

## **Hybrid CNN–LSTM–Attention Architecture for Effective IoT Malware Detection and Identification**

Banoth JansiRani

[jansi.banoth09@gmail.com](mailto:jansi.banoth09@gmail.com)

**Abstract:** In this initiative, we focus on safeguarding our ever-growing network of smart devices. With the rise of IoT in homes, healthcare, and more, ensuring the security of these interconnected gadgets is crucial. As technology advances, so do the risks. We delve into the realm of malware attacks, studying notorious instances like the Mirai botnet. By understanding these threats, we aim to develop effective countermeasures. This project has a dual objective. Firstly, we're developing robust security systems tailored for IoT devices. Secondly, we're creating a classification system to identify the specific type of malware targeting these devices, offering a more precise defense. And we are using machine learning and deep learning. OUR goal is to equip computers with the ability to learn and adapt autonomously, reducing dependence on constant human intervention for security updates. And we are Introducing the innovative multitask LSTM-based model – a sophisticated solution that not only detects potential threats to IoT devices but also identifies the exact nature of the threat. It's a cutting-edge protector against evolving cyber-attacks. Including the project, CNN and CNN+LSTM models enhance feature extraction for robust IoT malware detection. Additionally, a Flask framework with SQLite facilitates user signup, signin, and testing, ensuring a user-friendly interface for efficient interaction and evaluation of advanced deep learning models.

*“Index terms - Multitask deep learning, multimodal learning, Cybersecurity, IoT malware detection,*

*malware identification, and heterogeneity traffic analysis”.*

### **1. INTRODUCTION**

Internet of Things (IoT) is transforming the connected world with automobiles, smart homes and cities, manufacturing, healthcare systems, retail, space applications, and cyber-physical systems because the number of portable Internet-connected devices is increasing continuously [1]. As a result, with the introduction of new IoT devices, technical advancement and the manufacturing simplicity of these intelligent devices continue to improve. Meanwhile, the creation of a slew of new security considerations is required, according to the 2020 IoT threat report [2]. The Mirai botnet, for example, is used in the well-known cyberattacks on DVN, which resulted in one of the most significant Distributed Denial-of Service (DDoS) attacks ever recorded on the Internet [3]. More importantly, the availability of the Mirai source code accelerated the development of powerful and sophisticated Mirai-like malware, such as Satori [4], Hajime [5], and BrickerBot [6], to mention a few. As a result, academics have sought to investigate complex solutions to address the security problem in recent years. However, the lack of empirical data regarding current IoT malware and understanding of the behavioral features of malware-infected devices make the implementation of complex solutions controversial in IoT. Various IoT-specific

honeypots have been set up to collect precise information on existing IoT malware [7].

Based on the literature review conducted in this study, we identified two distinct problems: IoT security against malware attacks [8], [9] and classification of IoT malware based on generated traffic [10]. The primary goal is to protect devices from malware attacks. However, due to the emergence of highly sophisticated ransomware, devices cannot be fully secured. It is more likely to target a particular type of malware at a given moment. As a result, it may be feasible to classify different malware types, shutting down services on the targeted malware rather than the entire system. We combined the objective of adequately protecting the IoT device twofold from the security and malware classification perspective. Thus, we proposed a multitask classification model to address both problems simultaneously.

Several Machine Learning (ML) approaches with flow based [13], [14], and packet-based [15], [16] features have been developed to identify IoT traffic accurately. However, classifiers based on ML frequently need domain expertise and time-consuming feature extraction and assessment activities. As IoT malware evolves, such customized features may be ineffective in detecting and classifying new malware families [17]. Therefore, recent work proposes the utilization of deep learning (DL)-based malware classification algorithms to address the limitations of ML. These studies propose the lowering of the cost of artificial feature generation while learning features directly from raw data without requiring extra feature engineering [18], [19]. Despite the human-level performance of DL, most state-of-the-art techniques still learn static or dynamic features from a single representation of the malware data, thereby restricting

the learning process while disregarding the advantages of employing different representations of the target data. Therefore, advancing a plausible dataset is crucial for building robust models and intrusion detection tools to identify and probe cyber-attacks.

