Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 13, No. 3, September 2025, pp. 750~757
ISSN: 2089-3272, DOI: 10.52549/ijeei.v13i3.6130

A Systematic Literature Review (SLR) of Mirai Botnet Compromise Detection in Internet of Things (IoT) Network

Ibukun Eweoya[1], Funminiyi Olajide[2], Jonathan Obed[3], Christian Asante[4]
[1,3]Department of Software Engineering, Babcock University, Nigeria
[2]Centre for Cyber Security, Information Privacy, and Privacy, Penn State University, USA
[4]Data, Technology & Information, NHS England, United Kingdom

Article Info

Article history:

Received Dec 12, 2024
Revised Jan 29, 2025
Accepted Aug 7, 2025

Keywords:

Mirai botnet
IoT security
Threat intelligence
Detection techniques
Artificial Intelligence

ABSTRACT

Since its invention, Mirai botnet has remained a significant concern in IoT network security. The botnet and its evolving variants are a major threat to professionals responsible for securing IoT infrastructures. The danger of the botnet is attributed to the fact that it has been utilized for the execution of numerous Distributed Denial of Service (DDoS) attacks on different network infrastructures in the past. Several researchers have proposed techniques in mitigating the effect of this botnet. This research systematically reviews existing detection techniques and evaluates how effective they are in mitigating Mirai botnet attacks between 2017 and 2024. Using PRISMA methodology, 177 articles were initially identified from Scopus, Springer Link, IEEE Xplore, and Web of Science in order to broaden the scope of the search. 27 studies passed the inclusion criteria, and were analyzed thereafter. Findings reveal a predominant reliance on AI-driven detection methods, such as LSTM and ensemble models, which demonstrate higher accuracy and scalability when compared to traditional techniques. This review also compares threat intelligence platforms like AlienVault, CrowdStrike, and Recorded Future, to assess their contributions to dynamic detection frameworks. Finally, the study explores research gaps and proposes future directions for developing scalable real-time detection systems integrating multi-source threat feeds.

Corresponding Author:

Ibukun Eweoya,
Department of Software Engineering,
Babcock University,
Illisan Remo, Ogun State, Nigeria.
Email: eweoyai@babcock.edu.ng

1. INTRODUCTION

The Internet of Things (IoT) has revolutionized modern technology by interconnecting billions of devices worldwide, enabling seamless data sharing and automation across diverse industries [1, 2]. IoT is now widely recognized as a technology that will transform the future. However, this advancement has also introduced significant security vulnerabilities and a corresponding high level of increased cyber-attacks [3]. For example, increased adoption of cloud computing will offer organizations with many good benefits, but at the same time, open these organizations to new cybersecurity concerns and vulnerability to attacks like Distributed Denial of Service (DDoS), SQL injection, etc. [4]. IoT devices with weak security configurations often become prime targets for cyber threats, particularly botnets like Mirai.

The Mirai botnet first gained notoriety in the year 2016, and has since then become popular in the IoT industry for orchestrating large-scale DDoS attacks that can disrupt IoT infrastructures globally [5, 6, 7]. Since then, its variants have evolved to exploit new vulnerabilities in IoT ecosystems. These attacks highlight the urgent need for robust techniques to protect IoT networks. The Mirai botnet first gained notoriety in the year 2016, and has since then become popular in the IoT industry for orchestrating

large-scale DDoS attacks that can disrupt IoT infrastructures globally [5, 6, 7]. Since then, its variants have evolved to exploit new vulnerabilities in IoT ecosystems. These attacks highlight the urgent need for robust techniques to protect IoT networks.

Despite progress, existing detection methods face challenges in scalability, computational demands, and adaptability to new variants. This study systematically reviews detection techniques for the Mirai botnet from 2018 to 2024. It explores the integration of threat intelligence feeds into IoT monitoring tools, identifies research gaps, and proposes future directions for modern and dynamic detection systems.

