Access, vol. 6, pp. 32910–32924, 2018.

[21] M. A. Almaiah, A. Ali, F. Hajjej et al., “A Lightweight Hybrid Deep Learning Privacy Preserving Model for FC-Based Industrial Internet of Medical Things,” vol. 22, no. 6, pp. 2112, 2022.

[22] Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R., & Srivastava, G. (2022). P2tif: A blockchain and deep learning

framework for privacy-preserved threat intelligence in industrial iot. IEEE Transactions on Industrial Informatics, 18(9), 6358-6367.

[23] M. Kadoguchi, S. Hayashi, M. Hashimoto, and A. Otsuka, “Exploring the dark web for cyber threat intelligence using machine leaning,” in Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI), Jul. 2019, pp. 200–202.

[24] L. Yang, and A. J. a. p. a. Shami, “A Transfer Learning and Optimized CNN Based Intrusion Detection System for Internet of Vehicles,” 2022.

[25] Ullah, and Q. H. J. I. A. Mahmoud, “Design and development of a deep learning-based model for anomaly detection in IoT networks,” vol. 9, pp. 103906-103926, 2021.

[26] Anand, S. Rani, D. Anand et al., “An efficient CNN-based deep learning model to detect malware attacks (CNN-DMA) in 5G-IoT healthcare applications,” vol. 21, no. 19, pp. 6346, 2021.

[27] Lalduhsaka, R., Nilutpol Bora, and Ajoy Kumar Khan. ”Anomaly-Based Intrusion Detection Using Machine Learning: An Ensemble Approach.” International Journal of Information Security and Privacy (IJISP) 16.1 (2022): 1-15.

[28] Zhang, Zhao, et al. ”SecFedNIDS: Robust defense for poisoning attack against federated learning-based network intrusion detection system.” Future Generation Computer Systems 134 (2022): 154-169.

[29] de Souza, Cristiano Antonio, Carlos Becker Westphall, and Renato Bobsin Machado. ”Two-step ensemble approach for intrusion detection and identification in IoT and fog computing environments.” Computers & Electrical Engineering 98 (2022): 107694.

[30] Javeed, D., Gao, T., Khan, M. T., & Shoukat, D. (2022). A hybrid intelligent framework to combat sophisticated threats in secure industries. Sensors, 22(4), 1582.

[31] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp, 1, 108-116.

Authors:

[1] Mr. K. Jaya Krishna, currently working as an Associate Professor in the Department of Master of Computer Applications, QIS College of Engineering and Technology,

Ongole, Andhra Pradesh. He did his MCA from Anna University, Chennai, M.Tech (CSE) from JNTUK, Kakinada. He published more than 10 research papers in reputed peer reviewed Scopus indexed journals. He also attended and presented research papers in different national and international journals and the proceedings were indexed IEEE. His area of interest is Machine Learning, Artificial intelligence, Cloud Computing and Programming Languages.

[2] Ms. Ponduri Venkata Sai Divya, currently pursuing Master of Computer Applications at QIS College of engineering and Technology (Autonomous), Ongole, Andhra Pradesh. She Completed B.Sc. in Computer Science from Sri Harshini Degree College, Ongole, Andhra Pradesh. Her areas of interests are Java, Python & Machine learning.