International Journal of Computer Sciences and Engineering
Vol.14, Issue 1, pp.01-05, February 2026
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

IJCSE
ISSN: 2347-2693 (E)

Review Article

A Detection Techniques for Botnet Attacks in Internet of Things Networks: A Comprehensive Literature Review

Sudhanshu Angiras[1*], Sukhvir Singh [2], Krishan Kumar[3]

[1]University Institute of Engineering and Technology, Panjab University, Chandigarh, India (Orcid ID: https://orcid.org/0009-0009-2431-8404)
[2]University Institute of Engineering and Technology, Panjab University, Chandigarh, (Orcid ID: https://orcid.org/0000-0002-2081-9887)
[3]University Institute of Engineering and Technology, Panjab University, Chandigarh, (Orcid ID: https://orcid.org/0000-0001-9877-0238)

Email address: sukhvirpu@gmail.com (Sukhvir Singh), k.salujauiet@gmail.com (Krishan Kumar)

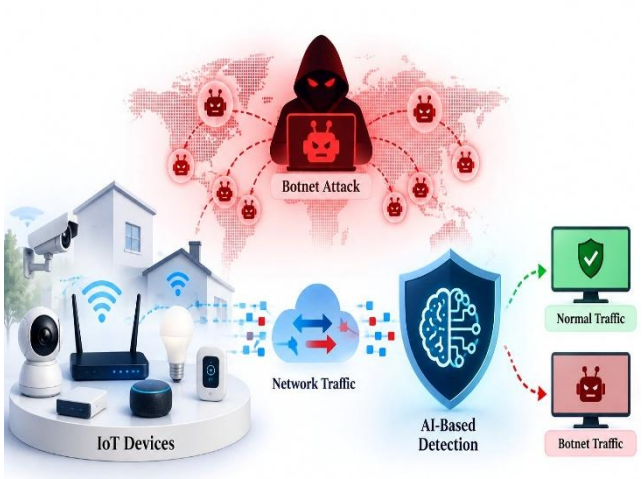
**Corresponding Author: sudhanshuangiras@gmail.com,*

Copyright © 2026 by author(s). This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited & its authors credited.

Abstract: The Botnet attacks are among the most common and dangerous cybersecurity threats in the Internet of Things (IoT) environments. This is because of the massive number of diverse, low-resource devices and weak security settings. Traditional botnet detection methods, such as signature-based and rule-based Intrusion Detection System (IDS), are still widely adopted, but they struggle to detect new botnet variants and unknown attacks. In recent years, Artificial Intelligence (AI) has improved the detection performance through identifying patterns in traffic behavior and features of network flows. This paper presents a comprehensive review of the IoT botnet detection approaches, which are classified as either a non-AI detection system (NAIDS-Botnet) or an AI detection system (AIDS-Botnet). It surveys recent studies and datasets and provides a comparative analysis of different approaches. The analysis shows that non-AI-based techniques typically achieve accuracies of 85% to 93%, while AI-based approaches generally report accuracies between 92% and 99%. It also discusses current challenges like data imbalance, lack of evaluation on real networks, concept drift, deployment issues, etc. Finally, the paper outlines the advantages of AI-based IDS and proposes future research directions.

Keywords: Botnet, IoT security, Intrusion Detection System (IDS), Machine Learning, Deep Learning, CNN, Anomaly Detection

Graphical Abstract-



1. Introduction

The Internet of Things has allowed many devices to be connected to each other in places such as hospitals and homes [1]. The IoT is also used in factories and cities. The IoT devices don't have much power to process information and aren't very good at protecting our information. This makes IoT devices very easy to get hacked and infected by a software. The IoT devices can also be used for creating groups of devices that can cause a lot of problems. IoT botnets are collections of compromised devices (bots) that are controlled by an attacker (botmaster) to carry out coordinated attacks, including distributed denial of service (DDoS), scanning, credential stuffing, spam distribution [3], and data exfiltration as shown in Fig. 1. The sheer volume and diversity of IoT traffic make botnet detection particularly challenging [13].

