International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

Machine Learning-Based Approaches for Prevention and Detection of IoT Botnet Attacks: A Comprehensive Review

[1]Neelendra Shekhar Gupta, [2]Satendra Kumar Jain

[1]MTech Scholar, Department of Computer Science and Engineering, Lakshmi Narain College of Technology, Bhopal

[2]Assistant professor, Department of Computer Science and Engineering, Lakshmi Narain College of Technology, Bhopal

[1]neelendrashekhar@gmail.com , [2]satendrakj@lnct.ac.in

ABSTRACT:

Significantly, the expansion of the Internet of Things has connected a complex web of devices better than ever before, riveting critical security risks. A trend has emerged that botnet attacks are a major problem in the IoT environment. In particular, Distributed Denial of Service (DDoS) attacks are an acute barrier to the IoT every now and then because of the nature of IoT environments. The traditional security mechanisms, the signature-based methods of detection, have been criticized by some researchers as they fail to recognize attacks based on the new version of novel and dynamic patterns. Thus, machine learning (ML) and deep learning (DL) have gained importance for the detection of both known and unknown threats through behavioral analysis. In this review, an elaborate discussion is presented on different traditional ML and DL strategies in order to prevent and detect IoT botnet attacks and their kinds. This includes both signature-based and anomaly-based, the focus being on the way each technique operates, the dataset upon which it was built, performance criteria, and drawbacks. Special attention is paid to recent advancements in deep neural networks and autoencoders, and hybrid frameworks that involve learning paradigms, concocting higher accuracy in detection. It will then discuss the few public datasets that may alternatively be used, issues with the feature list, consideration of a clear downside and a clear application scenario when it comes to evaluating parameters in the results. Despite numerous significant advancements, several issues linger, including data imbalance, cross-environment generalization, false positive rates, and computational overhead. This paper schedules an open research issue and suggests, implicitly the future direction-with, shorter models, real-time detection systems, and getting the opportunities enhanced IoT security.

Keywords: Internet of Things (IoT), Botnet Attacks, Machine Learning, Deep Learning, Intrusion Detection System (IDS), Distributed Denial of Service (DDoS)

1. INTRODUCTION

The rapid evolution of the Internet of Things (IoT) has resulted in various ways of making our assets, equipment, and resources interacts, communicates, or services in various other domains from healthcare to smart homes, from transportation to industrial automation. The IoT helps connect entirely heterogeneous devices such as sensors, smart appliances, wearable gadgets, and the realm of embedded systems thus making all the systems processes more efficient, productive and user-friendly. However, the expanding attack surface that comes with such

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

growth in interconnectivity poses security hazards as IT systems of the IoT ecosystems get stepped up to withstand external and internal cyber threats [1]. Foremost, botnet attacks imminently emerge as posing perhaps the largest risk for the security of IoT infrastructures, introducing risks gravely concerning especially when they come through not only individual users but also large network infrastructures. IoT botnets are compromised device networks that an attacker manipulates to perform coordinated malevolent activities-including Distributed Denial of Service attacks, spam, data theft, and unauthorized access. In an IoT system, such attacks use inherent security weaknesses, such as poor methods of authentication, lack of firmware updates, limited computational resources, and bad security configurations [2]. Devices become part of a botnet once successfully compromised and can be remotely controlled through command-and-control servers to pull off large-scale cyberattacks. The Mirai botnet example demonstrated the catastrophic potential of IoT botnets by disrupting major online services through enormous DDoS traffic, illustrating the urgent necessity for strong defense mechanisms. Traditional security mechanisms like signature-based intrusion detection systems (IDS) and rules-based firewalls are commonly used to detect and counter cyber threats. However, these approaches are largely effective for recognized attack patterns and lack the ability to spot or fend off newly emerging threats [3]. The figure 1 illustrates how attackers exploit zero-day vulnerabilities while software teams identify, disclose, and patch them through a coordinated update process.

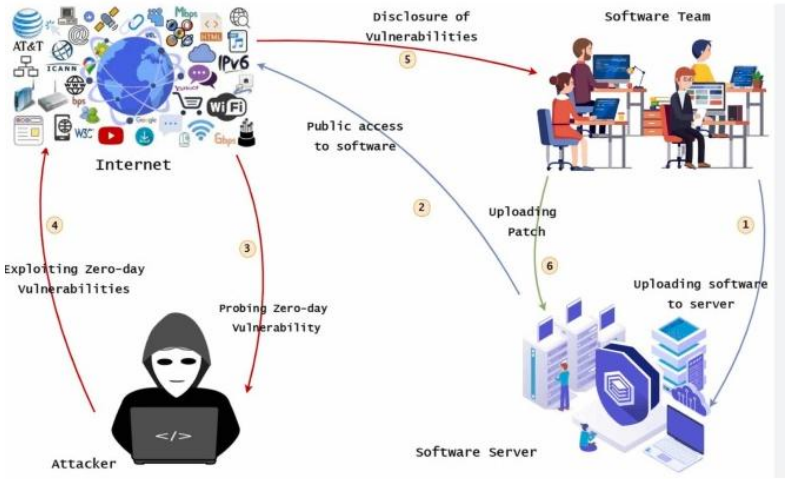

Figure 1: Lifecycle of Zero-Day Vulnerability Exploitation and Patch Management Process

