EFFECTIVE MULTITASK DEEP LEARNING FOR IOT MALWARE DETECTION AND IDENTIFICATION USING BEHAVIORAL TRAFFIC ANALYSIS

Vishnu Bannurkar
M. Tech Student
Department of
Computer science and
Engineering
School of Engineering,
Anurag university
Hyderabad, Telangana, India
vishnu.bannurkar13@gmail.com

Jayendra Kumar
Assistant Professor
Department of
Computer science and
Engineering
School of Engineering,
Anurag university
Hyderabad, Telangana, India
jayendrakumarcse@anurag.edu.in

Dr. G. Vishnu Murthy
Professor and Dean
Department of
Computer Science and Engineering
School of Engineering
Anurag University
Hyderabad,Telangana,India
deancse@anurag.edu.in

Abstract: This program emphasizes the protection of our expanding network of intelligent devices. The IoT device in residential, health and other industries requires the need to ensure these network technologies. Technological progress also increases related risks. We examine the domain of attacks on malware, including prominent cases such as Botnet Mirai. By understanding these risks, we want to develop effective countermeasures. This initiative has two goals. We create resistant security solutions specially designed for IoT devices. Secondly, we are developing a categorization method to detect accurate malware attacking these devices, and therefore we provide more accurate defense. We use machine learning techniques and deep learning. Our goal is to allow computers to learn and adapt independently, and therefore minimize the need for constant involvement of a person for security upgrade. Introducing a unique model based on multitask LSTM-intelligent solutions that detect possible risks for IoT devices and determines the exact nature of danger. It is the most modern defense against advancing cyber threats. The experiment shows that CNN and CNN+LSTM models improve the extraction of elements for effective IoT malware detection. In addition, a flask -integrated flask allows users, verification and testing, providing intuitive interfaces for efficient interaction and evaluation of sophisticated deep learning models.

"Index terms *- Multitask deep learning, multimodal learning, Cybersecurity, IoT malware detection, malware identification, and heterogeneity traffic analysis".*

1. INTRODUCTION

The Internet of Things (IoT) revolutionizes the interconnected international through vehicles, smart houses and cities, production, medical systems, retail, space applications and cyber, whilst the spread of portable net devices continues [1]. As a result, new IoT gadgets increase technological progress and simplifies the production of those sensible gadgets. At the equal time, it's far vital to determine several new safety concerns, as said in the Danger of IoT of 2020 [2]. For example, Botnet Mirai is concerned in infamous attacks on DVN, which culminated in one of the maximum crucial "Distributed Denial-of Service (DDoS)" attacks ever documented on the Internet [3]. It is critical that the accessibility of the Mirai supply code has elevated the creation of

a robust and superior malware of a comparable Mirai, together with Satori [4], Hajime [5] and Brickerbot [6]. As a result, scientists have tried to explore the complicated strategies of solving the safety trouble in current years. The absence of empirical statistics on simultaneous IoT malware and understanding of behavioral traits of gadget infected with malware is to perform complicated answers disputed within the IoT area. Many Medonopots specific to IoT were installed to collect accurate records on simultaneous malware IoT [7].

Research of the literature of this observe found out particular troubles: IoT security regarding malware assaults [8], [9] and categorization of IoT malware -primarily based operations [10]. The principal aim is to defend the device from attacks on malware. However, the arrival of very advanced ransomware excludes entire protection of the device. It is more likely to awareness on a sure shape of malware at a certain time. As a result, it can be feasible to categorize exceptional forms of malware and deactivate offerings associated with a specific virus in place of the complete gadget. We targeted on sufficiently safety of IoT system from protection threats and troubles with categorization of malware. As a result, we designed the Multitask class version that might solve both troubles in parallel.

Various machine learning methodologies using the flow [13], [14] and packets [15], [16] were determined to reliably detect IoT operation. However, the classifiers of machine learning often need domain knowledge and extraction processes and the evaluation of functions at work. As IoT malware proceeds, such adapted attributes can become insufficient for detection and classification of developing malware families [17]. As a result, new research advocates the use of algorithms of Malware -based classification to overcome machine learning deficiencies. These research propose a discount in the value of manufacturing synthetic features by using gaining knowledge of features immediately from uncooked statistics, and consequently put off the need for in addition engineering of elements [18], [19]. Regardless of the effectiveness of deep learning degree, maximum of the pinnacle methodologies preserve to gain static or dynamic residences from the precise representation of malware records, restricting the mastering method and neglecting the advantages of the usage of exceptional illustration of the goal information. As a result, the improvement of a honest records set is necessary for the development of durable fashions and detection systems to stumble on and analyze cyber attacks.

