International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/55 Volume 12, Issue 6, November – December (2025)

REVIEW ARTICLE

Machine Learning Approaches for IoT Botnet Detection and Mitigation: A Comprehensive Review

Vibhor Harit
Department of Computer Science and Engineering, Desh Bhagat University, Mandi Gobindgarh, Punjab, India.
✉ vibhordev@gmail.com

Rajeev Dahiya
Department of Computer Science and Engineering, Desh Bhagat University, Mandi Gobindgarh, Punjab, India.
raj8878@gmail.com

Umang Garg
School of Computer Science and Engineering, IILM University, Gurugram, Haryana, India.
umangarg@gmail.com

Received: 16 July 2025 / Revised: 01 November 2025 / Accepted: 25 November 2025 / Published: 30 December 2025

Abstract – The Internet of Things (IoT) has changed many industries including transport, industrial automation, and smart homes. IoT ecosystems are becoming more vulnerable to severe security risks due to this quick growth, especially botnet attacks that use weak equipment for malicious intentions such as distributed denial of services (DDoS), data violations, and illegal monitoring. This paper has a thorough review of the most recent developments in IoT Botnet Detection and Mitigation Techniques. The model that improves the explainable AI (XAI) - Driven model, as well as the model that improves the accuracy and transparency of detection, examines the signature-based, discrepancy-based, and DNS-based IDS. Major challenges are discussed, including device asymmetry, resource barriers, real-time detection demand, and developing an attack vector, which is discussed to highlight the complications in securing the IoT environment. In addition, this article outlines the role of machine learning, deep learning, and blockchain technologies in strengthening IoT defense, offering adaptive, scalable, and decentralized safety solutions. The study of the recent case of major IoT Botnet events is analyzed to portray practical implications and lessons learned. Light IDS models, privacy security, and IoT networks and equipment requirement in the equipment is one of the open research issues mentioned in the article mentioned in the article. By combining various approaches, this study provides practical information for researchers, developers, and safety professionals who are working to protect things from increasing threats to the Internet.

Index Terms – IoT, IoT Botnet, DDoS, Detection Technique, Privacy, Botnet Architecture.

1. INTRODUCTION

Through sensors, software, and other technologies, the Internet of Things' network of "things" connects to other systems and devices on the Internet. The IoT network should employ contemporary security methods to safeguard IoT organizations, companies, and individuals. Botnet-based DDoS attacks, in which hackers infect equipment with scripts, are the most dangerous security threats in the Internet of Things [1]. DDoS attacks use a large botnet to overwhelm a target network or server, preventing the intended users from accessing it. Companies are targeted by DDoS for political or personal reasons, or they may withdraw funds to stop the attack. The distributed architecture of botnets distinguishes them from building malware with different families. Botnets can hack millions of devices, just like a virus. A botnet's zombie nodes can collaborate and be controlled by a central server, unlike insects. The dispersed architecture of botnets prevents them from being categorized as other types of malware [2] [3]. The primary classification fields of the botnet, its exploitation strategy, its dissemination technique, and the attacker's actions are the topology of the utilized C & C infrastructure. The C&C server acts like the brain of the botnet, distributing malware to the bots, starting DDoS attacks, and performing harmful tasks, including more [4].

It is necessary to identify the C&C server to reduce botnet attacks. The ability of the bot to execute the command and successfully destroy the botnet ends by detecting and stopping the connectivity between them and the C&C server. This requires advanced methods, including machine learning-based anomalies, network traffic analysis, behavioral anomalies, C&C communication patterns, and the ability to separate them from real traffic. P2P botnet attacks should be detected and minimized using refined methods, including network traffic analysis, behavioral succession, and machine learning-based anomaly detection [5]. These methods analyze network traffic patterns and find the family of Botnets such as odd communication patterns, high traffic versions, unauthorized

REVIEW ARTICLE

behavior, and signatures. Finding and blocking known botnet domains or IP addresses, as well as cooperation with ISPs and other stakeholders, to block or carry botnet nodes, there are other ways to disrupt P2P botnets [6]. In addition to the possibility of physical injury and identity theft, many victims of botnets are unaware that their equipment is being used in this way.

1.1. Motivation

There are several factors that motivate us to work on the distinct methods utilized for the detection the IoT botnet.

Not taking any safety precautions: In the design and construction of many IoT devices, adequate safety measures are often neglected in favor of functionality costs. Weak or default passwords, frequent security updates, missing patches, and encryption of the device-transmitted or collected data are some of these [7]. Due to these safety flaws, botnet attackers can more easily compromise and control the IoT devices.

IoT device proliferation: IoT devices have spread quickly throughout homes and businesses, which has greatly increased the attack surface for botnet attackers. IoTs include billions of gadgets, including medical equipment, industrial control systems, smart home appliances, and more. Because there are so many and diverse vulnerabilities, hackers have a high chance of finding and exploiting weaknesses [8].

User Ignorance: Many users of IOT devices may be unaware of the potential security dangers associated with them and are unable to take proper safety measures. Because users are unable to upgrade firmware, install security updates, or change default passwords, their devices are vulnerable to botnet attacks [9]. The problem can be extended by the fact that some IOT devices may not have a user-friendly interface or security guidelines.

Older and Traditional equipment: Many older pieces of equipment can continue to work without security updates or manufacturer support, and IOT devices often have a long lifetime. These vintage and archaic equipment are particularly vulnerable to botnet attacks because they may be aware of the flaws that have not been patched or corrected, which makes them a simple goal for the attackers [10].

Low Resources: Some IoT devices may have adequate bandwidth, storage, or lack processing capacity, especially in low-cost applications or used in developing countries. This can be more challenging to implement strong security measures. In addition, IoT device manufacturers can overcome financial obstacles to invest in strong safety measures due to a lack of cost ideas or legal obligations.

IoT devices, user education and awareness, frequent updates and patches, and the design and construction of the safety of IoT devices in industry-wide standards and rules are all challenges that call for a versatile approach. These standards and rules include a guarantee of IoT device safety and are industry-wide standards and rules to protect against botnet attacks. The IoT botnet can be prevented using a variety of strategies. A botnet attacks a computer when users see a dangerous or attractive website that takes advantage of a software vulnerability or when bugs or viruses are installed. Maintaining the safety and integrity of the computer system, especially in susceptible settings for cyber-attack, requires many important processes to follow [11]. First and most important, periodic updates of operating systems are important as they patch known weaknesses and increase system stability. Users should avoid downloading attachments from suspicious or unknown emails, which are common vectors for malware and phishing attacks. Additionally, Peer-to-Peer (P2P) file sharing must be minimized or fully avoided, as it often exposes the system to rejected and potentially malicious files.

Similarly, clicking on suspicious or unknown web links should be avoided, as there may be downloads or phishing sites designed to steal sensitive information from such links. Installing iconic antivirus software is an indispensable layer of defence, providing real-time security against known malware and other dangers [12]. It is also important to create a strong, complex password and update it regularly to prevent unauthorized access. Regular systems can help identify security check weaknesses and unauthorized changes that may indicate a compromise. Awareness about third-party applications is important; Users should unknowingly install software from reliable sources to avoid installing malicious programs [13]. Network-level security, such as NIDS, is required to monitor traffic and detect potential intrusions. Rootkit detection tools can help uncover deeply embedded malware that traditional methods cannot detect. Additionally, network sniffers can be employed for traffic analysis to detect anomalies or suspicious activities on the network. Together, these measures form a robust defence strategy against a wide range of cybersecurity threats [14].

1.2. IoT Botnet Working

Botnets propagate by making use of zero-day weaknesses, P2P connections, phishing, Bitcoin networks, and lightning networks. Additionally, botnets propagate very quickly, have distinct attacks and vulnerabilities, a destructive nature, and substantial network flaws in the IoT network. Finally, as botnets are typically in a passive mode, they frequently lack traditional attack features and merely sustain the connection status via C&C channels [15]. Authors will describe the operation of the IoT botnet and the key detection techniques that have been applied to identify IoT botnet attacks. And we will emphasize the difficulties for the upcoming projects. There are distinct tools for IoT botnet:

"Bot: A 'zombified' or infected device that awaits orders from the master bot.

REVIEW ARTICLE

A "horde" of zombie computers, a network of bots, or a web of bots controlled by a master bot and used for either individual or collective goals.

The botmaster communicates with the bots under their control via the C&C channel.

Internet Relay Chat (IRC) is a widely used instant messaging service that offers one-to-one or one-to-many chat on several networks covering a variety of topics through distinct channels.

Three types of botnet structures can be distinguished: distributed, hybrid, and central. Client-server (C/s) mode is used by central structures, whereas non-central P2P mode is used by dispersed structures. By combining distributed and central structures, mixed structures improve the strength and efficiency of communication. Botnet control requires these structures [16]. The paper gives a thorough overview of how to use SVM and Random Forest algorithms for botnet attack analysis and detection to identify the disparity. This method improves network security by utilizing traffic quantities, packet flows, and communication patterns [17].

Supervised and unsupervised approaches detect anomalies using network traffic analysis. This is a new approach using supervised Machine Learning Algorithms, integrating decision tree and a multilayer classifier. The Anomalies Detection System (ADS) is tested and evaluated for accuracy and computing time [18]. Due to the increase in network attacks, which will highlight the vulnerability of all attacking devices, a search for machine learning (ML) has been developed as a possible solution to combat this problem. We would suggest an enhanced machine learning framework to identify botnet attacks on the Internet of Things devices by fusing the decision tree classification model with the bias optimization Gaussian process [19].

