International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

Review Paper on Autonomous Detection of IoT Botnet Attacks using Deep Learning Technique

Raja Ram
M. Tech. Scholar
Department of Computer Science and Engineering
Oriental Institute of Science & Technology, Bhopal
Prof. Sanjay Pal
Assistant Professor
Department of Computer Science and Engineering
Oriental Institute of Science & Technology, Bhopal

Abstract

The rapid proliferation of Internet of Things (IoT) devices has significantly increased network connectivity while simultaneously exposing critical security vulnerabilities. Due to weak authentication mechanisms, limited computational resources, and large-scale deployment, IoT devices have become prime targets for botnet attacks such as Mirai, Bashlite, and Mozi. These botnets can compromise thousands of devices and launch severe cyberattacks, including Distributed Denial of Service (DDoS), data leakage, and service disruption. Traditional intrusion detection systems based on signatures and rule-based techniques are often ineffective against evolving and zero-day IoT botnet threats. Consequently, deep learning (DL) techniques have emerged as a powerful solution for autonomous IoT botnet detection.

This review paper presents a comprehensive analysis of deep learning-based approaches for the autonomous detection of IoT botnet attacks. It examines widely used DL models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), autoencoders, and hybrid CNN–LSTM architectures. The paper discusses how these models automatically learn complex spatial and temporal patterns from IoT network traffic, eliminating the need for manual feature engineering. Additionally, commonly used benchmark datasets, evaluation metrics, and performance comparisons with traditional machine learning techniques are reviewed.

The study also highlights key challenges, including computational complexity, scalability, dataset generalization, and real-time deployment in resource-constrained IoT environments.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

Finally, future research directions such as lightweight models, online learning, explainable AI, and edge-based deployment are outlined. This review provides valuable insights for researchers and practitioners aiming to develop robust, intelligent, and autonomous IoT botnet detection systems.

Keywords: - Internet of Things (IoT), IoT Botnet Attacks, Deep Learning, Autonomous Intrusion Detection, Convolutional Neural Network (CNN), LSTM, Network Traffic Analysis, Cybersecurity

1. INTRODUCTION

The Internet of Things (IoT) has revolutionized modern digital infrastructure by enabling seamless connectivity among billions of smart devices, including sensors, actuators, smart appliances, medical equipment, and industrial control systems. These devices are increasingly deployed across diverse domains such as smart cities, healthcare, agriculture, transportation, and industrial automation. While IoT technology enhances operational efficiency and real-time data-driven decision-making, it also introduces significant security challenges. Most IoT devices are resource-constrained, lack robust security mechanisms, and are often deployed with default credentials or outdated firmware, making them highly vulnerable to cyberattacks [1, 2].

Among the various security threats, IoT botnet attacks have emerged as one of the most severe and disruptive forms of cybercrime. Botnets such as Mirai, Bashlite, Mozi, and Hajime exploit compromised IoT devices to form large-scale malicious networks capable of launching Distributed Denial of Service (DDoS) attacks, malware propagation, unauthorized access, and data exfiltration. These attacks can disrupt critical services, cause substantial financial losses, and compromise user privacy. The increasing sophistication and rapid evolution of botnet strategies make early and accurate detection extremely challenging using conventional security solutions [3].

Traditional intrusion detection systems (IDS) primarily rely on signature-based or rule-based detection techniques. While these methods are effective in identifying known attack patterns, they fail to detect zero-day attacks and adaptive botnet behaviors. Additionally, manual feature engineering and static rule sets limit their scalability and effectiveness in dynamic IoT environments characterized by heterogeneous devices and high-volume network traffic. As a result, there is a growing need for intelligent and autonomous security mechanisms capable of adapting to evolving threats with minimal human intervention [4].

In recent years, deep learning (DL) techniques have gained significant attention in the field of IoT security due to their powerful representation learning capabilities. Unlike traditional machine learning approaches, DL models can automatically extract high-level and discriminative features directly from raw or minimally processed network traffic data. Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM) networks, autoencoders, and hybrid architectures have been widely explored for IoT botnet detection. CNNs are particularly effective in learning spatial correlations among traffic features, while LSTM and RNN models capture temporal dependencies in sequential data. Hybrid models combine these strengths to improve detection accuracy and robustness [5, 6].