Moreover, these traditional methods cannot operate in scenarios such as the IoT, where the attack pattern is highly volatile and diversified. Plus, the resource constraints of IoT devices would deny the direct deployment of any sophisticated security system on the devices, thereby calling for more intelligent and adaptive solutions. In recent years, Machine Learning (ML) has emerged as a powerful tool for enhancing cybersecurity, especially dismissing attacks from IoT botnets. These approaches have directed themselves towards data-driven techniques that would help in pattern learning over normal or malicious behavior depicted through network traffic; this would enable them to identify anomalies and unseen attacks from before [4]. They

accompany the capacity to analyze huge volumes of data on-the-fly and are, thus, suitable for dynamic and centralized IoT-embedded environments. Many well-proven Machine Learning (ML) algorithms that include Decision Trees, Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), and Naive Bayes are utilized widely for the duties of intrusion detection and botnet classification [5].

Deep learning approaches provide great benefits concerning extraction of features in a large dataset with higher dimensions by some automatic manner. Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), Recurrent Neural Networks (RNN), and autoencoders showed precision in the identification of more sophisticated cyber threats like IoT botnet attacks. These models are able to learn spatial and temporal patterns in network traffic, thus providing a better insight into attack behaviors. Furthermore, hybrid models combining machine learning and deep learning techniques could further enhance detection accuracy and reduce false positives. Although machine learning (ML) and deep learning (DL) algorithms have made substantial progress in detecting false alarms, they are still plagued by a number of challenges [6]. The most serious of these is the lack of access to the right kind and quality of datasets for training and evaluation. Many of the existing datasets are either out of date, imbalanced, or lack sufficient diversity, greatly reducing the generalization ability of the models trained on these datasets. Furthermore, feature selection can significantly improve model accuracy while reducing the required computational cost under resource-constrained IoT environments. Another challenge that needs to be addressed is the high number of false alarms, which will create unnecessary resource consumption while undermining the confidence in the detection system [7].

Additionally, there are issues of scalability and real-time processing in large-scale deployments of IoT. The number of connected devices is persistently increasing; this results in data explosively increasing in volume for purposes of better data processing and analytics. Within the IoT domain, models that are lightweight and energy-efficient are essential for their seamless integration. They should be given in such a way that their performance is not jeopardized. There are some emerging batteries such as edge computing and federated learning that could provide quite effective solutions by allowing decentralized data processing and joint training while concerning data privacy. This review paper intends to offer an inclusive discourse on machine-learning techniques in use for the prevention and detection of IoT botnet threats. Drawing upon a detailed literature review, the study has presented classification of various detection techniques that exist in the field along with their associated pros and cons [8]. The study also examines a limited number of commonly accepted datasets, feature engineering, and evaluation metrics usage for the attacks. The main gaps relevant in between and thus can guide future works are also discussed, such as how the future projects should address the development of secure, adaptive, scalable, and lightweight solutions that also incorporate an element of context for deployment in IoT scenarios. Therefore, securing the Internet of Things (IoT) has to become an equally pressing concern as it continues to proliferate worldwide and beyond into critical infrastructures. Using machine learning or deep learning techniques to overcome the intrinsic weaknesses of traditional security measures has become significant. But major hurdles still

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

need to be addressed, and new investigative studies will enlighten new angles to solve existing challenges and develop reliable, scalable, and efficient security mechanisms capable of countering the growing onslaughts of IoT botnet threats. The review presented herein is a valuable resource for researchers and practitioners interested in advancing the domain of IoT security through intelligence and data-driven solutions.

2. BACKGROUND OF IOT AND BOTNET ATTACKS

The internet of things (IoT) can be imagined as a new paradigm in modern technology, in which physical objects are paired wirelessly through the internet to gather, exchange, and process data with very little human intervention. In most cases, IoT ecosystems contain a variety of devices such as sensors, actuators, smart home appliances, wearable devices, and industrial control systems. These devices use various communication protocols and find numerous applications in sectors, such as healthcare, agriculture, smart cities, and industrial automation. While IoT improves operational efficiency and automation, its speedy growth comes with pressing security concerns, because of weak device security settings, small computational capacity, and a lack of standardized security frameworks [8]. The biggest threat is massive botnet-based attacks on IoT environments. Botnets refer to a network of compromised devices called "bots" or "zombies" directed by an attacker known as a botmaster. In IoT botnets, the vulnerable IoT devices are taken over completely through malware and controlled from the C&C server. They are then used as a weapon against the real victims by participating in DDoS attacks, among others. Through this means, the bots are used to perform tasks such as data exfiltration, phishing, or mass-spam campaigns. Poorly secured IoT devices—poised for the taking—allow a situation in which massive botnets can be easily built, proliferated, and skillfully directed to cause attacks [9].