2. LITERATURE SURVEY

Technical company speaks about the IoT. The powerful cloud computing architecture and the smooth integration of sensors and drives with the environment allow this "network of autonomous objects" [1]. From intelligent wearable to intelligent cities, from home to industry, IoT flourishes. Gartner Inc. It predicts 26 billion IoT devices by 2020. We assume that we will soon see IoT applications in the urban transit system or intelligent energy network. [1] This article briefly solves the development of IoT and their consequences for everyday life. Cloud computing, autonomous control and AI are also important in IoT. For efficient IoT technologies, the Internet, wireless sensors and drives and distributed computer technology must be synchronized.

Modern houses quickly receive IoT gadgets. Home IoT security is difficult because for the diversity of these devices that differ from low - range sensors to smart TVs. Moreover, many consumer devices are uncertain because manufacturers do not use safety procedures such as software repair. [8] This observe introduces a cooperative mechanism between the home gateway and the Internet provider provider for the identification and insulation of IoT security threats the usage of statistics. We provide green IoT safety offerings for the safety of personal information combos of great view from ISP (the usage of powerful gadget getting to know strategies on visitors footprints) and a nice - grained view of activity from home (the use of EDGE processing techniques) [8,14,21].

With the development of current communication technologies, the size of the IoT has grown to an unprecedented level and threatened the ecosystem. Due to the scattered nature of IoT networks, it is hard to create an anomaly detection device [9]. Invitation and dangerous conduct are increasingly complex and sudden. Other issues in designing a machine of detection of anomalies based totally on behavior consist of the absence of a sufficient wide variety of IoT and privateness samples. The technique of detection of hierarchical anomalies with the usage of a "generative adversial network (GAN) and auto-enabled (AE)" cooperation solves those demanding situations [9,28]. The reconstruction of the sampling fund for a centralized driver using IoT network turbines addresses information and personal facts safety. After adapting to local uncooked facts from IoT nodes, the centralized worldwide AE is skilled and supplied to local anomalies detection community. The UNSW Bot-IoT data report suggests that our approach overcomes others.

Today's safety business is fighting to characterize traffic. It's hard because new applications and services and encrypted conversations are still coming out. [10] VPN are a popular encrypted communication solution for avoiding censorship and access to geographically limited services. In this research, we test time -based time -based time to identify the operation of the VPN and classify encrypted communication by type (viewing, streaming, etc.). We verify your correctness of functions using C4.5 and KNN, two popular machine learning methods. High accuracy and power indicate that point -associated variables are appropriate classifiers for encrypted visitors characterization.

IoT with progress in the field of large data, communication and network technology benefits health, energy, industry and transport. ICT manufacturers and operators deploy IoT devices across network infrastructures with low security thanks to their business strategies and offer new attack vectors. Traditional algorithms Detection of rules of rules used network management systems cannot detect new attacks because they use predefined offensive signatures. In parallel, the detection strategies have excessive false superb speeds because of inadequate statistical verification of ground information at the fact used to profile the everyday network behavior. We use anomaly detection, "cyber threat intelligence (CTI)" and parallel processing for profiling and identifying the threatening cyber attacks [39,41,49]. Citrus is a new framework for detection of disruption that collects and denotes

lively data on the attack from different points of the Internet to detect and classify harmful behavior with a graph -based metric and ML algorithms. Flexible design Citrus software enables profiling, detection and categorizing the development of cyber attacks in optimal computing costs. Verification of ground truth data is important. As a result, it is a realistic and practical possibility for the defense and resistance of the new generation network.

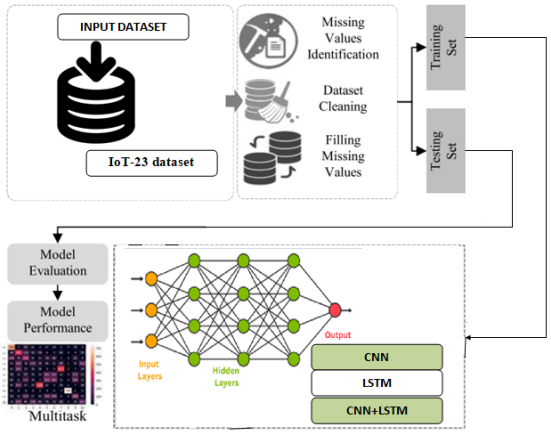
3. METHODOLOGY

i) Proposed Work:

Using the IoT-23 data file, our research implements a LSTM. The model precisely captures time trends in IoT data. The design integrates two layers of LSTM for extensive extraction of elements that followed the Custom attention layer to highlight the basic elements in the time sequence. This systematic technique improves the potential of the model for powerful detection and class of IoT malware and equip it to deal with diverse and changing threats within IoT [14,33,34]. Research includes "CNN and CNN+LSTM" models to expand LSTM -based techniques and therefore increases the extraction of elements for more thorough IoT malware. A flask associated with SQLite has been created and increases the ability to register the user, signin and test. This update offers an intuitive interface that allows the interaction and evaluation of sophisticated deep learning models effortlessly, increasing the practical usability of the project.

