International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 13, Issue 8, August 2024)

Review of Botnet Attack Prediction in the Internet of Things Network Application

[1]Kirti Rawat, [2]Prof. Rupali Chaure, [3]Mr. Arun Jhapate, [4]Dr. Ritu Shivastava

[1]M.Tech Scholar, [2&3]Professor, [4]Head of department
Department of Computer Science & Engineering
Sagar Institute of Research & Technology, Bhopal, India

***Abstract*— The rapid proliferation of Internet of Things (IoT) devices has transformed various industries, from healthcare to smart cities, by enabling unprecedented connectivity and automation. However, this connectivity has also made IoT networks attractive targets for cybercriminals, particularly through botnet attacks. These attacks, where a network of compromised devices is used to execute malicious activities, pose significant threats to the security, privacy, and functionality of IoT systems. This review examines the current landscape of botnet attack prediction within IoT networks, highlighting the challenges posed by the unique characteristics of IoT environments, such as resource constraints, heterogeneous devices, and the need for real-time processing. We discuss various machine learning and deep learning approaches that have been proposed for predicting botnet attacks, emphasizing their strengths, limitations, and the trade-offs involved.**

***Keywords*— Bot-Net, AI, IOT, Cyber, Security, Privacy.**

I. INTRODUCTION

The Internet of Things (IoT) represents a revolutionary shift in the digital landscape, characterized by the interconnection of billions of devices that can communicate and interact with each other and their environment. This paradigm has led to the development of smart homes, intelligent transportation systems, healthcare monitoring solutions, and many other applications that enhance efficiency, convenience, and quality of life. However, the widespread adoption of IoT technology has also introduced significant cybersecurity challenges, with botnet attacks emerging as one of the most critical threats.

Figure 1: Cyber security

Botnets are networks of devices that have been compromised and are under the control of malicious actors, often without the knowledge of the device owners. These networks can be used to launch distributed denial-of-service (DDoS) attacks, steal sensitive information, or spread malware, among other malicious activities. The Mirai botnet, which harnessed IoT devices to launch one of the largest DDoS attacks in history, is a stark example of the potential damage that such threats can cause. As IoT devices typically have limited processing power, memory, and energy resources, traditional cybersecurity measures are often inadequate, making these devices particularly vulnerable to botnet infiltration.

Predicting botnet attacks in IoT networks is a complex and challenging task due to the dynamic nature of these networks, the diversity of devices involved, and the evolving tactics of cybercriminals. Machine learning (ML) and deep learning (DL) techniques have shown promise in enhancing botnet detection and prediction, offering the ability to analyze large volumes of data and identify patterns that may indicate an impending attack. These techniques can be used to develop predictive models that can detect anomalies, classify traffic, and predict the likelihood of a device being compromised by a botnet.

In recent years, researchers have explored various approaches to improving botnet attack prediction, including the use of ensemble learning, neural networks, and hybrid models that combine multiple algorithms. These approaches aim to address the unique challenges posed by IoT networks, such as the need for lightweight solutions that can operate on resource-constrained devices, the requirement for real-time detection and prediction, and the need for scalability to handle the vast number of devices in an IoT network.

Moreover, emerging technologies such as blockchain and federated learning offer new opportunities for enhancing botnet prediction in IoT networks. Blockchain can provide a decentralized and tamper-resistant ledger for recording and verifying network activity, while federated learning allows for collaborative model training across multiple devices without the need to share sensitive data. These technologies have the potential to address some of the limitations of current botnet prediction methods and offer more robust and scalable solutions.

Smart Cars
Smart Airports
Smart Cities
IoT
Baseline security IoT
Smart Hospitals
Industry 4.0

Figure 2: IOT smart infrastructure security

This review provides a comprehensive analysis of the state-of-the-art in botnet attack prediction for IoT networks. It examines the various ML and DL techniques that have been proposed, evaluates their effectiveness, and discusses the trade-offs involved in their implementation. Additionally, the review identifies key research gaps and outlines future directions for advancing botnet attack prediction in the rapidly evolving landscape of IoT networks. Through this analysis, the paper aims to contribute to the development of more effective and resilient cybersecurity measures that can protect IoT networks from the growing threat of botnet attacks.