Artificial Intelligence (AI) has become a promising approach for modern cybersecurity because it can learn complex traffic behavior and detect unknown patterns more effectively than traditional mechanisms [26]. ML/DL-based IDS can outperform signature-based IDS when dealing with evolving

© 2026, IJCSE All Rights Reserved

botnet variants and zero-day behavior [3,5,17]. IoT bots can be grouped in ways based on how they are controlled and how they spread. Some IoT bots rely on one server that tells them what to do. On the other hand, some IoT bots work together and make decisions among themselves which makes it hard to stop them. Then there are IoT bots that use both of these methods [3]. IoT bot families, like the ones that are similar to Mirai, usually take advantage of bad passwords and open doors to spread quickly [14,26].

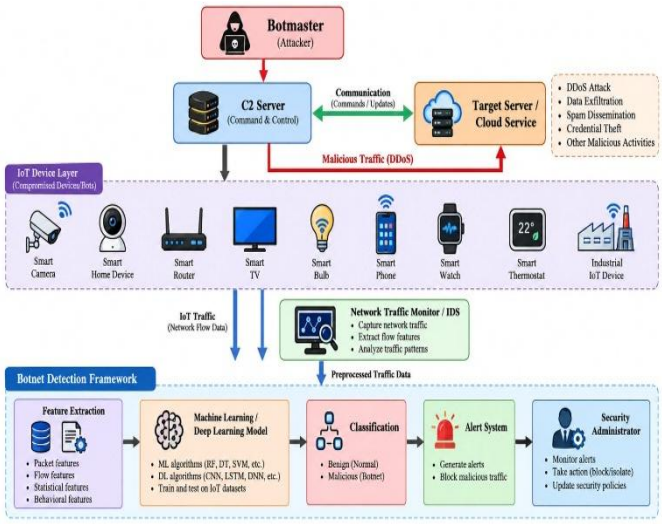


Figure 1: General Architecture of IoT Botnet and Detection Framework

Although numerous studies investigate botnet detection, many focus on a narrow subset of techniques or evaluate models only on controlled datasets [15]. This paper aims to support researchers designing lightweight and robust IoT botnet detection systems [21, 23].

1.1 Problem Statement of the Study

Botnet attacks usually involve scanning devices, trying to guess passwords, sending out software, talking to the people in charge, and flooding websites with too much traffic. To catch these botnet attacks, researchers look at how the internet traffic is moving, what is happening with the data, how the packets of data are behaving, and what the devices are doing. They have to check the traffic patterns, the flow features, the packet statistics and the behavioral indicators of the botnet attacks to figure out what is going on.

1.2 Objective of the Study

The key Objectives of this paper are:

i) To find new taxonomy for botnet detection techniques.

ii) To perform comparative analysis of datasets, techniques, and reported performance.

iii) To Identify open research challenges in real-world IoT environments.

1.3 Organization

This article is organized as follows: Section 1 introduces IoT botnet attacks and their detection. Section 2 presents the taxonomy of detection techniques. Section 3 discusses related work and comparative analysis. Section 4 describes the datasets used for IoT botnet detection. Section 5 identifies research gaps, Section 6 discusses open challenges, and Section 7 presents the conclusion and future research directions.

2. Taxonomy of Detection Techniques

In this review, the mechanism of detection techniques is categorized into two groups: Non-AI-Based Detection Systems (NAIDS) and AI-Based Detection Systems (AIDS). NAIDS relies on traditional methods such as signature-based, rule-based, and statistical detection techniques [12,20], whereas AIDS employs ML and DL algorithms to automatically detect malicious activities from network traffic.

These approaches are based on predefined rules or known attack patterns and are valued for their interpretability and low computational overhead as shown in Fig. 2.

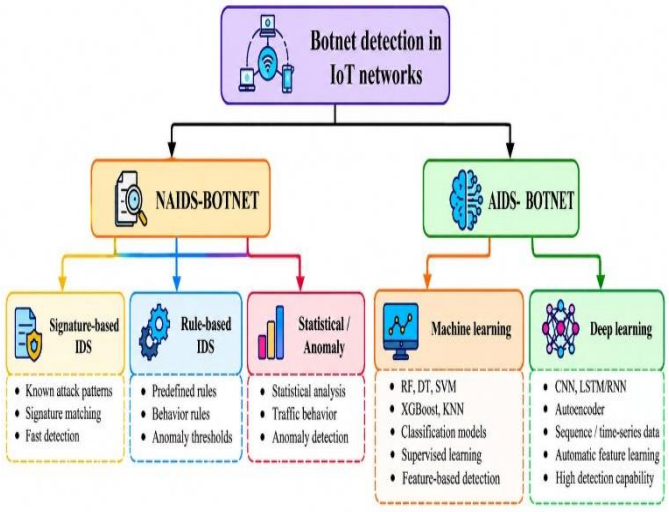


Figure 2: Proposed Taxonomy of IoT Botnet Detection Techniques.

