A Sustainable Intelligent Intrusion Detection System for Smart Consumer Electronics Network

[1] *Sakthidharan Gangadharan Rajappa*, [2]*Neeli Sravani.,*
[1 2] Department of Computer Science and Engineering GRIET, Hyderabad, India.
drgrsdharan@gmail.com

Abstract: New consumer electronics (CE) are smarter and more connected owing to IoT. By connecting sensors, motors, appliances, and other consumer products, the CE network can acquire more data and operate autonomously. However, CE devices are diversifying and spreading, boosting data flow. Standard static network architecture requires CE device setup and administration. Related to aforesaid concerns. To solve these problems, we suggest combining SDN architecture with Deep Learning to construct an intelligent IDS for smart CE networks. We divide control and data planes for smart CE network spread design. The IDS detects smart CE network vulnerabilities using Cuda-enabled Bidirectional Long Short-Term Memory (Cu-BLSTM). In CICIDS-2018 dataset models, the proposed solution beats the newest and most powerful security methods. This makes it perfect for future smart CE networks.

1. INTRODUCTION

The IoT is a set of devices that transmit and receive data online. These gadgets have sensors and software. The next generation of consumer electronics (CEs) features higher intelligence and connectivity thanks to the Internet of Things (IoT). More data is available and the CE network can handle itself automatically because sensors, motors, appliances, and other consumer products are all linked together. At the same time, computers, laptops, smartphones, and smartwatches can now be used to connect to CE devices remotely at any time and from anywhere in the world, as long as they are linked to a network. These smart gadgets can be used in many areas, such as in smart homes. DDoS attacks employ many hijacked servers to flood the target server with worthless traffic. Servers rapidly overuse their resources and ban users. DDoS assaults have been researched for almost 20 years, yet they remain the most fascinating and popular sort of attack. SDN and IDS sit at the heart of the next-generation smart CE network.

The study's goal is to create a high-tech Intelligent Intrusion Detection System (IDS) that is specifically designed to protect Smart Consumer Electronics Networks. The research's goal is to create and use an intrusion detection system (IDS) that uses AI and machine learning to find and fix possible security holes in the network before they happen. The study wants to improve the security of smart consumer gadgets by reaching this goal. This will protect the safety and purity of users' data and devices.

There are more online dangers and illegal accesses because more Smart Consumer Electronics are linked to each other. The breach monitoring tools we have now are not flexible or smart enough to stop complex attacks on these networks. Because of this, we need to make an Intrusion Detection System right away that uses advanced machine learning and AI methods to find and stop possible breaches, protecting the privacy and security of Smart Consumer Electronics Networks.

2. LITERATURE SURVEY

C. K. Wu et.al., This essay looks at how the Internet of Things (IoT) is changing things and how it has a big effect on how the physical and digital worlds work together. It sees widespread information sharing, with consumer products playing a key part as the main link. It is expected that the use of IoT technologies will improve customer goods and services, which will grow the market for consumer gadgets. But the problem is getting worse because of links that aren't organized and technology interfaces that aren't controlled, which leaves holes. The paper calls for building a trusted infrastructure right away, describing the next generation of consumer gadgets and making sure they work with the new Internet of Things standard IEEE 2668. Even though the benefits might be there, they are hard to get because they are hard to apply and need to keep changing to deal with security risks. The paper lays out a plan for future study by focusing on things like complicated network analysis and safety measures to help make the growth of next-generation consumer goods more reliable, efficient, safe, and secure.

Al Razib et.al., The article describes how to deploy a Deep Learning-powered SDN IDS to secure IoT. This DNNLSTM model identifies common and uncommon IoT hacking risks. The system's Accuracy, Precision, Recall, and F1-Score are assessed following CICIDS 2018 training. Comparative DNNGRU and BLSTM testing show it works. The suggested system surpasses others with 99.55% accuracy, 99.36% precision, 99.44% memory, and 99.42% F1-score. IoT security is improved by this work's robust technique to defend against smart environment cyberthreats.

Prabhakar, G. A et.al., This work introduces a novel Speech Emotion Recognition (SER) approach that avoids the issues with magnitude spectrum-based features. The proposed multichannel architecture uses CNN-BLSTM and an attention mechanism. It employs phase and magnitude spectral characteristics. Modified Group Delay Function phase information is supplemented by Mel Frequency Cepstral Coefficients (MFCCs). CNN-BLSTM learns from both feature sets. Combine these representations and feed them to an SVM for classification. Deep Canonical Correlation Analysis (DCCA) improves SER by improving magnitude-phase relationships. Testing on the IEMOCAP database outperforms MFCC features and one-mode SER techniques. The proposed concept is shown in consumer-oriented systems using a real-time web server application.

