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 IoT Botnet Detection: Techniques, Challenges, and Future Research Directions: A Comprehensive Review

[1]Cabdiraxmaan Cabdinuur Faarax, [2]Dr. Gagan Sharma

[1]Department of Computer Science and Engineering,RKDF University, Bhopal, Madhya Pradesh, India

maamanlucky@gmail.com

[2]Department of Computer Science and Engineering,RKDF University, Bhopal, Madhya Pradesh, India

gagansharma.cs@gmail.com

* Corresponding Author: Dr. Gagan Sharma

Abstract

The rapid proliferation of the Internet of Things (IoT) devices has increased the attack surface of current networks, thus enabling IoT environments to be more penetrable to botnet-based cyber-attacks such as DDoS, scanning, malware spread, etc. The conventional simple security measures are often not much help because of IoT being highly diverse, highly resource-constrained, and large scaled. Therefore, ML and DL have been touted as promising mechanisms for facilitative-botnet detection in IoT. This review paper informs on those aspects of the recent ML methods from supervised, unsupervised, semi-supervised, and hybrid models that have been made use of in the exploration of novel ways of doing IoT botnet detections and analyses where forest Random, Support Vector Machine, ensemble, CNN, RNN, and Planning Systems are discussed critically in terms of detection efficiency, false alarm rate, and computational complexity. The paper also explores new paradigms like explainable artificial learning, federated learning, and the integration of cyber threat intelligence to promote the addictiveness and resilience of IoT systems. Even after achieving true detection accuracies greater than 95% from research exercises using benchmarked datasets, present approaches struggle with multiple shortcomings, which include class imbalance, lack of real-time deployment, high computational cost, nonexistent generalization capabilities to zero-day threats, and the fact that they do not work well for IoT devices. Through an extensive comparative analysis, a discussion of the existing vulnerabilities, and a summary of research gaps, this study altogether indicates the more desirable route of building efficient, scalable, and adaptive IoT botnet detection frameworks. While stressing the design of lightweight models, real-time detection, generalization across multiple datasets, and coupled prevention and detection mechanisms toward the building of resilient IoT cyber defenses, this paper discusses future research directions.

Keywords: IoT Security, Botnet Detection, Machine Learning, Deep Learning, Intrusion Detection Systems, Cybersecurity, Network Traffic Analysis

I. INTRODUCTION

The Internet of Things (IoT) has redefined technology by allowing real-world things to interconnect and interact with one another over the Internet, affecting human lifestyles.

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 |

Companies have witnessed an explosion in the smart IoT devices with increasing popularity, which include smart cameras, smart TVs, wearable devices, smart toys, and intelligent lighting systems. This trend in computing lets day-to-day things talk among themselves autonomously, thereby underscoring a diminished need for human involvement in creating a more connected, efficient, and smarter environment [1]. The IoT powers smart devices to automate operations, giving real-time analytics. IoT devices include consumer gadgets, wearables, connected cars, and smart city infrastructures. The main purpose is creating ordinary objects that can sense, process, and exchange knowledge to become more efficient, convenient, and accurate at decision-making. Such is tech that it drives transformation across industries, from healthcare to manufacturing, transport, and energy management [2]. Figure 1 represents Internet of Things (IoT).

Figure 1: Internet of Things (IoT)

Growth and Applications

The growth of the IoT ecosystem over the past decade is nearly exponential, driven by wireless technology, miniaturized sensors, cloud computing, and artificial intelligence. Around the globe, this march of billions of connected devices has launched a new era – one that promises to transform both personal and industrial landscapes. For smart homes, IoT is adaptable, providing control over lighting, climate, and security applications [3]. Wearable devices track health precise metrics, and thus provide essential clues for personalized health care. Industry deploys mature Industrial Internet of Things (IIoT) to deliver better production lines, to predict equipment failures in advance, and to increase throughput efficiency from supply chains. Smart cities mainly utilize this technology for smooth traffic, clean cities, and well-distributed energy for improving quality of life and sustainability [4]. The usage of IoT in agriculture is quite significant due to practices like precision farming, soil condition monitoring, and irrigation systems regulation. This slew of applications presents the transformative possibilities of IoT to each and every sector and evokes progressive changes in innovation and efficiency, while at the same time introducing some new challenges in terms of interoperability, scalability, and security [5].