AIDS approaches use machine learning classifiers such as Random Forest, Support Vector Machines [2,21], Decision Trees, and XGBoost. Deep learning architectures such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks [1,5,18], and autoencoders are also widely used to learn traffic patterns automatically and detect anomalous behavior in network flows [17,19].

© 20XX, IJCSE All Rights Reserved

3. Related Works

In recent years, researchers have proposed different techniques for detection of botnet attacks. Broadly these techniques may be divided into the following two categories:

3.1 NAIDS-BOTNET

Traditional intrusion detection systems are deployed in IoT networks because of interpretability and low computational cost. As discussed in section 2, these techniques are divided into the following three types:

i. Signature-based IDS
ii. Rule-based IDS
iii. Statistical/anomaly-based detection

Signature-based IDS can effectively detect known botnet patterns but have challenges in detecting unknown or polymorphic attacks [12]. Rule-based IDS offers customized detection rules and better alert generation when IoT-specific rules are implemented [3,27]. Statistical anomaly detection techniques create models of normal network behavior, but they are subject to false positives in dynamic IoT traffic environments [4]. In real-world deployments, honeypot-based approaches have been shown to be effective in capturing novel attack samples [27]. Modeling communication relationships between devices using graph-based detection has also been used for non-AI botnet classification with reasonable accuracy [28]. Domain Name System-based traffic analysis is a feasible non-AI approach for early botnet command\&control channel identification [25].

3.2 AIDS - BOTNET

AI based techniques are good in detecting malicious patterns in network traffic. As mentioned in the previous section, these techniques can be categorized into two:

a) ML-BASED
b) DL-BASED

A CNN-based intrusion detection system achieved an accuracy of 99.51% on IoT traffic datasets [1]. Machine learning algorithms, e.g., decision tree models and an optimized classification framework, have also been used for botnet detection in datasets such as BoT-IoT-2018[11]. More recently, ensemble-based ML frameworks based on the UNSW-NB15 dataset reported a test accuracy of up to 97.94% [2,5]. Federated learning has been proposed [25] as a privacy-preserving approach for distributed IoT botnet detection, where multiple devices can collaboratively train a shared model without disclosing raw traffic data. Lightweight transformer-based models have been explored for IoT edge environments, which provide high detection accuracy with reduced inference latency. Additionally, Explainable AI (XAI) techniques such as Shapley Additive explanations (SHAP) and Local Interpretable Model-agnostic Explanations (LIME) are increasingly being incorporated into the botnet detection pipeline to help network administrators interpret the decisions of black-box ML models [26].

The main steps of AIDS-Botnet are mentioned in Algorithm 1 written below:

Algorithm 1: AIDS-Botnet Detection Framework

Input: Network traffic data
Output: Classification labels and detection alerts

Step 1: Capture network traffic from IoT devices.
Step 2: Extract relevant network traffic features.
Step 3: Pre-process the extracted features.
Step 4: Apply the trained model to predict the class of each sample (x).
Step 5: If (x) is classified as malicious:
i. Generate a botnet detection alert.
ii. Notify the security administrator.
iii. Investigate the detected traffic.
Step 6: If mitigation is authorized and appropriate,
i) block or isolate the malicious traffic.
Otherwise:
i. Label (x) as benign.
ii. Continue network monitoring.
Step 7: Repeat the process for each traffic sample.
Step 8: Return classification labels and alerts.

3.3 COMPARATIVE ANALYSIS

Key studies on botnet detection techniques, including the datasets used, algorithms applied, and accuracy, are summarized in table 1 and table 2.