Despite the promising performance of deep learning-based intrusion detection systems, several challenges remain. High computational complexity, large training data requirements, limited generalization across different datasets, and deployment constraints in resource-limited IoT and edge environments hinder practical implementation. Moreover, most existing solutions focus on offline detection and lack autonomous adaptation to emerging attack patterns in real time.

This review paper provides a comprehensive analysis of deep learning techniques for the autonomous detection of IoT botnet attacks. It systematically examines existing DL-based approaches, commonly used datasets, evaluation metrics, and performance comparisons. Furthermore, it identifies key research challenges and gaps, and discusses future directions toward developing scalable, lightweight, and adaptive deep learning-based security frameworks for protecting large-scale IoT ecosystems [7, 8].

2. LITERATURE REVIEW

S. I. Popoola et al., [1] Deep learning (DL) is a productive technique for botnet assault recognition. Nonetheless, the volume of organization traffic information and memory space required is generally huge. It is, hence, exceptionally difficult to execute the DL technique in memory-compelled Web of-Things (IoT) gadgets. In this article, we decrease the component dimensionality of huge scope IoT network traffic information utilizing the encoding period of long transient memory autoencoder (LAE). To group network traffic tests accurately, we dissect the drawn out between related changes in the low-layered highlight set created byLAE utilizing deep bidirectional long transient memory (BLSTM). Broad tests are performed with the BoT-IoT informational index to approve the adequacy of the proposed half and half DL

strategy. Results show that LAE altogether decreased the memory space expected for huge scope network traffic information capacity by 91.89%, and it beat cutting edge include dimensionality decrease strategies by 18.92-27.03%. Regardless of the huge decrease in include size, the deep BLSTM model shows power against model underfitting and overfitting. It additionally accomplishes great speculation capacity in parallel and multiclass order situations.

S. I. Popoola et al., [2] Deep Learning (DL) has been generally proposed for botnet assault discovery in Web of Things (IoT) organizations. Be that as it may, the customary Unified DL (CDL) strategy can't be utilized to recognize beforehand obscure (zero-day) botnet assault without breaking the information protection freedoms of the clients. In this work, we propose United Deep Learning (FDL) strategy for zero-day botnet assault discovery to keep away from information security spillage in IoT edge gadgets. In this strategy, an ideal Deep Brain Organization (DNN) design is utilized for network traffic characterization. A model boundary server remotely facilitates the autonomous preparation of the DNN models in different IoT edge gadgets, while Unified Averaging (Fed Avg) calculation is utilized to total nearby model updates. A worldwide DNN model is delivered after various correspondence adjusts between the model boundary server and the IoT edge gadgets. Zero-day botnet assault situations in IoT edge gadgets is recreated with the Bot-IoT and N-BaIoT informational collections. Analyze results show that FDL model: (a) distinguishes zero-day botnet assaults with high order execution; (b) ensures information protection and security; (c) has low correspondence upward (d) requires low memory space for the capacity of preparing information; and (e) has low organization idleness. Subsequently, FDL technique beat CDL, Confined DL, and Circulated DL strategies in this application situation.

B. H. Schwengber et al., [3] the organizations of contaminated gadgets (a.k.a., botnets) compromise network security because of their dynamic nature and backing to various assaults (e.g., Circulated Forswearing of Administrations and individual information burglary). Identifying botnets is a difficult undertaking on the grounds that the tainted gadgets (bots) are various, broadly and topographically spread. Huge consideration has been given to work on the productivity, vigor and versatility of organization security draws near. Nonetheless, in the writing, botnet identification methods as a rule overlook quick changes in measurable information appropriation, performing over static windows, for example fixed timespans or fixed amount of streams. Changes in factual information dispersion are known as idea floats

and they make the grouping models outdated. Moreover, those works utilizing approaches mindful of idea float utilize managed AI, which is slow, exorbitant, and inclined to blunder. Accordingly, this article presents TRUSTED, a framework for on the web and solo botnet identification mindful of idea floats. Not at all like different works, the Believed framework further develops the learning system for botnet discovery, applying idea float in an on the web and unaided grouping. Assessments involve disconnected and online situations. Results show that the Believed framework recognizes botnets utilizing idea float distinguishing proof, coming to 87% to 95% exactness, accuracy, review, and F1-scores.

