An Intelligent Intrusion Detection System for SmartConsumer Electronics Network

Mrs.M.Sonia[1], Racha Niharika[2] , Singoji Shiva Priya[3],Thupakula Vijaya Lakshmi[4],
Assistant Professor[1] Scholar[2,3,4]
Department of Computer Science and Engineering,
Nalla Narasimha Reddy Education Society's Group of Institutions,Hyderabad,India

***Abstract*—The evolution of traditional Consumer Electronics (CE) into advanced, connected devices through the Internet of Things (IoT) has revolutionized the landscape, enhancing both connectivity and intelligence. This interconnectedness among sensors, actuators, and appliances within the CE network has not only amplified data availability but also facilitated automated control.However, this proliferation of connected devices has led to a significant surge in data traffic, owing to the diversity and decentralization of CE devices. Additionally, conventional network infrastructure-based techniques for managing CE devices require manual setup and administration, posing challenges in scalability and efficiency.To overcome these obstacles, we propose an innovative approach that merges Software-Defined Networking (SDN) architecture with Deep Learning (DL) to develop an intelligent Intrusion Detection System (IDS) tailored for smart CE networks. By segregating the control and data planes, our approach effectively addresses the distributed nature of smart CE networks.Our IDS leverages Cuda-enabled Bidirectional Long Short-Term Memory (Cu-BLSTM) to detect various attack types within the smart CE network. Through simulations conducted on the CICIDS-2018 dataset. The effectiveness of our proposed approach is confirmed, demonstrating that it is superior to existing security solutions. This shows that its potential to be a groundbreaking solution for the next generation of Smart Consumer Electronics networks is validated.**

***Index Terms*—Consumer Electronics, Cyber-Attacks, Deep learning, Internet of Things, Intrusion Detection System, Software-Defined Networking**

I. INTRODUCTION

Our interactions with technology have changed dramatically as a result of the Internet of Things' (IoT) convergence with consumer electronics (CE). IoT makes it possible for commonplace objects to communicate, share data, and connect to the internet, building a network of smart devices that are all interconnected. Next-generation CEs with more connectivity, intelligence, and functionality have been made possible by this combination.

One of the key benefits of IoT-enabled CEs is the ability to automate tasks and improve efficiency. For example, smart thermostats can learn users' preferences and adjust temperature settings accordingly, while smart lighting systems can automatically adjust brightness based on ambient light levels. This automation not only enhances convenience but also helps to optimize energy usage and reduce costs.

In addition to automation, IoT-enabled CEs also offer enhanced monitoring and control capabilities. Users can remotely monitor and control their devices using smartphones, tablets, or computers, regardless of their location. While they are away from home, homeowners can, for instance, check security cameras or change the settings on their smart home gadgets.

IoT device connectivity has expanded connectivity, but it also presents new security risks.. Due to the increasing number of devices connected to the internet, which expands the attack surface for hackers and other cybercriminals, IoT networks are vulnerable to security breaches and cyberattacks. Distributed denial of service (DDoS) attacks, in which an attacker overloads a target server with excessive traffic, are particularly dangerous for Internet of Things (IoT) networks.

Technologies such as IDS (intrusion detection system) and Software-Defined Networking (SDN) are essential in addressing these security issues. SDN makes it possible to monitor and control network resources centrally, which facilitates the quicker identification and remediation of security problems. IDS, has the capacity to monitor network activity and spot suspicious activity, on the other hand, helping to detect security breaches early.

All things considered, there is a lot of room for innovation and convenience when IoT is incorporated into consumer products. However, to safeguard IoT-enabled CE networks from potential dangers and attacks, it is crucial to prioritize security and put strong cybersecurity measures in place.

A. SDN

Software-Defined Networking (SDN) represents a groundbreaking approach to network management and architecture by separating the control plane from the data plane, thus enabling centralized control and programmability of network resources. Unlike traditional networking models where devices handle both data forwarding and traffic control locally, SDN decentralizes these functions. Instead, a centralized controller provides a comprehensive view of the network, making decisions about traffic forwarding based on network-wide policies and goals. This separation fosters enhanced flexibility, scalability, and automation in network management. At the core of SDN lies the SDN controller, which serves as the central management point for the entire network. By communicating with network devices through standardized protocols like OpenFlow, the controller directs them on how to process incoming data packets according to predetermined rules and policies. This centralized control empowers administrators to dynamically adjust network configurations, prioritize traffic, and enforce security measures in real-time, eliminating the need for manual device configuration. Moreover, SDN facilitates the virtualization of network resources, enabling the creation of logical network overlays that abstract the underlying physical infrastructure. This capability allows for the deployment of customized virtual networks tailored to specific applications or services, thereby optimizing resource utilization and enhancing flexibility.