## 2. LITERATURE SURVEY

The Internet of Things (IoT) has become a hot topic in the present tech-driven world. A strong framework of cloud computing, backed up by a seamless blending of sensors and actuators with the environment around us, is making this “network of networks of autonomous objects” a reality [1]. From smart wearables to smart cities, from domestic life to industries, the IoT is expanding itself to different areas. According to Gartner Inc., the IoT will include 26 billion units installed by 2020. Smart security solutions, smart home automation, smart health care, smart wearables etc. are in-trend applications of IoT, and by the near future we expect to see its application to a city's transportation system or smart power grids. [1] This paper presents a brief overview on different trends of the IoT and also discusses about the effects of the IoT on our day-to-day life. It also discusses the importance of cloud computing, autonomous control, artificial intelligence in the context of the IoT. Lastly, it's concluded with the need of synchronization of the Internet, wireless sensors and actuators and distributed computing for successfully enabling technologies for the IoT.

Modern households are deploying Internet of Things (IoT) devices at a fast pace. The heterogeneity of these devices, which range from low-end sensors to smart TVs, make securing home IoT particularly challenging. To make matters worse, many consumer-IoT devices are hard or impossible to secure because



device manufacturers fail to adopt security best practices (e.g., regular software patches). [8] In this paper we propose a novel, cooperative system between the home gateway and the Internet Service Provider (ISP) to provide data driven security solutions for detecting and isolating IoT security attacks. Our approach is based on a combination of a large-scale view from the ISP (using powerful machine learning techniques on traffic traces), and the fine-grained view of the per-device activity from the home (using edge processing techniques) to provide efficient, yet privacy-aware IoT security services [8,14,21].

With the advances in modern communication technologies, the application scale of Internet of Things (IoT) has evolved at an unprecedented level, which on the other hand poses threats to the IoT ecosystem. As the intrusions and malicious actions are becoming more complex and unpredictable, developing an effective anomaly detection system, considering the distributed nature of IoT networks, remains a challenge [9]. Moreover, the lack of sufficiently large amount of data samples of IoT traffic and data privacy pose further challenges in developing a behavior-based anomaly detection system. To address these issues, we present an unsupervised hierarchical approach for anomaly detection through cooperation between generative adversarial network (GAN) and auto-encoder (AE) [9,28]. The problems of data aggregation and privacy preservation are addressed by reconstructing a sampling pool at a centralized controller using a collection of generators from the individual IoT networks. Then, a centralized global AE is trained and passed to individual local networks for anomaly detection after a final adaptation with the local raw data from the IoT nodes. The performance is evaluated using the UNSW Bot-IoT dataset and the results demonstrate the effectiveness of

our proposed approach which outperforms other approaches.

Traffic characterization is one of the major challenges in today's security industry. The continuous evolution and generation of new applications and services, together with the expansion of encrypted communications makes it a difficult task. [10] Virtual Private Networks (VPNs) are an example of encrypted communication service that is becoming popular, as method for bypassing censorship as well as accessing services that are geographically locked. In this paper, we study the effectiveness of flow-based time-related features to detect VPN traffic and to characterize encrypted traffic into different categories, according to the type of traffic e.g., browsing, streaming, etc. We use two different well-known machine learning techniques (C4.5 and KNN) to test the accuracy of our features. Our results show high accuracy and performance, confirming that time-related features are good classifiers for encrypted traffic characterization.