Botnets are a major safety concern since they employ complex control techniques and are always evolving globally. Hacking groups have created bots that can deploy malware, send unsolicited emails, handle remotely infected networks, and steal private information. Approximately 80 percent of all internet traffic is linked to botnet activities. The Domain Name Service (DNS) is used by botnets to obtain server IP addresses. This study uses machine learning methods to assess the effectiveness of the bonnet detection approach using DNS query data. Data from DNS queries can be monitored to identify malicious behavior [20].

Using command-and-control servers, botnets are sophisticated malware networks that operate under the supervision of botnets and cause enormous financial damage. Because of their adaptability, detection techniques like masking and community-based procedures are ineffective [21]. ML classification methods are perfect for identifying botnets and are useful for network security and intrusion detection. However, as the default versions could not be sufficient for the best performance, it is crucial to modify these models to guarantee their maximum capacity [22]. Due to the potential for data loss and illegal access to computer systems, networks, and equipment, internet security is crucial. Malware-infected computer networks, or botnets, are posing a serious cybersecurity threat. Botnets are an army of bots that are created and managed by botmasters using C & C channels [23]. Hacker-controlled gadgets known as "botnets" act as a foot soldier for their master. They represent a serious risk to data security, and botmasters are always honing their craft.

Emerging botnets are difficult for current detection techniques to handle [24]. The study used a unique machine learning technique to identify IoT botnet attacks, which use malware-infected connected devices. As more devices turn into possible botnets, this technique increases the accuracy of identifying and differentiating botnets, which is an essential component of computer security [25]. Because of their increasing quantity, IoT devices are susceptible to cyberattacks. Although high-dimensional data can cause performance problems, machine learning can identify these dangers. The effect of wrapper and hybrid feature selection methods on machine learning models for IoT botnet detection is assessed in this research [26]. IoT devices are becoming more susceptible to attacks, making standard IDS inadequate. The complexity and difficulties in gathering routine, everyday data make it difficult to apply the machine learning-based architecture for botnet attack detection, even if it has been developed [27].

By employing a discrepancy-based botnet detection system that uses IP headers to distinguish between Botnet DNS requests, the study aims to address the significant problem of protection against botnets, which can propagate like internet insects and participate in DDOS attacks [28]. As internet services rely more on them, privacy, availability, and integrity must be preserved. Machine learning, a foundational concept in botnet identification, attempts to lessen the impact of malicious activity [29].

1.3. IoT Botnet Life Cycle

A newly registered DDNS connection is sent out to the first bot in the network, which is set up by the botmaster, also known as the botherder, in accordance with the Botnet Lifecycle (Figure 1). They spread by doing this, attacking various targets with denial-of-service attacks [30]. The botnets gather data by using a technique known as "traffic sniffing." Is Traffic Sniffing Explained? Bluetooth connections, both functional and unworkable, are typically blamed for it. It observes while cornering a target into being "captured" and examined. It listens in on conversations like a herding tactic. [31] Due to the fact that they are not all owned by the same person and can have distinct, hostile goals, a botnet may occasionally lose its edge to another horde of

REVIEW ARTICLE

botnets [32]. The botnet leaves its location and unregisters from the DDNS after it has been routed or has lost its usefulness. The Single Bot Lifestyle, displayed on the right from the left image, provides a closer-up view of the bots and what they do while left idle, if they have been used effectively. As explained below, there are at least three major stages in which an IoT botnet functions [33].

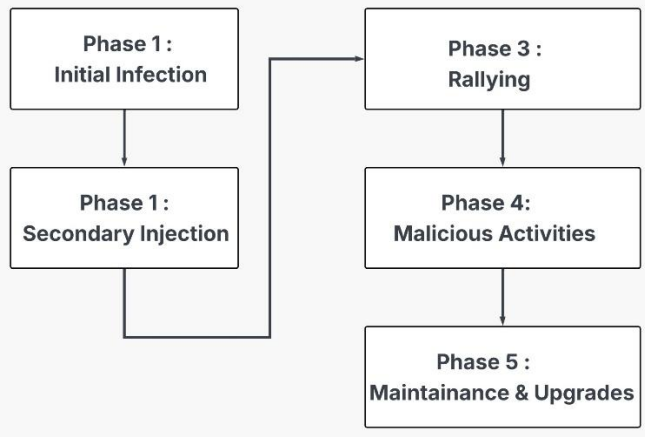

Figure 1 Botnet Lifecycle

Figure 1 represents the detailed lifecycle of an IoT botnet attack, systematically divided into five distinct but interconnected phases, illustrating the progressive stages through which a botnet evolves and sustains itself to carry out various malicious operations.

Step 1: The first phase, Initial Infection, marks the entry point of the botnet into the IoT ecosystem. During this phase, attackers exploit the inherent vulnerabilities of IoT devices, such as weak or default credentials, unpatched firmware, or unsecured communication protocols, to gain unauthorized access to the device [34]. This exploitation allows the botnet malware to implant its code, thereby compromising the target system.

Step 2: Secondary injection, where additional malicious payloads or components are injected into an infected device. The purpose of these additional injections is to strengthen the control of the botnet on the compromised devices, establish firmness, and potentially enable more complex malicious functionalities [35]. This phase may include the download and execution of the module that helps maintain a stable leg, such as rootkits or modules that are designed to be detected by safety solutions.

After these early transition stages, a lifeline cycle transition in step 3 rally. In this phase, the compromised IoT equipment, now turned into bots or corpses, attempts to establish contact with the attacker's C&C infrastructure. This communication is important for the centralized coordination of the botnet network. The rally process may include the exchange of keys, obtaining configuration files, or obtaining instructions for further actions. In some cases, Botnet employs refined techniques such as P2P communication, DGA, or encrypted channels to hide their traffic and to avoid detection by traditional network safety mechanisms [36]. Through this rally process, all infected equipment becomes part of an organized botnet army, which is ready to receive and work in concert according to the objectives of the attacker.

Step 4: Once the botnet has successfully captured its component devices under the control of the C&C server, it proceeds in step 4 malicious activities. This phase is the execution phase, where real damage is inflicted. The agreement made IOT devices are directed to participate in a variety of cyber-attacks, including DDOS, which can overload targeted servers or networks with traffic and result in service blocks. In addition to the DDOS attacks, botnets can be used for credential stuffing, spamming campaigns, based on the goals of the attacker [37], click on fraud, crypto mining, and even data exfiltration. This phase highlights the dangerous capacity of IOT botnets, resulting in extensive operations, financial and reputational damage to individuals, organizations, and significant infrastructure.

Step 5: After performing its malicious tasks, the botnet enters step 5: maintenance and upgradation. This is an important phase for the long-term stability of the botnet. During this phase, the attackers issue updates or patches in the botnet code to improve their performance, increase their ability to evade detection by security systems, or adapt to changing network conditions. Maintenance activities may include avoiding blacklisting, modifying communication protocols, or rotating the C&C server to deploy new payloads that take advantage of the newly discovered weaknesses. Some advanced botnets, removing competitive malware from infected equipment in this phase, include strengthening the safety of the botnet against rival attackers or security researchers against efforts to acquire [38]. The cyclical nature of this life cycle is clear as the maintenance and upgradation phase prepares the botnet for the latter period of malicious activity, which eliminates the transition cycle.

The figure 2 shows that IoTs are not stable institutions, but increasingly dynamic, developed dangers that continuously adapt to ensure their existence and effectiveness. Each stage builds on the previous one, creating a strong and flexible structure that can execute a complex cyber-attack, opposing the efforts to detect and remove it. The dual mention of "phase 1" in the figure underlines the leveled complexity of the initial transition process, including several stages to establish a safe and frequent appearance on the target devices. This life cycle also reflects the challenges faced by cybersecurity professionals in protecting the IOT ecosystems, where traditional safety measures may be reduced due to the distributed, asymmetrical, and resource-limited nature of IOT

REVIEW ARTICLE

devices [39]. Effective defense against such botnets requires a multi-pronged approach that includes securing devices against initial infections, monitoring for unusual rallying behavior, disrupting C&C communications, detecting malicious activities in real time, and preventing the botnet from receiving updates or maintenance instructions. Understanding the intricacies of this lifecycle, as depicted in the figure, is essential for developing comprehensive and proactive strategies to mitigate the growing threat of IoT botnets in today's interconnected digital world. This helps to prevent any infections of real field tissue. The accuracy of identifying malicious code is significantly influenced by all the data gathered from the Sandbox. Collecting benign files is not as simple as gathering virus samples, though. Many malware sample databases are available, including Detux and IoTPot, among others. Consequently, when machine learning models are used in sandbox environments, the data set used for training them has bias. As a result, the authors use the one-class categorization approach to address the issue. One-class classification is a technique that uses distinct samples for the identification of patterns that exist in the class [40].

The remaining paper can be categorized into the following sections: Section 2 focuses on the latest research that has been conducted for the detection and mitigation of IoT botnet techniques. Section 3 discussed the detection of IoT botnet techniques, which include signature, anomaly, and DNS-based techniques. Section 4 focused on the different techniques for the mitigation of IoT botnet. The problems and challenges of open research were the main topic of Section 5. The article is finally concluded in Section 6.