B. CU-BLSTM

Convolutional Unit Bidirectional Long Short-Term Memory, or CU-BLSTM for short, is a unique type of neural network architecture that combines the temporal modelling skills of bidirectional long short-term memory (BLSTM) networks with the spatial feature extraction capabilities of convolutional neural networks (CNNs). This fusion combines CNNs' capability to extract hierarchical patterns in spatially structured data, such as images, with BLSTMs' proficiency in capturing long-range correlations and temporal dynamics in sequential data. By integrating these strengths, CU- BLSTM enhances robustness to input variations and facilitates efficient learning of intricate patterns without the need for extensive manual feature engineering. This architecture has found widespread applications in domains like speech recognition, natural language processing, gesture recognition, and time-series analysis, where both spatial and temporal characteristics are crucial for accurate predictions and classifications.

C. IDS

An Intrusion Detection System (IDS) stands as a pivotal element within network security infrastructure, aimed at promptly identifying and addressing unauthorized access or malicious activities within a computer network or system. Functioning in real-time, IDS scrutinizes network traffic or system activities, meticulously analyzing patterns and anomalies to flag potential security breaches or threats. Broadly categorized into two types, namely network-based IDS (NIDS) and host-based IDS (HIDS), each serves a distinct purpose. NIDS monitors network traffic, inspecting packets as they traverse the network to detect suspicious patterns or signatures indicative of known attacks like port scans, denial-of-service (DoS) attacks, or malware communications. Conversely, HIDS operates on individual hosts or endpoints, overseeing system logs, file integrity, and user activities to pinpoint unauthorized access attempts, anomalous file modifications, or suspicious processes running on the host. Employing an array of detection techniques encompassing signature-based detection, anomaly-based detection, and behavioral analysis, IDS remains vigilant against evolving threats. Signature-based detection involves matching observed network traffic or system activities against patterns or signatures of known attacks, while anomaly-based detection identifies deviations from normal behavior using statistical models or predefined thresholds.

II. RELATED WORK

The related work for the proposed project encompasses various research areas, offering valuable insights into enhancing security in smart Consumer Electronics (CE) networks. Firstly, studies on SDN-based security solutions delve into leveraging SDN for bolstering security in IoT and CE networks through techniques like traffic monitoring, access control, and threat detection. Additionally, The use of Deep Learning techniques, such as CNNs and RNNs, to identify and classify malicious activities in network traffic provides valuable knowledge in the field of intrusion detection research. Moreover, investigations into integrating SDN and DL shed light on combining SDN controllers' programmability with DL models' learning capabilities to bolster network security. Special challenges, such as resource constraints and heterogeneity, are addressed in separate studies aimed at detecting intrusions on the Internet of Things and Consumer electronics networks. In addition, the benchmarking of effectiveness and efficiency is provided by comparing various approaches to integrated development services, including existing methods and new techniques like SDN or DL based Integrated Development Services. Studies on anomaly detection tailored for the Internet of Things and CE environments, reinforcement learning algorithms to mitigate dynamic threats as well as intrusion sensing mechanisms appropriate for IoT with limited devices can also be explored further. Additionally, in order to create strong defences, study of actual attack data and case studies provides useful information on the limitations and efficacy of current security measures.. Combining Deep Learning with Software Defined Networking (SDN) for Intrusion Detection Systems (IDS) is an efficient method of thwarting emerging cyberthreats. Advances in speech emotion recognition, the integration of blockchain and deep learning for cybersecurity in Software-Defined Industrial IoT (SDIIoT), and LSTM-based Some of the foundational papers demonstrating exceptional performance in identifying cyber threats in IoT networks and consumer applications are deep learning models for Network Intrusion Detection Systems (NIDS) in IoT networks.These groundbreaking works give a solid basis for understanding today's state of knowledge about the Internet of Things cybersecurity, as well as forthcoming research directions in this area.