II. LITERATURE SURVEY

M. W. Nadeem et al.,[1] Software-Defined Networking (SDN) is an emerging architecture that enables flexible and easy management and communication of large-scale networks. It offers programmable and centralized interfaces for making complex network decisions dynamically and seamlessly. However, SDN provides opportunities for businesses and individuals to build network applications based on their demands and improve their services. In contrast, it started to face a new array of security and privacy challenges and simultaneously introduced the threats of a single point of failure. Usually, attackers launch malicious attacks such as botnets and Distributed Denial of Service (DDoS) to the controller through OpenFlow switches. Deep learning (DL)-based security applications are trending, effectively detecting and mitigating potential threats with fast response.

S. I. Popoola et al.,[2] presented framework is assessed on the notable benchmark informational index NSL-KDD for examination with other existing strategies. The exploratory outcomes exhibit that contrasted and existing beginning of-the-craftsmanship strategies, our framework has better recognition execution for various kinds of cyberattacks. What's more, the low-recurrence network assault types have higher arrangement precision and a lower misleading discovery rate.

M. A. Ferrag et al.,[3] present At long last, we give an exploratory examination of unified profound learning with three profound learning draws near, in particular, Intermittent Brain Organization (RNN), Convolutional Brain Organization (CNN), and Profound Brain Organization (DNN). For every profound learning model, we concentrate on the presentation of brought together and unified learning under three new genuine IoT traffic datasets, specifically, the Bot-IoT dataset, the MQTTset dataset, and the TON_IoT dataset. The objective of this article is to give significant data on combined profound learning approaches with arising innovations for network protection. Furthermore, it exhibits that combined profound learning approaches beat the work of art/incorporated forms of AI (non-unified learning) in guaranteeing the protection of IoT gadget information and give the higher exactness in distinguishing assaults.

G. Yoo et al.,[4] In doing as such, we utilize an autoencoder-based perception move conspire for methodicallly preparing a bunch of adaptable control approaches and a collected model-based learning plan for information effectively preparing an undeniable level orchestrator in an order. Our examinations show that rocorl is hearty against different states of disseminated sensor information refreshes, contrasted and a few different models including a cutting edge POMDP technique.

G. Apruzzese et al.,[5] present a unique procedure for countering antagonistic annoyances focusing on interruption identification frameworks in view of arbitrary timberlands. As a reasonable application, we coordinate the proposed safeguard technique in a digital locator breaking down network traffic. The trial results on huge number of named network streams show that the new locator has a twofold worth: it beats cutting edge identifiers that are likely to ill-disposed assaults; it displays strong outcomes both in antagonistic and non-ill-disposed situations.

M. Saharkhizan et al.,[6] presents plan a methodology utilizing progressed profound figuring out how to distinguish digital assaults against IoT frameworks. In particular, our methodology incorporates a bunch of long transient memory (LSTM) modules into an outfit of locators. These modules are then combined utilizing a choice tree to show up at an accumulated result at the last stage. We assess the viability of our methodology utilizing a genuine informational index of Modbus network traffic and acquire an exactness pace of more than close to 100% in the discovery of digital assaults against IoT gadgets.

S. - K. Kim et al.,[7] The General Presentation (Over powered) as a recently proposed exhibition measure is the consolidated exhibition metric of different validation measures in this review. The exhibition of the proposed framework utilizing a disarray network has been assessed and it has accomplished up to 95% exactness by minimal information investigation. The Amang ECG (amgecg) tool compartment in MATLAB is applied to the mean square mistake (MSE) based upper-range control limit (UCL) which straightforwardly influences three verification execution measurements: the quantity of acknowledged examples, the precision and the Over powered. In light of this methodology, it is observed that the Over powered could be boosted by applying a UCL of 0.0028, which shows 61 acknowledged examples inside 70 examples and guarantees that the proposed validation framework accomplishes 95% precision.

A. Hassan et al.,[8] The proposed plot permits all members in the framework model to freely check the accuracy of the encoded information. Besides, a unidirectional intermediary re-encryption (UPRE) plot is utilized to decrease the high computational expenses alongside various information suppliers. The cloud server implants clamor in the scrambled information, permitting the examination to apply AI strategies and safeguard the security of information suppliers' data. The outcomes and analyses tests exhibit that the proposed plot can decrease computational expenses and correspondence overheads.