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 |

a. IoT Architecture

The architecture of the Internet of Things (IoT) frequently consists of multiple levels, each performing dedicated roles to provide a nearly seamless service for connectivity and data processing at least. The perception layer or sensing layer captures and collects input data from the physical environment utilizing devices like sensors, actuators, and RFID tags. This is where physical events such as temperature changes, movement, or pressure are penetrated by digital signals [6]. The network layer ensures the data to reach from the field devices to the centralized servers or cloud platforms through various communication protocols such as MQTT, CoAP, or HTTP over wireless and wired networks. The processing layer does not refer to doing the calculation alone but rather refers to the combination with cloud or edge computing systems, providing aggregation, analysis, and storage services, facilitating intelligent decision-making [7]. The application layer, with dashboarding, mobile apps, or automated systems, delivers insights and services to end-users for human needs in domains such as smart homes, industrial monitoring, or healthcare alerts. There could also be in place a business layer that handles system management, service orchestration, and monetization strategies. The affected layered architecture accommodates the enormous scale and interoperability requirements for a rapidly growing environment of IoT networks [8]. Figure 1 represents IoT Architecture.

Figure 2: IoT Architecture

IoT Communication Protocols

IoT communication protocols facilitate efficient, reliable, and secure data exchange over networks among devices. They establish rules that govern data transmission, reception, and interpretation, helping ensure interoperability among heterogeneous devices [9]. MQTT, CoAP, and HTTP are protocols used in the departments of lightweight messaging, resource-constrained communication, and standard web-centric interactions. Proper selection of protocol is an essential benchmark for an IoT network to perform its best, reduce latency, and support its scaling needs.

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: Importance in Device Connectivity [11]

Protocol	Strengths	Weaknesses	Typical Use Cases
MQTT	Lightweight, real-time, low bandwidth	Requires broker, not ideal for high data volume	Smart homes, telemetry, sensors
CoAP	Low overhead, suitable for constrained devices, UDP-based	Limited reliability, smaller ecosystem	Industrial IoT, sensor networks
HTTP	Widely supported, integrates with web services	High overhead, slower on low-resource devices	Web-enabled IoT devices, APIs, dashboards

b. IoT Security Challenges

IoT security issues creep up due to the vast scale, diversity, and resource constraints of connected devices. Vulnerabilities in hardware, software, and communication protocols lead to IoT networks being open to attacks. Data integrity, privacy, and secure communication across such hetero.devices form the prerequisites of trust and reliability in any IoT environment [12].

Limited Device Resources: - The design challenge is significant for resource-constrained devices. A plethora of current assumptions rely upon substantial computational power, memory, and energy in such devices, however these resources seem to be unavailable. Such strong assumptions include the availability of encryption, authentication, and intrusion detection mechanisms requiring significant amounts of energy. These constraints allow the attackers to exploit simple, successful attacks to breach device integrity, load malware, or intercept sensitive information. In device-specific contexts, an appropriate lightweight security approach becomes paramount. Device-specific lightweight solutions optimized with respect to power consumption cannot neglect the operation of energy-efficient, secure performance; in this way, the IoT still remains uncertain while relying upon large numbers of devices that nearly work in the decentralized networks consuming data without interruption [13].

Heterogeneity of Devices: - IoT networks consist of a wide variety of devices having different hardware architectures, operating systems, communication protocols, and softwares. Such heterogeneity poses serious challenges in establishing standardized security policies across the network, thereby leaving devices with lesser security wide open. Along with security, when the devices do not get along with each other, the required authenticated sessions to encryption and data validation mechanisms will be thrown wide open, making the systems vulnerable. Moreover, managing updates or patches proves tremendously challenging, thereby increasing the risk of exploitation. Interoperability is a major concern when considering security. Security frameworks should bear the consideration of such diversity so that they can offer flexible, scalable, and adaptive solutions to all device types without undermining their functionality [14].

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 |

Network Vulnerabilities: - The potential of IoT from a network perspective is wireless communication with multiple kinds of technology, such as Wi-Fi, Bluetooth, Zigbee, and cellular networks. The security risks are highly likely like eavesdropping, threatening the integrity of assuring authentication channels between devices and networks, man-in-the-middle attacks, DDoS attacks making the network unavailable for continued development. Having network protocols which are feasible, lacking security settings, and wrong authentication processes lead to enormous difficulties for the IoT subjects of interest. This weakness is the same for a time and is very compromising against attackers whose motive is to illegally penetrate the system's information and disrupt its operation if not encouraged. When one adds devices on a large scale, then the chance of coordinated attacks trying at distributed denial of service, but by large-scale devices with the capability to form IoT botnets is even higher. The investment in protected channels of communication, as well as powerful detection of the intrusion, and the potential for ongoing observation of network traffic, is a must to fend off these vulnerabilities in IoT firewall [15].