1.1. Rationale

Mirai botnet explores the vulnerability of IoT devices with weak security configurations to carry out ravaging attacks that continue to threaten the stability and security of IoT networks [10]. Given its evolving architecture, the detection of Mirai and its variants remain complex. Professionals face the challenge of identifying early infection indicators and implementing scalable detection systems. Notable public threat intelligence platforms report and offer real-time IoCs associated with Mirai like URLs, file hashes, IP addresses, domains and host names of different Mirai botnet pulses, which become highly relevant when developing detection systems.

Notable progress is seen in the emerging adoption of AI to develop Mirai botnet detection systems [11], and as such this work systematically reviews previous studies on Mirai botnet detection and evaluates the feasibility of utilizing threat intelligence feeds for improved network monitoring. The review also aims to highlight strengths and limitations in current approaches and give a direction for future research toward adaptive, AI-driven detection systems.

1.2. Objectives

The objectives of this research are to:

a. Explore existing detection techniques for the Mirai botnet in IoT network.
b. Assess the integration of threat intelligence feeds into IoT monitoring tools.
c. Investigate available Mirai IoCs on AlienVault OTX to evaluate their utility in real-time detection systems.
d. Identify research gaps, and recommend future research directions.

2. RESEARCH METHOD

A detailed search to retrieve accessible related literature to support this SLR was conducted in full compliance to PRISMA 2020 guidelines [12]. The literature search was conducted across multiple databases including Scopus, Spring Link, IEEE Xplore, and Web of Science databases. The search covered articles published between January 2017 and July 2024 in peer-reviewed journals and written in English. Search keywords included: Mirai, IoT network, threat intelligence, and malware.

2.1. Eligibility Criteria

The first search to retrieve supporting literature returned a good result that included articles, conference papers, book chapters etc. Proceeding after the first search, the results were screened thoroughly by the researchers, and only relevant articles that provided specific insights about Mirai detection were marked to be eligible. To ensure that the screening is done properly, “Population, Intervention, Comparison, Outcomes and Study” (PICOS) framework was adopted [13]. The blueprint for retaining and selecting relevant articles as outlined by PICOS framework established the inclusion and exclusion criteria.

2.2. Inclusion Criteria

a. Articles focusing on detection techniques for Mirai botnet.
b. English-language publications from 2018 – 2024.
c. Studies discussing the integration of threat intelligence into IoT security systems.

2.3. Exclusion Criteria

a. Non-English publications.
b. Conference papers, book chapters, reviews not centered on Mirai detection.
c. Studies that discussed botnets or malwares in general that are not primarily Mirai botnets.

2.4. Information Sources

The procedure for retrieving related literature started with developing an advanced Scopus search query to find articles that contain or project the relevant keywords, and also searching on other databases. A total of 177 results were retrieved by both the Scopus search query below, and from other databases: "TITLE-ABS-KEY(mirai OR (mirai AND (based OR variant))) AND (botnet* OR malware*) AND (compromise OR attack* OR threat* OR vulnerability) AND (detect* OR discovery) AND (network*) AND PUBYEAR > 2017 AND PUBYEAR < 2025 AND (LIMIT-TO (SRCTYPE,"j")) AND (LIMIT-TO (PUBSTAGE,"final")) AND (LIMIT-TO (DOCTYPE,"ar")) AND (LIMIT-TO (LANGUAGE,"English"))"

2.5. Information Sources

The careful review of scholarly articles was done by the researchers. Researchers utilized automated tools to make the selection process fast. The results of the initial search were exported and downloaded as either RIS or CSV or PDF formats. The exported search results were then uploaded to "Hubmeta" [14], and a check for duplicates was carried out. Once this step was completed, the review of titles was also done. At the completion of marking and excluding studies that were not relevant, the remaining articles were exported and uploaded to "Mendeley reference manager", for easy retrieval of the full-texts of the selected articles.

