iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XII **Month of publication:** December 2023

DOI: https://doi.org/10.22214/ijraset.2023.57668

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XII Dec 2023- Available at www.ijraset.com

An Encompassing Literature Review on Predicting Botnet Attacks in Web using Machine Learning Approaches

M V Varun[1], Yashila R[2], Gurudeep R[3], Yogitha S[4], Renuka Patil[5]
K.S Institute of Technology

Abstract: ***A botnet attack is the most widely found, multi-stage cyber-attack in the Internet of Things (IoT), jumping with a scanning exertion and leading to Distributed Denial of Service (DDoS) attack. Botnets are malware that use malicious programs to risk functionality and gain access to error-free computer systems. The current study focuses on performing a literature survey for detecting botnet attacks using Machine Learning (ML) approaches. In this perspective survey is done by extracting work from last decade.***

Keywords: botnet attack, ML, Literature survey

I. INTRODUCTION

The threats associated with the global Internet are changing significantly. Instead of focusing only on attacks that knock down infrastructure, they are now more focused on individuals and organizations. These concerning new attacks endanger multinational governments and corporations and also directly affects millions of people. A Botnet program detects spam, phishing attacks, peer-to- peer attacks and command- and- control attacks. A peer- to- peer attack is fulfilled by turning a botnet attack from one system to another within a peer- to- peer network, while a command- and- control attack is fulfilled by a botmaster attack on one server. Different transactions are changed with the systems in the network, and these bumps in the network act as slaves. This report provides an overview of ways for botnet discovery and identifies the ways to understand the datasets. To show the effectiveness of the proposed dual approach, we trained ResNet18 models on different datasets to describe scanning attacks and DDoS attacks, and compared their performance. Experimental results show that the proposed dual approach can efficiently help and describe botnet attacks compared to other trained models.

II. RELATED WORK

In recent years, there has been a surge in research efforts addressing the critical issue of IoT security, particularly in the context of botnet attacks. A study in 2023 (1) focuses on enhancing security against botnet attacks in IoT networks by employing dimensionality reduction techniques such as PCA and autoencoder on the Bot-IoT dataset, utilizing memory-efficient DL algorithms like LSTM and CNN. Another approach in the same year (2) proposes a hybrid model integrating k-means, rule-based systems, and decision trees for detecting botnet attacks in network traffic, achieving notable accuracy rates. In a novel statistical approach introduced in 2023 (3), time gap activity analysis is utilized to provide an overview of botnet datasets, determining optimal threshold values for effective separation of botnet, normal, and background activity. Addressing security challenges in Software-Defined Networking (SDN), a 2023 study (4) employs deep learning techniques for detecting and mitigating botnet attacks, achieving high detection rates for both normal flows and attacks. In the realm of IoT-enabled Automated Guided Vehicles (AGVs), a 2022 study (5) advocates for an intrusion prediction system to enhance network reliability and security against botnet attacks. A 2022 investigation (6) delves into machine learning-based IoT-BotNet attack detection, comparing various algorithms and highlighting the superiority of tree-based classifiers. Acknowledging the rising use of household IoT devices, a 2022 work (7) emphasizes the importance of AI-based botnet attack classification and detection, evaluating six ML and three DL models and implementing the top performer as an API for enhanced security. Moving to 2021, a comprehensive overview of machine learning for misuse-based network intrusion detection is presented (8), introducing a unified evaluation framework and showcasing the effectiveness of deep learning in real-time applications. An innovative intrusion detection method based on sequential information preserving log embedding algorithms and anomaly detection is proposed in 2021 (9), highlighting the limitations of pattern-matching-based methods. In 2020, a systematic literature review on IoT-based botnet attacks (10) provides a comprehensive overview of the state of the art in this field. The need for IoT-specific tools and methods is addressed in a 2020 framework called IoT-Flock (11), aiming to enhance security through context-aware solutions.