Table 1: Comparative Analysis of Relevant NAIDS-Based Botnet Detection Techniques

Reference/Year	Dataset	Technique	Accuracy
Al-Haija et al. [27] (2025)	Honeypot Logs	Traffic Monitoring	~93% detection rate
Zheng et al. [28] (2025)	IoT Graph	Graph-Based Analysis	~90% classification
Kaleem et al. [25] (2025)	DNS Traffic	DNS Behavior Analysis	~88% detection
Mumtaz et al. (2024)	IoT Network	Rule-Based IDS	85–90% detection rate
Dutta et al. (2020)	IoT Data	Statistical Analysis	~88% accuracy
M. Egele et al. (2012)	IoT Executables	Opcode Matching	~85% accuracy
G. Gu et al. (2008)	IoT Dataset	Rule + Signature-Based	~91% accuracy
A. Karasaridis et al. (2007)	IoT Executables	Graph-Based Analysis	~92% classification accuracy

© 20XX, IJCSE All Rights Reserved

D. Moore et al. (2005)	NetFlow Data	Threshold-Based Detection	~83% accuracy
U. Bayer et al. (2006)	IoT Malware	Sandbox Behavior	~87% detection rate
L. Spitzner (2003)	IoT Honeypot	Traffic Monitoring	~90% detection rate
L. Feinstein et al. (2003)	DNS Logs	Statistical Entropy	~89% anomaly detection
M. Roesch [12] (1999)	Live Traffic	Signature-Based IDS	~95% (known attacks)

Table 2: Comparative Analysis of Relevant AIDS-Based Botnet Detection Techniques

Reference/Year	Dataset	Technique	Accuracy
Saied et al. [26] (2025)	IoT Dataset	Random Forest + XAI	High interpretability
Kaleem et al. [25] (2025)	Edge-IoT	Lightweight Transformer	98.6%
Mothukuri et al. [24] (2024)	IoT-Federated	Federated Learning	97.3%
Saba et al. [1] (2022)	IoT Traffic	CNN	99.51%
Alissa et al. (2022)	UNSW-NB15	Decision Tree	94%
Nguyen et al. (2022)	IoT Samples	Hybrid ML	98.1%
Pokhrel et al. (2021)	BoT-IoT	KNN, MLP	92.1%
Injadat et al. (2020)	BoT-IoT	ML Optimization	High accuracy
Hammoudeh et al. (2020)	UNSW-NB15	GRU	99.59%
Sriram et al. [ref5, ref9] (2019)	Network Flow	Deep Learning	Improved detection
Anthi et al. (2019)	Smart Home	Decision Tree	96.2%
Kumar et al. (2019)	P2P Dataset	XGBoost	99.88%
Doshi et al. (2018)	IoT Dataset	Random Forest	99.8%

From Table 2, it is clearly observed that the AIDS botnet technique has higher accuracy as compared to the NAIDS botnet. It involves less feature learning and pattern recognition using AI techniques.

4. Datasets Used in IoT Botnet Detection

Reliable and representative datasets are the backbone of any intrusion detection study. Several publicly available datasets have been widely adopted by the research community. The BoT-IoT dataset was built in a realistic IoT network testbed and contains labeled traffic from DDoS, DoS, reconnaissance, and information theft attacks [11]. The UNSW-NB15 dataset provides a blend of real modern normal activities and synthetic attack behavior generated by the IXIA Perfect Storm tool, covering nine attack families including Backdoors, DoS, Exploits, and Worms [29]. The IoT-23 dataset consists of labeled network traffic from 23 different IoT malware captures along with benign traffic, making it suitable for multiclass botnet classification [30]. The N-BaIoT dataset was constructed by capturing traffic from nine commercial IoT devices infected with real botnet malware (Mirai and BASHLITE), offering device-specific behavioral signatures [17]. The TON_IoT dataset covers telemetry data from IoT and industrial IoT sensors and supports both binary and multiclass detection tasks [13]. NetFlow-based datasets Provide a standardized feature format that makes cross-dataset comparisons more reliable [15].

Table 3: Summary of Commonly Used IoT Botnet Datasets.