F. Hussain et al., [4] the botnet assault is a multi-stage and the most pervasive digital assault in the Web of Things (IoT) climate that starts with checking action and finishes at the circulated disavowal of administration (DDoS) assault. The current investigations generally center around recognizing botnet assaults after the IoT gadgets get compromised, and begin playing out the DDoS assault. Additionally, the presentation of the vast majority of the current AI based botnet discovery models is restricted to a particular dataset on which they are prepared. As a result, these arrangements don't perform well on other datasets because of the variety of assault designs. Along these lines, in this work, we first produce a nonexclusive checking and DDoS assault dataset by creating 33 kinds of output and 60 sorts of DDoS assaults. Furthermore, we to some degree incorporated the sweep and DDoS assault tests from three openly accessible datasets for most extreme assault inclusion to all the more likelytrain the AI calculations. Subsequently, we propose a two-overlap AI way to deal with forestall and identify IoT botnet assaults. In the principal crease, we prepared a cutting edge deep learning model, i.e., ResNet-18 to recognize the checking action in the untimely assault stage to forestall IoT botnet assaults. While, in the subsequent crease, we prepared another ResNet-18 model for DDoS assault recognizable proof to distinguish IoT botnet assaults. Generally, the proposed two-overlay approach shows 98.89% exactness, 99.01% accuracy, 98.74% review, and 98.87% f1-score to forestall and distinguish IoT botnet assaults. To exhibit the adequacy of the proposed two-overlap approach, we prepared three other ResNet- 18 models north of three distinct datasets for identifying check and DDoS assaults and contrasted their presentation and the proposed two-crease approach. The exploratory outcomes demonstrate that the proposed two-crease approach can proficiently forestall and identify botnet assaults when contrasted with other prepared models.

R. Li et al., [5] Web of Things (IoT) has entered a phase of quick turn of events and expanding organization. In the interim, these low-power gadgets regularly can't uphold complex security instruments and consequently are profoundly vulnerable to malware. This work proposes ADRIoT, a peculiarity identification system for IoT networks which use edge registering to reveal expected dangers. An edge is engaged with an irregularity recognition module, which comprises of a traffic captor, a traffic preprocessor and an assortment of peculiarity locators committed to each sort of gadget. Every identifier is developed by a LSTM autoencoder in an unaided way that requires no marked assault information and can deal with arising zero-day assaults. At the point when a gadget associates with the edge, the edge will get the relating locator from the cloud and execute it locally. Another issue is the asset imperative of a solitary edge gadget like a home switch ruins the arrangement of such an identification module. To relieve this issue, we plan a multi-edge cooperative instrument that incorporates the asset of numerous edges in a nearby organization to expand the general burden limit.

B. H. Schwengber et al., [6] the organizations of tainted gadgets (a.k.a., botnets) compromise network security because of their dynamic nature and backing to various assaults (e.g., Circulated Forswearing of Administrations and individual information robbery). Recognizing botnets is a difficult undertaking on the grounds that the tainted gadgets (bots) are various, generally and topographically spread. Huge consideration has been given to work on the proficiency, vigor and versatility of organization security draws near. Be that as itmay, in the writing, botnet recognition strategies typically overlook quick changes in measurable information dissemination, performing over static windows, for example fixed time frames or fixed amount of streams. Changes in measurable information dispersion are known as idea floats and they make the grouping models outdated. Besides, those works utilizing approaches mindful of idea float utilize regulated AI, which is slow, expensive, and inclined to mistake. Subsequently, this article presents TRUSTED, a framework for on the web and solo botnet discovery mindful of idea floats. Not at all like different works, the Believed framework further develops the learning system for botnet location, applying idea float in an on the web and unaided grouping. Assessments include disconnected and online situations. Results show that the Believed framework distinguishes botnets utilizing idea float recognizable proof, coming to 87% to 95% exactness, accuracy, review, and F1-scores.