The lifecycle of an IoT botnet attack typically consists of a few different steps: scanning, exploitation, malware injection, command and control communication, and action of malicious activities. First, the attackers have to scan the networks to gain access to devices whose defenses are compromised with an open port or weak credentials. For devices thus identified, they initiate attackers to infect their malware into the devices, thus earning them with bots. And, these bots keep on communicating with their botmaster by allowing their masters to give them commands in order to precipitate synchronized attacks. The distributed nature of IoT devices implies that botnets are difficult to spot and to reduce using conventional defense techniques. Botnet attacks via IoT are dangerous as they can be conducted on a large scale, are unified and use 'junk' traffic in huge amounts [10]. This danger will worsen due to the absence in most IoT machines of proper security updates and default credentials. Unlike other computers, IoT devices are often lacking in such operations as rebooting, going to sleep, or being taken offline. This makes them rather attractive for various types of persistent attacks, additionally. This dictates the necessity of understanding different aspects of botnet attacks in order to devise detection and defense measures that can achieve some desired level of confidence [11]. The listed table 1 shows ten most common IoT botnet attacks along with the peculiar characteristics, methodology, target patterns, impact, and possible challenges.

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

Table 1: Types of IoT Botnet Attacks

S. No.	Type of Attack	Description	Attack Technique	Target	Impact	Advantages (for attacker)	Limitations
1	DDoS (Distributed Denial of Service)	Overwhelms target with massive traffic from multiple bots	Flooding (TCP/UDP/HTTP)	Servers, websites	Service disruption	High scalability	Requires large botnet
2	Mirai Botnet	Exploits weak credentials in IoT devices	Brute-force login	IoT devices	Large-scale DDoS	Easy propagation	Detectable patterns
3	Phishing-based Botnet	Uses bots to distribute phishing links	Social engineering	End users	Data theft	High success rate	User awareness reduces success
4	Spam Botnet	Sends bulk unsolicited emails	SMTP exploitation	Email systems	Network congestion	Low cost	Easily filtered
5	Data Exfiltration Attack	Steals sensitive data from devices	Malware injection	IoT databases	Privacy breach	High-value data gain	Requires access control bypass
6	Cryptojacking	Uses device resources for crypto mining	Malware scripts	IoT devices	Resource exhaustion	Continuous profit	High energy usage detectable
7	Command Injection Attack	Executes malicious commands remotely	Input manipulation	Embedded systems	Full system control	Direct access	Needs vulnerability

8	DNS Amplification Attack	Amplifies traffic using DNS servers	Reflection attack	Web servers	Bandwidth exhaustion	High amplification	Depends on open DNS servers
9	SYN Flood Attack	Exploits TCP handshake process	Half-open connections	Network servers	Resource depletion	Simple execution	Mitigation techniques exist
10	IoT Worm-based Botnet	Self-propagating malware across devices	Automated scanning	IoT networks	Rapid infection spread	Fast propagation	Network segmentation reduces spread

3. TYPES AND LIFECYCLE OF IOT BOTNET ATTACKS

IoT botnet attack sophistication is rising as devices find themselves more inter-connected at the rapid pace and with relative lack of security. Broadly speaking, these attacks can be classified according to their functionality and attack approach. Among the most common types of botnet attack are Distributed Denial of Service (DDoS) attacks, which involve sending huge amounts of traffic to a target's system; scanning attacks, where perpetrators identify vulnerable devices; malware injection, which spoils devices; and data exfiltration attacks, seeking to steal confidential information. Moreover, IoT botnets are often used for spamming, outbox phishing, cryptojacking, and command injections. Each type of attack exploits various vulnerabilities but with the ultimate aim being to gain unauthorized control over IoT devices and use them for malicious purposes [11]. Usually, an IoT botnet attack has several stages in a fixed process that allows the attacker to build and effectively use botnets. The first is called scanning, where attackers scan networks to detect incompetently secured IoT devices with default credentials or open ports. Next is the exploitation stage, where the vulnerabilities found are exploited to gain access. Then all concerned devices are injected with malware, which eventually acquires the standing of modified nodes or zombies [12].