Dataset	Year	Attack Types	Notable Feature
IoT-23 [30]	2020	20+ botnet families	Multi-device captures
TON_IoT [13]	2020	Multi-protocol attacks	IoT telemetry included
NetFlow DS [15]	2020	Multi-class	Standardised flow features
BoT-IoT [11]	2019	DDoS, DoS, Recon, Theft	Realistic IoT testbed
N-BaIoT [17]	2018	Mirai, BASHLITE	Device-level behaviour
UNSW-NB15 [29]	2015	9 attack families	Hybrid real + synthetic

5. Identified Gaps in Existing Approaches

The gaps are identified and summarized as follows:

5.1 NAIDS - BOTNET

a) Simple Design

Nevertheless, many real deployments still rely on NAIDS approaches such as signature-based and rule-based IDS due to their simplicity. However, they are always challenged by polymorphic or unseen botnet variants, which expose the network to zero-day attacks [12,20].

© 20XX, IJCSE All Rights Reserved

b) Class Imbalance

Few studies address the class imbalance issue in a rigorous way, as many datasets have many more benign samples than attack samples, and techniques such as Synthetic Minority Over-sampling Technique (SMOTE) or class-weighted loss functions are used inconsistently in the literature [15,21].

5.2 AIDS - BOTNET

a) Controlled Dataset

Most AI-based models are evaluated on a single dataset in a controlled laboratory setting, and their performance in real, noisy IoT environments is largely unknown [15,21].

b) Accuracy

A model scoring over 99\% accuracy may perform differently when deployed in real-world IoT environments with diverse devices, heterogeneous traffic, and changing network conditions.

c) Computational overhead

Deep learning models such as Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN) have high computational overhead, making it difficult to directly deploy them on resource-limited IoT edge devices, and lightweight or distilled alternatives are just beginning to be studied [18,23].

d) Less Explainability

Existing AI-based detection frameworks lack explainability to a large extent. This is important because the network administrators need to understand and trust the model's decisions before acting upon an alert. Filling these gaps is critical to advance botnet detection research from controlled benchmarks to real-world IoT deployments [16].

6. Open Challenges in Botnet Attack Detection

There is good progress in botnet detection research, but still several technical and practical issues prevent reliable deployment of intrusion detection systems in real-world IoT environments. These challenges arise from the dynamic, heterogeneous, and resource-constrained nature of IoT systems.

i. Dataset imbalance and Bias:

Many IDS datasets are class-imbalanced, affecting model reliability. The attack traffic often constitutes a small percentage of total samples, causing the models to be biased toward the majority class. Although methods such as SMOTE are used for over-sampling, their performance is different for different attack types and network topology. A promising direction is to explore the use of Generative Adversarial Networks (GANs) to synthesize realistic botnet traffic from the minority class, to achieve more balanced training sets [15,21].

ii. Lack of real-network evaluation:

Lab datasets may not train models that generalize to noisy and encrypted traffic. Future work should invest in testbeds that simulate real-world conditions, including legitimate background traffic, encrypted HTTPS/TLS flows, and device-level behavioral variance. Multi-organization federated evaluation frameworks can provide a more realistic performance benchmark [24].

iii. Concept drift:

Botnet behavior is dynamic, so static models are less effective. Online and incremental learning techniques can be used to deal with this problem, where the models are continuously updated when new traffic patterns emerge. ML pipelines can be integrated with drift detection algorithms such as Adaptive Windowing (ADWIN) or Drift Detection Method (DDM) that trigger retraining when significant behavioural shifts are detected [21].

iv. Resource constraints:

DL models require large amounts of computational resources and memory that cannot be directly deployed on IoT endpoints. Some directions of ongoing research that would bring detection capabilities to the edge with minimal loss of accuracy include model compression techniques such as pruning, quantization, and knowledge distillation [23,25].

v. Lack of explainability:

Most high-performing botnet detection models are treated as black boxes, reducing trust and adoption by security practitioners. One promising research direction is the integration of XAI frameworks, such as SHAP, LIME, or attention visualization, into detection pipelines. These approaches could help bridge the gap between detection performance and operational transparency [16,26].

vi. Zero-day and polymorphic attacks:

Signature- and rule-based systems are inherently unable to detect attacks they have not seen before. In this context, anomaly-based detection with unsupervised models such as autoencoders or isolation forests shows promise, but these methods tend to generate higher false-positive rates that need to be controlled in practice [12,17,19].

vii. Multi-protocol and heterogeneous IoT environments:

IoT networks use dozens of protocols, including MQTT, CoAP, Zigbee, and Z-Wave. Detection models trained on the traffic characteristics of one protocol often do not work effectively for

© 20XX, IJCSE All Rights Reserved

another. Therefore, there is a need for protocol-agnostic feature extraction strategies and multi-protocol datasets [13,21].