Y. Xin et al.,[9] With the advancement of the Web, digital assaults are changing quickly and the network safety circumstance isn't hopeful. This review report depicts key writing studies on AI (ML) and profound learning (DL) strategies for network examination of interruption location and gives a concise instructional exercise portrayal of every ML/DL technique. Works addressing every strategy were listed, read, and summed up in light of their worldly or warm relationships. Since information are so significant in ML/DL strategies, we depict a portion of the generally utilized network datasets utilized in ML/DL, examine the difficulties of utilizing ML/DL for online protection and give ideas to explore bearings.

N. R. Sabar et al.,[10] presents a clever hyper-heuristic structure for bi-objective enhancement that is autonomous of the issue space. This is whenever that a hyper-heuristic first has been produced for this issue. The proposed hyper-heuristic system comprises of a significant level technique and low-level heuristics. The undeniable level procedure utilizes the hunt execution to control the choice of which low-level heuristic ought to be utilized to produce another SVM arrangement. The low-level heuristics each utilization various guidelines to successfully investigate the SVM design search space. To address bi-objective advancement, the proposed system adaptively incorporates the qualities of decompositionand Paretobased ways to deal with rough the Pareto set of SVM designs.

Y. Wang et al.,[11] Misleading information infusion digital actual danger is a normal trustworthiness assault in current shrewd matrices. Nowadays, information scientific techniques have been utilized to alleviate misleading information infusion assaults (FDIAs), particularly when huge scope brilliant frameworks produce enormous measures of information. In this work, a clever information logical strategy is proposed to identify FDIAs in light of information driven worldview utilizing the edge setting calculation (MSA). The exhibition of the proposed strategy is shown through reenactment utilizing the six-transport power network in a wide region estimation framework climate, as well as exploratory informational collections. Two FDIA situations, playback assault and time assault, are examined. Exploratory outcomes are contrasted and the help vector machine (SVM) and counterfeit brain organization (ANN). The outcomes demonstrate that MSA yields better outcomes as far as identification precision than both the SVM and ANN when applied to FDIA discovery.

F. Wang et al.,[12] this work investigates the chance of allowing the specialist to gather expected objectives through activities over space with numerous items, utilizing the momentary award to allot credit spatially. A past strategy, consideration gated RL utilizes a multi-facet perceptron prepared with backpropagation, yet it is inclined to nearby minima ensnarement. We propose a quantized consideration gated part RL (QAGKRL) to stay away from the neighborhood minima transformation in spatial credit task and sparsify the organization geography. The test results show that the QAGKRL accomplishes higher effective rates and more steady execution, demonstrating its strong translating capacity for more modern BMI assignments as expected in clinical applications.

III. BOTNET ATTACK CHALLENGES

The unique characteristics of Internet of Things (IoT) networks present several challenges in the detection, prediction, and mitigation of botnet attacks. These challenges arise from the intrinsic nature of IoT devices, the scale and diversity of IoT ecosystems, and the sophistication of modern botnet strategies. Addressing these challenges is crucial for developing effective security measures that can safeguard IoT networks against botnet threats.

1. Resource Constraints

IoT devices are typically designed with minimal processing power, memory, and battery life to reduce costs and enhance energy efficiency. These resource constraints limit the ability of IoT devices to run complex security protocols and algorithms, making them vulnerable to botnet attacks. Implementing lightweight security solutions that do not compromise device performance is a significant challenge in botnet attack prevention and detection.

2. Heterogeneity of Devices

IoT networks consist of a vast array of devices with varying capabilities, communication protocols, and operating systems. This heterogeneity complicates the development of standardized security measures, as a solution effective for one type of device may not be suitable for another. The diverse nature of IoT devices also poses difficulties in creating universal models for botnet detection and prediction, requiring tailored approaches for different device types.

3. Scalability

The number of IoT devices is rapidly increasing, with estimates suggesting billions of devices will be connected to the internet in the coming years. This massive scale poses challenges for botnet detection systems, which must be capable of monitoring and analyzing data from a vast number of devices in real-time. Ensuring that botnet prediction methods can scale effectively without compromising accuracy or performance is a critical concern.