ii) System Architecture:

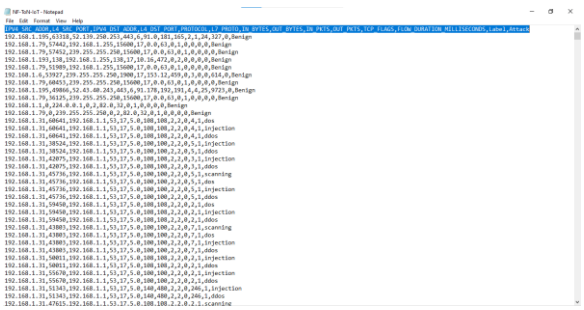
The project architecture begins with data input, followed by pre -work and trains divisions. Three separate models – "CNN, LSTM and CNN+LSTM" - are developed to capture geographical and time relations in IoT network data. The models are then evaluated in terms of their efficiency in detection of harmful communication and categorization of IoT malware [4,6]. The complete multitask strategy provides extensive solutions to improve the Internet security with the current solution of several aspects of identification and categorization of threats.



"Fig 1 Proposed architecture"

iii) Dataset collection:

The research uses the IoT-23 data file, which is an extensive compilation of network traffic data, especially a curator for investigating malware IoT. IoT-23 includes many traffic situations, facilitating the training and evaluation of "CNN, LSTM and CNN+LSTM" models. The amount of data ensures accurate display of IoT network behavior and thus improves the efficiency of the proposed category system Multitask.



"Fig 2 IOT-23 dataset"

iv) Data Processing:

data processing converts unrefined records to usable data for establishments. facts scientists frequently address records processing, inclusive of series, organization, cleansing, validation, analyzes and facts transformation into interpretable representations along with graphs or articles. facts processing can be done by means of 3 strategies: guide, mechanical and digital. The goal is to growth the cost of statistics and make selections more efficient. This allows companies to strengthen their operations and carry out quick strategic choices. in this context, computerized facts processing technologies, including software program development, are crucial. it is able to transform large facts units, mainly huge facts, to good sized expertise of excellent and selection - making.

v) Feature selection:

The selection of functions is the manner of figuring out the most convertible, non -applicable and relevant traits for the development of the version. The systematic minimalization of the size of the statistics set is essential, on the equal time as the quantity and diversity of statistics sets persist in boom. The number one intention of choosing elements is to boom the overall performance of the predictive model and on the same time restrict the computing expenses of modeling.

the selection of features, the basic aspect of useful engineering includes identification of the most vital traits for coming into the gadget mastering algorithms. the choice strategy is used to reduce the quantity of enter variables through the exclusion of redundant or needless features, and consequently improves the set to the ones which might be maximum suitable for the machine learning version. primary benefits of choosing features earlier before allowing the machine learning version to pick the most vital houses.

vi) Algorithms:

This study uses "long short-term memory (LSTM)" network, a sort of "recurrent neural networks (RNN)", for its ability to seize complex relationships and time styles in IoT community visitors data. Unlike traditional RNN, LSTMS alleviates the trouble of disappearing gradient, which makes it less complicated to version long reach relationships vital to recognize complicated sequences. LSTMs are useful in identifying pleasant formulas that imply vulnerability of safety within the dynamic and improvement surroundings of network site visitors IoT inside the place of disturbance detection. Thanks to their capability to store prolonged sequences, they are best for amassing sequential traits of community traffic and creating a stable base to create a unique and green gadget of intrusion detection.

"Convolutional neural networks (CNN)" are deep architecture of learning developed for image recognition and processing. In the CNNS convention layers, they use input data filters, allowing autonomously and adaptively to obtain hierarchical representations. This project selects CNN for its efficiency in collecting spatial relations in IoT network traffic. Convolutional layers can recognize the formulas in traffic data, so CNN will detect anomaly and classification of various types of Malware IoT, and therefore increases the overall resistance and accuracy of the proposed classification model Multitask.

The "**CNN+LSTM"** is a hybrid design that integrates a CNN with a LSTM. This experiment

shows that CNN effectively captures geographical relationships in IoT network data, while LSTM emphasizes the analysis of time formulas. The amalgamation of both models makes it easier to study data by CNN for extraction of elements and LSTM for sequential learning. This synergy is useful for the aim of the project detection and classification of Malware IoT, as it allows the model to capture both geographical and time fineness in comprehensive network traffic samples, thereby improving the accuracy and flexibility of the system.