7. Conclusion

Botnet attacks are one of the biggest concerns in IoT networks because of the large number of connected devices and their inherent security limitations. In this review, various techniques of botnet attack detection have been discussed based on recent research findings using both AIDS and NAIDS-based approaches. Machine learning and deep learning techniques—including Random Forest, Decision Tree, SVM, and CNN—have shown high accuracy on datasets such as BoT-IoT, IoT-23, and UNSW-NB15, with several studies reporting detection rates above 97% [1,5,9,17]. Emerging techniques such as federated learning and lightweight transformer models are further pushing the boundaries of what is achievable under real-world constraints [24,25]. Deep autoencoder-based approaches provide unsupervised detection capability that is particularly useful when labelled data is scarce [17,19].

However, these techniques come with a disadvantage in terms of high computational resource requirements and the need for large volumes of training data [22,23]. NAIDS-based techniques such as signature-based IDS, rule-based systems, and statistical anomaly detection remain viable in many practical situations because they are generally faster to deploy, less computationally intensive, and easier to audit [12,20].

Benefits of AIDS—BOTNET

i) Learn Behavior

AIDS botnet detection systems have various advantages over traditional signature-based and rule-based intrusion detection mechanisms. One of the big advantages is that they can detect unknown or zero-day attacks since they learn behavioral patterns from network traffic rather than just signatures.

ii) Modeling Capabilities

Machine learning and deep learning models can automatically extract complex and high-dimensional features from flow-level and packet-level data, which alleviates the need for manual feature engineering. Specifically, deep learning architectures, including CNNs, RNNs, and autoencoders, are capable of modeling nonlinear relations and temporal dependencies in IoT traffic for improved detection performance [5,9].

iii) Scalability

Another important benefit of AIDS approaches is scalability. IoT environments generate huge amounts of heterogeneous data. AI models are able to deal with large-scale data efficiently when trained. AIDS detection frameworks typically attain higher accuracy, lower false negative rates, and better generalization on different datasets [1,5].

The major benefits can be summarized as follows:

1. Learning behaviour to improve detection of unknown attacks.
2. Ability to model complicated patterns in large network flows.
3. Less dependence on hand-coded rules.
4. Automatic feature learning ability in DL architectures such as CNN and LSTM [1,5].

On the whole, the comparative analysis suggests that both families of methods have a role in IoT security. While AIDS methods offer greater adaptability and detection strength, traditional methods provide greater efficiency and simplicity. A hybrid approach combining intelligent learning models with rule-based validation is likely to offer the most robust solution for securing modern IoT systems from botnet attacks [20,21].

Future Research Directions

Looking ahead, several open problems deserve focused attention from the research community.

AIDS Future Directions:

a) *Federated and Privacy-Preserving Detection:* As IoT deployments scale across multiple organizations, sharing raw traffic data becomes legally and practically difficult. Future work should extend federated learning frameworks to support heterogeneous, non-IID IoT traffic distributions [24].
b) *Continual and Online Learning:* Botnets continuously evolve to evade detection. Systems that update model parameters incrementally as new attack behaviors emerge are a critical research need [19,21].
c) *Explainable and Trustworthy AI:* Developing XAI techniques tailored specifically for network intrusion detection, where explanations are actionable for network administrators, is an important step toward operational adoption [16,26].
d) *Graph Neural Networks for Botnet Topology Analysis:* The communication graph formed by a botnet has distinctive structural properties. GNNs offer a natural representation for modelling device-to-device interactions that flow-level features may miss [28].
e) *Lightweight Edge-Deployable Models:* Knowledge distillation and model pruning should be applied to high-accuracy DL models so that effective detection can run on resource-constrained IoT gateways [23,25].