Connected, basically the devices create communication with the Command and Control (C&C) server, which serves as an overall authority for instruction delivery. This part is considered botnet connection. Subsequently, upon the commands giving the malicious activity to engage in the synchronized destruction by the compromised device, this is termed as command execution. Then, the maintenance and updates stage consistently updates the main malware, maintains undetectability, and recruits new devices so the botnet may operate for an indefinite time. The understanding of the types and life cycles of IoT botnet attacks is important for coming up with proper shielding and detection mechanisms, particularly machine learning techniques for spotting the attack at the beginning.

4. MACHINE LEARNING TECHNIQUES FOR BOTNET DETECTION

A two-staged machine learning method for IoT botnet detection was proposed in recent research [1]. The focus was on early-stage scanning followed by DDoS attack identification. For improved accuracy on multiple datasets, deep learning models especially ResNet-18 were used. One big part of the study was the construction of the all-comprehensive dataset that combines scanning and DDoS traffic. The model provides good performance results concerning accuracy, precision, recall, or F1 score. It shows higher generalization over single-dataset models. However, one of the pitfalls of the technique is its high computational complexity from deep-learning models. The system performs while facing deployment challenges in the event of IoT environments that are resource-constrained. An advanced intrusion detection system which incorporates machine learning with deep learning technologies for big data-based IoT ecosystems was presented in [2]. This proposed framework targets the improvement of detection accuracy with large scale network traffic processing: this compared to the use of multiple learning models, primarily because of their usefulness in reducing false positives and enhancing reliability. It provides in-depth study of multiple attack patterns existing in cognified networks. It has been noted that hybrid models based on deep learning present higher performance in comparison with traditional ID signatures. However, the integration of different models increases the computational load of the model. Works lack real-time details concerning the viability of the IDS in real-time environments. Scalability challenges are found in highly dynamic IoT environments. The authors in [3] describe the development of an adaptive deep learning system for real-time monitoring and alerting-in healthcare IoT applications. The research is oriented around IoT-based continuous monitoring and anomaly detection to show that the proposed deep learning technique can guarantee timely alerts and improved system responsiveness. A preliminary indication that Deep Learning techniques can be effectively applied to IoT security is exhibited by MILDCOM. In response to the described data position, we need to underline that real-time processing of data is so far better known. Nevertheless, the attempt is to establish a universal method as the domain-dependent design is not good for other tasks related to network security. The research lacks any testing against security data sets studied so far. The work does not show how the system can be tested by combining the intrusion detection modules. A promising deep learning-based intrusion detection method is proposed in [4]. To foster classification accuracy, the system presents a method to select significant features from huge datasets. An integration of different optimization strategies to eliminate redundancy and bolster performance capability is also presented. With an increased rate of positivity, the model is now good at detecting attacks perpetrated by IoT botnets. The experiment works display great efficiency compared to "traditional" models based on machine learning; however, we must consign our attention to the fact that a very heavy pre-processing job is involved due to the feature selection. The approaches seem not to be useful on unseen data; real-time applicability has to be verified. The work in [5] presents a deep learning solution for identifying and tracking IoT botnet activities, emphasizing tracking malicious behaviors patterns through time. The paper suggests that

security management is improved when detection and monitoring mechanisms greatly integrates. This model performs remarkably on the identification of botnet traffic across various occurrences, but dataset quality and availability, overhead, overfitting, among others, are crucial factors dictating model performance, and they need to be well addressed. Moreover, computational costs are very high because of massive model complexity, thus demanding huge resources. Real-world deployment issues still stand up to this day. A deep learning-based detection system for RPL attacks in IoT mobile networks is presented in [6]. The vulnerability is specifically in the routing protocol of IoT systems. In this proposed method, advanced deep learning models are used for the detection of anomalous routing behavior which results in improved detection accuracy in dynamic network conditions. The proposed method is found ineffective for other types of attacks. However, generalization to other types of botnet attacks is not covered. The model is demanding in computational resources. Lightweight implementation may never be an option. The research in [7] introduces a machine learning-based framework for detecting Man-in-the-Middle (MITM) ARP spoofing attacks. The model analyzes network traffic features to identify anomalies. It demonstrates improved detection performance compared to traditional methods. The approach is effective for network-level security threats. However, it focuses on a specific attack scenario. It does not address large-scale IoT botnet attacks. Scalability issues are not discussed. Integration with broader IDS frameworks is limited. The research encompassing the implementation of a bot-detection system using machine learning techniques obtains an approximate identification effectivity, relying on the fusion of disparate attributes in time and semantics. On account of the performance on several feature types combined as presented in different scenarios is proving very commendable - essentially so in detecting automated bot-like activities. The model has been successful in exposing its sheer effectiveness in the dense social networking scenarios rather limited in IoT environments. A very well-trained dataset could become practically induced to the system. Experiments of the model are given using futuristic adaptation. Generalization over different fields remains an issue. In [9], the work aimed at providing a light weight deep learning model for recognizing identity attacks from non-humans. The model was developed with a focus on efficiency and greatly reduced computation. The model can be deployed in resource-constrained environments and yield good accuracy using minimal resources. The main limitation of the model was that it can detect identity threats but not exactly IoT botnets. Furthermore, the identification capability of the proposed model is restricted to specific scenarios without exploring large scale of IoT networks. No effort was made towards scaling the model and making it suitable for broader applications. The internet-based electric scooter sharing service is widely recognized by the operator Bird as promoting green urban transport. It is fashionable to prefer non-car transportation. The service is extremely popular among youth as they are open to new ideas that focus on the environment. Other important groups are people between 30 and 50 who have a propensity for pursuing new ideas aimed at saving the environment. This industry is now in danger of turning into a monopoly with a high concentration of one type of customer. The work presented in [11] introduces a deep learning-based security architecture that involves an energy anomaly detection mechanism for network