4. EXPERIMENTAL RESULTS

Accuracy: A test capacity towards create a proper difference between healthy & sick cases is a measure of accuracy. We can determine accuracy of a test through calculating proportion of cases undergoing proper positivity & genuine negative. It is possible towards express this mathematically:

$$\text{"Accuracy"} = \frac{\text{"TP + TN"}}{\text{"TP + FP + TN + FN"}} (1)$$

Precision: Precision quantifies the percentage of efficiently identified positive cases or samples. Precision is decided by using the components:

$$\text{"}Precision\text{"} = \frac{\text{"True Positive"}}{\text{"True Positive + False Positive"}} (2)$$

Recall: ML recall assesses a model's potential to choose out all relevant times of a class. It demonstrates a version's efficacy in encapsulating times of a class by using comparing nicely anticipated high satisfactory observations to the general variety of positives.

$$\text{"}Recall\text{"} = \frac{\text{"TP"}}{\text{"TP + FN"}} (3)$$

F1-Score: The accuracy of a system ML of model is classed the usage of the F1 score. Integrating the precision and do not forget metrics of the model. The accuracy metric quantifies the frequency of proper predictions made through a model at some level inside the dataset.

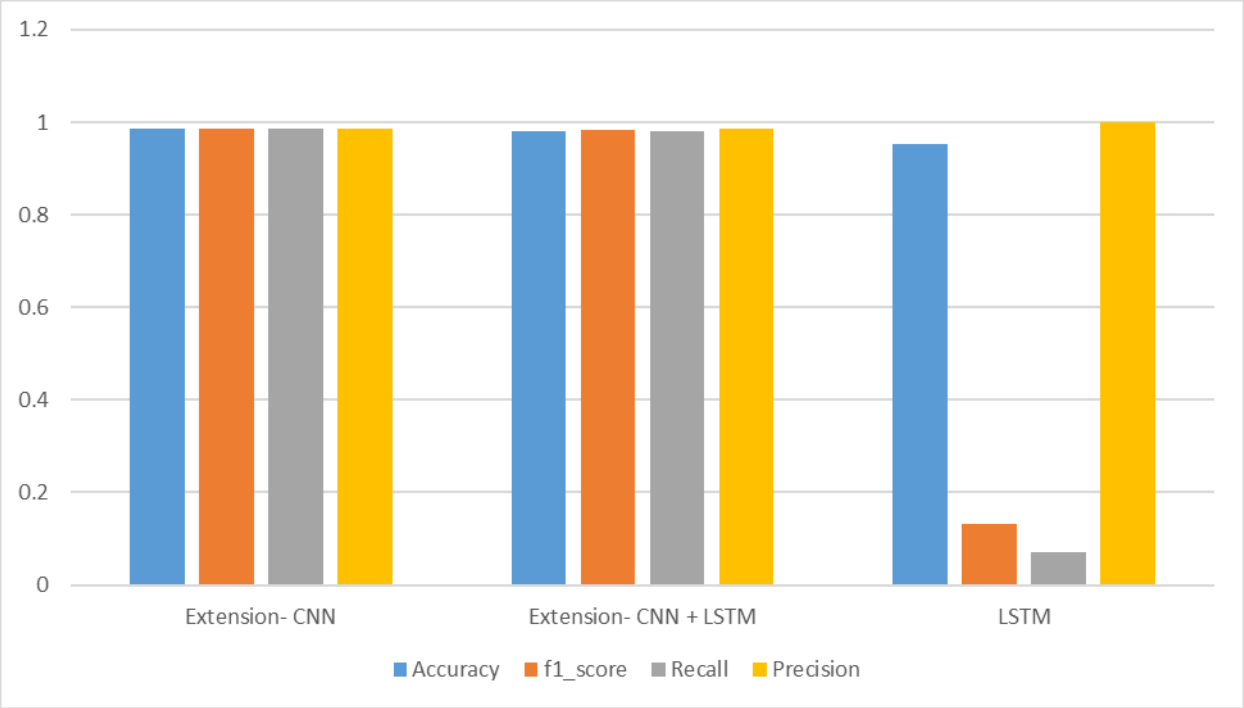
$$\text{"}F1\ Score\text{"} = \text{"2"} * \frac{\text{"}Recall \text{ X } Precision\text{"}}{\text{"}Recall + Precision\text{"}} * \text{"100"} (4)$$

Table (1) assesses the "performance metrics—accuracy, precision, recall, and F1 score"—for each method. The CNN routinely surpasses all other algorithms across all measures. The tables provide a comparative examination of the metrics for the alternative methods.