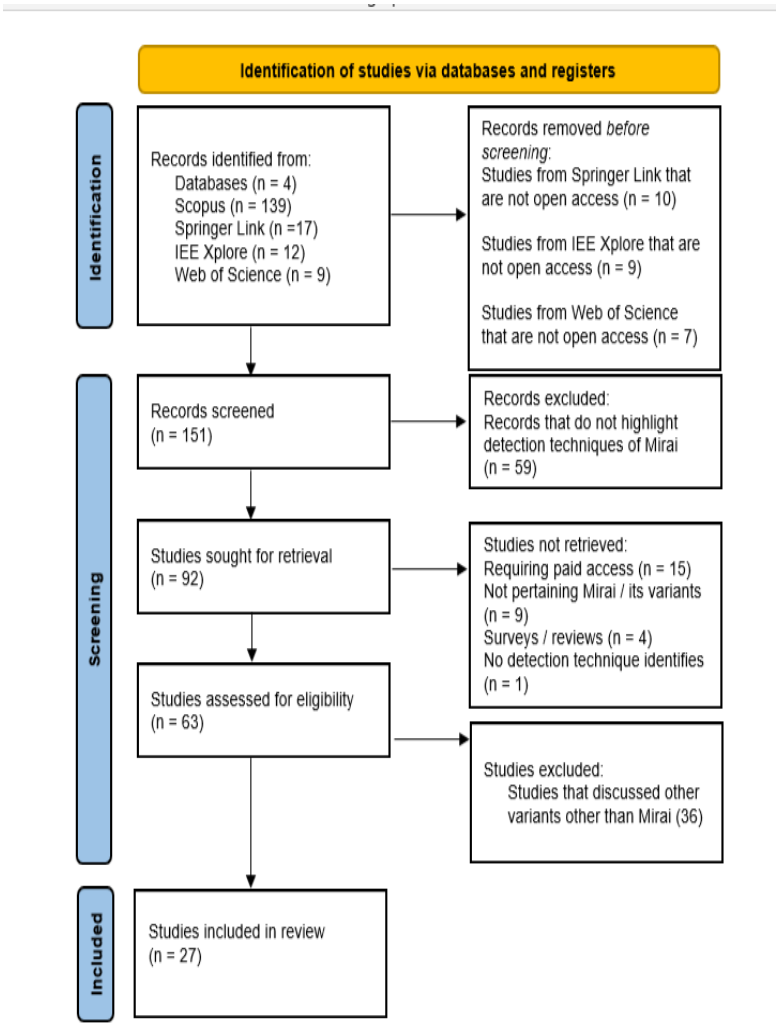

Figure 1. Prisma flowchart

The figure 1 [12] describes the procedure of how 177 search results were carefully screened by the researchers.

2.6. Mirai Identification Techniques in IoT Networks

To ensure that this review is in-depth, it was important to study related works and identify several Mirai botnet detection techniques developed / proposed in these studies. There is significant advancement in adopting Artificial intelligence models for Mirai compromise detection in IoT networks. As a matter of fact, the investigation showed that some techniques proposed in related works despite being novel, performed greatly. The wide adoption of AI in this regard is a shift away from traditional approaches where cybersecurity professionals had to perform traditional (manual) rule-based network scans and investigations before Mirai IoCs are identified as shown in Table 1.