The Internet of Things (IoT), in combination with advancements in Big Data, communications and networked systems, offers a positive impact across a range of sectors including health, energy, manufacturing and transport. By virtue of current business models adopted by manufacturers and ICT operators, IoT devices are deployed over various networked infrastructures with minimal security, opening up a range of new attack vectors. [11] Conventional rule-based intrusion detection mechanisms used by network management solutions rely on pre-defined attack signatures and hence are unable to identify new attacks. In parallel, anomaly detection solutions tend to suffer from high false positive rates due to the limited statistical validation of ground truth data, which is used for profiling normal

network behavior. In this work we go beyond current solutions and leverage the coupling of anomaly detection and Cyber Threat Intelligence (CTI) with parallel processing for the profiling and detection of emerging cyber-attacks [39,41,49]. We demonstrate the design, implementation, and evaluation of Citrus: a novel intrusion detection framework which is adept at tackling emerging threats through the collection and labelling of live attack data by utilizing diverse Internet vantage points in order to detect and classify malicious behavior using graph-based metrics as well as a range of machine learning (ML) algorithms. Citrus considers the importance of ground truth data validation and its flexible software architecture enables both the real-time and offline profiling, detection and classification of emerging cyber-attacks under optimal computational costs. Thus, establishing it as a viable and practical solution for next generation network defense and resilience strategies.

### 3. METHODOLOGY

#### i) Proposed Work:

Leveraging the IoT-23 dataset, our project employs Long Short-Term Memory (LSTM) networks. The model intricately captures temporal patterns in IoT data. Its architecture incorporates dual LSTM layers for comprehensive feature extraction, followed by a custom attention layer to emphasize critical aspects in the temporal sequence. This structured approach enhances the model's capacity for robust IoT malware detection and classification, making it adept at handling diverse and evolving threats in the IoT landscape [14,33,34]. And also included in the project is, CNN and CNN+LSTM models were incorporated to complement the LSTM-based approach, enhancing feature extraction for more comprehensive IoT

malware detection. Furthermore, a Flask framework integrated with SQLite was developed, extending functionality to user signup, signin, and testing. This addition provides a user-friendly interface, facilitating seamless interaction and evaluation of the advanced deep learning models, thereby enhancing the project's practical utility.

#### ii) System Architecture:

The project's system architecture begins with data input, followed by preprocessing and a train-test split. Three distinct models—CNN, LSTM, and CNN+LSTM—are trained to capture spatial and temporal dependencies in IoT network traffic. The models are then tested and evaluated for their performance in identifying malicious traffic and classifying IoT malware types [4,6]. The overarching multitask approach ensures a comprehensive solution to enhance IoT security by simultaneously addressing various aspects of threat detection and classification.

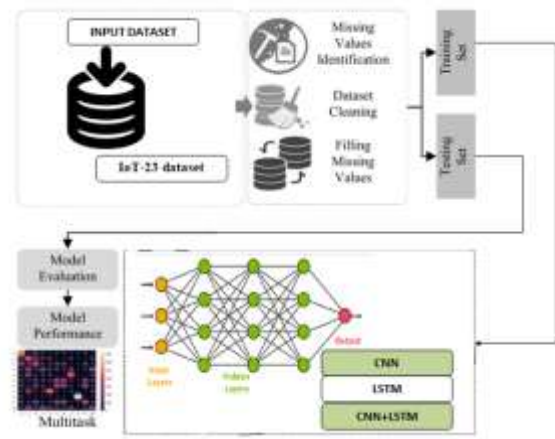


Fig 1 Proposed architecture

#### iii) Dataset collection:

The project utilizes the IoT-23 dataset, a comprehensive collection of network traffic data

specifically designed for IoT malware analysis. IoT-23 encompasses diverse traffic scenarios, enabling the training and evaluation of CNN, LSTM, and CNN+LSTM models. Its richness ensures a realistic representation of IoT network behaviors, enhancing the effectiveness of the proposed multitask classification system.