intrusion detection. The technique concentrates on scrutinizing the energy consumption patterns for malicious activities in IoT networks. The model is made to exhibit good performance in detection and is among very few models where dependency on features actually got reduced. The work may pose a risk of generating false positives with environmental change. Noise immunity is also the key problem, hindering the realization of true application. The method might have a dire footprint of the non-alleviant noise in IoT device data. The findings also, in delicate terms, do not validate across the IoT devices. It requires further validation. An interpretable deep learning-based intrusion detection system for heterogeneous networks has been proposed in [12]. The model emphasizes transparency and explainability in DL models. It raises trust in automated detection systems, ensuring that the approach provides high accuracy while providing explanations of its decisions. The issue of interpretation comes with computational overhead and does not go well with real-time processing. The performance of the system can be heavily affected by the choice of data. Scalability is a major concern. A machine-learning based DDoS attack-detection approach is brought to light by [13]. The method identifies the abnormal behavior on the ground of analyzing traffic patterns. In a controlled environment, it potentially delivers a high rate of accuracy. Processes are put into practice for large-scale attack detection in a wireless world. However, the method could possibly perform less well in the encrypted traffic. The feature selection plays a pivotal role in the performance. The model is not adapted to anticipating attack patterns. Its real-world verification is yet to be provided. Lastly, the Cortes-Garcia et al. IDS approach, based on deep learning techniques, is implemented through the use of CNN and Transformer models. One of the key features that help this hybrid model is its capability of feature extraction and time domain analysis. High attack detection accuracy is obtained for IoT networks. Implementation of the Transformer also enhances the capabilities of sequence learning. However, this model is computationally expensive, which creates more difficulty in deployment scenarios in IoT environments, given that IoT environments are typically resource-constrained. A large dataset is needed for training the IDS, and all data processing must be done in real time.

5. DEEP LEARNING-BASED DETECTION APPROACHES

The research work considered a deep learning-based intrusion detection system for IoT networks through a combination of CNN and Transformer models. It combines CNN for spatial feature extraction and Transformer for capturing temporal dependencies in network flows, and the architecture hybridization consequently acts towards increasing detection accuracy for complex attack patterns. From the research, the proposed solution has outperformed traditional deep learning models in experiments. However, tremendous computational resources burden these methods. Thus, these types of architectures may not be suitable for the resource-constrained IoT devices. The chapter has not given the needed justification to tap this technique into real-time deployment. For fulfilling practical deployment, this implementation of training requires optimization. In [15], an algorithm for hybrid reinforcement learning for intrusion detection and their mitigation system is presented from encrypted network traffic. The system learns attack patterns dynamically and adopts mitigation strategies in addition, to efficient security in environments where traffic inspection is limited by encryption. In the particular