©IJRASET: All Rights are Reserved

Several studies in 2020 contribute to the efficiency of bot detection mechanisms. A lightweight bot detection method called BotFP (12) analyzes frequency distributions of protocol attributes, demonstrating scalability and accuracy on the CTU-13 dataset. In the context of smart cities, a study introduces a network flow-based deep learning botnet detection system (13), showcasing its effectiveness in handling large-scale attacks from compromised IoT devices. Furthermore, a performance evaluation of botnet detection using deep learning techniques (14) demonstrates the potential for real-world application by achieving high detection rates and low false positives with the CTU-13 dataset.

These works collectively reflect the multifaceted efforts to bolster IoT security against botnet attacks, incorporating diverse methodologies ranging from statistical analysis and hybrid models to deep learning techniques and systematic literature reviews. The field continues to evolve as researchers strive to enhance the resilience of IoT ecosystems against emerging security threats.

III. SURVEY PAPER

Sl. No	Year of *publication*	Project Titles	Description
1.	2023 [1]	Botnet Attack Detection in IoT Networks using CNN and LSTM	To address IoT device security against botnet attacks, employ dimensionality reduction techniques such as PCA and autoencoder on the Bot-IoT dataset. These methods reduce feature dimensions, enabling the use of memory-efficient DL algorithms like LSTM and CNN for botnet attack detection. Evaluate performance using metrics like accuracy, precision, recall, and confusion matrix.
2.	2023[2]	A Hybrid Model for Botnet Detection using Machine Learning	A hybrid machine-learning model, integrating k-means, rule-based systems, and decision trees, was proposed for detecting botnet attacks in network traffic. Using the CTU-13 dataset and features from the Barnacles Mating Optimizer, the experiment achieved high accuracy (99%). This approach enhances robustness against various botnet attacks, with k-means, decision tree, and rule-based system exhibiting 99.32%, 99.11%, and 97.14% accuracy, respectively. Precision rates were 98.93%, 98.37%, and 95.93%, respectively.
3.	2023[3]	Botnet Dataset Overview Using Statistical Approach Based on Time Gap Activity Analysis	This paper introduces a novel approach to detect botnet malware by analysing time gaps in botnet datasets using a statistical method. The proposed technique aims to determine optimal threshold values, with experimental results suggesting three thresholds—highest at 4,756s, lowest at 28.69s, and an average maximum time gap of 810.61s for effective separation of botnet, normal, and background activity.
4.	2023[4]	Detecting and Mitigating Botnet Attacks in Software-Defined Networks Using Deep Learning Techniques	Software-Defined Networking (SDN) enables flexible network management but introduces security challenges. Addressing threats like DDoS attacks, this study employs Deep Learning (DL) in an SDN environment. Utilizing a self-generated dataset, feature weighting, and tuning, the study identifies a lightweight DL method. Results show CNN's superior performance with a 99% detection rate for normal flows and 97% for attacks.
5.	2022[1]	Botnet Attack Intrusion Detection In IoT Enabled Automated Guided Vehicles	The 21st century thrives on the Internet of Things (IoT) and Automated Vehicles, streamlining tasks within seconds. IoT integrates devices, machines, and people to transfer data seamlessly. Automated Guided Vehicles (AGVs) rely on IoT networks, demanding robust security. This study advocates an intrusion prediction system using N-Balo dataset to foresee botnet attacks, enhancing AGV network reliability and security.
6.	2022[2]	Machine Learning based IoT-BotNet Attack Detection Using Real-time Heterogeneous Data	IoT device security is a significant challenge, prompting exploration of machine learning algorithms for attack detection. This study assesses Logistic Regression, Gaussian Naive Bayes, Decision Trees, Random Forest, K-Nearest Neighbours, and Extreme Gradient Boosting for detecting malicious activity in IoT network traffic. Tree-based classifiers outperform LR and GNB, achieving 99% accuracy and a 0.99 Fl-score in binary classification, while multiclass results highlight DT, KNN, RF, and XGB with 98% accuracy and a 0.98 Fl-score. Feature reduction impact on accuracy and training time is also analysed.
7.	2022[3]	AI-based botnet attack classification and detection in IoT devices.	Rising use of household IoT devices poses security risks, challenging traditional rule-based systems. AI offers a solution by employing machine learning and deep learning to detect and classify IoT botnets. Six ML and three DL models are evaluated, with the top performer implemented as an API for enhanced security against threats.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