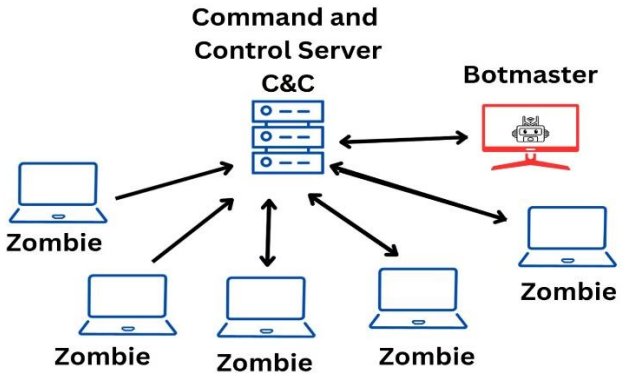

Figure 2 IoT Botnet Attacks

2. LITERATURE REVIEW

The vulnerabilities of IoT applications-built botnet attacks are a significant cyber safety concern. It is crucial for the IoT system and for safeguarding the data and system's availability, integrity, and privacy. Because machine learning algorithms may learn from patterns and anomalies in data to identify malicious actions, they have demonstrated promising skills in detecting botnet attacks in IoT data. In this overview of the literature, we examine the current work on employing ML algorithms to identify botnet IoT attacks.

Numerous studies have suggested different machine learning methods for IoT botnet detection. In order to train the classifier and achieve high identification accuracy, the authors used network traffic data's packet size, protocol type, and port number. Authors [41] suggested feature selection methods to detect malicious activity in IoT data. They also suggested a cloth-based botnet detection method that uses vector machines, the logistic region, the best neighbours, and feature selection methods. The detection demonstration of his method was superior to that of the individual classifier. In the Internet of Things, botnet detection has also made use of deep learning techniques like CNN and RNN. A CNN-based technique for analyzing network traffic patterns to detect botnet attacks in the IoT was proposed by Tan et al. [42]. The authors used a CNN model to learn characteristics to detect botnet attacks with excellent accuracy. An RNN-based method for identifying botnets in IOT by examining device activity was presented by Singh et al. [43]. Analyzing RNNs, the authors were able to detect botnet assaults with high accuracy by analyzing sequential data from IOT device operations.

IoT botnet detection has also made use of clothing learning techniques like boosting, bagging, and stacking. Yin and associates, to make a final choice and get a better detection than the individual classifier, integrated the output of the base classifier. Using several decision tree classifiers, Wang et al. [44] presented a boosting-based ensemble method for IoT botnet detection. The authors combined the decision tree classifiers' outputs using adaptive boosting to attain high detection accuracy.

IoT botnet detection has made extensive use of feature selection and dimensionality reduction approaches to simplify and boost machine learning algorithms' effectiveness. Using recursive feature elimination and information gain, Yang et al. [45] suggested a feature selection method for choosing the most pertinent features for IoT botnet detection. By narrowing down the feature space and making the model easier to understand, the authors were able to enhance detection performance. Alzubi et al. [46] suggested a PCA-based method for reducing dimensionality in IoT botnet detection. The most informative characteristics were captured by the authors using PCA, which reduced the dimensionality of the feature space and increased detection performance.

Hooshmand et al. [47] proposed a ML-based sequential detection framework with a lightweight sequential ML architecture with feature selection for IoT-botnet detection. It detects the 99% overall accuracy using ANN, J48, Naïve Bayes on evaluated datasets. The article has limited evaluation on diverse real-time IoT traffic and constrained-device deployment analysis. Nakip et al. [48] compared

REVIEW ARTICLE

traditional ML and deep-learning models for IoT botnet detection and proposes an integrated framework. The DL models achieved high accuracy but with greater resource cost. However, the energy and latency trade-offs that constraints deeper exploration.

Mishra et al. [49] presented a CNN-LSTM model capturing spatial–temporal features of network flow for botnet detection. The results of the article provide robust detection and good generalization on benchmark datasets. The article has the limitation in terms of explainability, adversarial robustness, and lightweight variants for IoT gateways remain open. Fu et al. [50] proposed an edge gateway architecture with lightweight detectors for early botnet detection. The early detection with low overhead at edge provides good accuracy. The scalability across heterogeneous gateways and long-term drift/adaptation mechanisms. Sicato et al. [51] utilized genetic-algorithm for feature selection with reducing dimensionality while preserving performance. The results generated with selected 40 features yielding 99.98% accuracy and faster training. The transferability of selected features to other datasets and robustness to evolving botnet behavior.

Cetin et al. [52] examined the adversarial attack impact and proposes defences for Mirai detection using robust ML techniques. It improved the resistance to crafted evasions compared to baseline detectors. The research gaps include broader adversarial scenarios, real-device experiments, and defensive cost analysis need study. Vinaykumar et al. [53] applied equilibrium optimization to select discriminative features for botnet detection. Results are improved with detection accuracy and reduced feature set compared to standard filters. Research gaps include comparative analysis with recent wrapper methods and evaluation on live network captures. Researchers [54] integrated feature-importance weighting with ensemble ML models to improve detection efficacy. It ensembles with feature significance outperformed single classifiers on Bot-IoT. The explainability of ensembles, deployment complexity, and sensitivity to mislabelled data. Authors [55] provided a realistic IoT botnet dataset (pcap/CSV) for training/evaluation. Results widely used benchmark enabling comparative studies. The dataset realism for modern IoT protocols, class imbalance, and need for continual/streaming data variants. Recent surveys and reviews [56] synthesized ML/DL approaches, challenges (resource limits, feature selection, datasets) and future directions. It highlights the progressive results but emphasize fragmented evaluations across inconsistent datasets. Its standardized benchmarks, reproducible experiments, edge-aware models, privacy-preserving detection, and adversarial robustness remain critical.

The study in [57] uses Equilibrium Optimization (EO) algorithm to enhance feature selection for IoT botnet detection. By effectively identifying the most discriminative features, the method improves detection accuracy and reduces computational redundancy. The approach demonstrates strong performance; However, this requires a thorough comparison with state-of-the-art wrappers and embedded feature-selection techniques. In [58], the authors present a feature-importance weighted ensemble learning approach, where the ensemble classifier is strengthened by integrating the importance of selected features. This method achieves better identification rates than a single model and increases robustness to the dataset. Despite its effectiveness, the function does not fully address the interpretability of aggregate predictions, limiting interpretability for security operations. The contribution in [59] focuses on the development of a comprehensive IoT botnet dataset that simulates realistic attack scenarios and traffic patterns. This dataset has become a widely used benchmark for training and evaluating ML-based intrusion detection models. However, it does not fully represent the modern IoT ecosystem, as it lacks new protocols, device diversity, and the real-time streaming behavior typical of the current environment. The work [60] provides a comprehensive review and classification of machine-learning and deep-learning-based IoT botnet detection approaches. The review highlights advances in algorithms, datasets and evaluation methods while identifying existing challenges. This emphasizes the need for standardized benchmarking practices, lightweight ML models suitable for edge deployments, and privacy-preserving identification techniques.

The literature review emphasizes how popular machine learning methods are for identifying botnet assaults in the IoT. To identify botnet assaults in IoT data, a variety of algorithms have been used, such as ensemble learning, neural networks, decision trees, and support vector machines. The detection models' efficiency and complexity have been increased by the application of feature selection and dimensionality reduction approaches. CNNs and RNNs, two deep learning algorithms, have also demonstrated encouraging detection capabilities. Table 1 shows the recent work that utilized to detect the IoT botnet.

Table 1 Contribution on IoT Botnet Detection

Reference	Technique used	What has been done (contribution)	Research gap
[41]	Measurement + traffic analysis	Large-scale empirical analysis of Mirai's propagation, C2, and attack	Focused on Mirai tactics limited on automated detection models or ML-based mitigation for

REVIEW ARTICLE

		patterns based on multi-source telemetry; baseline for IoT botnet behavior.	evolving variants.
[42]	Classical ML (ANN, J48, Naïve Bayes) + feature selection	Proposed a lightweight sequential-detection ML framework with feature selection; reported ~99% detection on evaluated datasets.	Evaluation mainly on limited/simulated datasets; generalization to unseen botnet variants and real-world IoT heterogeneity not shown.
[43]	SLR / taxonomy	Comprehensive taxonomy of IoT botnet DDoS attacks and detection techniques; summarizes ML/DL and classical detection approaches.	High-level synthesis, lacks experimental comparisons and standardized benchmarks across methods.
[44]	Edge-based ML modules (lightweight)	Designed a set of lightweight modules for early botnet detection deployable on edge gateways to reduce latency and resource use.	Trade-offs between detection accuracy and resource constraints need broader real-world validation.
[45]	Lightweight deep learning NIDS (two-stage)	Proposed a two-stage lightweight NIDS tailored for IoT networks; emphasizes deployability and low feature requirements.	May still struggle with novel protocol behaviors and encrypted traffic; benchmark diversity limited.
[46]	SDN-based detection + ML overview	Surveys ML applications for botnet detection in SDN-enabled IoT and discusses SDN advantages for global visibility.	SDN-centric approaches assume SDN infrastructure — many IoT deployments lack SDN, limiting applicability.
[47]	Feature-selection techniques review	Evaluates filtering-based feature-selection methods and their suitability for IoT botnet detection.	Needs concrete guidance on feature pipelines for specific IoT classes and real-time constraints.
[48]	ML classifiers (various)	Developed ML-based models to detect botnet attacks and validated on selected datasets; practical model-building details provided.	Limited dataset diversity and little discussion on adversarial robustness or online deployment.
[49]	Deep learning (ResNet-style)	Introduces a residual-network DL approach for distinguishing botnet traffic in IoT; shows improved classification on chosen test sets.	DL models are heavier — deployment on constrained devices/gateways and interpretability remain open issues.
[50]	AI/ML survey (recent)	Latest survey summarizing recent AI-driven detection approaches and challenges in IoT botnet detection (includes datasets, benchmarks).	Identifies need for standardized, up-to-date benchmark datasets and evaluations against evolving botnet variants.