R. Kumar et.al., This paper describes a novel SDI IoT safety method. It uses blockchain and Deep Learning. SDI IoT is vulnerable to several dangers because to its wireless nature. The centralization of SDN controllers makes this worse. The proposed system utilizes a blockchain with a Clique Proof-of-Authority (C-PoA) agreement method to securely communicate data. The novel LSTMSCAE-AGRU flow analyzer combines the LSTM Stacked Contractive Auto Encoder and the Attention-based Gated Recurrent Unit. It extracts low-dimensional characteristics and discovers odd control plane switch requests. This combination approach reduces SDI IoT single-point malfunctions and typical cyber risks. This safeguards industrial networks.

Saurabh, Kumar, et al. A novel method for securing IoT networks employing sophisticated intruder detection systems is LBDMIDS. To address the expanding amount of IoT and edge device hacking vulnerabilities, the research employs Deep Learning (DL) technologies, particularly an LSTM Autoencoder and a 13-feature DNN model. These models outperform Decision Trees (DT) on widely used datasets like UNSW-NB15 and Bot-IoT. Stacking and bidirectional LSTM variants of the recommended LBDMIDS outperform typical machine learning approaches. It outperforms typical machine learning approaches and matches well-known deep neural networks. This suggests it might safeguard IoT networks from hacking.

ALGORITHMS

In this we used algorithms like BiLSTM , GRU, DNN, CNN, CNN + LSTM

BiLSTM: RNN layers called bidirectional LSTM (BiLSTM) layers understand how time steps in a time series or chain connect across time. These limitations may help the RNN learn from the complete time series at each time step.

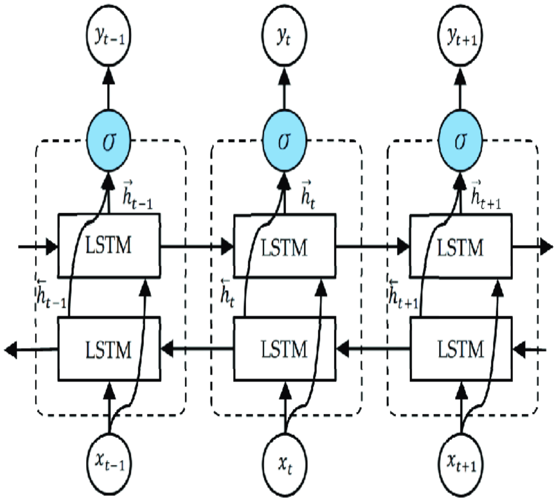

Fig 1 BiLSTM architecture

GRU: Cho et al. created the Gated Recurrent Unit (GRU) in 2014 as an easier option to LSTM (LSTM) networks. It is a type of recurrent neural network (RNN). In the same way that LSTM can, GRU can handle sequential data like speech, text, and time lines.

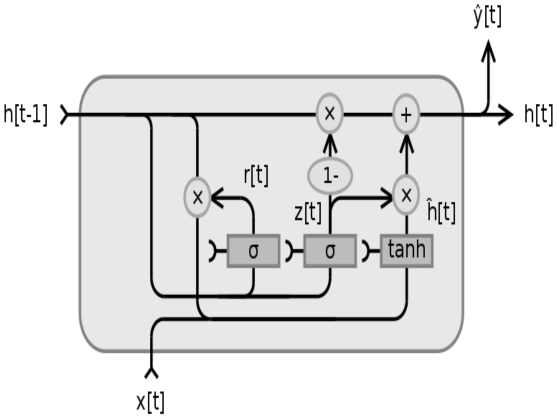

Fig 2 GRU architecture

DNN: Deep neural networks (DNN) are a type of ML programs that are like ANN and try to work like the brain does when it comes to handling information. One or more hidden layers (l) are placed between the input and output levels by DNN.