8.	2021[1]	Machine learning for misuse-based network intrusion detection: Overview, unified evaluation and feature choice comparison framework	Advanced communication network security depends on the uses of Network Intrusion Detection Systems with Machine Learning and artificial intelligence present viable alternatives to the original hardcoding. In the face of a wide range of datasets and metrics available in the literature, our work introduces detection and identification scores and defines universal comparison standards. An algorithm implementation workflow that transforms raw packet flows into machine learning input. The demonstration promises real-time, low-cost deep learning with the raw-traffic characteristics by our results, which outperform the state of the art.
9.	2021[2]	Intrusion detection based on sequential information preserving log embedding methods and anomaly detection algorithms	Previous methods for system intrusion detection have mainly consisted of those based on pattern matching that employs prior knowledge extracted from experts' domain knowledge. However, pattern matching-based methods have a major drawback that it can be bypassed through various modified techniques. It proposed an end-to-end abnormal behaviour detection method based on sequential information preserving log embedding algorithms and machine learning-based anomaly detection algorithms.
10.	2020[1]	Systematic literature review on iot-based botnet attack	The adoption of the Internet of Things (IoT) technology is expanding exponentially because of its capability to provide a better service. This technology has been successfully implemented on various devices. The growth of IoT devices is massive at present. various kind of attacks are possible due to this vulnerability, with IoT-based botnet attack being one of the most popular. In this study, we conducted a comprehensive systematic literature review on IoT-based botnet attacks. Existing state of the art in the area of study was presented and discussed in detail. A systematic methodology was adopted to ensure the coverage of all important studies. This methodology was detailed and repeatable.
11.	2020[2]	Iot-flock: An open-source framework for iot traffic generation	The Internet of things (IoT) has emerged as a topic of intense interest among the research and industrial community as it has had a revolutionary impact on human life. The rapid growth of IoT technology has revolutionized human life by inaugurating the concept of smart devices, smart healthcare, smart industry, smart city, smart grid, among others. IoT devices' security has become a serious concern nowadays, especially for the healthcare domain, where recent attacks exposed damaging IoT security vulnerabilities. Traditional network security solutions are well established. However, due to the resource constraint property of IoT devices and the distinct behaviour of IoT protocols, the existing security mechanisms cannot be deployed directly for securing the IoT devices and network from the cyber-attacks. To enhance the level of security for IoT, researchers need IoT-specific tools, methods, and datasets. To address the mentioned problem, we provide a framework for developing IoT context-aware security solutions to detect malicious traffic in IoT use cases. The proposed framework consists of a newly created, open-source IoT data generator tool named IoT-Flock.
12.	2020[3]	Botnet fingerprinting: a frequency distributions scheme for lightweight bot detection	Efficient bot detection is vital for security, with recent methods replacing flow-based techniques with graph-based features. However, scalability challenges arise. Addressing this, BotFP simplifies communication graphs by analysing frequency distributions of protocol attributes. It characterizes host behaviour, learns through clustering or ML, and classifies hosts as benign or bots. Validated on the CTU-13 dataset, BotFP proves lightweight, scalable, and more accurate than existing techniques in handling large datasets.
13.	2020[4]	Network flow based iot botnet attack detection using deep learning	Governments globally advocate for adva city applications to improve urban life. The rise in Internet of Things (IoT) devices contributes to a surge in botnet attacks. To cushion cybersecurity, this paper introduces a deep learning (DL) botnet detection system for smart cities. By transforming network traffic flows into connection records, the DL model advances in detecting attacks from compromised IoT devices, outperforming traditional machine learning models in extensive experiments on benchmark datasets.
14.	2020[5]	Performance evaluation of botnet detection using deep learning techniques	Cybersecurity is seriously threatened by Botnets, which are controlled networks of compromised computers. The evolving techniques used by botnet operators make it difficult for traditional methods of botnet identification to stay up. Machine learning has become increasingly effective in recent years as a means of identifying and reducing these