III. METHODOLOGY

The initial step involves loading data from the provided CIC IDS 2018 dataset, containing various attack scenarios. Subsequently, data preprocessing is conducted to explore the dataset's structure, handle missing values, encode categorical variables, and scale numerical features. For the purpose of training and evaluating machine learning models,the dataset is divided into training and testing sets. Model generation follows, where architectures such as BiLSTM, GRU, DNN, CNN, and CNN + LSTM are built and trained on the training data. Their performance is evaluated on the testing data to calculate accuracy. Concurrently, modules for user signup and login are implemented to facilitate user access to the system, along with a module for user input to receive data for prediction. Predictions are made on the user-input data using the trained models, and the final predictions are displayed to the user. An ensemble method combines the predictions of multiple individual models, enhancing prediction robustness and accuracy. Additionally, various algorithms, including BiLSTM, GRU, DNN, CNN, and CNN + LSTM, are implemented to leverage their respective capabilities in processing sequential data, deep learning, and computer vision tasks. Through these steps, a comprehensive system for intrusion detection is developed, aiming to effectively identify and mitigate security threats within the network environment.

In addition to the core methodology outlined, several crucial aspects help ensure that the intrusion detection system (IDS) is implemented successfully. based on machine learning algorithms. Robust data preprocessing techniques are essential to ensure dataset quality and consistency, including handling outliers, noise, and imbalanced classes, which can significantly impact model performance. Furthermore, feature selection and engineering play a crucial role in extracting relevant information from the dataset and improving model efficiency and accuracy. Techniques such as dimensionality reduction and feature scaling may be employed to enhance model training and prediction capabilities.

Furthermore, in order to appropriately evaluate the generated IDS's performance, model evaluation and validation techniques are essential. For a thorough grasp of the model's advantages and disadvantages, relevant measures including accuracy, precision, recall, F1-score, and receiver operating characteristic (ROC) curve analysis should be used. Cross-validation methods, such k-fold cross-validation, contribute to the model's robustness and generalizability across various data subsets.

Continuous monitoring and adaptation of the IDS are critical to address evolving security threats and maintain effectiveness over time. This involves implementing mechanisms for real-time detection, response, and feedback loops to update the model based on new data and emerging attack patterns. Additionally, incorporating user feedback and expert domain knowledge can further enhance the IDS's capabilities and improve its ability to differentiate between legitimate and malicious network activities.

Lastly, ensuring the system's scalability, efficiency, and compatibility with existing network infrastructures are essential considerations for practical deployment. Optimizing computational resources, leveraging parallel processing techniques, and integrating the IDS seamlessly into the existing network architecture facilitate smooth operation and minimize disruption to network functionality. Additionally, implementing appropriate safety precautions to safeguard the IDS itself from potential attacks is crucial to maintain its integrity and reliability in safeguarding network assets. By addressing these additional factors, the IDS can be effectively deployed and maintained to mitigate cybersecurity risks and protect against potential threats in dynamic network environments.

IV. ARCHITECTURE

A. BLSTM

Bidirectional Long Short-Term Memory (BiLSTM) is an advanced recurrent neural network (RNN) architecture tailored for handling sequential data processing tasks. Unlike conventional LSTM networks that operate solely in a unidirectional manner, BiLSTM networks have the unique ability to process sequences bidirectionally, assimilating insights from both past and future time steps. This is achieved by implementing two LSTM layers: one for forward sequence processing and the other for backward sequence processing. Each LSTM layer is composed of memory cells and gating mechanisms, enabling the network to effectively capture long-term dependencies and sequential patterns. At each time step, the output representations from both the forward and backward LSTM layers are amalgamated, generating a unified representation that encapsulates information from preceding and subsequent contexts. BiLSTM networks find extensive utility in diverse applications such as natural language processing tasks like sentiment analysis and named entity recognition, as well as in domains necessitating sequential data analysis like speech recognition and intrusion detection. Leveraging its bidirectional nature, BiLSTM excels in discerning intricate relationships within sequences, rendering it a potent tool for an array of sequence processing endeavors.