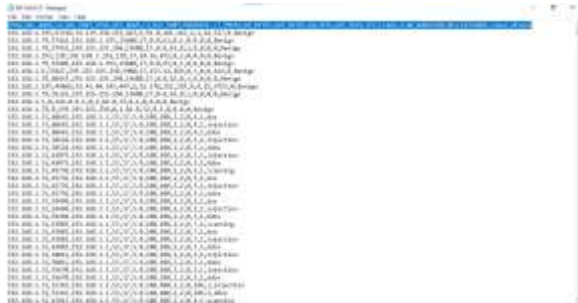


Fig 2 IOT-23 dataset

#### 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:

**Long Short-Term Memory (LSTM)** networks, a type of recurrent neural network (RNN), are employed in this project for their ability to capture intricate dependencies and temporal patterns within IoT network traffic data. Unlike traditional RNNs, LSTMs address the vanishing gradient problem, enabling the modeling of long-range dependencies crucial for understanding complex sequences. In the context of intrusion detection, LSTMs prove effective in recognizing nuanced patterns indicative of security threats in the dynamic and evolving landscape of IoT network communication. Their capacity to retain information over extended sequences makes them well-suited for capturing the sequential nature of network traffic, providing a robust foundation for the

development of an accurate and efficient intrusion detection system.

**Convolutional Neural Networks (CNNs)** are deep learning models designed for image recognition and processing. In CNNs, convolutional layers apply filters to input data, enabling the network to automatically and adaptively learn hierarchical representations. For this project, CNN is chosen due to its effectiveness in capturing spatial dependencies within IoT network traffic. The convolutional layers can identify patterns in the traffic data, making CNN well-suited for detecting anomalies and classifying diverse IoT malware types, contributing to the overall robustness and accuracy of the proposed multitask classification model.

The **CNN+LSTM** model, a hybrid architecture, combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. In this project, CNN excels at capturing spatial dependencies in IoT network traffic, while LSTM focuses on understanding temporal patterns. The integration of both models allows for a comprehensive analysis of the data, leveraging CNN for feature extraction and LSTM for sequence learning. This synergy proves effective for the project's objective of IoT malware detection and classification, as it enables the model to capture both spatial and temporal nuances in the intricate patterns of network traffic, enhancing the accuracy and adaptability of the system.

#### 4. EXPERIMENTAL RESULTS

**Accuracy:** The accuracy of a test is its ability to differentiate the patient and healthy cases correctly. To estimate the accuracy of a test, we should calculate the

proportion of true positive and true negative in all evaluated cases. Mathematically, this can be stated as:

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

**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:

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

**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.

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

**F1-Score:** F1 score is a machine learning evaluation metric that measures a model's accuracy. It combines the precision and recall scores of a model. The accuracy metric computes how many times a model made a correct prediction across the entire dataset.

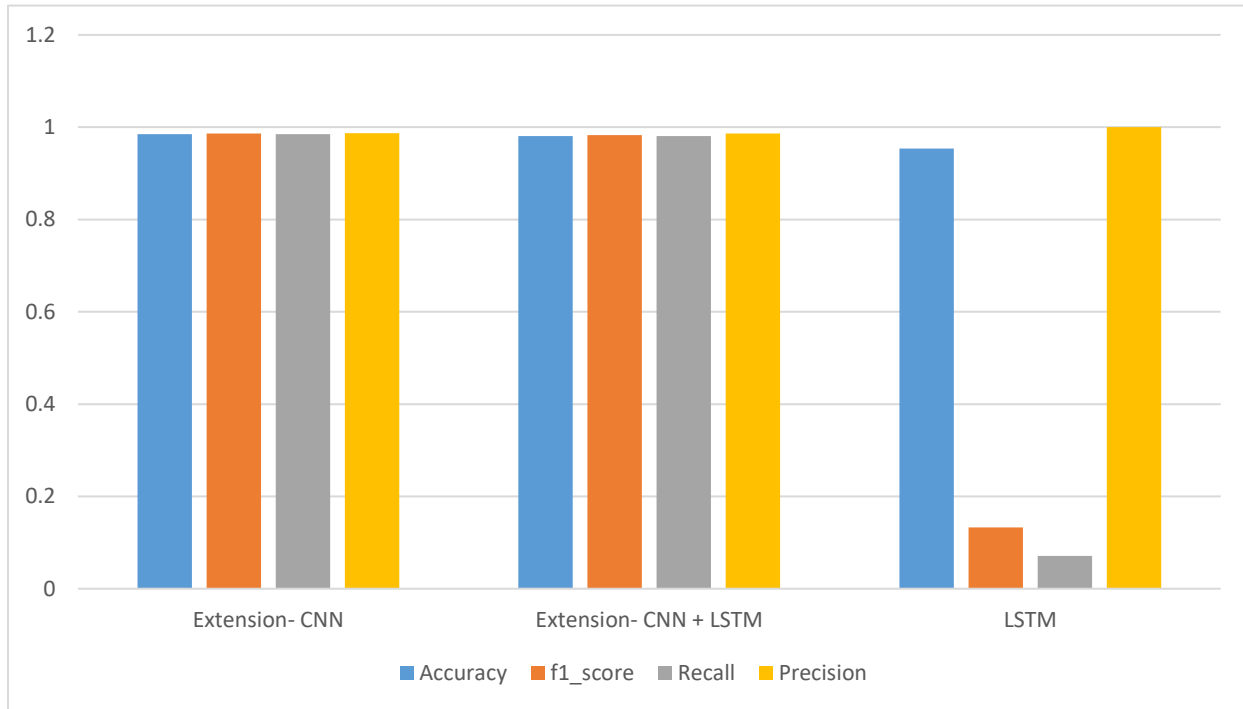
$$F1 \text{ Score} = 2 * \frac{\text{Recall} * \text{Precision}}{\text{Recall} + \text{Precision}} * 100 \quad (1)$$