A. Alharbi et al., [7] Distinguishing botnet dangers has been a continuous exploration try. AI (ML) procedures have been broadly utilized for botnet location with stream based highlights. The excellent difficulties with stream based highlights are that they have high computational upward and don't completely catch network correspondence designs. As of late, chart based ML has seen a sensational expansion in consideration. In correspondence organizations, diagram information offers bits of knowledge data about correspondence designs between has. In this work, we propose a chart based ML model for botnet recognition that first considers the meaning of diagram highlights prior to fostering a summed up model for distinguishing botnets in view of the chose significant elements. We investigate different capabilities chose utilizing five channel based highlight assessment measures got from different speculations like consistency, connection, and data. Two heterogeneous botnet datasets, CTU-13 and IoT-23, were utilized to assess the adequacy of the proposed chart based botnet identification with a few regulated ML calculations. Analyze results show that utilizing highlights decreases preparing time and model intricacy.

S. Qureshi et al., [8] the amazing development of refined steadily advancing digital dangers and assaults tosses the whole Web of-Things (IoT) framework into tumult. As the IoT has a place with the foundation of interconnected gadgets, it brings along critical security challenges. Digital danger investigation is an increase of an organization security framework that basically underscores on discovery and avoidance of complex organization based dangers and assaults. Besides, it requires the security of organization by examination and characterization of pernicious exercises. In this review, we propose a DL-empowered malware recognition plot utilizing a half breed method in light of the blend of a Deep Brain Network(DNN) and Long Transient Memory(LSTM) for the effective ID of multi-class malware families in IoT framework. The proposed plot uses most recent 2018 dataset named as N_BaIoT. Moreover, our proposed conspire is assessed utilizing standard execution measurements, for example, exactness, review, accuracy, F1-score, etc. The DL-based malware discovery framework accomplishes 99.96% location precision for IoT based dangers. At long last, we likewise contrast our proposed work and other strong and cutting edge discovery plans.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

3. INTERNET OF THINGS (IOT)

The Web of things (IoT) depicts the organization of actual items that are implanted with sensors, programming, and different advances to associate and trading information with different gadgets and frameworks over the Web.

Things have advanced because of the union of different innovations, ongoing investigation, AI, universal registering, product sensors, and inserted frameworks. Customary fields of installed frameworks, remote sensor organizations, control frameworks, robotization (counting home and building computerization), and others all add to empowering the Web of things. In the shopper market, IoT innovation is generally inseparable from items relating to the idea of the "shrewd home", including gadgets and machines (like lighting installations, indoor regulators, home security frameworks and cameras, and other home apparatuses) that help one or more normal environments, and can be controlled through gadgets related with that biological system, for example, cell phones and savvy speakers. The IoT can likewise be utilized in medical care frameworks. There are various not kidding worries about risks in the development of the IoT, particularly in the space of protection and security, and therefore industry and legislative moves to address these worries have started including the advancement of worldwide norms. IoT framework engineering, in its shortsighted view, comprises of three levels: Level 1: Gadgets, Level 2: the Edge Door, and Level 3: the Cloud. Gadgets incorporate arranged things, for example, the sensors and actuators found in IoT hardware, especially those that utilization conventions like Modbus, Bluetooth, Zigbee, or exclusive conventions, to associate with an Edge Passage. The Edge Passage layer comprises of sensor information total frameworks called Edge Entryways that give usefulness, for example, pre-handling of the information, tying down network to cloud, utilizing frameworks like WebSockets, the occasion center, and, even now and again, edge investigation or mist figuring. The Web of things requires colossal adaptability in the organization space to deal with the flood of gadgets. IETF 6LoWPAN would be utilized to interface gadgets to IP organizations. With billions of gadgets being added to the Web space, IPv6 will assume a significant part in taking care of the organization layer adaptability. IETF's Obliged Application Convention, ZeroMQ, and MQTT would give lightweight information transport.

Haze registering is a reasonable choice to forestall such an enormous eruption of information move through the Web. The edge gadgets' calculation ability to break down and deal with

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

information is incredibly restricted. Restricted handling power is a vital trait of IoT gadgets as their motivation is to supply information about actual articles while staying independent. Weighty handling necessities utilize more battery power hurting IoT's capacity to work. Adaptability is simple on the grounds that IoT gadgets just inventory information through the web to a server with adequate handling power.

4. BOT-IOT ATTACK

The powerful component determination and exact Bot-IoT assaults distinguishing proof in IoT network climate a new create dataset is utilized.