c. Introduction to IoT Botnets

IoT botnets come into being when hackers remotely compromise different IoT devices so that behavior coordinated maliciously. Most IoT devices are infiltrated by malware through minor security vulnerabilities, old firmware, and outdated network environments. IoT devices once compromised thus lode itself silently in the botnet without alerting customers. The primary use of IoT botnets is for carrying out large-scale cyber-attacks characterized by DDoS attack, data extraction, and network scans [16]. Given the proliferation of IoT devices and their relatively low levels of security, botnets have a significant number of threats to network stability and data protection, and critical infrastructure security. Figure 2 represents IoT Botnets.

Figure 3: IoT Botnets

Table 2: Key Characteristics [17]

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 |

Aspect	Description
Definition	A collection of IoT devices infected with malware and controlled by a centralized attacker
Control Mechanism	Command and Control (C&C) servers or peer-to-peer communication
Device Types	Smart cameras, routers, wearables, sensors, home appliances
Stealth Nature	Operates silently without user awareness
Scalability	Rapid expansion due to large IoT deployments
Attack Capability	Enables large-scale coordinated cyberattacks

Lifecycle of IoT Botnet Attacks

The IoT botnet attack workflow, which starts from the scanning phase, is designed to find IoT devices that might be vulnerable due to weak credentials or outdated variety of firmware aboard the internet. After finding such devices, malware is introduced through them into the IoT devices updated for attackers' control [18]. The infected devices are now connected to the command and control servers' remote management of the botnet. The compromised devices set up scans to search for more devices to be infected, thereby enlarging the speedily expanding botnet network. Once the botnet goes live in the execution phase of an attack, the botnet would execute any number of malicious actions, such as DDoS, malware dispersal, etc [19]. At this moment, understanding the workflow of the attack is pivotal when it comes to design to prevent such attacks and detect such threats. Figure 4 represents Lifecycle of IoT Botnet Attacks [19]

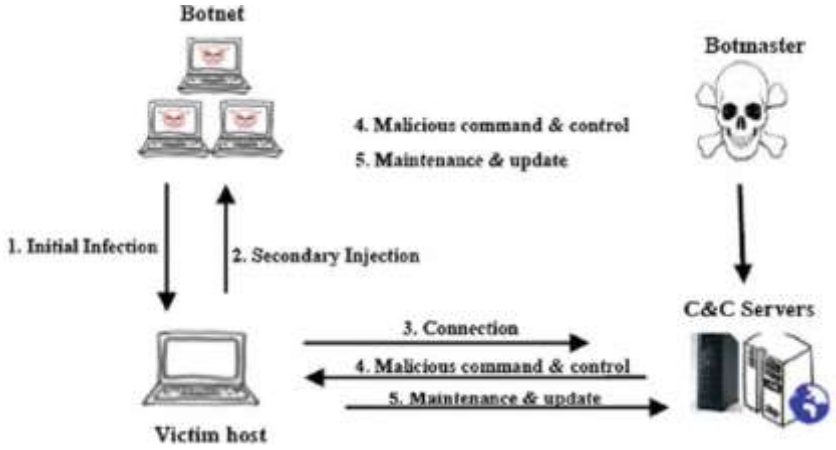

Figure 5: Lifecycle of IoT Botnet Attacks [19]

d. Types of IoT Botnet Attacks

Exploitation of IoT botnets for the purpose of orchestrating joint malicious actions against systems and networks is a serious concern today. The motivation behind these attacks is to leverage the capability of massive distribution and weak security of IoT devices to infiltrate

businesses, exploit services, and steal out valuable information. Knowing what types of attacks are there is critical for successful mitigation [20].

Distributed Denial of Service (DDoS):- DDoS attacks continue to be a devastating IoT botnet attack type. For such an attack, a huge number of compromised IoT devices will simultaneously send a huge volume of data to the victim machine, service, or network, to exceed the point where they are able to deal with the requests while still being available to legitimate users. Because of the IoT devices being spread all over the globe and having a persistent on state, the smart cameras, routers, and home appliances are perfect bots with the ability to generate a high amount of traffic. Detection and mitigation of IoT-based DDoS are difficult to protect against because the traffic types are often indistinguishable from the legitimate traffic produced by trustworthy sources. The cases of high-profile attacks by the Mirai botnet itself provide clear-cut proof of the capability of IoT botnets to disrupt critical internet infrastructure. These attacks cause financial losses, service failures, and reputational harm; thereby showcasing the need for intelligent detection and protection mechanisms [21].