Real-World Applications:

a) *Smart Healthcare:* Medical IoT devices such as remote patient monitors and infusion pumps are prime botnet

© 20XX, IJCSE All Rights Reserved

targets. Lightweight detection systems can protect patient safety and data integrity in life-critical environments [21].

b) *Industrial IoT and Critical Infrastructure:* Factories, power grids, and water treatment plants rely on IoT sensors. Botnet-driven attacks on these systems can cause physical damage. Context-aware detection models that understand industrial protocols such as MODBUS and OPC-UA are needed [15].

c) *Smart Cities:* Traffic management systems, smart grids, and public surveillance networks can be compromised by botnets. Distributed, city-scale detection infrastructure that aggregates alerts from multiple network segments while preserving citizen privacy is an important applied research direction [14,20].

d) *Autonomous Vehicles and Vehicular Networks:* Connected vehicles communicate over Dedicated Short-Range Communications (DSRC) and Cellular Vehicle-to-Everything (C-V2X) protocols. Ensuring that vehicular IoT networks remain free of botnet infections is critical for road safety [21,22].

In summary, the field of IoT botnet detection has matured considerably, but a gap remains between laboratory performance and real-world deployment. Bridging this gap will require interdisciplinary collaboration between machine learning researchers, network security engineers, and IoT system designers.

Author's statements

Acknowledgements: The authors are grateful to the reviewers for their valuable comments and suggestions, which helped improve the manuscript.

Funding Source- None.

Authors' Contributions- Author1 contributed to the literature review, analysis of existing IoT botnet detection techniques and comparative analysis. Author2 provided academic guidance, reviewed the manuscript, and contributed to its improvement. Author3 reviewed the manuscript and provided the inputs on its structure. All authors reviewed and approved the final manuscript.

Conflict of Interest- The authors declare that they have no conflict of interest.

Data Availability- No new datasets were generated or analysed in this review article. The publicly available datasets discussed in the manuscript are cited in the references.

References

[1] T. Saba, A. Rehman, A. Alkhayyat, and M. R. Islam, "Anomaly-based intrusion detection system for IoT networks through deep learning model," Computers & Electrical Engineering, vol. 99, Art. no. 107810, 2022.

[2] M. N. Injadat, A. Moubayed, and A. Shami, "Detecting Botnet Attacks in IoT Environments: An Optimized Machine Learning Approach," in Proc. IEEE International Conference on Microelectronics (ICM), 2020, pp. 1–4.

[3] S. L. Mumtaz, M. Ahmed, and S. Hassan, "Detection of Botnet in the IoT Network," ITM Web of Conferences, vol. 63, Art. no. 01007, 2024.

[4] V. Dutta, M. Choras, M. Pawlicki, and R. Kozik, "Detection of Cyberattack Traces in IoT Data," Journal of Universal Computer Science, vol. 26, no. 11, pp. 1422–1434, 2020.

[5] S. Sriram, R. Vinayakumar, M. Alazab, and K. P. Soman, "Network Flow Based IoT Botnet Attack Detection Using Deep Learning," in Proc. IEEE Conference on Advances in Computing, 2019, pp. 1–6.

[6] A. Saied, R. E. Overill, and T. Radzik, "Detection of Known and Unknown Botnet Commands Using Machine Learning," IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 5, pp. 1108–1121, 2020.

[7] E. Anthi, L. Williams, M. Burnap, and P. J. Edwards, "A Supervised Intrusion Detection System for Smart Home IoT Devices," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9042–9053, 2019.

[8] S. Pokhrel, M. Mohammadi, and H. A. Khattak, "Machine Learning Based Botnet Detection in IoT Networks Using BoT-IoT Dataset," Future Generation Computer Systems, vol. 122, pp. 45–56, 2021.

[9] M. Hammoudeh, A. Aldwairi, and M. Alenezi, "Deep Learning-Based Detection of IoT Botnet Attacks," IEEE Access, vol. 8, pp. 15652–15663, 2020.

[10] R. Doshi, N. Apthorpe, and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," in Proc. IEEE Security and Privacy Workshops (SPW), 2018, pp. 29–35.

[11] N. Moustafa and J. Slay, "The BoT-IoT Dataset: A New Dataset for IoT Network Intrusion Detection," IEEE Access, vol. 7, pp. 78593–78603, 2019.