Table 1. Summary of studies that passed inclusion criteria

Article/Authors	Botnets identified	Detection technique	Year of publication
[15]	Mirai	Statistical hypothesis	2021
[16]	Mirai	Federated Learning (FL)	2023
[17]	Mirai	Adaptive online learning strategy	2021
[18]	Mirai	Trusted Monitor (TM)	2024
[19]	Mirai	ETM hardware tracer	2024
[20]	Mirai	Malware distribution simulator	2021
[21]	Mirai	RF algorithm	2021
[22]	Mirai	Split-and-Merge	2020
[23]	Mirai	Gotham testbed	2024
[24]	Mirai	Hybrid detection model	2023
[25]	Mirai	Machine learning based multi-class classifier	2023
[26]	Mirai	Artificial Intelligence	2023
[27]	Mirai	MicroVNF	2022
[28]	Mirai	Artificial Neural Network model	2021
[29]	Mirai	Network intrusion detection system by applying ensemble model	2024
[30]	Mirai	Machine Learning Algorithm	2021
[31]	Mirai	collaborative threat intelligence sharing mechanism using Ethereum Virtual Machine and Hyperledger	2022
[32]	Mirai	supervised learning models	2022
[33]	Mirai	BotMiner, BotProbe, and BotHunter	2024
[34]	Mirai	IoTSecSim	2024
[35]	Mirai	Imrc	2022
[36]	Mirai	Long Short Term Memory term (LSTM) and XGBoost	2024
[37]	Mirai	MCELIECE	2021
[38]	Mirai	Open - source analysis tools and QEMU	2021
[39]	Mirai	IoT-Praetor	2021
[40]	Mirai	Recurrent Neural networks and Bidirectional Long Short Term Memory (BLRNN)	2022
[41]	Mirai	Botnet Impact Estimation using Traffic Flow Features	2022

2.7. Findings

Out of the 177 studies initially screened, 27 met the inclusion criteria and were selected for full analysis. Among these, approximately 65% adopted AI-driven detection approaches, including LSTM, Federated Learning (FL), and ensemble models. These approaches generally reported higher accuracy and scalability compared to traditional rule-based or anomaly detection models from platforms like AlienVault's OTX, Recorded Future, and CrowdStrike. These integrations were used to enhance detection pipelines with real-time Indicators of Compromise (IoCs). The studies also demonstrated increasing interest in integrating threat intelligence feeds. Table 1 summarizes the studies, including the techniques employed and the year of publication.

3. RESULTS AND DISCUSSION

A deep dive and analysis showed that several reviewed studies reported accuracy levels exceeding 90%, with LSTM-XGBoost hybrids achieving up to 98.4% accuracy [36]. In terms of data sources, Bot-IoT and CICIDS2017 were the most commonly used datasets, although limitations in traffic realism and scope were observed. Notably, only a few studies validated their detection models in real-time or production-grade IoT environments, highlighting a gap between theoretical models and applied security solutions. The integration of threat intelligence feeds, particularly from platforms like AlienVault OTX, Recorded Future, and CrowdStrike emerged as a promising avenue.

The open-source AlienVault's OTX Direct Connect API that is hosted on "GitHub" [42], for instance, all allows researchers to programmatically access real-time IoCs through SDKs available in Python, Go, C, Java, and JavaScript. These tools facilitate automatic ingestion of threat data into detection pipelines, enabling faster response to Mirai related threats. However, integration challenges remain. The OTX API for example restricts access to subscribed pulses, requiring researchers to manually subscribe to each threat feed, while both Recorded Future and CrowdStrike are not open-sourced. Furthermore, while AlienVault's OTX API subscription is free, it introduces operational limitations in scalability and coverage.

It is also important to contextualize these findings within the evolution of ML techniques from 2018 to 2024. Early studies often relied on simpler models with limited generalization capabilities. In contrast, recent works demonstrate a shift toward resource-optimized, distributed, and interpretable AI systems.

3.1. Taxonomy of Detection Techniques

The reviewed studies showed diverse detection methods. A taxonomy was developed to classify these methods into five main categories: signature-based, anomaly-based, AI (ML)-based, hybrid systems, and threat intelligence-based detection as shown in Table 2.