			hazards. The CTU-13 dataset, a frequently used dataset in the field of cybersecurity, is used in this study to offer a machine learning-based method for botnet detection. The suggested methodology makes use of the CTU-13, which is made up of actual network traffic data that was recorded in a network environment that had been attacked by a botnet. Results from experiments show how well the machine learning based approach detects botnet with accuracy. It is potential for use in actual world is demonstrated by the suggested system's high detection rates and low false.
15.	2020[6]	Iot dos and ddos attack detection using resnet	Rising household adoption of IoT devices amplifies security risks like DoS and spoofing. Traditional rule-based systems struggle with diverse IoT devices. Addressing this, AI techniques leverage machine learning and deep learning algorithms to detect and classify IoT botnets. Six ML and three DL models are evaluated, with the top-performing model deployed as an API.
16.	2020[7]	A hierarchical hybrid intrusion detection approach in iot scenarios	Implementing H2ID, a two-stage hierarchical Network Intrusion Detection system for IoT security. Leveraging a MultiModal Deep AutoEncoder for anomaly detection and soft-output classifiers for attack classification, H2ID outperforms baselines by reducing false positives by up to -40%. The system ensures efficiency, flexibility, and privacy preservation in IoT scenarios, requiring minimal re-training.
17.	2020[8]	A survey on botnet detection techniques	The paper explores methods for detecting Botnets, malicious networks controlled by a Botmaster. It distinguishes between general bot and IoT-bot detection techniques, employing the UNSW-NB15 dataset. The proposed model utilizes a real-time IoT-Bot detection algorithm based on deep learning, with Wireshark capturing network traffic for analysis.
18.	2020[9]	Detection of slow port scanning attacks	Port scanning attacks pose a significant challenge in cybersecurity. This study leveraged seven machine learning classifiers, employing principal component analysis to enhance results. XGBoost emerged as the most effective, boasting a remarkable 99.98% accuracy, no false positives, 99.99% precision, 99.98% recall, and a 99.99% area-under-curve, outperforming other classifiers and prior research.
19.	2020[10]	Towards a universal features set for iot botnet attacks detection	IoT device vulnerabilities expose them to exploitation, enabling attackers to integrate them into botnets. These compromised devices are then utilized to orchestrate large-scale distributed denial of service (DDoS) attacks, rendering target websites or services unresponsive to legitimate users. Existing botnet detection techniques face limitations as their performance relies on specific training datasets, lacking adaptability across diverse attack patterns. This paper introduces a universal feature set designed to enhance botnet attack detection, demonstrating superior results across three distinct botnet attack datasets.
20.	2019[1]	A botnet detection method on sdn using deep learning	Analysing malware traffic on a network, we employ deep learning to classify normal and malicious data, countering unknown threats unaddressed by rule-based antivirus software. By programming a software-defined network, we dynamically manage malware, preventing host detection and subsequent damage. Our approach includes adding an external connection block for network isolation, thwarting internal infections.
21.	2019[2]	Probe delay based adaptive port scanning for iot devices with private ip address behind net	We propose a DPDK-based scanner, leveraging advanced port scanning techniques for improved network security. Overcoming speed and accuracy limitations of traditional methods, our solution employs protocol-specific probes, evasive scans, and hardware acceleration. In experiments, it achieved a 2× speedup, 99.5% open port identification accuracy, and a 40% reduction in CPU and memory usage, enhancing network visibility and security.
22.	2019[3]	Developing realistic distributed denial of service (ddos) attack dataset and taxonomy	Expanding internet services heightens the risk of cyber threats, particularly from increasingly complex Distributed Denial-of-Service (DDoS) attacks. This study introduces an efficient Long Short-Term Memory (LSTM) model for early detection of DDoS threats in network traffic packets. Trained on the CICDDoS2019 dataset, the LSTM model demonstrates a remarkable 98% accuracy, showcasing superior performance over traditional machine learning methods.