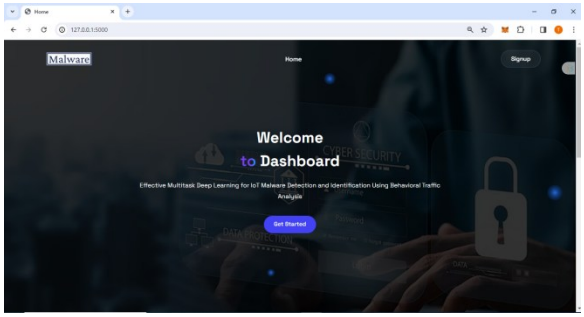
"Table.1 Performance Evaluation Table"

ML Model	Accuracy	f1_score	Recall	Precision
Extension- CNN	**0.985**	**0.986**	**0.985**	**0.987**
Extension- CNN + LSTM	0.981	0.983	0.981	0.986
LSTM	0.954	0.133	0.071	1.000

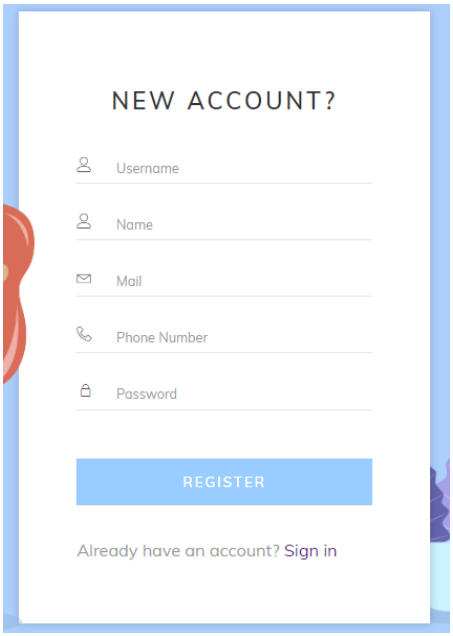
"Graph.1 Comparison Graph"



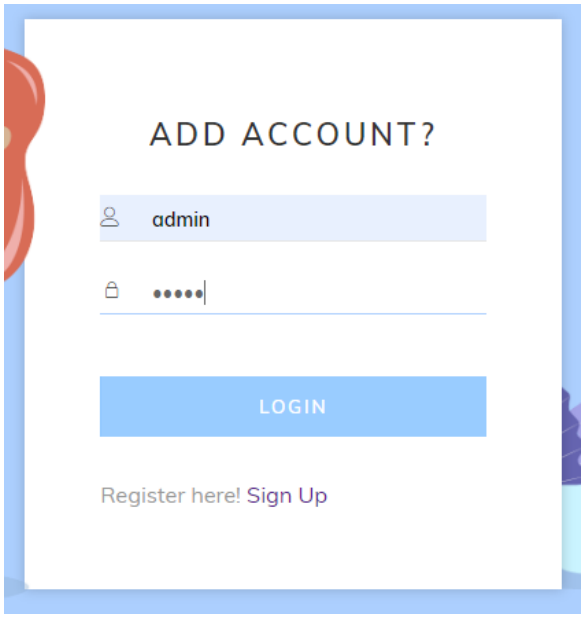
In Graph (1), "accuracy is shown in blue, precision in yellow, recall in grey, and F1-Score in orange". Relative to the other models, the CNN demonstrates enhanced performance across all measures, attaining the highest values. The graphs above graphically represent these results.



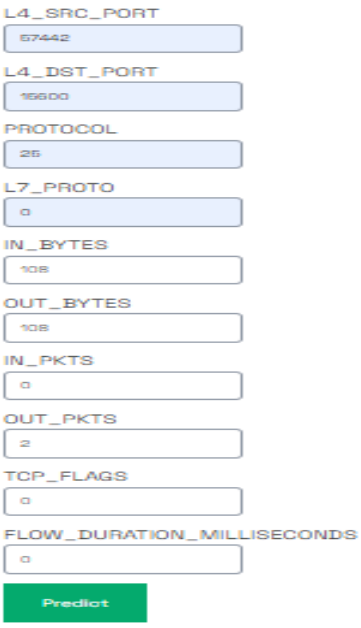
"Fig 3 Home page"



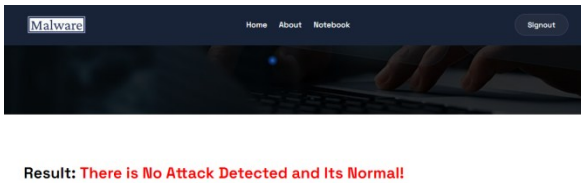
"Fig 4 Signin page"



"Fig 5 Login page"



"Fig 6 User input"



"Fig 7 Predict result for given input"

5. CONCLUSION

The study effectively solved the complexity of IoT security and demonstrated the efficiency of a model based on LSTM multitasks in identifying the emerging risks of malware. The models showed flexibility for different situations of IoT by integrating heterogeneity of data file, and therefore allowed effective disruption detection in a number of devices and cyber threats. [52, 53] Using LSTM networks improved time series data analysis and improved the ability of the model to understand complex formulas in IoT network traffic. The project has effectively linked theory and practice by offering a practical solution through a user-friendly front-end flask, allowing users to participate and evaluate the model predictions. The integration of the flask and SQLite increases the user's accessibility and expands the model's audience. The front-end design makes it easier to test users, verify input and predict the smooth model, thereby improving practical usability. Alternative methods using "CNN and CNN+LSTM" architecture have increased the security of the Internet of Things. Both models worked great, with CNN showing a small advantage. This clear advantage has led to the deliberate implementation of the CNN model and emphasized its efficiency in strengthening the system against various and developing threats of IoT malware.