B. GRU

Gated Recurrent Unit (GRU) stands out as a distinctive recurrent neural network (RNN) architecture designed to streamline the complexity of Long Short-Term Memory (LSTM) networks while preserving their capability to capture prolonged dependencies within sequential data. GRU networks are structured around recurrent units featuring gating mechanisms, which encompass an update gate and a reset gate. These gates govern the flow of information throughout the network, with the update gate regulating the incorporation of current input and previous hidden state information into the present hidden state, while the reset gate dictates the extent to which the prior hidden state should be disregarded. This adaptive gating mechanism empowers GRU to selectively retain or discard information from prior time steps, enabling it to adeptly capture both short-term and long-term dependencies within sequences. Notably, GRU boasts a simpler architectural design with fewer parameters compared to LSTM, resulting in expedited training times while maintaining performance parity across various sequence modeling tasks. GRU networks are highly useful in a wide range of applications, including speech recognition, time series analysis, and natural language processing, where it is critical to process sequential data with complex relationships. With the help of its adaptive gating mechanism, GRU shows itself to be a flexible solution that can successfully interpret the complexity of sequential data analysis.

C. DNN

Artificial neural networks with numerous layers of hierarchically arranged connected nodes, or neurons, are referred to as Deep Neural Networks (DNNs). Every neuron in a DNN receives input signals, adds their weights together, and then uses an activation function to produce an output. DNNs typically consist of an output layer, an input layer, and one or more hidden layers. The hidden layers, whose number and size can vary, facilitate the learning of increasingly abstract representations of the input data through successive transformations. DNNs leverage methodologies like backpropagation and gradient descent to iteratively adjust the connection weights between neurons during the training process, thereby optimizing the network to minimize the disparity between its predictions and the actual target values. DNNs have garnered considerable success across diverse machine learning tasks, including but not limited to image recognition, natural language processing, and speech recognition. This achievement is a result of their innate ability to autonomously learn hierarchical feature representations from raw input data. DNNs are distinguished by their capability to discern intricate patterns and relationships within high-dimensional data, rendering them indispensable tools in contemporary artificialintelligence applications.

D. CNN

Convolutional Neural Networks (CNNs) represent a specialized deep learning architecture tailored explicitly for processing structured grid-like data, such as images. CNNs are composed of multiple layers, comprising convolutional layers, pooling layers, and fully connected layers. Within a CNN, convolutional layers employ filters or kernels to apply convolution operations across input images, thereby extracting features by spatially convolving them throughout the image. Subsequently, pooling layers downsample the feature maps, reducing their spatial dimensions while preserving crucial information. Ultimately, fully connected layers amalgamate the extracted features and execute classification or regression tasks. CNNs leverage concepts like parameter sharing and local connectivity to adeptly acquire hierarchical representations of visual features, allowing them to capture patterns across multiple levels of abstraction. By virtue of their capacity to autonomously discern pertinent features from raw input data, CNNs have emerged as pivotal tools in various computer vision tasks, encompassing image classification, object detection, and image segmentation. The efficacy of CNNs in handling high-dimensional data, coupled with their ability to acquire hierarchical representations, positions them as foundational components within modern machine learning and artificial intelligence paradigms.

E. SDN

Software-Defined Networking (SDN) represents a groundbreaking paradigm in network management, distinguished by its separation of the control plane from the data plane within network devices like switches and routers. In the realm of SDN architecture, the control plane finds centralization within a software-based controller, which orchestrates the network's behavior by dynamically programming forwarding rules in network devices. This decoupling of the control and data planes fosters a more adaptable and programmable approach to network management, empowering administrators to delineate network policies and automate tasks through software applications.

SDN boasts an array of advantages, including streamlined network management, heightened scalability and agility, and fortified network security via centralized policy enforcement. By encapsulating network intelligence within software-based controllers, SDN paves the way for the implementation of advanced networking functionalities like traffic engineering, load balancing, and network slicing. Consequently, SDN has witnessed substantial adoption across enterprise and data center environments, ushering in a transformative era wherein networks are conceptualized, deployed, and operated in novel and dynamic ways.