REVIEW ARTICLE

[51]	Sequential ML framework (ANN, J48, Naïve Bayes)	Proposed lightweight sequential detection model with optimized feature selection achieving 99% accuracy on IoT datasets.	Limited evaluation on real-world IoT traffic and resource-constrained devices.
[52]	Traditional ML and Deep Learning comparative analysis	Compared ML vs DL models for IoT botnet detection and developed an integrated intelligent framework.	Trade-offs between energy, latency, and model complexity not fully addressed.
[53]	CNN–LSTM hybrid model	Designed a CNN–LSTM model capturing spatial-temporal features in IoT network traffic for efficient detection.	Lack of explainability, adversarial robustness, and lightweight adaptation for IoT gateways.
[54]	Edge-deployed lightweight ML modules (EDIMA)	Developed an edge architecture for early IoT botnet detection using lightweight ML models.	Scalability across heterogeneous gateways and long-term adaptability untested.
[55]	Genetic Algorithm (GA)-based feature selection	Applied GA for dimensionality reduction on Bot-IoT dataset while maintaining detection accuracy.	Transferability of selected features to other datasets and robustness to evolving attacks need validation.
[56]	Adversarial learning-based detection	Proposed adversarial-resilient ML models to enhance Mirai botnet detection accuracy and robustness.	Requires broader adversarial scenario evaluation and real-world device experimentation.
[57]	Equilibrium Optimization algorithms	Used equilibrium optimization for selecting optimal features, improving accuracy and reducing redundancy.	Needs comparison with advanced wrapper methods and testing on live IoT networks.
[58]	Feature-importance weighted ensemble learning	Combined feature-importance metrics with ensemble classifiers to boost detection performance.	Explainability of ensemble models and robustness to mislabeled or noisy data not explored.
[59]	Dataset generation and benchmarking	Developed a large-scale realistic IoT botnet dataset widely adopted for ML-based detection studies.	Dataset lacks coverage for newer IoT protocols and real-time streaming scenarios.
[60]	Review and taxonomy of ML/DL-based detection methods	Summarized advancements, challenges, and datasets in IoT botnet detection.	Identified need for standardized evaluation, edge-aware ML models, and privacy-preserving frameworks.

3. IOT BOTNET DETECTION METHODS

Botnets are challenging to identify since they use minimal computational resources. In recent years, network security specialists have focused a lot of their research on botnet tracking and detection. Numerous solutions have been put forth, and they can be categorized into two groups. Using honeypots and honeynets is the first technique, which is a form of active analysis. The method focuses on passive network processing and evaluation, and can be categorized as DNS-based, signature-based, anomaly-based, or mining techniques.

REVIEW ARTICLE

3.1. Honeypots Based IDS

Honeypot establishes an environment that builds vulnerabilities and identifies the attack and intrusion. A large-scale network is made up of various-sized honeynets. The toolkit features and range of capabilities of Linux-based honeynets make them popular. In order to trick botnets and other attackers into engaging with the system, a honeypot is a single decoy system that is purposefully left open to attack (Figure 3). Despite being isolated from the main network and constantly monitored to spot any suspicious activity, the honeypot seems to be a legitimate system. For instance, an IoT device that is known to be vulnerable, such as a thermostat or smart camera, can be mimicked by a honeypot and made available online. When a botnet tries to enter the honeypot by taking advantage of the vulnerabilities, the security team may detect the attack and take the necessary precautions to stop additional harm.

A honeynet is a collection of decoy systems that imitates an entire network environment, complete with different devices and services. The goal of the honeynet is to draw in and identify botnets that try to infiltrate the network and get unauthorized access. Using various device kinds, operating systems, and services, the honeynet can mimic a small network or even an entire enterprise network. The security team can identify the activity and obtain important data on the traits and actions of the botnet when it infiltrates the honeynet and tries to spread or link to command-and-control servers. Because they offer a controlled environment for observing botnet behavior without endangering the real production systems or networks, honeypots and honeynets are useful tools for identifying botnet attacks. They enable security professionals to obtain important information about botnets, such as their communication means, propagation strategies, and assault patterns. Using this information, successful countermeasures to stop and lessen botnet attacks in actual production settings can be created.

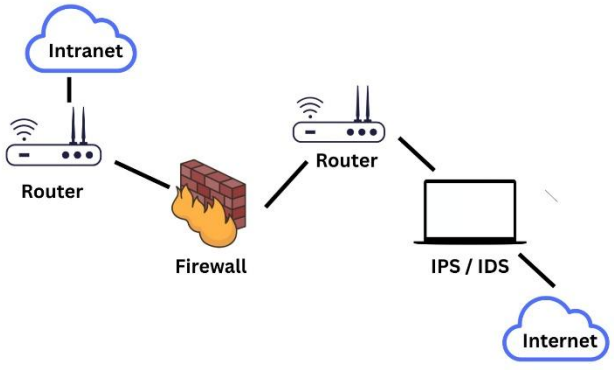

Figure 3 Honeypot-Based IDS

To simulate a smart home network, for instance, a security team might install a honeynet with a variety of IoT devices, including smart speakers, smart cameras, and smart thermostats. The honeynet can identify the attack and offer information on the activity of the botnet, including the devices it targets, the communication protocols it employs, and the orders it sends to the compromised devices, as it tries to get access by taking advantage of flaws in these IoT devices. Real smart home networks can then be shielded from similar botnet attacks by using this knowledge to create patches, upgrades, or other defenses.

3.2. Signature-Based Detection

Malware detection and classification frequently employ malware signatures. When it comes to categorizing executables that are running on a system, the signatures of detected malware are incredibly powerful. Detecting malware signatures is possible using Snort and other rule-based intrusion detection systems. For indications of intrusion, they examine IoT communications. Malware may be recognized by its executable signature or by the peculiar signatures it produces in the traffic from Internet of Things devices (Figure 4). Additionally, identification based on signatures can be used to identify known botnets. For anonymous bots, this approach's consequences are meaningless.

When it comes to identifying established botnet assaults that employ recognizable patterns or behaviors, signature-based detection can be useful. It is limited, though, because it depends on a database of known signatures and might not be able to identify novel or unidentified botnets that don't match any signatures already in existence. By concealing their actions from signature-based detection systems through obfuscation, encryption, or other means, botnet operators can also avoid detection by signatures.

Moreover, false positives or false negatives could also arise via signature-based detection. False positives happen when system behaviours or normal network traffic are mistakenly identified as botnet activity, causing needless interruption or blocking. When botnet activity does not match any recognized signatures, it is referred to as a false negative and goes unnoticed.

Despite its drawbacks and the requirement to be used in conjunction with other detection techniques for comprehensive botnet detection and prevention, signature-based detection can be a helpful technique for detecting known botnet attacks. The precision and efficacy of botnet detection and mitigation initiatives can be raised by routinely updating the signature databases in combination with other cutting-edge methods, including behavior-based analysis, anomaly detection, and machine learning.

Using antivirus software to identify and stop botnets is an example of signature-based detection. Antivirus software searches files or network traffic for signatures of recognized malware, including malware linked to botnets, and keeps a

REVIEW ARTICLE

database of these signatures. The antivirus program can quarantine the compromised file, halt the activity, or notify the user or system administrator.

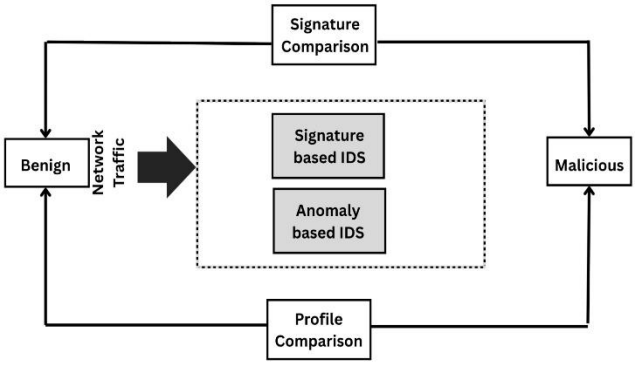

Figure 4 IDS with Signature-Based Techniques

3.3. Anomaly-Based Detection

Researching new network traffic-based botnet detection methods is time-consuming. An unusual network latency, NetFlow on unusual and unoccupied ports, a high traffic percentage for a semi-network, or odd structure behaviors that might indicate the presence of unauthorized entities in the network are examples of network behavior anomalies that are used in botnet detection. When it comes to identifying unexpected or zero-day botnet attacks that don't match any known signatures or patterns, anomaly-based detection works incredibly well. Because behavioral abnormalities may still be identified even when attack tactics change, it can also identify botnets that employ complex evasion strategies like encryption, obfuscation, or dynamic behavior changes (Figure 5).