6. FUTURE SCOPE

Future enhancements may include optimizing "CNN, LSTM and CNN+LSTM" models by integrating sophisticated deep learning architectures. This may include exploring new neuron network architectures or optimization methods to improve the accuracy and flexibility of models. The investigation of the integration of the

methodologies of computational edge methods means using decentralized processing capabilities. This optimizes real -time data processing and decision -making, reduces latency and increases the overall efficiency of the system by allocating the workload of the workload to IoT [2]. Implementation of Dynamic Threat Intelligence Feeds requires a constant update of the system with data on the evolving threats of IoT malware in real time. This ensures that the system can quickly adjust and respond quickly, which offers continuous protection against emerging safety threats in the IoT environment. [12] Model modification to support the wider range of IoT devices and communication protocols, seeks to improve its adaptability. By integrating different IoT ecosystems, the model can provide increased safety measures and guarantee effective protection against a wide range of possible attacks in different contexts of IoT.

REFERENCES

[1] H. N. Saha, A. Mandal, and A. Sinha, "Recent trends in the Internet of Things," in Proc. IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC), 2017, pp. 1–4.

[2] "2020 unit 42 IoT threat report." Unit 42. Mar. 2020. Accessed: Apr. 17, 2022. [Online]. Available: https://start.paloaltonetworks.com/ unit-42-iot-threat-report

[3] M. Antonakakis et al., "Understanding the mirai botnet," in Proc. 26th USENIX Security Symp. (USENIX Security), 2017, pp. 1093–1110.

[4] J. Vijayan. "Satori botnet malware now can infect even more IoT devices." 2018. [Online]. Available: https://www.darkreading.com/ vulnerabilities-threats/satori-botnet-malware-now-can-infect-evenmore-iot-devices

[5] C. Cimpanu et al., "Hajime botnet makes a comeback with massive scan for MikroTik routers." 2018. [Online]. Available: https://www. radware.com/newsevents/mediacoverage/2018/ hajime-botnet-makes-acomeback-with-massive-scan/

[6] L. Pascu. "78% of malware activity in 2018 driven by IoT botnets, NOKIA finds." 2018. [Online]. Available: https://www.bitdefender.com/ blog/hotforsecurity/78-malware-activity-2018-driven-iot-botnets-nokiafinds

[7] P.-A. Vervier and Y. Shen, "Before toasters rise up: A view into the emerging IoT threat landscape," in Proc. Int. Symp. Res. Attacks Intrusions Defenses, 2018, pp. 556–576.

[8] H. Haddadi, V. Christophides, R. Teixeira, K. Cho, S. Suzuki, and A. Perrig, "Siotome: An edge-ISP collaborative architecture for IoT security," in Proc. IoTSec, 2018, pp. 1–4.

[9] T. Zixu, K. S. K. Liyanage, and M. Gurusamy, "Generative adversarial network and auto encoder based anomaly detection in distributed IoT networks," in Proc. IEEE Global Commun. Conf. (GLOBECOM), 2020, pp. 1–7.

[10] G. Draper-Gil, A. H. Lashkari, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of encrypted and VPN traffic using time-related features," in Proc. 2nd Int. Conf. Inf. Syst. Security Privacy (ICISSP), 2016, pp. 407–414.

[11] R. Mills, A. K. Marnerides, M. Broadbent, and N. Race, "Practical intrusion detection of emerging threats," IEEE Trans. Netw. Service Manag., vol. 19, no. 1, pp. 582–600, Mar. 2022.

[12] T. M. Booij, I. Chiscop, E. Meeuwissen, N. Moustafa, and F. T. H. den Hartog, "ToN_IoT: The role of heterogeneity and the need for

standardization of features and attack types in IoT network intrusion data sets," IEEE Internet Things J., vol. 9, no. 1, pp. 485–496, Jan. 2022.

[13] I. Ullah and Q. H. Mahmoud, "Network traffic flow based machine learning technique for IoT device identification," in Proc. IEEE Int. Syst. Conf. (SysCon), 2021, pp. 1–8.

[14] Z. Chen et al., "Machine learning-enabled IoT security: Open issues and challenges under advanced persistent threats," ACM Comput. Surv., to be published. [Online]. Available: https://doi.org/10.1145/3530812

[15] M. R. P. Santos, R. M. C. Andrade, D. G. Gomes, and A. C. Callado, "An efficient approach for device identification and traffic classification in IoT ecosystems," in Proc. IEEE Symp. Comput. Commun. (ISCC), 2018, pp. 304–309.