23.	2018[1]	A method to detect internet of things botnets	This paper addresses IoT security challenges, focusing on unauthorized access. It examines prevalent botnet characteristics and proposes a logistic regression-based method for detecting compromised IoT devices within botnets. The model estimates the likelihood of a connected device being a bot. Additionally, the article lists network protocols used for unauthorized access and communication with command-and-control servers.
24.	2018[2]	N-baiot—network-based detection of iot botnet attacks using deep autoencoders	The surge in vulnerable IoT devices has led to a rise in IoT-based botnet attacks. Addressing this, we introduce N-BaIoT, a novel network-based anomaly detection method for IoT. Utilizing deep autoencoders, it captures behaviour snapshots to swiftly identify and differentiate between short and prolonged IoT-based attacks. Tested on nine infected commercial IoT devices, including Mirai and BASHLITE botnets, our method consistently and promptly detected ongoing attacks.
25.	2017[1]	Port scanning detection based on anomalies	The paper presents a machine-learning-based detection system for identifying reconnaissance attacks on IoT devices. With an explainable ensemble model, the system efficiently detects scanning and reconnaissance activities, offering a 99% accuracy. It boasts low false positive (0.6%) and false negative (0.05%) rates, ensuring effectiveness resource-constrained environments with minimal resource consumption.
26.	2016[1]	Deep residual learning for image recognition	We introduce a residual learning framework to facilitate training substantially deeper neural networks, reformulating layers as residual functions with reference to inputs. Empirical evidence demonstrates improved optimization ease and accuracy gains from increased depth. Our 152-layer residual networks, 8× deeper than VGG nets, achieved a 3.57% error on ImageNet, winning 1st place in ILSVRC 2015. Additionally, our deep representations yielded a 28% relative improvement on COCO object detection.
27.	2016[2]	Implementation and vulnerability test of stealth port scanning attacks using zmap of censys engine	Residual learning facilitates the training of deeper neural networks, surpassing prior limitations. By redefining layers as learning residual functions relative to inputs, we achieve up to 152-layer depth, outperforming VGG nets. Empirical evidence on ImageNet demonstrates enhanced optimization and accuracy, winning the ILSVRC 2015 classification task with a 3.57% error rate. The approach, showcased with 100 and 1000 layers on CIFAR-10, emphasizes the crucial role of representation depth. Notably, the deep residual networks contribute to a 28% improvement in COCO object detection, securing 1st places in ILSVRC & COCO 2015 competitions across various tasks.
28.	2015[1]	Botnet Forensics Framework: Is Your System a Bot	Rising sophisticated cyber-attacks pose threats to network stability. Botnets, a focus of current research, orchestrate malicious activities by connecting compromised machines to a command-and-control server. This paper outlines botnet types, defines architectures, and introduces a framework for detecting and preventing their spread, safeguarding network security.
29.	2015[2]	Botnet in DDoS Attacks: Trends and Challenges	The escalating threat of DDoS attacks stems from the rapid expansion of computer networks and software applications. Botnets, commonly utilized in internet crimes, pose a significant hazard, particularly in DDoS attacks, causing severe depletion of network resources. This survey provides a thorough examination of DDoS, encompassing causes, types, attack tools, botnet architectures, and associated research challenges.
30.	2014[1]	A SDN-oriented DDoS blocking scheme for botnet-based attacks	This paper explores leveraging software-defined networks (SDN) to counter sophisticated DDoS attacks that target specific services with minimal, legitimate-looking traffic. The focus is on developing a DDoS blocking application operating on the SDN controller through the standard OpenFlow interface, offering an effective defence against large-scale botnet-driven attacks.
31.	2013[1]	Survey on botnet: Its architecture, detection, prevention and mitigation	Botnets pose a significant cybersecurity threat to individuals, organizations, and governments. Crafted by adept hackers, these malicious networks challenge the IT community in detecting, preventing, and mitigating attacks. This paper explores the botnet life cycle, topologies, detection methods, and outlines essential measures for safeguarding against future botnet threats.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

32.	2013[2]	Botnets in 4G cellular networks: Platforms to launch DDoS attacks against the air interface	This paper reveals a vulnerability in the 4G LTE air interface, exposing it to Distributed Denial-of-Service (DDoS) attacks orchestrated by botnets. Simulations using an LTE simulator demonstrate that a botnet affecting only 3% of subscribers can significantly degrade voice quality, while at 6%, it can cause a complete outage. These findings highlight the need for enhanced security measures in telecommunication services.