Table 2. Taxonomy of Mirai Botnet Detection Techniques

Category	Description	Examples	Strengths	Limitation
Signature-based	Works by detecting known patterns in network traffic	Snort, Suricata	Fast, simple, accurate for known attacks	Ineffective against unknown variants
Anomaly-based	Works by detecting deviations from normal behaviour	BotHunter, Bro IDS	Detects zero-day attacks	Quite prone to false positives.
AI (ML)-based	Learns patterns using labeled datasets	LSTM, RF, FL, XGBoost	High accuracy, adaptable	Needs large data, low transparency
Hybrid	Combines ML, signatures, and heuristics	AI + threat intelligence, anomaly + signature	Balanced detection	Complex to build and train
Multi- Threat Intelligence Integration	Uses threat intelligence feeds (IoCs)	AlienVault OTX, Recorded Future	Real-time detection updates	Dependent on feed updates.

3.2. Performance Detection Models from Reviewed Studies

Selected studies from the review were evaluated and the performance metrics of proposed AI-based detection models are discussed in Table 3 and Figure 2:

Table 3. Performance Summary of AI-Based Detection Models

Model Type	Accuracy (%)	Dataset Used	Summary
LSTM + XGBoost	98.34	Bot-IoT	High precision, long training time
FL	95.2	N-Balot	Lightweight and distributed
Ensemble Model	94.3	CICIDS2017	Balanced recall and precision
ANN	91.8	Bot-IoT	Good baseline but less interpretable
RF	90.5	Bot-IoT	Quick training, but prone to overfitting

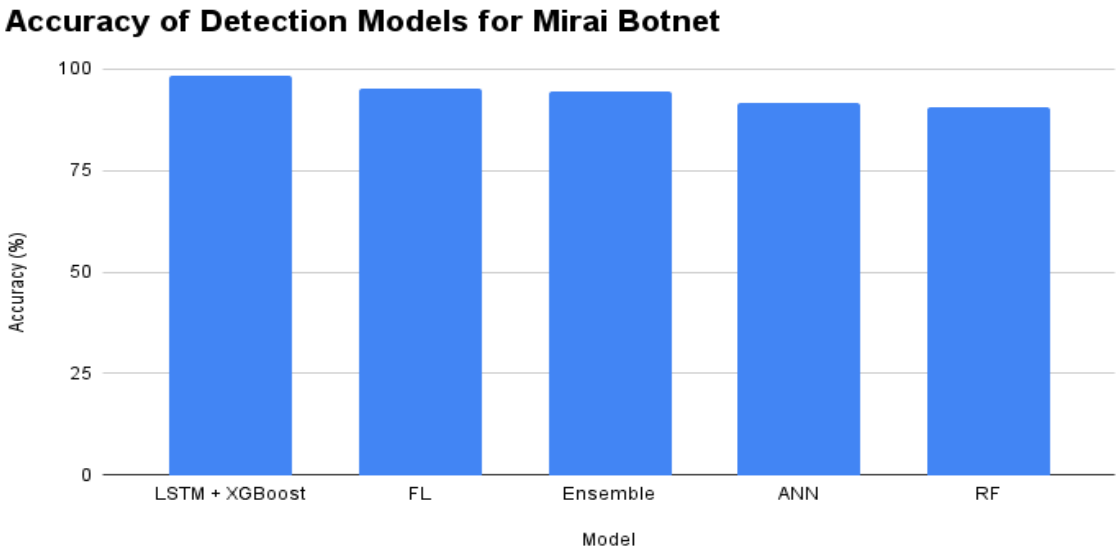

Figure 2. Comparative Accuracy of Selected Detection Models

3.2. Threat Intelligence Platform Comparison

Threat intelligence feeds play a crucial role in enhancing the responsiveness of detection technioques. Table 4 compares three widely referenced platforms in the reviewed literature.

Table 4. Comparison of Threat Intelligence Platforms

Platform	Open Source	Real-Time IoCs	API Access
AlienVault OTX	Yes	Yes	Public
Recorded Future	No (Commercial, no open SDK)	Yes	Paid
CrowdStrike	No (Enterprise-only access)	Yes	Paid

Overall, the results support that multi-source threat intelligence-driven detection method is viable, and call for future efforts to bridge the gap between academic proposals and deployable cybersecurity solutions for IoT environments.