[16] A. Sivanathan, H. H. Gharakheili, and V. Sivaraman, "Managing IoT cyber-security using programmable telemetry and machine learning," IEEE Trans. Netw. Service Manag., vol. 17, no. 1, pp. 60–74, Mar. 2020.

[17] M. Alhanahnah, Q. Lin, Q. Yan, N. Zhang, and Z. Chen, "Efficient signature generation for classifying cross-architecture IoT malware," in Proc. IEEE Conf. Commun. Netw. Security (CNS), 2018, pp. 1–9.

[18] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, "Mobile encrypted traffic classification using deep learning: Experimental evaluation, lessons learned, and challenges," IEEE Trans. Netw. Service Manag., vol. 16, no. 2, pp. 445–458, Jun. 2019.

[19] A. M. Sadeghzadeh, S. Shiravi, and R. Jalili, "Adversarial network traffic: Towards evaluating the robustness of deep-learning-based network traffic classification," IEEE Trans. Netw. Service Manag., vol. 18, no. 2, pp. 1962–1976, Jun. 2021.

[20] A. H. Lashkari, G. Draper-Gil, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of Tor traffic using time based features," in Proc. ICISSp, 2017, pp. 253–262.

[21] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2671–2701, 3rd Quart., 2019.

[22] R. Zhao. "NSL-KDD." 2022. [Online]. Available: https://dx.doi.org/10. 21227/8rpg-qt98

[23] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in Proc. IEEE Symp. Comput. Intell. Security Defense Appl., 2009, pp. 1–6.

[24] N. Moustafa, 2019, "UNSW_NB15 Dataset," IEEE DataPort. [Online]. Available: https://dx.doi.org/10.21227/8vf7-s525

[25] S. Garcia, M. Grill, J. Stiborek, and A. Zunino, "An empirical comparison of botnet detection methods," Comput. Security, vol. 45, pp. 100–123, Sep. 2014. [Online]. Available: https://doi.org/10.1016/j. cose.2014.05.011

[26] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. B. Idris, A. M. Bamhdi, and R. Budiarto, "CICIDS-2017 dataset feature analysis with information gain for anomaly detection," IEEE Access, vol. 8, pp. 132911–132921, 2020.

[27] H. Kang, D. H. Ahn, G. M. Lee, J. D. Yoo, K. H. Park, and H. K. Kim, 2019, IoT network intrusion dataset," IEEE DataPort. [Online]. Available: https://dx.doi.org/10.21227/q70p-q449

[28] Y. Meidan et al., "N-BaIoT—Network-based detection of IoT botnet attacks using deep

autoencoders," IEEE Pervasive Comput., vol. 17, no. 3, pp. 12–22, Jul.–Sep. 2018.

[29] S. Garcia, A. Parmisano, and M. J. Erquiaga, Jan. 2020, "IoT-23: A Labeled Dataset with Malicious and Benign IoT Network Traffic," Zenodo. [Online]. Available: https://www.stratosphereips.org/datasetsiot23

[30] G. Gu, P. A. Porras, V. Yegneswaran, M. W. Fong, and W. Lee, "BotHunter: Detecting malware infection through IDS-driven dialog correlation," in Proc. USENIX Security Symp., vol. 7, 2007, pp. 1–16.

[31] G. Gu, J. Zhang, and W. Lee, "BotSniffer: Detecting Botnet command and control channels in network traffic," in Proc. Netw. Distrib. Syst. Security Symp. (NDSS), San Diego, CA, USA, 2008, pp. 1–8. [Online]. Available: https://www.ndss-symposium.org/ndss2008/botsnifferdetectingbotnetcommandandcontrolchannelsinnetworktraffic/

[32] Q. Sun, E. Abdukhamidov, T. Abuhmed, and M. Abuhamad, "Leveraging spectral representations of control flow graphs for efficient analysis of windows malware," in Proc. ACM Asia Conf. Comput. Commun. Security, 2022, pp. 1240–1242.

[33] R. Islam, R. Tian, L. M. Batten, and S. Versteeg, "Classification of malware based on integrated static and dynamic features," J. Netw. Comput. Appl., vol. 36, no. 2, pp. 646–656, 2013.

[34] Z. Ma, H. Ge, Y. Liu, M. Zhao, and J. Ma, "A combination method for android malware detection based on control flow graphs and machine learning algorithms," IEEE Access, vol. 7, pp. 21235–21245, 2019.

[35] P. R. Kanna and P. Santhi, "Unified deep learning approach for efficient intrusion detection system using integrated spatial–temporal features," Knowl. Based Syst., vol. 226, Aug. 2021, Art. no. 107132.