IV. CONCLUSION

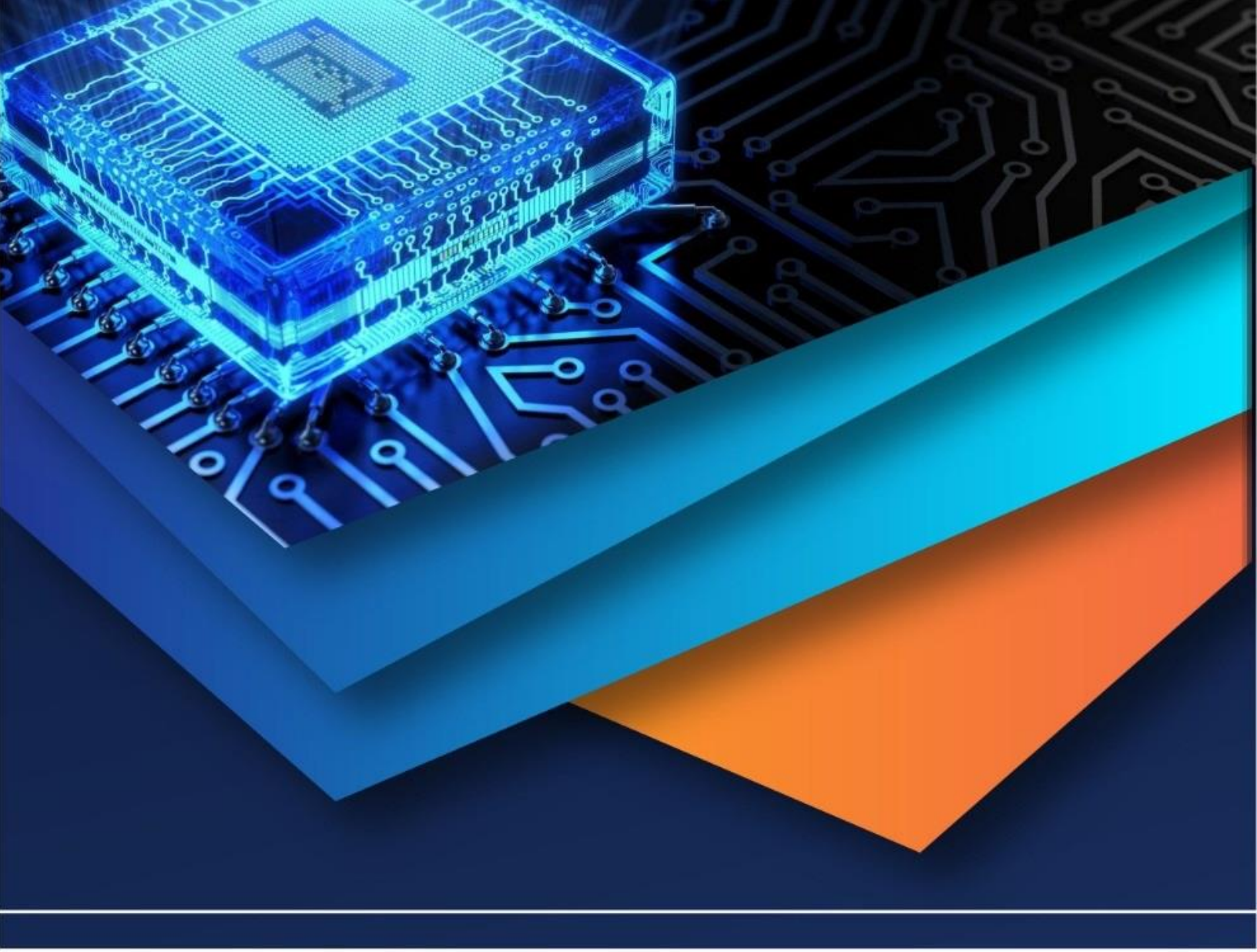
This survey provides an intact overview of recent upgrades in botnet discovery and security, with a focus on IoT networks. The integration of deep learning, hybrid models, and the exploration of versatile feature sets showcases the unfolding geography of cybersecurity against botnet threats. unborn research should continue to address the dynamic nature of botnet attacks and the evolving IoT ecosystem.