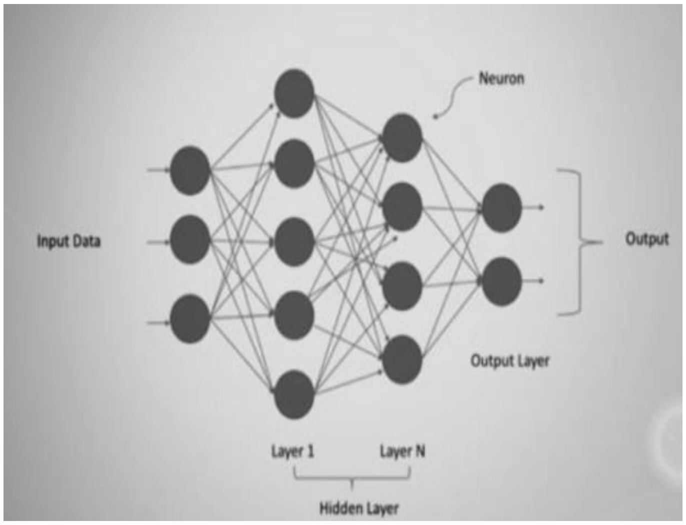

Fig 3 DNN architecture

CNN: In Computer Vision, a CNN is a type of DL neural network design that is often used. A area of AI called computer vision makes it possible for computers to understand and make sense of images and other visual data.

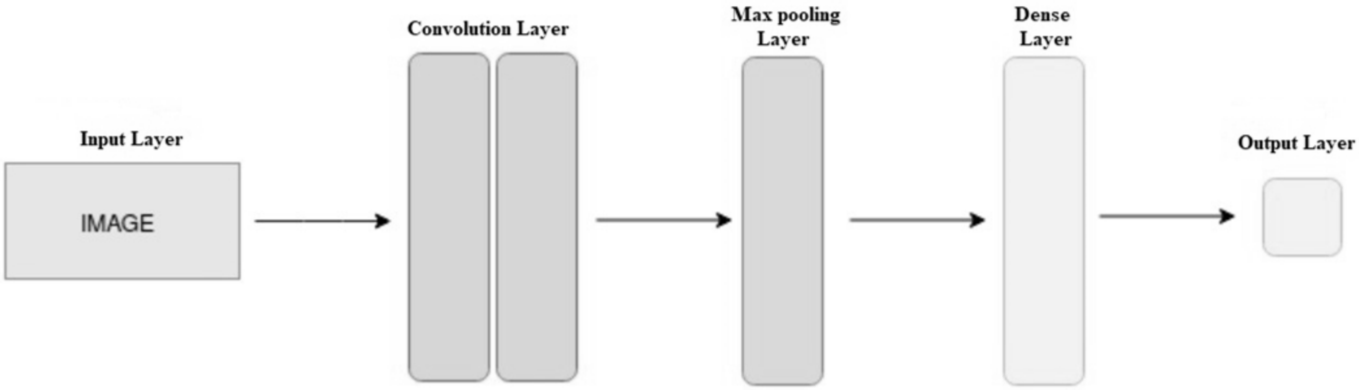

Fig 4 Simple CNN architecture

CNN + LSTM: Sequence data is processed by a CNN by moving convolutional filters on the input. It is possible for a CNN to learn traits from both space and time. An LSTM network learns long-term relationships between time steps by running over them over and over again.

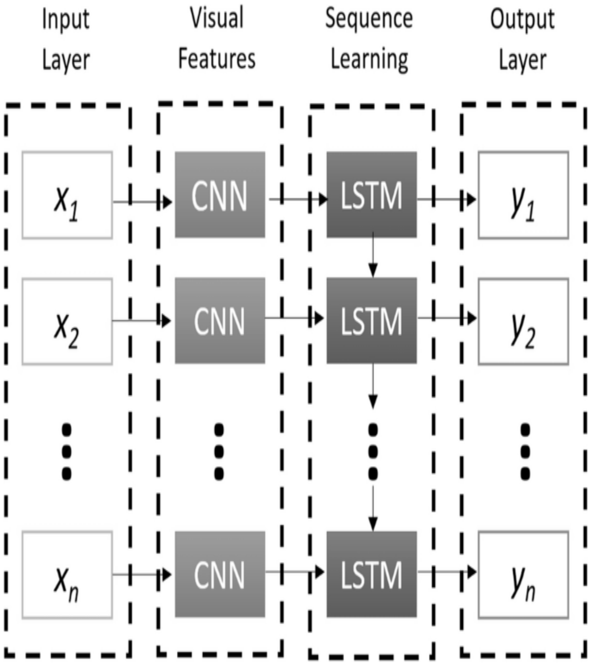

Fig 5 CNN + LSTM architecture

ARCHITECTURE

The recommended intelligent Intrusion Detection System (IDS) for smart Consumer Electronics (CE) networks includes SDN and DL. The architecture separates the control plane and data plane, making smart CE network deployment easy. The IDS detects several threats using a Cuda-enabled Bidirectional LSTM (Cu-BLSTM) model. System algorithms include BiLSTM, GRU, DNN, CNN, and CNN-LSTM. Simulations on the CICIDS-2018 dataset reveal that the strategy outperforms modern security methods.