[12] M. Roesch, "Snort—Lightweight Intrusion Detection for Networks," in Proc. USENIX LISA '99, 1999, pp. 229–238.

[13] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems," IEEE Access, vol. 8, pp. 165130–165150, 2020.

[14] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran et al., "Understanding the Mirai Botnet," in Proc. USENIX Security Symposium, 2017, pp. 1093–1110.

[15] M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann, "NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems," in Big Data Technologies and Applications, Springer, 2020, pp. 117–135.

[16] S. Ali, T. Abuhmed, S. El-Sappagh, K. Muhammad, J. M. Alonso-Moral, R. Confalonieri, R. Guidotti, A. Del Ser, N. Díaz-Rodríguez, and F. Herrera, "Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence," Information Fusion, vol. 99, Art. no. 101805, 2023.

[17] 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.

[18] A. Diro and N. Chilamkurti, "Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things," Future Generation Computer Systems, vol. 82, pp. 761–768, 2018.

[19] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection," in Proc. Network and Distributed System Security Symposium (NDSS), 2018.

[20] H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, "A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets," arXiv preprint arXiv:1806.03517, 2018.

[21] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646–1685, 2020.

[22] K. Sethi, R. Kumar, N. Prajapati, and P. Bera, "Deep Reinforcement Learning Based Intrusion Detection System for Cloud Infrastructure,"

© 20XX, IJCSE All Rights Reserved

in Proc. IEEE International Conference on Communications (ICC), 2020, pp. 1–6.
[23] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do They Differ From Traditional IT Security Solutions?" IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41–49, 2018.
[24] V. K. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A Survey on Security and Privacy of Federated Learning," Future Generation Computer Systems, vol. 115, pp. 619–640, 2021.
[25] H. Kaleem, A. Lim, and T. Baker, "Lightweight Transformer-Based Intrusion Detection for Resource-Constrained IoT Edge Nodes," IEEE Internet of Things Journal, vol. 12, no. 4, pp. 3210–3224, 2025.
[26] A. Saied, M. Kaleem, and N. Al-Haija, "Explainable AI-Driven Botnet Detection Using SHAP-Augmented Random Forest for IoT Traffic," IEEE Access, vol. 13, pp. 12034–12049, 2025.
[27] Q. A. Al-Haija and M. Al-Shua'ibi, "Honeypot-Driven IoT Botnet Traffic Capture and Non-AI Rule-Based Classification," Computers & Security, vol. 148, Art. no. 103972, 2025.
[28] Y. Zheng, L. Wu, and Z. Chen, "Graph-Based Non-AI Detection of Botnet Communication Topology in IoT Networks," Journal of Network and Computer Applications, vol. 228, Art. no. 103892, 2025.
[29] N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data set for Network Intrusion Detection Systems," in Proc. Military Communications and Information Systems Conference (MilCIS), 2015, pp. 1–6.
[30] S. Garcia, M. Parmisano, and M. J. Erquiaga, "IoT-23: A Labeled Dataset with Malicious and Benign IoT Network Traffic," Zenodo, 2020. doi: 10.5281/zenodo.4743746.

AUTHORS PROFILE

Mr. Sudhanshu Angiras is a student of Masters of Information Technology in University Institute of Engineering and Technology, Panjab University, Chandigarh. His research interests include network security and artificial intelligence. He is currently working on detection techniques for Botnet detection.



Dr. Sukhvir Singh is an Assistant Professor in the Department of Information Technology at the University Institute of Engineering and Technology (UIET), Panjab University, Chandigarh, India. He holds a B.E. degree, an M.E. degree, and a Ph.D. His research interests include cybersecurity, artificial intelligence, wireless networks and emerging information technologies. His academic activities encompass teaching, research, and the advancement of information technology and cybersecurity.



Dr. Krishan Kumar is a Professor at the University Institute of Engineering and Technology (UIET), Panjab University, Chandigarh, India. He holds a B.E. degree, an M.E. degree, and a Ph.D. His academic and research interests include network security, cyber security, and emerging technologies. His professional activities encompass teaching, research, academic administration, and the promotion of innovation in engineering education.



© 20XX, IJCSE All Rights Reserved