REFERENCES

[1] A. Sharma, P. B. Mishra and G. Geetha, "Botnet Attack Detection in IoT Networks using CNN and LSTM," 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India, 2023, pp. 1270-1275, doi: 10.1109/ICECAA58104.2023.10212330.
[2] A. Zaheer, S. Tahir, M. F. Almufareh and B. Hamid, "A Hybrid Model for Botnet Detection using Machine Learning," 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2023, pp. 1-8, doi: 10.1109/ICBATS57792.2023.10111161.
[3] M. A. Rachman Putra, T. Ahmad and D. P. Hostiadi, "Botnet Dataset Overview Using Statistical Approach Based on Time Gap Activity Analysis," 2023 11th International Symposium on Digital Forensics and Security (ISDFS), Chattanooga, TN, USA, 2023, pp. 1-6, doi: 10.1109/ISDFS58141.2023.10131832.
[4] 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, doi: 10.1109/ACCESS.2023.3277397.
[5] S. Shaikh, C. Rupa, G. Srivastava and T. Reddy Gadekallu, "Botnet Attack Intrusion Detection In IoT Enabled Automated Guided Vehicles," 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, 2022, pp. 6332-6336, doi: 10.1109/BigData55660.2022.10020355.
[6] A. Ahmed and C. Tjortjis, "Machine Learning based IoT-BotNet Attack Detection Using Real-time Heterogeneous Data," 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), Prague, Czech Republic, 2022, pp. 1-6, doi: 10.1109/ICECET55527.2022.9872817.
[7] V. Puri, A. Kataria, V. K. Solanki and S. Rani, "AI-based botnet attack classification and detection in IoT devices," 2022 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT), Soyapango, El Salvador, 2022, pp. 1-5, doi: 10.1109/ICMLANT56191.2022.9996464.
[8] L. Le Jeune, T. Goedemé, and N. Mentens, “Machine learning for misusebased network intrusion detection: Overview, unified evaluation and feature choice comparison framework,” Ieee Access, 2021.
[9] C. Kim, M. Jang, S. Seo, K. Park, and P. Kang, “Intrusion detection based on sequential information preserving log embedding methods and anomaly detection algorithms,” IEEE Access, vol. 9, pp. 58 088–58 101, 2021.
[10] I. Ali, A. I. A. Ahmed, A. Almogren, M. A. Raza, S. A. Shah, A. Khan, and A. Gani, “Systematic literature review on iot-based botnet attack,” IEEE Access, 2020.
[11] S. Ghazanfar, F. Hussain, A. U. Rehman, U. U. Fayyaz, F. Shahzad, and G. A. Shah, “Iot-flock: An open-source framework for iot traffic generation,” in 2020 International Conference on Emerging Trends in Smart Technologies (ICETST). IEEE, 2020, pp. 1–6.
[12] A. Blaise, M. Bouet, V. Conan, and S. Secci, “Botnet fingerprinting: a frequency distributions scheme for lightweight bot detection,” IEEE Transactions on Network and Service Management, 2020.
[13] S. Sriram, R. Vinayakumar, M. Alazab, and K. Soman, “Network flow based iot botnet attack detection using deep learning,” in IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2020, pp. 189–194.
[14] B. Nugraha, A. Nambiar, and T. Bauschert, “Performance evaluation of botnet detection using deep learning techniques,” in 2020 11th International Conference on Network of the Future (NoF). IEEE, 2020, pp. 141–149.
[15] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, “Iot dos and ddos attack detection using resnet,” in 2020 IEEE 23rd International Multitopic Conference (INMIC), 2020, pp. 1–6.
[16] G. Bovenzi, G. Aceto, D. Ciuonzo, V. Persico, and A. Pescapé, “A hierarchical hybrid intrusion detection approach in iot scenarios,” in GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE, 2020, pp. 1–7.
[17] S. Gaonkar, N. F. Dessai, J. Costa, A. Borkar, S. Aswale, and P. Shetgaonkar, “A survey on botnet detection techniques,” in 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE). IEEE, 2020, pp. 1–6.
[18] M. u Nisa and K. Kifayat, “Detection of slow port scanning attacks,” in 2020 International Conference on Cyber Warfare and Security (ICCWS). IEEE, 2020, pp. 1–7.
[19] F. Hussain, S. G. Abbas, U. U. Fayyaz, G. A. Shah, A. Toqeer, and A. Ali, “Towards a universal features set for iot botnet attacks detection,” in 2020 IEEE 23rd International Multitopic Conference (INMIC), 2020, pp. 1–6.
[20] S. Maeda, A. Kanai, S. Tanimoto, T. Hatashima, and K. Ohkubo, “A botnet detection method on sdn using deep learning,” in 2019 IEEE International Conference on Consumer Electronics (ICCE). IEEE, 2019, pp. 1–6.
[21] F. Tang, Y. Kawamoto, N. Kato, K. Yano, and Y. Suzuki, “Probe delay based adaptive port scanning for iot devices with private ip address behind net,” IEEE Network, vol. 34, no. 2, pp. 195–201, 2019.
[22] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, “Developing realistic distributed denial of service (ddos) attack dataset and taxonomy,” in 2019 International Carnahan Conference on Security Technology (ICCST). IEEE, 2019, pp. 1–8.
[23] A. O. Prokofiev, Y. S. Smirnova, and V. A. Surov, “A method to detect internet of things botnets,” in 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). IEEE, 2018, pp. 105–108.