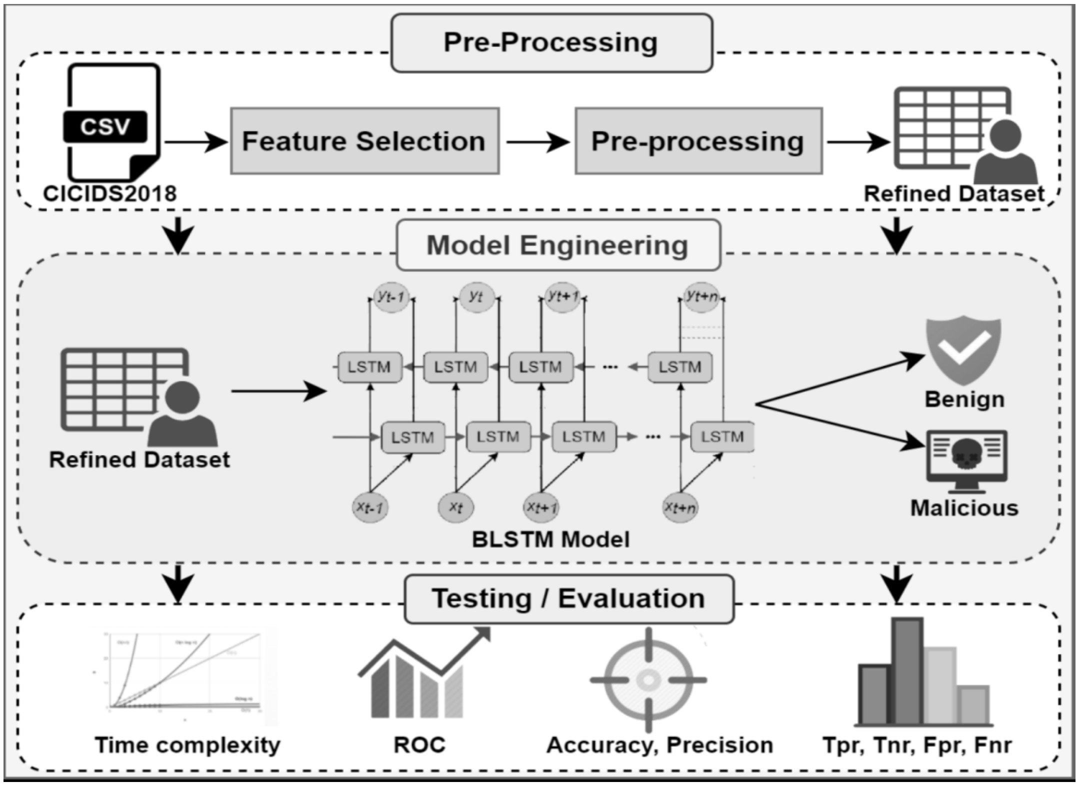

Fig 6 System Architecture

SUMMARY

A smart Consumer Electronics (CE) network Intrusion Detection System (IDS) will be built using SDN and Deep Learning. SDN spread design separates control and data planes. Cuda-enabled Bidirectional Long Short-Term Memory (Cu-BLSTM) lets the IDS identify numerous sophisticated CE network attacks. Simulations of the CICIDS-2018 dataset reveal that our strategy works and outperforms current security alternatives. Important algorithms include BiLSTM, GRU, DNN, CNN, and a CNN-LSTM mix.

CONCLUSION

Our innovative breach detection technology uses software-defined networking and deep learning to secure consumer goods networks. For the system's distributed architecture and various consumer electronics, a software-defined networking design and consumer electronics network were created. Next, a cuda-enabled bidirectional long short-term memory IDS was implemented at the control plane to identify hazards. We demonstrated that the recommended IDS is accurate, precise, and fast using the CICIDS-2018 dataset. We also tested the anticipated IDS against other cutting-edge approaches. We'll train the model with various datasets to discover intrusions in these networks better. Finally, we provide DL-based Intelligent models to swiftly detect risks in the future generation of smart consumer electronics networks.

FUTURE SCOPE

We plan to improve the suggested smart intruder detection system in the future by teaching the model on a variety of datasets to make it more flexible and able to do more. This will help improve the ways that intruder detection systems work in consumer electronics networks as they change. We also want to look into new developments in deep learning methods and see how they can be combined with software-defined networking to make danger identification even stronger. Our goal is to keep improving and making deep learning-based clever models better at finding threats in the next wave of smart consumer electronics 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.