**Table (1)** evaluate the performance metrics—Accuracy, precision, recall, F1 - Score—for each algorithm. Across all metrics, the CNN consistently outperforms all other algorithms. The tables also offer a comparative analysis of the metrics for the other algorithms.

*Table.1* Performance Evaluation Table

ML Model	Accuracy	f1 score	Recall	Precision
Extension- CNN	<b>0.985</b>	<b>0.986</b>	<b>0.985</b>	<b>0.987</b>
Extension- CNN + LSTM	0.981	0.983	0.981	0.986
LSTM	0.954	0.133	0.071	1.000

**Graph.1** Comparison Graph 1 Performance Evaluation Table



Accuracy is represented in blue, precision in yellow, recall in grey and F1 - Score in orange in **Graph (1)**. In comparison to the other models, the CNN shows superior performance across all metrics, achieving the highest values. The graphs above visually illustrate these findings.

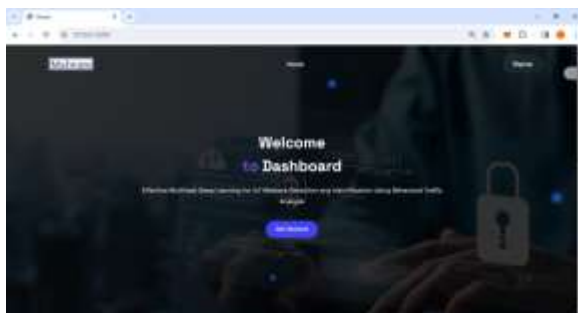


Fig 3 Home page

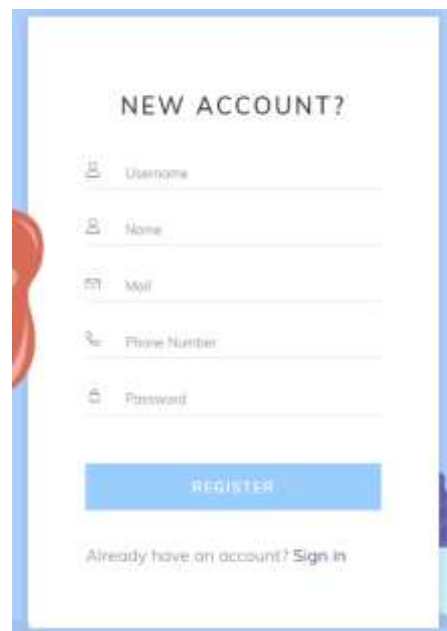


Fig 4 Signin page

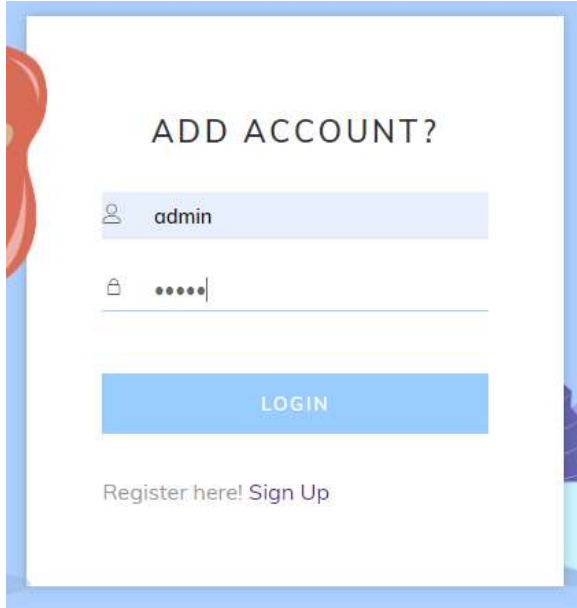
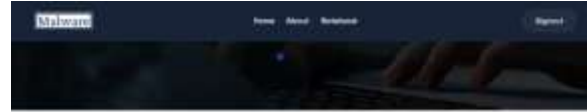


Fig 5 Login page

L4_SRC_PORT	67442
L4_DST_PORT	16600
PROTOCOL	25
L7_PROTO	0
IN_BYTES	108
OUT_BYTES	108
IN_PKTS	0
OUT_PKTS	0
TCP_FLAGS	0
FLOW_DURATION_MILLISECONDS	0
<input type="button" value="Predict"/>	

Fig 6 User input



Result: **There is No Attack Detected and Its Normal**

Fig 7 Predict result for given input

## 5. CONCLUSION

The project successfully addressed the complexity of IoT security, showcasing the efficacy of multitask LSTM-based model in detecting evolving malware threats. By incorporating dataset heterogeneity, the models demonstrated adaptability to various IoT scenarios, ensuring robust intrusion detection across a spectrum of devices and cyber-attacks. [52,53] Leveraging LSTM networks facilitated a leap forward in analyzing time-series data, enhancing the model's ability to grasp nuanced patterns in IoT network traffic. Bridging the gap between theory and practice, the project provided a tangible solution with user-friendly Flask front-end, empowering users to interact with and assess the model's predictions. The incorporation of Flask and SQLite facilitates