instance of the system, we assume a static network while the environment is dynamic. Better models for the identification of byte sequences of attack patterns are possible in future. This system showed better adaptability with r high resilience in decision making. However, the challenge of time lags while training reinforcement learning models is significant. The system requires continuous learning for optimal performance. Computational overhead is significant. Scalability to large IoT networks remains a concern. Next, in [16] have made a systematic review on deep-learning-based intrusions detection systems using narrative extracts for networks on IOT. Improvement is being sought on the transparency and interpretability in DL models. Different Explainable AI Techniques have been analyzed and compared. The security of the system is mainly based on trust, the paper suggests. However, a trade-off between accuracy and interpretability remains a challenge. For many models, computational complexities have been increased. So, the application in real time is minimal. In turn, this review contemplates the need for elementary explainable models. In this study, the paper presented a challenge on a minimalistic technique suiting lightweight design requirements such as embedded-style application software for the device. In a global perspective, despite the huge diversity, there is a severe race in the management of lightweight IoTs. Features of provided software comprise software demonstration for the claim of practical applicability, which lures to more prominent outcomes on behalf of the considerable range of applications previously introduced in this research. Still, a few contradictions are detected when light of perspective is put back on the IoT picture. Light application means performance improvements where cores are concerned because of the ultra-embedded nature of an application running on them, whereas field application assignment of sensor-to-gateway communication simplifies the tasks of the gateway, decreasing the resources required for OTA down load and server feature. A study in [18] has given a detailed view on Machine Learning-based IoT botnet detection methods. ML models are divided into numerous categories, as well as the data sets and evaluation metrics utilized in this study. This report highlights certain key challenges, such as dataset imbalance and high number of false positives. Opportunities for further research to improve the detection systems are discussed here. The review provides an understanding of the different ways already described. But, test results are not included. Comparison of performance is lacking. Implementation aspects in practice are not elaborated on.

Hence, IoT botnet detection was compared with deep learning and traditional machine learning methods. Studies for this purpose were conducted using several datasets. Deep learning models deliver satisfactory results frequently above traditional methods. However, a major benefit of ML models lies in their greater efficiency for a lower computational cost. The framework is balanced in its consideration of the performance and the complexity. The limitations include: Datasets need to be of high quality. Hence, generalization is still an issue for common use across different environments. The last subset of these limitations would see the resolution of real-time security. It contains myriad attack scenarios and exhibits realistic traffic behavior, with the purpose of enabling ML and DL model preparation and testing. While the data confirms one fact---up-to-date datasets are necessary---compiling it and labeling it are not so easy endeavours. The dataset could, nevertheless, be limited or lacking in types of attacks, for

which baseline comparatives are limited...hence, further validation towards hands-on applications is still quite strongly enticing. So, in [21], an IDS with machine learning that utilizes sophisticated preprocessing and feature generation is introduced. The article entails the truth that carefully chosen preprocessing might give state-of-the-art performance of deep learning. It crunches the computation while keeping high accuracy. The framework suits for practical use. The feature engineering requires domain knowledge. Nevertheless, it is questionable as to whether the technology can accommodate a change of attack profile. This is where the issues of scalability are still red herrings. However, unfortunately real-time validation is still a challenge. In [22], research focuses on improving security in software-defined networks using deep learning methods. This is achieved through the proposal of a model that we propose for enhanced intrusion detection through network-analysis capacities. The model is mostly dependent on SDN architecture for control and monitoring functions to act in an improved detection capacity. However, scenarios of IoT security integration are still not directly addressed by the research postulation. The system demands high computational resources. Scalability remains a concern. There is also some limitation on its real-time performance evaluation. Furthermore, a deep learning-based framework for real-time threat detection model is proposed for Internet of Things environments [23]. The project is focusing on real-time and accurate detection of threats. DL models are used to analyze network traffic. The system yields a great detection performance. Yet, with a real-time attitude, maximum resources are required. It may face latency issues. While the dataset covers a limited range of threat scenarios, it should be feasible for a large-scale deployment.

Botnet detection is an interdisciplinary problem in the cybersecurity space. In [24], (such a study) conducts a very thorough analysis of machine learning techniques for the detection of botnets. The paper illuminates existing ML algorithms, boom! its relative success understood. The article accentuates the strengths and shortcomings of infinite approaches. Fine results regarding feature selection are observed for their costlier model performance. Again, it provides the fact that the concern lying within the present approach remains mostly theoretical in nature. Very few experimental comparisons have been made, without any real time implementation. Hardly any mention is made of practical challenges. In [25], another intelligent ensemble model created for intrusion detection in IoT networks on the basis of intricate supervision through deep-learning is described. Its principle is simply employing many DL models to maximize the possibility of detection and simultaneously strengthen the protection measures against diversified attacks. The experiments imply that this outperforms the current models against cyber-attacks; however, the ensemble ones suffer from higher computational complexity. The historical operation times (i.e. training times) are revealing. Implementation into the IoT environment happens to be immensely tough for multilayered entity. Hence, optimization towards efficiency becomes a mandate. Lastly, [26] presents a machine-learning-based approach to detecting IoT botnets using modeling of energy consumption patterns. The models against energy usage anomalies to some extent confirm the occurrence of malicious activities within IoT devices of various nature for the first time; also, it seems to provide a novel perspective when it comes to detecting intrusions via energy

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

patterns-furthermore, making the detection method lightweight and suitable for IoT devices. However, false positives might be generated due to environmental variations. A big challenge includes gathering data because it serves no first purpose for providing the data. Lastly, one must keep in mind that the validity of the cross-comparison across devices ceases in this context, and validation thereof is greatly needed. Table 2 presents a concise overview of key challenges and limitations in existing IoT botnet detection approaches, highlighting their impact on system performance and potential improvement strategies.