However, there are drawbacks to anomaly-based detection as well. False positives may result from it since warnings may be triggered by real differences in system behaviors or network traffic. For instance, an abrupt spike in network traffic brought on by normal events like an upgrade in software or an anomaly in the traffic pattern. False positivity can be reduced by detecting fine-tuning discrepancy and setting suitable thresholds.

An effective way to identify botnet attacks that do not fit recognized patterns or characteristics is discrepancy-based detection. For full botnet identity and prevention, it can be used with other identification methods and provides an additional line of protection against botnet attacks. The performance measurement of the anomaly-based detection can be monitored, including baseline statistics updates and anomaly detection algorithm modification.

Establishing typical network traffic patterns by statistical analysis is an example of anomaly-based detection. Real-time network traffic is compared to baseline statistics like volume of traffic, distribution of packet size, and protocol distribution that are determined by looking at historical data by an anomaly detection system. A warning suggesting a possible botnet attack may be triggered by any notable departures from the predetermined baseline.

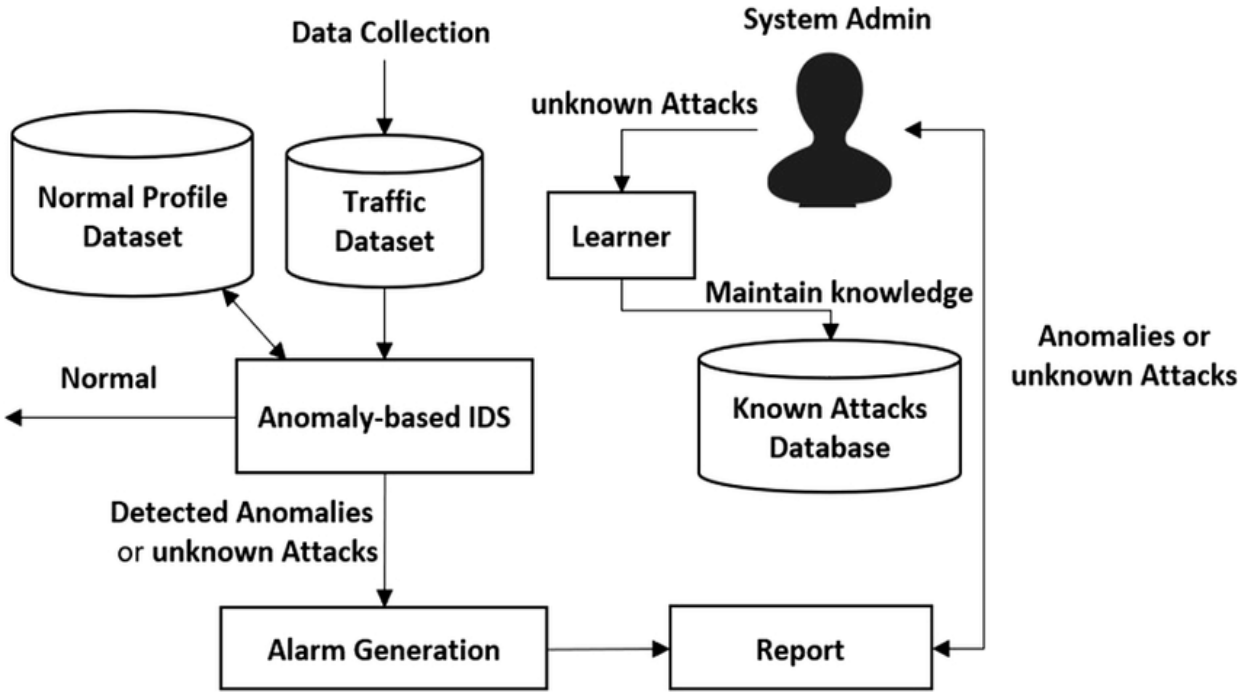

Figure 5 Anomaly-Based Detection

REVIEW ARTICLE

3.4. DNS-Based Detection

The absence of intrusiveness of DNS-based detection methods is similar to that of other anomaly-based detection systems. Their foundation is often the detection of anomalous DNS network activity produced by bots. Therefore, by keeping an eye on DNS operations and spotting odd or unexpected DNS queries, it is possible to detect botnet DNS activity (Figure 6).

By providing important visual information, established a method for administrators and security consultants to identify botnets. The suggested method is predicated on DNS traffic, which makes up a very small percentage of all network traffic. Thus, real-time analysis can also be done with this technology.

Threat intelligence feeds, which are repositories of botnet-related IP addresses or known malicious domain names, can also be used for DNS-based detection. These threat intelligence feeds employ DNS data comparison to find patterns that can point to botnet activity. Additionally, DNS-based detection can employ machine learning methods that examine DNS traffic for trends or actions that can point to botnet activity. In order to detect anomalies from the regular behaviors that have been taught, such as odd query patterns, domain names, or IP addresses linked to botnets, machine learning algorithms, for instance, can be trained on enormous datasets of typical DNS traffic.

There are some restrictions in DNS-based identity, however. To avoid DNS-based identity, botnet use a variety of strategies, such as encryption, hiding C&C communication in ordinary DNS data, and domain generation algorithms (DGA) to produce random domain names. Furthermore, because legitimate activities, such as actual DNS requests from devices that are not configured for correct or legitimate use of CDNS (material distribution network), can mimic botnet activity by specific methods, DNS-based identity can produce false status.

When identifying the Botnet attack that uses DNS for C&C communication, DNS-based identity is a useful method. It can be combined with other detection methods to achieve botnet detection and prevention, and it can offer an additional line of protection against botnet attacks. The accuracy and efficacy of DNS-based identity in identifying botnet attacks can improve the DNS analysis algorithm by adding machine learning techniques and updating the intelligence feed of regular danger.

The DNS Query Pattern exam is an example of DNS-based identity. To interact with your C&C server, a botnet often makes a lot of DNS requests. Some symptoms, such as high frequency, asymmetrical domain names, or recurring search, may be present in these requests. By checking DNS query traffic, a DNS-based detection system can spot patterns that differ from specific or expected DNS query behavior and mark them as a sign of a botnet attack.

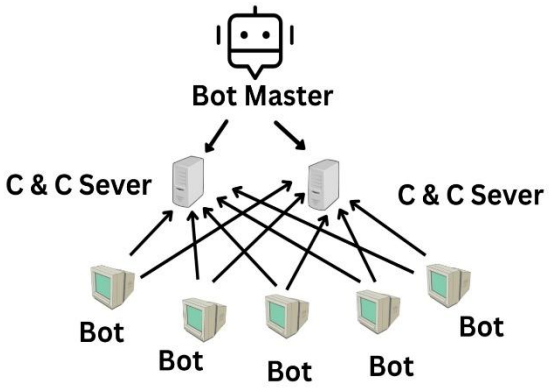

Figure 6 DNS-Based Detection

3.5. Mining-Based Detection

In everyday traffic, it can be challenging to discern C&C attacks. In this sense, unanticipated network patterns can be found with the aid of machine learning-based data mining algorithms that aid in pattern detection. Davis and Clark give a summary of the pre-processing operations that are currently being performed for anomaly and mining-based intrusion detection methods. Strayer suggested a method for passively examining network flow data to find botnet C&C activities. Strayer's methodology focuses on the flow of attributes like bits/sec, packets, duration, and others. Nagaraja and his colleagues created BotGrep, a novel and efficient method for identifying bots using structured graphs. Since recent bot architectures use a decentralized C&C architecture, sub-graph network detection is a very practical and helpful IDS technique (Figure 7).

But mining-based detection is not without its drawbacks. Numerous strategies, including encryption, obfuscation, and polymorphic malware, can be used by botnets to hide their operations and avoid being discovered by miners. Additionally, since genuine software or activities may display patterns or behaviors that mimic those of botnets, mining-based detection may produce false positives or false negatives.

Mining-based detection is a potent method for identifying botnet attacks since it uses data mining and machine learning algorithms to find trends, anomalies, or behaviors connected to botnet activity. It can provide useful details about botnet activities that traditional methods might not be able to detect. To improve the accuracy and efficacy of mining-based detection in identifying botnet assaults, multiple detection techniques can be integrated, mining algorithms can be tuned, and training data can be updated often. Network traffic analysis for odd patterns or behaviors is one instance of mining-based detection. To allow infected devices to connect

REVIEW ARTICLE

with their C&C servers, botnets typically create a lot of network traffic. In order to find trends like communication with dubious IP addresses, the use of strange ports, or unusual data transfer rates that can point to botnet activity, mining-based detection systems, for instance, may examine network traffic data, such as packet headers, payload content, or flow data.

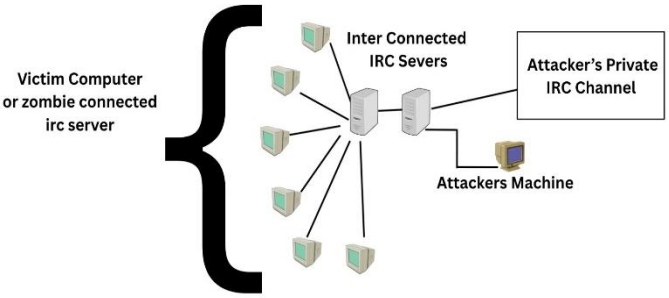

Figure 7 Data Mining-Based IDS

Network traffic data can easily be subjected to data mining and machine learning algorithms. Flow data does not require a lot of preparation because it is linked and structured. Additionally, flow data indicates internal trends, which simplifies and improves the study of data mining techniques. As a result, flow-based approaches are more persuasive because they only focus on finding network flow information, which can be considered network flow meta-information without any content.