4. CONCLUSION AND FUTURE DIRECTIONS

Numerous threat detection techniques exist as reflected in this review. This review has also showcased the advancements in adopting AI techniques for Mirai detection. However, challenges of real-time adaptability and multi-platform integration remain unresolved, making the inspiration of developing a Mirai detection technique through integrating multi-threat intelligence an undeniably brilliant idea at this time. Future research should focus on developing scalable frameworks that dynamically incorporate IoCs from multiple threat intelligence platforms.

REFERENCES

[1] M. G. Karthik and M. B. M. Krishnan, "Securing an Internet of Things from Distributed Denial of Service and Mirai Botnet Attacks Using a Novel Hybrid Detection and Mitigation Mechanism," *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 1, pp. 113–123, 2021, doi: 10.22266/IJIES2021.0228.12.

[2] N. Widiyasono, I. A. D. Giriantari, M. Sudarma, and L. Linawati, "Detection of Mirai Malware Attacks in IoT Environments Using Random Forest Algorithms," *TEM Journal*, vol. 10, no. 3, pp. 1209–1219, 2021, doi: 10.18421/TEM103-27.

[3] T. G. Palla and S. Tayeb, "Intelligent mirai malware detection for iot nodes," *Electronics (Switzerland)*, vol. 10, no. 11, 2021, doi: 10.3390/electronics10111241.

[4] L. Karimli, "Cloud Risks and Solutions Review," *SSRN Electronic Journal*, Dec. 2023, doi: 10.2139/SSRN.4665811.