[24] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, “N-baiot—network-based detection of iot botnet attacks using deep autoencoders,” IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, 2018.
[25] E. V. Ananin, A. V. Nikishova, and I. S. Kozhevnikova, “Port scanning detection based on anomalies,” in 2017 Dynamics of Systems, Mechanisms and Machines (Dynamics). IEEE, 2017, pp. 1–5.
[26] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, pp. 770–778.
[27] S. Lee, S.-y. Im, S.-H. Shin, B.-h. Roh, and C. Lee, “Implementation and vulnerability test of stealth port scanning attacks using zmap of censys engine,” in 2016 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2016, pp. 681–683
[28] S. Bansal, M. Qaiser, S. Khatri and A. Bijalwan, "Botnet Forensics Framework: Is Your System a Bot," 2015 Second International Conference on Advances in Computing and Communication Engineering, Dehradun, India, 2015, pp. 535-540, doi: 10.1109/ICACCE.2015.124.
[29] N. Hoque, D. K. Bhattacharyya and J. K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2242-2270, Fourthquarter 2015, doi: 10.1109/COMST.2015.2457491.
[30] S. Lim, J. Ha, H. Kim, Y. Kim and S. Yang, "A SDN-oriented DDoS blocking scheme for botnet-based attacks," 2014 Sixth International Conference on Ubiquitous and Future Networks (ICUFN), Shanghai, China, 2014, pp. 63-68, doi: 10.1109/ICUFN.2014.6876752.
[31] I. Ullah, N. Khan and H. A. Aboalsamh, "Survey on botnet: Its architecture, detection, prevention and mitigation," 2013 10th IEEE INTERNATIONAL CONFERENCE ON NETWORKING, SENSING AND CONTROL (ICNSC), Evry, France, 2013, pp. 660-665, doi: 10.1109/ICNSC.2013.6548817.
[32] M. Khosroshahy, D. Qiu and M. K. Mehmet Ali, "Botnets in 4G cellular networks: Platforms to launch DDoS attacks against the air interface," 2013 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), Montreal, QC, Canada, 2013, pp. 30-35, doi: 10.1109/MoWNet.2013.6613793.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)