Table 2: Challenges and Limitations in Existing IoT Botnet Detection Approaches

S. No.	Challenge	Description	Impact on Detection System	Existing Approaches Limitation	Possible Improvement
1	Dataset Imbalance	Most datasets contain more normal traffic than attack data	Biased model training	Poor detection of minority attack classes	Use data balancing techniques (SMOTE, GANs)
2	Lack of Generalization	Models trained on one dataset fail on others	Reduced real-world applicability	Overfitting to specific datasets	Use cross-dataset training and validation
3	High False Positive Rate	Normal traffic misclassified as attacks	Resource wastage and alerts overload	Low precision in detection models	Improve feature selection and hybrid models
4	Feature Selection Complexity	Large number of irrelevant features	Increased computation time	Inefficient model performance	Use optimized feature selection techniques
5	Resource Constraints in IoT	Limited memory, power, and processing capacity	Difficulty in deploying complex models	Heavy ML/DL models not suitable	Develop lightweight and edge-based models
6	Evolving Attack Patterns	New and unknown attacks emerge frequently	Difficulty in detecting zero-day attacks	Signature-based systems fail	Use anomaly-based and adaptive learning
7	Real-Time Detection Issues	Delay in processing large-scale data	Slow response to attacks	Batch processing limitations	Implement real-time streaming analytics

8	Scalability Issues	Increasing number of IoT devices	System performance degradation	Centralized models become inefficient	Use distributed and cloud-edge architectures
9	Encrypted Traffic Analysis	Difficulty in inspecting encrypted data	Reduced visibility of attacks	Traditional methods ineffective	Use traffic behavior analysis techniques
10	Lack of Standard Datasets	No unified benchmark datasets	Inconsistent performance evaluation	Difficult comparison across studies	Develop standardized and updated datasets
11	Model Interpretability	Black-box nature of deep learning models	Hard to understand decisions	Lack of transparency	Use explainable AI (XAI) techniques
12	Energy Consumption	High computational cost of ML/DL models	Reduced device efficiency	Unsuitable for battery-powered devices	Optimize models for low energy consumption

6. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

The rapid proliferation of the Internet of Things (IoT) has made the botnet attack risk a critical concern in modern network infrastructures. Here, we provide an exhaustive review article on the machine learning and deep learning-based frameworks to counteract and observe IoT botnet attacks. Various technologies such as conventional machine learning models, deep neural networks, and hybrid frameworks were examined in terms of methodologies, performances, and limitations. The analysis has revealed that while deep learning models generally result in better detection rates, they are highly computationally intensive and poorly interpretable, thus becoming rather unsuitable for IoT environments with resource constraints. The review also focused on the significance of datasets, feature selection, and evaluation metrics in the evaluation of detection systems. Some of the challenges which limit the efficiency of the present solution lies in the imbalanced datasets, continuously changing attack patterns characterized by heterogeneous new threats, a large number of false positives, and scalability issues. Regardless, machine learning-based methods hold significant promise in recognizing both known and unknown threats by implementing smart data analytics. The application of thin models, AI that will be explainable, and real-time detection capabilities would provide an extra push-up toward enhanced system performance. This provides the existing solutions with the correct understanding and some caveats, suggesting more efficient, quiet, and scalable approaches that will make IoT security quite robust in the face of emergent botnet threats. Develop lightweight adaptive machine learning models with interpretability in edge and federated learning for real-time, scalable IoT botnet detection.

REFERENCES

[1] F. Hussain, S. G. Abbas, I. M. Pires, S. Tanveer, U. U. Fayyaz, N. M. Garcia, G. A. Shah, and F. Shahzad, "A two-fold machine learning approach to prevent and detect IoT botnet attacks," IEEE Access, vol. 9, pp. 163412–163426, 2021, doi: 10.1109/ACCESS.2021.3131014.

[2] Abbas, Ghulam, et al. "An Enhanced Machine Learning & Deep Learning based Intrusion Detection System for Intelligent Network Security: A Comprehensive Analysis to Avoid Intrusions in Big Data-based IoT Ecosystem." The Asian Bulletin of Big Data Management 6.1 (2026): 26-33.

[3] Anandhi, S. V., et al. "Adaptive Deep Learning based Real-Time Intravenous Drip Monitoring and Alerting System." IETE Journal of Research (2026): 1-10.

[4] Harit, Vibhor, Rajeev Dahiya, and Umang Garg. "An optimized deep learning-based intrusion detection system for IoT botnets using hybrid feature selection." Recent Advances in Computational Methods in Science and Technology. CRC Press, 2026. 318-327.