[36] A. A. Abd El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5G Internet of Things scenario," IEEE Trans. Netw. Service Manag., vol. 17, no. 1, pp. 118–131, Mar. 2020.

[37] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for Internet of Things in smart city," Future Gener. Comput. Syst., vol. 107, pp. 433–442, Jun. 2020.

[38] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," Internet Things, vol. 7, Sep. 2019, Art. no. 100059.

[39] Q. Sun, M. Abuhamad, E. Abdukhamidov, E. Chan-Tin, and T. Abuhmed, "MLxPack: Investigating the effects of packers on MLbased Malware detection systems using static and dynamic traits," in Proc. 1st Workshop Cybersecurity Soc. Sci., 2022, pp. 11–18.

[40] J. Singh, D. Thakur, T. Gera, B. Shah, T. Abuhmed, and F. Ali, "Classification and analysis of android malware images using feature fusion technique," IEEE Access, vol. 9, pp. 90102–90117, 2021.

[41] S. Lagraa, J. François, A. Lahmadi, M. Miner, C. Hammerschmidt, and R. State, "BotGM: Unsupervised graph mining to detect botnets in traffic flows," in Proc. 1st Cyber Security Netw. Conf. (CSNet), 2017, pp. 1–8.

[42] R. Bhatia, S. Benno, J. Esteban, T. V. Lakshman, and J. Grogan, "Unsupervised machine learning for network-centric anomaly detection in IoT," in

Proc. 3rd ACM CONEXT Workshop Big Data Mach. Learn. Artif. Intell. Data Commun. Netw., 2019, pp. 42–48.

[43] N. Gao, L. Gao, Q. Gao, and H. Wang, "An intrusion detection model based on deep belief networks," in Proc. 2nd Int. Conf. Adv. Cloud Big Data, 2014, pp. 247–252.

[44] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," IEEE Trans. Emerg. Topics Comput. Intell., vol. 2, no. 1, pp. 41–50, Feb. 2018.

[45] G. Bendiab, S. Shiaeles, A. Alruban, and N. Kolokotronis, "IoT malware network traffic classification using visual representation and deep learning," in Proc. 6th IEEE Conf. Netw. Softw. (NetSoft), 2020, pp. 444–449.

[46] R. Shire, S. Shiaeles, K. Bendiab, B. Ghita, and N. Kolokotronis, "Malware squid: A novel IoT malware traffic analysis framework using convolutional neural network and binary visualisation," in Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Cham, Switzerland: Springer, 2019, pp. 65–76.

[47] I. Baptista, S. Shiaeles, and N. Kolokotronis, "A novel malware detection system based on machine learning and binary visualization," in Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops), 2019, pp. 1–6.

[48] J. François, C. Wagner, R. State, and T. Engel, "SAFEM: Scalable analysis of flows with entropic measures and SVM," in Proc. IEEE Netw. Oper. Manag. Symp., 2012, pp. 510–513.

[49] S. García, V. Uhlíˇ r, and M. Rehak, "Identifying and modeling botnet C&C behaviors," in Proc. 1st Int. Workshop Agents CyberSecurity, 2014, pp. 1–8.

[50] M. Singh, M. Singh, and S. Kaur, "Detecting bot-infected machines using DNS fingerprinting," Digit. Investig., vol. 28, pp. 14–33, Mar. 2019.

[50] M. Singh, M. Singh, and S. Kaur, "Detecting bot-infected machines using DNS fingerprinting," Digit. Investig., vol. 28, pp. 14–33, Mar. 2019.

[51] M. Dib, S. Torabi, E. Bou-Harb, and C. Assi, "A multi-dimensional deep learning framework for IoT Malware classification and family attribution," IEEE Trans. Netw. Service Manag., vol. 18, no. 2, pp. 1165–1177, Jun. 2021.

[52] A. Sagheer and M. Kotb, "Unsupervised pre-training of a deep LSTMbased stacked autoencoder for multivariate time series forecasting problems," Sci. Rep., vol. 9, no. 1, pp. 1–16, 2019.

[53] T. Abuhmed, S. El-Sappagh, and J. M. Alonso, "Robust hybrid deep learning models for alzheimer's progression detection," Knowl. Based Syst., vol. 213, Feb. 2021, Art. no. 106688.

[54] S. El-Sappagh, T. Abuhmed, S. M. R. Islam, and K. S. Kwak, "Multimodal multitask deep learning model for alzheimer's disease progression detection based on time series data," Neurocomputing, vol. 412, pp. 197–215, Oct. 2020.

[55] A. Felkner. "Dataset of legitimate IoT data (VARIoT)." 2022. [Online]. Available: https://www.data.gouv.fr/fr/datasets/dataset-of-legitimate-iotdata/