4. MITIGATION OF IOT BOTNET

The mitigation of IoT botnets requires a multi-layered approach combining strong device-level security, continuous software maintenance, real-time threat detection, information sharing, and secure design principles. Only through the joint efforts of manufacturers, users, service providers, and regulatory bodies can the pervasive threat of IoT botnets be effectively controlled and minimized. As IoT adoption grows worldwide, proactive and collaborative cybersecurity measures will be crucial in safeguarding the digital infrastructure from large-scale botnet attacks. To mitigate the IoT botnet, there are distinct mechanisms available, such as:

Securing IoT Devices through Strong Authentication and Access Control: A fundamental step in mitigating IoT botnets is the enforcement of strong authentication mechanisms and strict access controls. Attackers can easily utilize the default usernames and passwords on many IoT devices to enlist devices in botnets. To prevent this, device manufacturers must ensure that every IoT product requires a password change upon initial setup and supports the use of complex, non-default credentials. Furthermore, implementing MFA can add an extra layer of security, making unauthorized access significantly more difficult.

Access control policies such as RBAC or ABAC should also be employed to limit device communication only to necessary endpoints, reducing the attack surface. Network segmentation is another useful technique, where IoT devices are isolated in separate subnets, preventing lateral movement by malware or unauthorized access to critical systems. Together, these measures ensure that even if an attacker manages to compromise one device, the damage can be contained, and the spread to other devices or the broader network can be avoided.

Regular Patch Management and Software Updates: Botnet malware frequently enters networks through outdated firmware and software flaws. Manufacturers and IoT users must prioritize timely software updates and patch management to fix security flaws that could be exploited by attackers. Unfortunately, many IoT devices in use today are rarely, if ever, updated post-deployment, leaving them vulnerable to known exploits.

To mitigate this risk, automated patching and secure over-the-air (OTA) updates should be integrated into IoT ecosystems. Device vendors should adopt secure development lifecycles (SDLCs), ensuring that software updates are cryptographically signed and verified to prevent malicious code insertion during the update process. Moreover, end-users need to be educated on the importance of installing updates immediately and ensuring that devices are not running end-of-life software that no longer receives security patches.

Policy-level interventions may also be necessary, with regulators mandating minimum update periods and vulnerability disclosure requirements for IoT manufacturers. This collective approach can drastically reduce the number of exploitable devices available to botnet herders.

Implementation of IDPS: Real-time identification and mitigation of IoT botnet threats is made possible in large part by IDPS. Indicators of botnet activity, such as abrupt surges in outbound traffic, connection attempts to known C&C servers, or involvement in DDoS attacks, can be detected by IDPS solutions that monitor network traffic.

Techniques for anomaly-based and signature-based detection are both crucial. Although signature-based systems are very good at identifying known botnet malware, anomaly-based systems can identify zero-day exploits and attack routes that haven't been seen before by highlighting odd or suspicious activity. Cutting-edge systems use machine learning algorithms to decrease false positives and increase detection accuracy while constantly learning from new threats and adjusting to changing attack techniques.

On detection of potential botnet activity, automated response mechanisms such as quarantining the affected device, blocking C&C server IPs, or limiting suspicious traffic can be activated to contain the threat and prevent further infection or

REVIEW ARTICLE

malicious activity. Deploying these solutions at both the device level and the network edge enhances the overall security posture against IoT botnets.

Threat Intelligence Sharing and Collaborative Defence Mechanisms: The fight against IoT botnet cannot be won in isolation; This requires coordinated efforts in the global cybersecurity community. The threat between organizations, ISPs, device manufacturers, and government agencies is important to ensure that new threats are quickly identified and neutralized. Information such as IOT device weaknesses, C&C server locations, botnet signs, and emerging attack techniques should be shared immediately through reliable channels.

Information sharing and analysis centers (ISACS) and associate platform stakeholders, such as the International Cyber Security Alliance, enable rapid, integrated reactions to botnet outbreaks. For example, ISPs can use shared intelligence to detect malicious traffic arising from IoT devices compromised within their network, thus preventing mass DDoS attacks such as Mirai and its variants.

This approach not only enhances security awareness but also reduces the time it takes to develop counters and apply them in various fields. In addition, global cooperation ensures that botnet operators face disruption in many courts, making it more difficult to execute continuous attacks.

Designing Secure-by-Default IoT Architectures: The long-term mitigation of the IOT botnet requires a change towards safe-by-design and safe-default IoT architecture. Manufacturers should prioritize cybersecurity during the product design phase, ensuring that equipment is designed with safety features that are naturally enabled, rather than manually configured by users. Features such as hardware-based safety modules (e.g., trusted platform modules or safe boot mechanisms), encrypted communication, and tampering-resistant firmware can greatly reduce the risk of compromise.

In addition, the device's lifestyles should be carefully planned, with the security aid period, end-of-life procedures, and clear policies on safe settlement guidelines. Reducing unnecessary services and communication channels can reduce the potential attack vector, making devices less attractive goals for botnet recruitment.

IOT- Developing specific safety structures and compliance standards can guide manufacturers and service providers in implementing these best practices. IoTs provide action to improve standard IOT security measures such as ISO/IEC 27030 (IOT Safety and Privacy Guidelines) or ETSI EN 303 645 (Cyber Security for Consumer IoT).

5. CHALLENGES AND OPEN RESEARCH ISSUES

IoT botnet detection and mitigation face numerous unresolved challenges and open research issues that demand immediate and sustained attention from the global research community. Key areas such as resource-aware detection algorithms, standardization of security frameworks, scalability, context-aware anomaly detection, privacy-preserving traffic analysis, evasion-resistant techniques, and integrated detection-mitigation architectures all offer fertile ground for innovation. Addressing these challenges holistically will be critical to securing the future of the IoT ecosystem against the growing threat of botnets.

Heterogeneity and Resource Constraints of IoT Devices: IoT device heterogeneity is one of the most significant obstacles to IoT botnet identification and mitigation. Devices in IoT networks vary widely in terms of their architecture, operating systems, communication protocols, and computational power. The CPU, memory, storage, and battery life of the majority of devices are limited. This diversity makes it difficult to develop a universal security solution that fits all devices without affecting their performance or usability. Lightweight and adaptable detection algorithms are required, but designing such solutions that do not overwhelm device resources while maintaining detection accuracy remains an open research issue.

Lack of Standardized Security Frameworks: The absence of universally accepted and enforced security standards for IoT device manufacturing and deployment presents a significant challenge. Many devices enter the market with minimal or no security provisions, such as default passwords, a lack of encryption, or the absence of secure update mechanisms. This inconsistency allows attackers to exploit weak devices to build or expand botnets. A significant research need is the creation of global, enforceable standards and certification programs that maintain baseline security practices for all IoT devices, independent of application or location. Without such standardization, fragmented security practices will continue to leave IoT ecosystems vulnerable.

Scalability of Detection Systems: It is anticipated that IoT networks could soon accommodate billions of connected devices, which will present a scalability issue for botnet detection systems. Conventional detection techniques, including signature-based intrusion detection systems, would not be able to effectively handle the enormous amount and speed of data produced by extensive IoT deployments.

Furthermore, anomaly detection systems need to be built to manage large volumes while minimizing false positives and false negatives. This demands scalable, distributed, and real-time detection techniques, possibly leveraging edge computing and federated learning. Research is needed to

REVIEW ARTICLE

develop solutions that can scale dynamically with network growth without sacrificing performance or accuracy.

Difficulty in Distinguishing Normal from Malicious Behavior: IoT devices often exhibit highly diverse and context-dependent behavior, making it difficult to differentiate between normal and malicious activities. For example, a surveillance camera may regularly upload data to a cloud server, which resembles a command-and-control communication pattern used by botnets. This overlap complicates the creation of reliable detection models. Open research issues include developing advanced behavioral models and context-aware anomaly detection systems that can accurately learn device-specific usage patterns and dynamically adapt to changes without triggering excessive false alarms. The application of unsupervised and semi-supervised machine learning for this purpose is an emerging area that warrants further exploration.

Encrypted Traffic and Privacy Preservation: The increasing use of encryption in IoT communications enhances data security but complicates traffic analysis for botnet detection. Encrypted traffic prevents deep packet inspection (DPI), a common method used in traditional IDS solutions to identify malicious content or commands. Therefore, researchers face the challenge of developing techniques that can detect anomalies in encrypted traffic without violating user privacy or decrypting sensitive data. Promising directions include flow-based analysis, machine learning models trained on metadata (such as packet size, timing, and frequency), and homomorphic encryption, but these methods require further validation and optimization for practical IoT environments.

Evasion Techniques Used by Botnets: IoT botnets are becoming more sophisticated, utilizing distinct techniques such as fast-flux DNS, P2P communication, DGA, and protocol obfuscation to avoid detection and takedown. These tactics make it difficult for conventional IDS and firewall-based defenses to identify and block malicious traffic.