4. Dynamic Network Topologies

IoT networks are inherently dynamic, with devices frequently joining and leaving the network, and changing their roles and communication patterns. This dynamic nature complicates the process of establishing a baseline for normal network behavior, which is essential for detecting anomalies indicative of botnet activity. The ability to adapt to changing network topologies and maintain accurate prediction models in the face of such variability is a key challenge.

5. Sophistication of Botnet Attacks

Botnets have evolved significantly in recent years, with attackers employing advanced evasion techniques to bypass traditional security measures. These techniques include polymorphic malware that changes its signature to avoid detection, encryption of communication channels to hide malicious traffic, and the use of peer-to-peer (P2P) architectures that eliminate the need for a centralized command and control (C&C) server. The increasing sophistication of botnet attacks requires equally advanced detection and prediction methods that can identify and counteract these tactics.

6. Real-time Detection and Response

Given the potential for rapid and widespread damage, botnet attacks in IoT networks necessitate real-time detection and response capabilities. However, the resource limitations of IoT devices, coupled with the need to process large volumes of data in real-time, make it challenging to implement effective real-time security measures. Achieving a balance between detection accuracy, speed, and resource consumption is a significant hurdle in the fight against botnets.

IV. CONCLUSION

The growing prevalence of IoT networks has introduced significant challenges in defending against botnet attacks, which exploit the inherent vulnerabilities of connected devices. The complexity of these attacks is compounded by the resource constraints, heterogeneity, and dynamic nature of IoT environments, necessitating the development of advanced, scalable, and real-time prediction models. While machine learning and emerging technologies like blockchain and federated learning offer promising avenues for enhancing security, substantial research gaps remain, particularly in creating universally applicable solutions that balance effectiveness with resource efficiency. Addressing these challenges is crucial for safeguarding the future of IoT networks and ensuring their resilience against evolving cyber threats.

REFERENCES

1. M. W. Nadeem, H. G. Goh, Y. Aun and V. Ponnusamy, "Detecting and Mitigating Botnet Attacks in Software-Defined Networks Using Deep Learning Techniques," in IEEE Access, vol. 11, pp. 49153-49171, 2023.
2. 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.
3. M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke and L. Shu, "Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis," in IEEE Access, vol. 9, pp. 138509-138542, 2021, doi: 10.1109/ACCESS.2021.3118642.
4. G. Yoo, M. Yoo, I. Yeom and H. Woo, "rocorl: Transferable Reinforcement Learning-Based Robust Control for Cyber-Physical Systems With Limited Data Updates," in IEEE Access, vol. 8, pp. 225370-225383, 2020, doi: 10.1109/ACCESS.2020.3044945.

5. G. Apruzzese, M. Andreolini, M. Colajanni and M. Marchetti, "Hardening Random Forest Cyber Detectors Against Adversarial Attacks," in IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 4, no. 4, pp. 427-439, Aug. 2020, doi: 10.1109/TETCI.2019.2961157.
6. M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K. -K. R. Choo and R. M. Parizi, "An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8852-8859, Sept. 2020, doi: 10.1109/JIOT.2020.2996425.
7. S. -K. Kim, C. Y. Yeun and P. D. Yoo, "An Enhanced Machine Learning-Based Biometric Authentication System Using RR-Interval Framed Electrocardiograms," in IEEE Access, vol. 7, pp. 168669-168674, 2019, doi: 10.1109/ACCESS.2019.2954576.
8. A. Hassan, R. Hamza, H. Yan and P. Li, "An Efficient Outsourced Privacy Preserving Machine Learning Scheme With Public Verifiability," in IEEE Access, vol. 7, pp. 146322-146330, 2019, doi: 10.1109/ACCESS.2019.2946202.
9. Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," in IEEE Access, vol. 6, pp. 35365-35381, 2018, doi: 10.1109/ACCESS.2018.2836950.
10. N. R. Sabar, X. Yi and A. Song, "A Bi-objective Hyper-Heuristic Support Vector Machines for Big Data Cyber-Security," in IEEE Access, vol. 6, pp. 10421-10431, 2018, doi: 10.1109/ACCESS.2018.2801792.