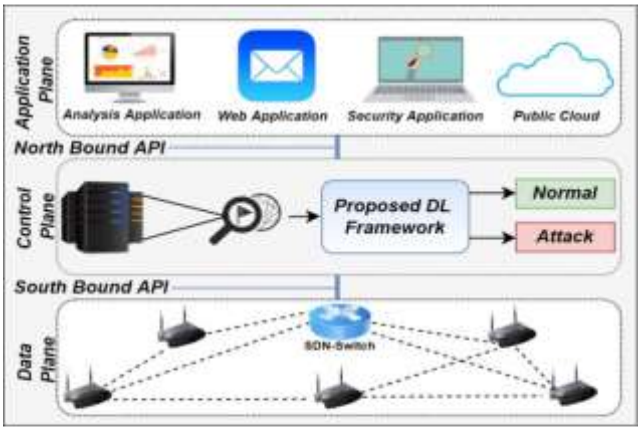
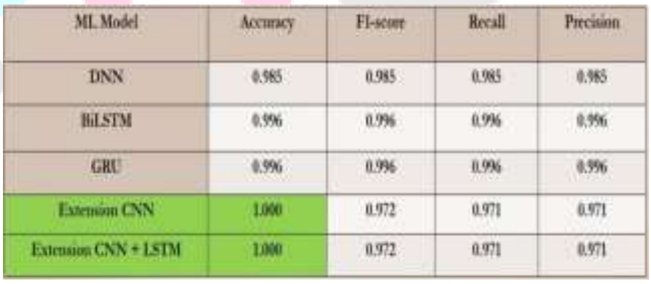


Fig. 1: Network Model.

V. EVALUATION

The proposed model is developed and trained using Python version "Python 3.8," utilizing the Keras framework integrated with TensorFlow and GPU-based packages to effectively harness computational resources. The testing environment features an Intel Core i7-7700 HQ CPU with a 2.80 GHz processor, 16 GB of RAM, and a 6 GB NVIDIA GeForce GTX 1060 GPU.The CICIDS-2018 dataset, which includes a variety of attack classes like Brute-force, DDoS, DoS, and SSH, is employed to assess the model. The dataset is preprocessed before training, with lines containing empty or non-numeric values removed and non-numeric values converted to numeric ones using label encoding from the sklearn library. Segment order effects are reduced by using one-hot encoding for the output labels, and model performance is improved by data normalization using the MinMax scalar function.To make model evaluation easier, the dataset is divided into 70% training and 30% testing data. In addition to the computation of performance metrics like accuracy (ACC), precision (PN), recall (RL), and F1-Score (FS), values for true positive (TP), true negative (TN), false positive (FP), false negative (FN), and Matthew's correlation coefficient (MCC) are also obtained through the use of a confusion matrix. In order to ensure a full evaluation of the proposed intrusion detection system and to provide a thorough assessment of its efficacy and robustness, mathematical formulas for these metrics are provided.



ML Model	Accuracy	FI-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. 2: Performance Evaluation

VI. RESULTS

Based on the evaluation of the intrusion detection system for smart consumer electronics networks, the how different models perform, including CNNLSTM, CNN, GRU, BiLSTM, and DNN, was assessed using key metrics such as accuracy, precision, recall, and F1 score. The following results were obtained:

Figure 3 displays the accuracy comparison, Figure 4 displays the precision comparison, Figure 5 displays the recall comparison, and Figure 6 displays the F1 Score comparison.

These results indicate the relative performance of each model in accurately detecting attacks on consumer electronics networks. Additionally, various network features, including forward packet length standard, forward packet length mean, forward packet length max, forward packet length size avg, packet length std, flow IAT Std, bwd packet length standard, bwd packet seg size Avg, packet size avg, and subflow fwd bytEs, were utilized as input features to predict network attacks, as shown in Fig 7. If an attack is detected, it is displayed in the output; otherwise, it is displayed as normal.

The hybrid CNN and LSTM model's exceptional accuracy, precision, recall, and F1 score—along with its user-friendly interface and suitability for Smart Consumer Electronics Networks—make it a compelling and strong choice for real-world deployment, according to the results.In smart consumer electronics networks, it has demonstrated greater efficacy in precisely recognising and mitigating security threats. To improve the intrusion detection system's performance in practical situations, more research and testing could be necessary.