[5] V. Vajrobol, B. B. Gupta, A. Gaurav, and H.-M. Chuang, "Adversarial learning for Mirai botnet detection based on long short-term memory and XGBoost," *International Journal of Cognitive Computing in Engineering*, vol. 5, pp. 153–160, 2024, doi: 10.1016/j.ijcce.2024.02.004.
[6] A. Rahmatulloh, G. M. Ramadhan, I. Darmawan, N. Widiyasono, and D. Pramesti, "Identification of Mirai Botnet in IoT Environment through Denial-of-Service Attacks for Early Warning System," *International Journal on Informatics Visualization*, vol. 6, no. 3, pp. 623–628, 2022, doi: 10.30630/joiv.6.3.1262.
[7] E. Y. Güven and Z. Gürkaş-Aydin, "Mirai botnet attack detection in low-scale network traffic," *Intelligent Automation and Soft Computing*, vol. 37, no. 1, pp. 419–437, 2023, doi: 10.32604/iasc.2023.038043.
[8] "LevelBlue - Open Threat Exchange." Accessed: May 18, 2024. [Online]. Available: https://otx.alienvault.com/
[9] "What are Threat Intelligence Feeds?" Accessed: May 18, 2024. [Online]. Available: https://www.recordedfuture.com/threat-intelligence-101/intelligence-sources-collection/threat-intelligence-feeds
[10] A. Affinito, S. Zinno, G. Stanco, A. Botta, and G. Ventre, "The evolution of Mirai botnet scans over a six-year period," *Journal of Information Security and Applications*, vol. 79, 2023, doi: 10.1016/j.jisa.2023.103629.
[11] M. Abu-Zanona, "Efficient IoT Security: Weighted Voting for BASHLITE and Mirai Attack Detection," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 12, pp. 925–933, 2023, doi: 10.14569/IJACSA.2023.0141293.
[12] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," Mar. 29, 2021, *BMJ Publishing Group*. doi: 10.1136/bmj.n71.
[13] A. M. Methley, S. Campbell, C. Chew-Graham, R. McNally, and S. Cheraghi-Sohi, "PICO, PICOS and SPIDER: a comparison study of specificity and sensitivity in three search tools for qualitative systematic reviews," *BMC Health Serv Res*, vol. 14, no. 1, 2014, doi: 10.1186/S12913-014-0579-0.
[14] "HubMeta – Systematic Review and Meta Analysis Cloud Platform." Accessed: May 18, 2024. [Online]. Available: https://hubmeta.com/
[15] A. R. Ramtin, P. Nain, D. S. Menasche, D. Towsley, and E. de Souza e Silva, "Fundamental scaling laws of covert DDoS attacks," *Performance Evaluation*, vol. 151, 2021, doi: 10.1016/j.peva.2021.102236.
[16] X. Sáez-de-Cámara, J. L. Flores, C. Arellano, A. Urbieta, and U. Zurutuza, "Clustered federated learning architecture for network anomaly detection in large scale heterogeneous IoT networks," *Comput Secur*, vol. 131, 2023, doi: 10.1016/j.cose.2023.103299.
[17] Z. Shao, S. Yuan, and Y. Wang, "Adaptive online learning for IoT botnet detection," *Inf Sci (N Y)*, vol. 574, pp. 84–95, 2021, doi: 10.1016/j.ins.2021.05.076.
[18] C. Eichler, J. Röckl, B. Jung, R. Schlenk, T. Müller, and T. Hönig, "Profiling with trust: system monitoring from trusted execution environments," *Design Automation for Embedded Systems*, vol. 28, no. 1, pp. 23–44, 2024, doi: 10.1007/s10617-024-09283-1.
[19] Y. Park, S. Choi, U. Y. Choi, H. Jin, N. H. M. Nor, and Y. Park, "A practical approach for finding anti-debugging routines in the Arm-Linux using hardware tracing," *Sci Rep*, vol. 14, no. 1, 2024, doi: 10.1038/s41598-024-65374-w.
[20] S.-Y. Hwang and J.-N. Kim, "A malware distribution simulator for the verification of network threat prevention tools," *Sensors*, vol. 21, no. 21, 2021, doi: 10.3390/s21216983.
[21] N. Widiyasono, I. A. D. Giriantari, M. Sudarma, and L. Linawati, "Detection of Mirai Malware Attacks in IoT Environments Using Random Forest Algorithms," *TEM Journal*, vol. 10, no. 3, pp. 1209–1219, 2021, doi: 10.18421/TEM103-27.
[22] A. Blaise, M. Bouet, V. Conan, and S. Secci, "Detection of zero-day attacks: An unsupervised port-based approach," *Computer Networks*, vol. 180, 2020, doi: 10.1016/j.comnet.2020.107391.
[23] X. Saez-De-Camara, J. L. Flores, C. Arellano, A. Urbieta, and U. Zurutuza, "Gotham Testbed: A Reproducible IoT Testbed for Security Experiments and Dataset Generation," *IEEE Trans Dependable Secure Comput*, vol. 21, no. 1, pp. 186–203, 2024, doi: 10.1109/TDSC.2023.3247166.
[24] S. S. B. Subrahmanyam, P. Goutham, V. K. R. Ambati, C. V Bijitha, and H. V Nath, "A hybrid method for analysis and detection of malicious executables in IoT network," *Comput Secur*, vol. 132, 2023, doi: 10.1016/j.cose.2023.103339.
[25] F. K. Örs and A. Levi, "Data driven intrusion detection for 6LoWPAN based IoT systems," *Ad Hoc Networks*, vol. 143, 2023, doi: 10.1016/j.adhoc.2023.103120.
[26] E. Y. Güven and Z. Gürkaş-Aydin, "Mirai botnet attack detection in low-scale network traffic," *Intelligent Automation and Soft Computing*, vol. 37, no. 1, pp. 419–437, 2023, doi: 10.32604/iasc.2023.038043.
[27] A. Febro, H. Xiao, J. Spring, and B. Christianson, "Edge security for SIP-enabled IoT devices with P4," *Computer Networks*, vol. 203, 2022, doi: 10.1016/j.comnet.2021.108698.
[28] A. Shalaginov and M. A. Azad, "Securing resource-constrained iot nodes: Towards intelligent microcontroller-based attack detection in distributed smart applications," *Future Internet*, vol. 13, no. 11, 2021, doi: 10.3390/fi13110272.
[29] M. Amru *et al.*, "Network intrusion detection system by applying ensemble model for smart home," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 3, pp. 3485–3494, 2024, doi: 10.11591/ijece.v14i3.pp3485-3494.
[30] T. G. Palla and S. Tayeb, "Intelligent mirai malware detection for iot nodes," *Electronics (Switzerland)*, vol. 10, no. 11, 2021, doi: 10.3390/electronics10111241.