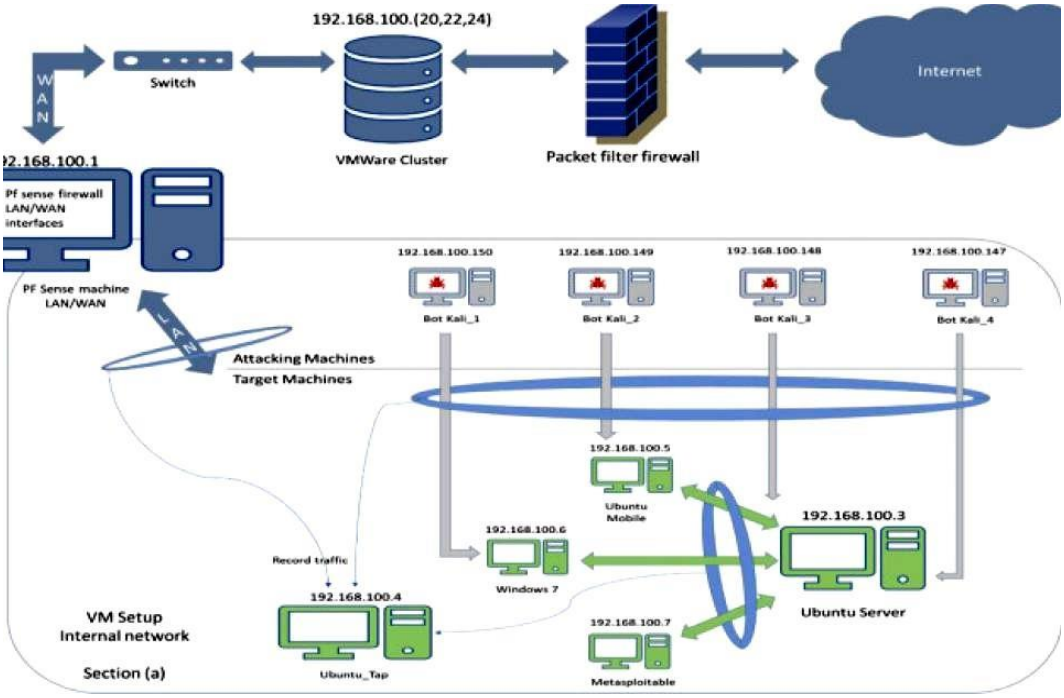

Figure 1: Bot-IOT

The dataset remembers for the Web of Things, and typical traffic streams as well as a few various digital assaults traffic streams of botnets assaults. To follow the exact traffic and create powerful dataset, the practical proving ground is utilized for the improvement of this dataset with successful data highlights. Additionally, to improve AI model execution and compelling forecast model, more elements were extricated and added with separated highlights set. Nonetheless, for better execution results, the separated highlights are named, for example, assault stream, classifications, and subcategories.

These days, the Web of Things (IoT) innovation is growing up more step by step, and in consistently, various gadgets are getting associated with this innovation. By utilizing this innovation, day to day existence turns out to be more helpful and efficient. For example, at first, IoT innovation was restricted to little workplaces and homes, however these days, IoT innovation incorporated into businesses for greater dependability and saving time. Nonetheless, IoT innovation is turning into a fundamental piece of our everyday existence.

5. CONCLUSION

The rapid expansion of the Internet of Things has significantly intensified security challenges, particularly due to the increasing prevalence of IoT botnet attacks that exploit vulnerable and resource-constrained devices. This review paper examined the state-of-the-art deep learning techniques employed for the autonomous detection of IoT botnet attacks, highlighting their effectiveness in overcoming the limitations of traditional intrusion detection systems. Deep learning models such as Convolutional Neural Networks, Recurrent Neural Networks, Long Short-Term Memory networks, autoencoders, and hybrid architectures have demonstrated strong capabilities in automatically learning complex spatial and temporal patterns from IoT network traffic, enabling accurate and timely detection of malicious activities.

The review emphasized that CNN-based and hybrid deep learning models generally outperform conventional machine learning approaches in terms of detection accuracy, adaptability, and robustness against evolving botnet behaviors. However, despite these advantages, several challenges remain, including high computational complexity, limited generalization across diverse datasets, class imbalance issues, and difficulties in deploying deep learning models in real-time, resource-constrained IoT and edge environments. The lack of explainability and continuous learning mechanisms also restricts the practical adoption of these models in critical security applications.