a user-friendly interface, making the model accessible to a broader audience. The front-end design allows for user testing, input validation, and seamless model predictions, enhancing practical usability. Other models incorporating CNN and CNN+LSTM models significantly bolstered IoT security. Both models excelled, with CNN exhibiting a slight performance edge. This nuanced advantage informed the strategic deployment of the CNN model, underscoring its efficacy in fortifying the system against diverse and evolving IoT malware threats.

## 6. FUTURE SCOPE



Future enhancements could involve refining the CNN, LSTM, and CNN+LSTM models by incorporating advanced deep learning architectures. This could include exploring newer neural network structures or optimization techniques to further enhance the accuracy and adaptability of the models. Exploring the integration of edge computing techniques implies leveraging decentralized processing capabilities. This can optimize real-time data processing and decision-making, reducing latency and enhancing overall system efficiency by distributing computational tasks closer to the IoT devices [2]. Implementing dynamic threat intelligence feeds involves continuously updating the system with real-time information about emerging IoT malware threats. This ensures that the system can adapt and respond promptly, providing continuous protection against evolving security challenges in the IoT landscape. [12] Adapting the model to accommodate a broader range of IoT devices and communication protocols aims to enhance its versatility. By accommodating diverse IoT ecosystems, the model can offer more robust security measures, ensuring effective protection against a wide array of potential threats in different IoT scenarios.

## 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. Booiij, 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. Tavallace, 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/botsnifferdetectingbotnetcommandandcontrolchannelinnetworktraffic/>
- [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. Uhlir, 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/>