Botnet developers are also increasingly using polymorphic and metamorphic malware, which frequently changes its code structure to bypass signature-based detection. This ongoing evolution presents an open research issue in designing adaptive, intelligent detection systems capable of recognizing evolving threats using AI-driven methods such as deep learning and continual learning to keep up with these advanced evasion strategies.

Integration of Detection and Mitigation Mechanisms: Many existing IoT security solutions focus separately on either detection or mitigation, but rarely offer an integrated framework that seamlessly transitions from identifying a botnet threat to actively mitigating it. The lack of integration limits the effectiveness of responses, as delayed or manual interventions provide attackers with time to cause harm. Moreover, automatic mitigation raises concerns about service availability and potential disruption to legitimate device operations. Developing self-healing IoT networks that can autonomously detect, isolate, and recover from botnet attacks without human intervention remains a major research challenge. Solutions involving Software-Defined Networking (SDN) and blockchain-based trust management systems show promise, but require further research to ensure robustness, efficiency, and practical deployment feasibility.

6. CONCLUSION

Since IOT devices continue to spread in diverse fields, their underlying weaknesses, limited computational resources, and inequality make them the major goals for botnet-based attacks. The most recent identity and mitigation methods in the form of signature-based, discrepancy-based, DNS-based, and persuadable AI-operated strategies have been examined in this article. Each of these methods adds something special for the improvement of IOT security. While machine learning and blockchain technologies provide promising solutions for adaptive and decentralized defense, issues such as high false positives, scalability, and privacy protection still obstruct practical deployment. In addition, the algorithm and constant innovation in the algorithm and defense mechanisms are required to detect the dynamic nature of botnet architecture and attack strategies. Light safety models, real-time monitoring systems, and integration of standardized protocols on IOT platforms are required to ensure wide security. Cooperative efforts between academics, industry, and policymakers are important to resolve these open research challenges and establish a strong safety structure for the IOT environment. Ultimately, the creation of faith in the IOT ecosystem depends on developing active, transparent, and efficient safety measures that are capable of adapting to the complex and sometimes changing danger landscape generated by botnets.

REFERENCES

[1] A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman, and Y. Nam, “Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication,” IEEE Access, vol. 8, pp. 60539–60551, 2020, doi: 10.1109/ACCESS.2020.2983117.

[2] K. Sahlmann, V. Clemens, M. Nowak, and B. Schnor, “Mup: Simplifying secure over-the-air update with mqtt for constrained IoT devices,” Sensors (Switzerland), vol. 21, no. 1, pp. 1–21, Jan. 2021, doi: 10.3390/s21010010.

[3] M. Panda, A. A. A. Mousa, and A. E. Hassanien, “Developing an Efficient Feature Engineering and Machine Learning Model for Detecting IoT-Botnet Cyber Attacks,” IEEE Access, vol. 9, pp. 91038–91052, 2021, doi: 10.1109/ACCESS.2021.3092054.

[4] S. Hosseini, A. E. Nezhad, and H. Seilani, “Botnet detection using negative selection algorithm, convolution neural network and

REVIEW ARTICLE

classification methods," Evolving Systems, vol. 13, no. 1, pp. 101–115, Feb. 2022, doi: 10.1007/s12530-020-09362-1.
[5] S. Bagui and K. Li, "Resampling imbalanced data for network intrusion detection datasets," J Big Data, vol. 8, no. 1, Dec. 2021, doi: 10.1186/s40537-020-00390-x.
[6] Manos, A.; April, T.; Bailey, M.; Bernhard, M.; Bursztein, E.; Cochran, J.; Durumeric, Z. Un-derstanding the mirai botnet. In Proceedings of the 26th {USENIX} security symposium ({USENIX} Security 17), Vancouver, BC, Canada, 16–18 August 2017; pp.1093–1110.
[7] E. Bertino and N. Islam, "Botnets and Internet of Things Security," Computer, vol. 50, no. 2, pp. 76–79, Feb. 2017.
[8] 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.
[9] McDermott, C.D.; Majdani, F.; Petrovski, A.V. Botnet detection in the internet of things using deep learning approaches. In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 8–13 July 2018; pp. 1–8.
[10] Singh, M.; Singh, M.; Kaur, S. Issues and challenges in DNS based botnet detection: A survey. Comput. Secur. 2019, 86, 28–52.
[11] M. Al-Kasassbeh, M. Almseidin, K. Alrfou and S. Kovacs, "Detection of IoT-botnet attacks using fuzzy rule interpolation," Journal of Intelligent & Fuzzy Systems, pp. 1-11.
[12] A. Karim, R. B. Salleh, M. Shiraz et al., ―Botnet detection techniques: review, future trends, and issues, Journal of Zhejiang University Science, vol. 15, no. 11, pp. 943–983, 2014.
[13] Beltrán-García, P.; Aguirre-Anaya, E.; Escamilla-Ambrosio, P.J.; Acosta-Bermejo, R. IoT botnets. In Communications in Computer and Information Science; Springer Science and Business Media LLC.: Berlin, Germany, 2019; pp. 247–257.
[14] Alzahrani, H.; Abulkhair, M.; Alkayal, E. A multi-class neural network model for rapid detection of IoT botnet attacks. Int. J. Adv. Comput. Sci. Appl. 2020, 11.
[15] Dange, S.; Chatterjee, M. IoT Botnet: The Largest Threat to the IoT Network. In Advances in Intelligent Systems and Computing; Springer: Singapore, 2019; pp. 137–157.
[16] Beltrán-García, P.; Aguirre-Anaya, E.; Escamilla-Ambrosio, P.J.; Acosta-Bermejo, R. IoT botnets. In Communications in Computer and Information Science; Springer Science and Business Media LLC.: Berlin, Germany, 2019; pp. 247–257.
[17] Yahya H, Mohammed Z (2024) Developing a hybrid feature selection method to detect botnet attacks in IoT devices. Kuwait J Sci 51(3):100222. https://doi.org/10.1016/j.kjs.2024.100222.
[18] Edwards, S.; Profetis, I. Hajime: Analysis of a decentralized internet worm for IoT devices. Rapidity Netw. 2016, 16, 1–18.
[19] K. Ansam, G. Iqbal, V. Peter, K. Joarder and A. Ammar, "A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks," Electronics, vol. 8, no. 11, p. 1210, 2019.
[20] Vishwakarma, R.; Jain, A.K. A Honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 23–25 April 2019; pp. 1019–1024.
[21] Tzagkarakis, C.; Petroulakis, N.; Ioannidis, S. Botnet attack detection at the IoT edge based on sparse representation. In Proceedings of the 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 17–21 June 2019; pp. 1–6.
[22] Nguyen, H.-T.; Ngo, Q.-D.; Le, V.-H. IoT Botnet Detection Approach Based on PSI graph and DGCNN classifier. In Proceedings of the 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), Singapore, 28–30 September 2018; pp. 118–122.
[23] Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D.; Elovici, Y. N-baIoT—network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Comput. 2018, 17, 12–22
[24] D. A. D. B. o. S. A. w. S. f. I. Environment, "Soe, Yan Naung; Santosa, Paulus Insap; Hartanto, Rudy;," 2019 Fourth International Conference on Informatics and Computing (ICIC), pp. 1-5, 2019.
[25] N. KoronIoTis, N. Moustafa and E. Sitnikova, "A New Network Forensic Framework based on Deep Learning for Internet of Things Networks: A Particle Deep Framework," Future Generation Computer Systems, 2020.
[26] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," 2015 military communications and information systems conference (MilCIS), pp. 1-6, 2015.
[27] Q. Miao, J. Liu, Y. Cao, and J. Song, "Malware detection using bilayer behavior abstraction and improved one-class support vector machines," International Journal of Information Security, vol. 15, no. 4, pp. 361–379, 2016.
[28] E. Burnaev and D. Smolyakov, "One-class SVM with privileged information and its application to malware detection," presented at the 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW), 2016, pp. 273–280.
[29] P. Perera and V. M. Patel, "Learning deep features for one-class classification," arXiv preprint arXiv:1801.05365, 2018.
[30] P.-T. De Boer, D. P. Kroese, S. Mannor, and R. Y. Rubinstein, "A tutorial on the cross-entropy method," Annals of operations research, vol. 134, no. 1, pp. 19–67, 2005.
[31] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "IoTpot: A novel honeypot for revealing current IoT threats," Journal of Information Processing, vol. 24, no. 3, pp. 522–533, 2016.
[32] K. Angrishi, "Turning internet of things (IoT) into internet of vulnerabilities (iov): IoT botnets," arXiv preprint arXiv:1702.03681, 2017.
[33] C. Kruegel and Y. Shoshitaishvili, "Using Static Binary Analysis to Find Vulnerabilities and Backdoors In Firmware," Black Hat USA, 2015.
[34] P. Celeda, R. Krejci, J. Vykopal, and M. Drasar, "Embedded malware-an analysis of the chuck norris botnet," presented at the Computer Network Defense (EC2ND), 2010 European Conference on, 2010, pp. 3–10.
[35] M. Catillo, A. Pecchia, and U. Villano, "A Deep Learning Method for Lightweight and Cross-Device IoT Botnet Detection †," Applied Sciences (Switzerland), vol. 13, no. 2, Jan. 2023, doi: 10.3390/app13020837.
[36] K. Alissa, T. Alyas, K. Zafar, Q. Abbas, N. Tabassum, and S. Sakib, "Botnet Attack Detection in IoT Using Machine Learning," Comput Intell Neurosci, vol. 2022, 2022, doi: 10.1155/2022/4515642.
[37] Saied, M., Guirguis, S. & Madbouly, M. Review of filtering based feature selection for Botnet detection in the Internet of Things. Artif Intell Rev 58, 119 (2025). https://doi.org/10.1007/s10462-025-11113-0.
[38] T. Hasan et al., "Securing Industrial Internet of Things Against Botnet Attacks Using Hybrid Deep Learning Approach," IEEE Trans Netw Sci Eng, vol. 10, no. 5, pp. 2952–2963, Sep. 2023, doi: 10.1109/TNSE.2022.3168533.
[39] U. Garg, S. Kumar, M. Kumar, U. Garg, S. Kumar, and M. Kumar, "INFRDET: IoT network flow regulariser-based detection and classification of IoT botnet," 2008.
[40] S. Thota and D. Menaka, "Botnet detection in the internet-of-things networks using convolutional neural network with pelican optimization algorithm," Automatika, vol. 65, no. 1, pp. 250–260, Jan. 2024, doi: 10.1080/00051144.2023.2288486.
[41] J. Azimjonov and T. Kim, "Designing accurate lightweight intrusion detection systems for IoT networks using fine-tuned linear SVM and feature selectors," Comput Secur, vol. 137, Feb. 2024, doi: 10.1016/j.cose.2023.103598.
[42] R. H. Randhawa, N. Aslam, M. Alauthman, M. Khalid, and H. Rafiq, "Deep reinforcement learning based Evasion Generative Adversarial