[5] Wasswa, Hassan. A Deep Learning-Based Approach for Detection and Tracking of IoT Botnet Activities. Diss. UNSW Sydney, 2026.

[6] Ghouri, Muhammad Nadeem, et al. "Next-Gen IoT Security: Deep Learning-Based Detection of RPL Attacks in Mobile Converged Networks." IEEE Open Journal of the Communications Society (2026).

[7] Akram, Amna, et al. "Detection of MITM ARP Spoofing Attack: A Machine Learning-Based Framework." 2026 7th International Conference on Advancements in Computational Sciences (ICACS). IEEE, 2026.

[8] Ghosh, Dhrubajyoti, et al. "Machine Learning Based Bot Detection on X With Temporal and Semantic Feature Integration." IEEE Transactions on Computational Social Systems (2026).

[9] Kumara, Shiva. "A Lightweight Deep Learning Based Classification Models for Non-Human Identity Threat Detection." 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC). IEEE, 2026.

[10] Xia, Lin, Yuanhe Chen, and Lin Han. "A deep learning-based IoT malware detection approach for electric vehicle charging stations." Scientific Reports 16.1 (2026): 10607.

[11] Kongngam, Kititach, and Prusayon Nintanavongsa. "Deep Learning-Based Intrusion Detection for IoT Devices Using Energy Anomaly." 2026 18th International Conference on Knowledge and Smart Technology (KST). IEEE, 2026.

[12] Onuorah, Martins Onyekwelu, Yanxia Sun, and Daniel Mashao. "Toward Generalization and Interpretable Deep Learning–based Intrusion Detection System for Heterogeneous Network Environments." IEEE Access (2026).

[13] Čatloch, Dušan, et al. "DDoS Attack Detection Using Machine Learning." 2026 IEEE 24th World Symposium on Applied Machine Intelligence and Informatics (SAMI). IEEE, 2026.

[14] Marrah, Saio Alusine, et al. "Deep Learning-Based Network Intrusion Detection for IoT Using CNN and Transformer Models." (2026).

[15] Pagoti, Sai Akshita Dimpu, Teja Sri Pacharu, and Kamalakanta Sethi. "A Hybrid Reinforcement Learning Based Intrusion Detection And Mitigation System for Encrypted Network Traffic." 2026 18th International Conference on COMmunication Systems and NETworks (COMSNETS). IEEE, 2026.

[16] Ogunseyi, Taiwo Blessing, et al. "Performance Analysis of Explainable Deep Learning-Based Intrusion Detection Systems for IoT Networks: A Systematic Review." Sensors 26.2 (2026): 363.

[17] Vincent, Elvis, and Prabu Jayant. "DefenSys: An Integrated Platform for Malware Detection and Containerized Attack Simulation using Deep Learning."

[18] Faarax, Cabdiraxmaan Cabdinuur, and Gagan Sharma. "Machine Learning–Based IoT Botnet Detection: Techniques, Challenges, and Future Research Directions: A Comprehensive Review." International Journal of Research & Technology 14.1 (2026): 367-382.

[19] Ullah, Saeed, et al. "Comparative analysis of deep learning and traditional methods for IoT botnet detection using a multi-model framework across diverse datasets." Scientific Reports 15.1 (2025): 31072.

[20] Koppula, Manasa, and LMI Leo Joseph. "A real-world dataset "IDSIoT2024" for machine learning/deep learning based cyber attack detection system for IoT architecture." 2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT). IEEE, 2025.

[21] Eren, Kazim Kivanç, et al. "Simple yet powerful: Machine learning-based IoT intrusion system with smart preprocessing and feature generation rivals deep learning." IEEE Access (2025).

[22] Naik, SK Lokesh, et al. "A Deep Learning Based Security Enhancements in Software Defined Networks." 2025 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC). IEEE, 2025.

[23] Almalki, Sultan Saaed. "A Deep Learning-Based Framework for Real-Time Detection of Cybersecurity Threats in IoT Environments." International Journal of Advanced Computer Science & Applications 16.3 (2025).

[24] Gupta, Neha. "Advancements in Botnet Detection: An Extensive Analysis of Machine Learning Techniques." 2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI). Vol. 3. IEEE, 2025.

[25] Sharma, Himanshu, Prabhat Kumar, and Kavita Sharma. "Deep Learning based Ensemble Model for Intrusion Detection in IoT Network." 2025 International Conference on Innovations in Intelligent Systems: Advancements in Computing, Communication, and Cybersecurity (ISAC3). IEEE, 2025.

[26] Wakili, Almustapha A., et al. "Advancing Machine Learning Strategies for Power Consumption-Based IoT Botnet Detection." Sensors 25.24 (2025): 7553.