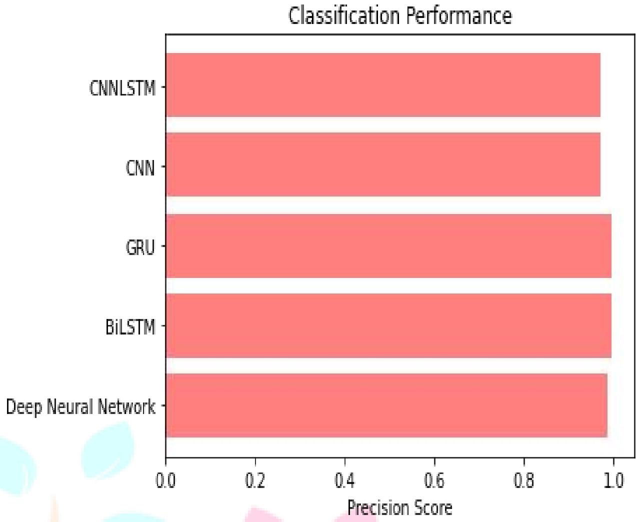


Fig. 4: Precision Comparison graph

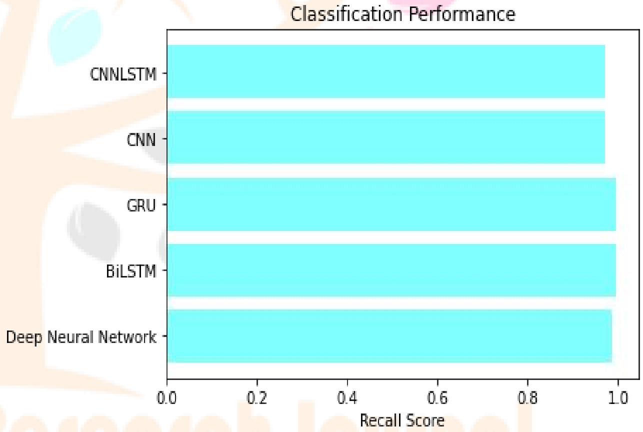


Fig. 5: Recall Comparison graph

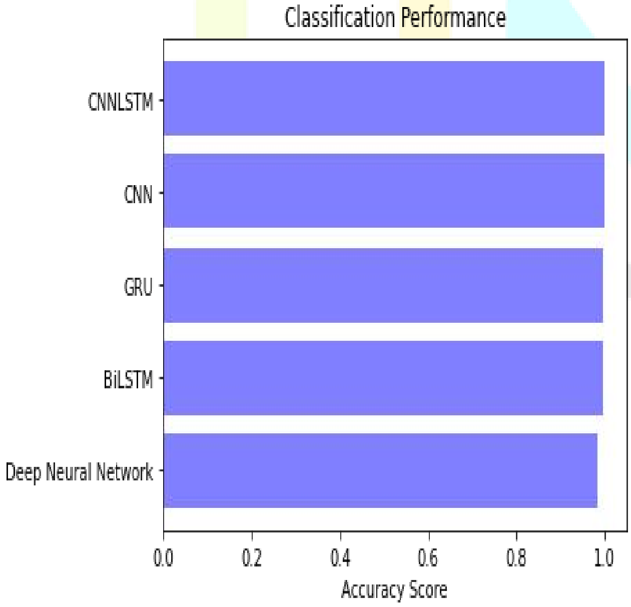


Fig. 3: Accuracy Comparison graph

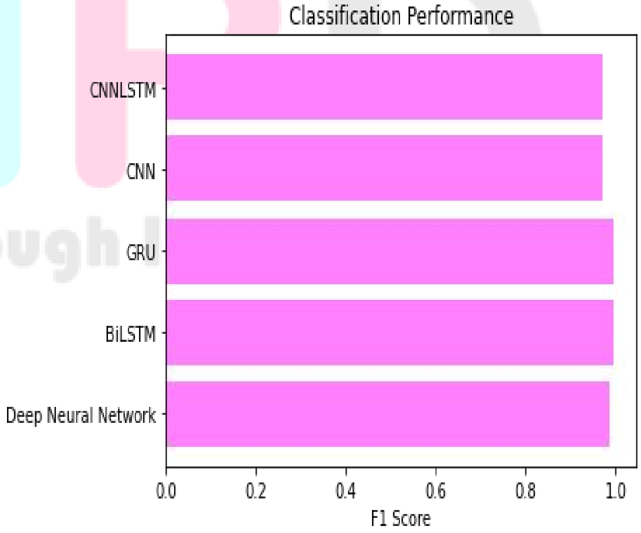
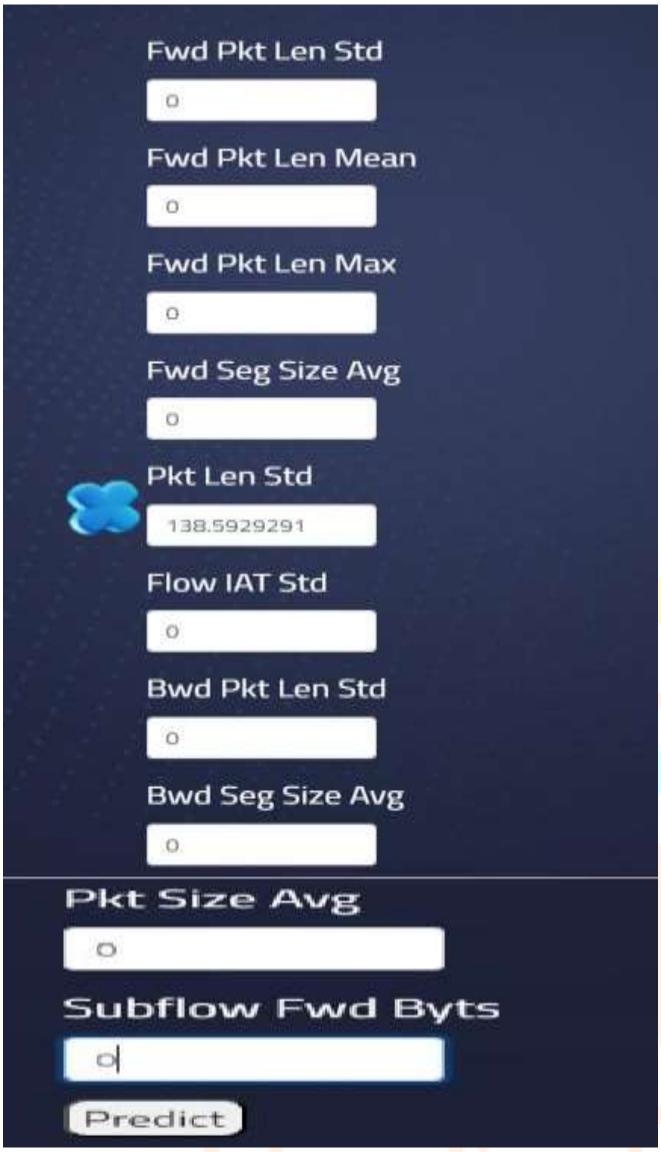


Fig. 6: F1 Score Comparison graph



Fwd Pkt Len Std
0

Fwd Pkt Len Mean
0

Fwd Pkt Len Max
0

Fwd Seg Size Avg
0

Pkt Len Std
138.5929291

Flow IAT Std
0

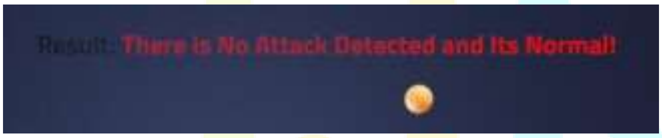
Bwd Pkt Len Std
0

Bwd Seg Size Avg
0

Pkt Size Avg
0

Subflow Fwd Byts
0

Fig. 7: Input Readings.



Result: There is No Attack Detected and Its Normal!

Fig. 8: Final Output.

VII. CONCLUSION

In this study, we introduced an innovative approach to safeguard consumer electronics networks through an intelligent intrusion detection system (IDS) leveraging software-defined networking (SDN) orchestrated deep learning techniques. Our methodology combined SDN architecture with consumer electronics networks to effectively manage their distributed nature and diverse device types. To enhance threat detection capabilities, we developed an IDS based on cuda-enabled bidirectional long short-term memory (BLSTM), strategically deployed at the control plane. Through extensive experimentation with the CICIDS-2018 dataset, we demonstrated the efficacy of our proposed IDS in terms of accuracy, precision, and operational efficiency. Comparative analysis against existing state-of-the-art techniques further validated the superiority of our approach. Looking ahead, By training the model on a variety of datasets, we want to expand the scope of our research and increase the model's efficacy in detecting intrusions within consumer electronics networks. Ultimately, we advocate for the adoption of DL-based intelligent models to bolster security measures in next-generation smart consumer electronics networks.

VIII. 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] aveed, 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.