REVIEW ARTICLE

Network for botnet detection," Future Generation Computer Systems, vol. 150, pp. 294–302, Jan. 2024, doi: 10.1016/j.future.2023.09.011.
[43] S. Mahadik, P. M. Pawar, and R. Muthalagu, "Efficient Intelligent Intrusion Detection System for Heterogeneous Internet of Things (HetIoT)," Journal of Network and Systems Management, vol. 31, no. 1, Mar. 2023, doi: 10.1007/s10922-022-09697-x.
[44] R. Sharma, S. Mohi ud din, N. Sharma, and A. Kumar, "Enhancing IoT Botnet Detection through Machine Learning-based Feature Selection and Ensemble Models," ICST Transactions on Scalable Information Systems, Sep. 2023, doi: 10.4108/eetsis.3971.
[45] 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 and Tutorials, vol. 22, no. 3, pp. 1646–1685, Jul. 2020, doi: 10.1109/COMST.2020.2988293.
[46] Alzubi, O. A., Alzubi, J. A., Qiqieh, I. & Al-Zoubi, A. An iot intrusion detection approach based on salp swarm and artificial neural network. Int. J. Netw. Manag. 35(1), e2296 (2025).
[47] M. K. Hooshmand, M. D. Huchaiah, A. R. Alzighaibi, H. Hashim, E.-S. Atlam, and I. Gad, "Robust network anomaly detection using ensemble learning approach and explainable artificial intelligence (XAI)," Alexandria Eng. J., vol. 94, pp. 120–130, May 2024, doi: 10.1016/j.aej.2024.03.041.
[48] E. Gelenbe and M. Nakip, "Traffic Based Sequential Learning During Botnet Attacks to Identify Compromised IoT Devices," IEEE Access, vol. 10, pp. 126536–126549, 2022, doi: 10.1109/ACCESS.2022.3226700.
[49] Saheed, Y. K. & Misra, S. Cps-iot-ppdnn: A new explainable privacy preserving dnn for resilient anomaly detection in cyber-physical systems-enabled iot networks. Chaos, Solitons & Fractals 191, 115939 (2025).
[50] Y. Fu, Z. Yan, J. Cao, O. Koné, and X. Cao, "An Automata Based Intrusion Detection Method for Internet of Things," Mobile Information Systems, vol. 2017, 2017, doi: 10.1155/2017/1750637.
[51] J. C. S. Sicato, S. K. Singh, S. Rathore, and J. H. Park, "A comprehensive analyses of intrusion detection system for IoT environment," Journal of Information Processing Systems, vol. 16, no. 4, pp. 975–990, Aug. 2020, doi: 10.3745/JIPS.03.0144.
[52] Çetin, A. & Öztürk, S. Comprehensive exploration of ensemble machine learning techniques for iot cybersecurity across multi-class and binary classification tasks. Journal of Future Artificial Intelligence and Technologies 1(4), 371–384 (2025).
[53] R. Vinayakumar, M. Alazab, S. Srinivasan, Q. V. Pham, S. K. Padannayil, and K. Simran, "A Visualized Botnet Detection System Based Deep Learning for the Internet of Things Networks of Smart Cities," IEEE Trans Ind Appl, vol. 56, no. 4, pp. 4436–4456, Jul. 2020, doi: 10.1109/TIA.2020.2971952.
[54] Ullah, S., Wu, J., Lin, Z. et al. Comparative analysis of deep learning and traditional methods for IoT botnet detection using a multi-model framework across diverse datasets. Sci Rep 15, 31072 (2025). https://doi.org/10.1038/s41598-025-16553-w.
[55] C. Singh and A. K. Jain, "A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network," e-Prime - Advances in Electrical Engineering, Electronics and Energy, vol. 8. Elsevier BV, p. 100543, Jun. 2024. doi: 10.1016/j.prime.2024.100543.
[56] M. Sanlı, "Detection and Mitigation of Denial of Service Attacks in Internet of Things Networks," Arabian Journal for Science and Engineering. Springer Science and Business Media LLC, Feb. 22, 2024. doi: 10.1007/s13369-023-08669-w.
[57] U. Garg, S. Kumar, and A. Mahanti, "IMTIBOT: An Intelligent Mitigation Technique for IoT Botnets," Future Internet, vol. 16, no. 6. MDPI AG, p. 212, Jun. 17, 2024. doi: 10.3390/fi16060212.
[58] B. Bojarajulu and S. Tanwar, "Customized convolutional neural network model for IoT botnet attack detection," Signal, Image and Video Processing, vol. 18, no. 6–7. Springer Science and Business Media LLC, pp. 5477–5489, Jun. 17, 2024. doi: 10.1007/s11760-024-03248-4.
[59] K. Kaur, A. Kaur, Y. Gulzar, and V. Gandhi, "Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies," Frontiers in Computer Science, vol. 6. Frontiers Media SA, Jun. 26, 2024. doi: 10.3389/fcomp.2024.1420680.
[60] M. Gelgi, Y. Guan, S. Arunachala, M. Samba Siva Rao, and N. Dragoni, "Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques," Sensors, vol. 24, no. 11. MDPI AG, p. 3571, Jun. 01, 2024. doi: 10.3390/s24113571.

Authors

Mr. Vibhor Harit is currently pursuing a Ph.D. in Computer Science and Engineering from Desh Bhagat University, Punjab, with more than 15 years of experience in academia and various technological domains, he is a passionate educator, researcher, and mentor committed to advancing the field of computer science education. Mr. Harit's research interests span Machine Learning, Artificial Intelligence, IoT Security, and Cloud Computing, where he continues to explore innovative solutions to emerging technological challenges. He has published several research papers in reputed IEEE conferences and Scopus-indexed journals. Throughout his career, he has contributed to academic excellence through his active involvement in teaching, curriculum development, and research initiatives. His current doctoral research is centered on developing optimized and hybrid approaches for IoT-based intrusion detection systems using Deep Learning, aligning with the growing global emphasis on cyber security and intelligent systems.

Dr. Rajeev Dhaiya is a distinguished academician and seasoned professional in Computer Science and Engineering with over 18 years of experience in teaching, research, and academic leadership. He is currently serving as a Professor in the Department of Computer Science and Engineering at Desh Bhagat University, Mandi Gobindgarh, where he contributes to academic excellence, research growth, and institutional development. Dr. Dhaiya holds a Ph.D. in Computer Science & Engineering with specialization in Vehicular Ad Hoc Networks (VANETs), supported by extensive work on routing protocols, soft computing techniques, and network optimization. He has published numerous research papers in national and international journals and conferences, including contributions in areas such as cloud computing, wireless networks, VANETs, and software development. Dr. Dhaiya is also an active researcher with multiple patents, reflecting his continuous commitment to technological innovation.

Dr. Umang Garg is currently working as an Associate Professor and Cluster Lead Cyber security and Intelligence in IILM University, Gurugram, Haryana, India. Dr. Garg is a distinguished academic leader, researcher, and innovator in Computer Science and Engineering. He is a dedicated educator with over 16 years of experience, has been deeply involved in research throughout his career. His research focuses on cyber security, with contributions in IoT security, adversarial machine learning, and IoT. He has published in reputed publishers such as IEEE, Springer, Wiley, and Taylor & Francis. Dr. Garg frequently collaborates with researchers to conduct reviews and longitudinal research on IoT security and machine learning. He is also a keynote speaker at national conferences and symposiums. He is an active member of IEEE. He has published multiple Scopus, Web of Science, and peer-reviewed articles on the effectiveness of malware detection and prevention.

REVIEW ARTICLE

How to cite this article:

Vibhor Harit, Rajeev Dahiya, Umang Garg, "Machine Learning Approaches for IoT Botnet Detection and Mitigation: A Comprehensive Review", International Journal of Computer Networks and Applications (IJCNA), 12(6), PP: 936-952, 2025, DOI: 10.22247/ijcna/2025/55.