In conclusion, deep learning-based autonomous intrusion detection systems represent a promising direction for securing IoT ecosystems against sophisticated botnet attacks. Future research should focus on developing lightweight and scalable models, integrating online and adaptive learning strategies, and incorporating explainable artificial intelligence to enhance trust and transparency. Addressing these challenges will contribute to more resilient, efficient, and intelligent IoT security frameworks capable of protecting next-generation interconnected systems.

REFERENCES

1. S. I. Popoola, B. Adebisi, M. Hammoudeh, G. Gui and H. Gacanin, "Hybrid Deep Learning for Botnet Attack Detection in the Internet-of-Things Networks," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4944-4956, 15 March15, 2021, doi: 10.1109/JIOT.2020.3034156.
2. S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh and O. Jogunola, "Federated Deep Learning for Zero-Day Botnet Attack Detection in IoT Edge Devices," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3100755.
3. B. H. Schwengber, A. Vergütz, N. G. Prates and M. Nogueira, "Learning from Network Data Changes for Unsupervised Botnet Detection," in IEEE Transactions on Network and Service Management, doi: 10.1109/TNSM.2021.3109076.
4. F. Hussain et al., "A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks," in IEEE Access, vol. 9, pp. 163412-163430, 2021, doi: 10.1109/ACCESS.2021.3131014.
5. R. Li, Q. Li, J. Zhou and Y. Jiang, "ADRIoT: An Edge-assisted Anomaly Detection Framework against IoT-based Network Attacks," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3122148.
6. B. H. Schwengber, A. Vergütz, N. G. Prates and M. Nogueira, "Learning from Network Data Changes for Unsupervised Botnet Detection," in IEEE Transactions on Network and Service Management, doi: 10.1109/TNSM.2021.3109076.
7. A. Alharbi and K. Alsubhi, "Botnet Detection Approach Using Graph-Based Machine Learning," in IEEE Access, vol. 9, pp. 99166-99180, 2021, doi: 10.1109/ACCESS.2021.3094183.
8. S. Qureshi et al., "A Hybrid DL-Based Detection Mechanism for Cyber Threats in Secure Networks," in IEEE Access, vol. 9, pp. 73938-73947, 2021, doi: 10.1109/ACCESS.2021.3081069.
9. W. N. H. Ibrahim et al., "Multilayer Framework for Botnet Detection Using Machine Learning Algorithms," in IEEE Access, vol. 9, pp. 48753-48768, 2021, doi: 10.1109/ACCESS.2021.3060778.

10. T. -L. Wan et al., "Efficient Detection and Classification of Internet-of-Things Malware Based on Byte Sequences from Executable Files," in IEEE Open Journal of the Computer Society, vol. 1, pp. 262-275, 2020, doi: 10.1109/OJCS.2020.3033974.
11. L. Vu, V. L. Cao, Q. U. Nguyen, D. N. Nguyen, D. T. Hoang and E. Dutkiewicz, "Learning Latent Representation for IoT Anomaly Detection," in IEEE Transactions on Cybernetics, doi: 10.1109/TCYB.2020.3013416.
12. S. M. Sajjad, M. Yousaf, H. Afzal and M. R. Mufti, "eMUD: Enhanced Manufacturer Usage Description for IoT Botnets Prevention on Home WiFi Routers," in IEEE Access, vol. 8, pp. 164200-164213, 2020, doi: 10.1109/ACCESS.2020.3022272.
13. A. Blaise, M. Bouet, V. Conan and S. Secci, "Botnet Fingerprinting: A Frequency Distributions Scheme for Lightweight Bot Detection," in IEEE Transactions on Network and Service Management, vol. 17, no. 3, pp. 1701-1714, Sept. 2020, doi: 10.1109/TNSM.2020.2996502.
14. Y. Jia, F. Zhong, A. Alrawais, B. Gong and X. Cheng, "FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9552-9562, Oct. 2020, doi: 10.1109/JIOT.2020.2993782.
15. L. Silva, L. Utimura, K. Costa, M. Silva and S. Prado, "Study on Machine Learning Techniques for Botnet Detection," in IEEE Latin America Transactions, vol. 18, no. 05, pp. 881-888, May 2020, doi: 10.1109/TLA.2020.9082916.