[31] S. M. Sajjad *et al.*, "Detection and Blockchain-Based Collaborative Mitigation of Internet of Things Botnets," *Wirel Commun Mob Comput*, vol. 2022, 2022, doi: 10.1155/2022/1194899.

[32] A. A. Alsulami, Q. Abu Al-Haija, A. Tayeb, and A. Alqahtani, "An Intrusion Detection and Classification System for IoT Traffic with Improved Data Engineering," *Applied Sciences (Switzerland)*, vol. 12, no. 23, 2022, doi: 10.3390/app122312336.

[33] A. Woodiss-Field, M. N. Johnstone, and P. Haskell-Dowland, "Examination of Traditional Botnet Detection on IoT-Based Bots," *Sensors*, vol. 24, no. 3, 2024, doi: 10.3390/s24031027.

[34] K. O. Chee, M. Ge, G. Bai, and D. D. Kim, "IoTSecSim: A framework for modelling and simulation of security in Internet of things," *Comput Secur*, vol. 136, 2024, doi: 10.1016/j.cose.2023.103534.

[35] P.-H. Thevenon *et al.*, "iMRC: Integrated Monitoring & Recovery Component, a Solution to Guarantee the Security of Embedded Systems," *Journal of Internet Services and Information Security*, vol. 12, no. 2, pp. 70–94, 2022, doi: 10.22667/JISIS.2022.05.31.070.

[36] V. Vajrobol, B. B. Gupta, A. Gaurav, and H.-M. Chuang, "Adversarial learning for Mirai botnet detection based on long short-term memory and XGBoost," *International Journal of Cognitive Computing in Engineering*, vol. 5, pp. 153–160, 2024, doi: 10.1016/j.ijcce.2024.02.004.

[37] M. G. Karthik and M. B. M. Krishnan, "Securing an Internet of Things from Distributed Denial of Service and Mirai Botnet Attacks Using a Novel Hybrid Detection and Mitigation Mechanism," *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 1, pp. 113–123, 2021, doi: 10.22266/IJIES2021.0228.12.

[38] S. Lee, H. Jeon, G. Park, and J. Youn, "Design of automation environment for analyzing various iot malware," *Tehnicki Vjesnik*, vol. 28, no. 3, pp. 827–835, 2021, doi: 10.17559/TV-20210202131602.

[39] J. Wang *et al.*, "IoT-Praetor: Undesired Behaviors Detection for IoT Devices," *IEEE Internet Things J*, vol. 8, no. 2, pp. 927–940, 2021, doi: 10.1109/JIOT.2020.3010023.

[40] T. A. Ahanger, A. Aldaej, M. Atiquzzaman, I. Ullah, and M. Y. Uddin, "Securing Consumer Internet of Things for Botnet Attacks: Deep Learning Approach," *Computers, Materials and Continua*, vol. 73, no. 2, pp. 3199–3217, 2022, doi: 10.32604/cmc.2022.027212.

[41] G. C. Swathi, G. K. Kumar, and A. P. S. Kumar, "Estimating Botnet Impact on IoT/IoE networks using Traffic flow Features," *Computers and Electrical Engineering*, vol. 102, 2022, doi: 10.1016/j.compeleceng.2022.108209.

[42] "AlienVault Open Threat Exchange." Accessed: May 19, 2024. [Online]. Available: https://github.com/AlienVault-OTX