Malware Propagation: - IoT botnet malware proliferation refers to the fast transfer of malicious code from one infiltrated device to another within the network or across the Internet. If the attackers exploit flaws in place so devices can be infected with default passwords, no updates, or open ports, the malware will spread to new devices. Once a device is infiltrated, it starts active scanning for more vulnerable IoT nodes. This exponential growth of botnets has been identified by an efficient expanding propagation mechanism. This kind of automatic propagation process means that being able to create large botnets in a short period. Malware spreading enhances the scalability and power of botnets but in reality decreases the performance of devices and network reliability. Malware affects devices in the ways of abnormal operation, increased power consumption, etc. An infected device can eventually completely fail. The stealthiness of malware propagation makes it very hard to detect so early-endorses need for machine-learning approaches that recognize unknown patterns of behavior in IoT traffic [22].

Data Exfiltration and Privacy Breach: - Data exfiltration and privacy breaches often take place when IoT botnets are misused for gaining sensitive data within traditional devices and networks. IoT devices tend to store personal, operational, or environmental data, which are some reasons why these devices are appealing targets for hackers. Once these devices are exploited, they can send user credentials, location information, health records, or video feeds surreptitiously to servers controlled by the attacker. This anomalous data transfer is bound to be traveling through encrypted or obfuscated communication channels and is very hard to detect. A privacy breach caused by IoT botnets can also lead to identity data theft, financial threat, and invasion of privacy. Such breaches could also lead to legal and safety trouble where industry and health settings are concerned [23]. To defend against exfiltration of data in IoT systems, there is a current need for constant supervision, secure communication protocols with sophisticated, intelligent detection techniques that can catch suspicion from minute deviations in the regular pattern of data transmission.

II. MACHINE LEARNING TECHNIQUES FOR IOT BOTNET DETECTION

The rapid proliferation of the Internet of Things (IoT) networks has increased the exposure to botnet-based cyberattacks significantly due to device heterogeneity, reduced computational capacity, and lack of security configurations. Traditional rule-based and signature-driven intrusion detection systems most often prove to be futile against the more sophisticated and adaptable IoT botnets. Henceforth, machine learning (ML) and deep learning (DL) have emerged as viable alternatives for identifying malicious activities through intelligent network traffic behavior analysis. Various studies have demonstrated that ML-driven botnet detection ornamentals can accurately detect anomalous traffic behaviors and raise timely alerts with high false alarm rates, ultimately [1]. In addition, these ML methods have also morphed into intricate hybrid learning frameworks since becoming the most accurate model that regards both spatial and temporal dependencies in IoT traffic, makes probable risk assessment, and allows for enhanced operation in the event of any change in these dynamic attack strategies [2].

Feature engineering and optimization are central in enhancing detection efficiency, particularly in resource-constrained IoT environments. Deep learning-based IDSs which use hybrid feature selection techniques have proved substantial reductions in dimensionality and computational overhead, all this without compromising detection accuracy [3]. The optimized CNN architectures have shown strong performance in autonomous botnet detection by extracting discriminative network traffic features, achieving higher accuracy and reducing false positives [4]. Also, the more substantial integration of deep learning models with software-defined networking has eased centralized traffic monitoring, rapid attack mitigation, and scalable security management in extensive IoT deployments [5].

Search efforts have also identified and studied botnet command-and-control communication networks, essential for early detection. Considering the various architectures of deep learning models, several possibilities have been presented to detect these communications via automatic technologies among a wide variety of communication contexts and network sizes [6]. Comparative model evaluations using mixed ML and DL algorithms demonstrate the consistent superior performance of ensemble models, or in some contexts, deep learning models, in terms of detection accuracy, adaptability to different threat environments, robustness to various attacks, and enhanced generalization capabilities [7]. Feature learning via autoencoders has been particularly efficient in identifying the stealthy IoT botnet; the models learn latent representations underpinning normal and malicious data, thus facilitating the efficient identification of bots in inverse-probability-inferencing dimensionality-reduction-based unsupervised scenarios [8].

The spurt in adoption of encryption for network communications has added another layer of intricacy to botnet detection. Therefore, solutions based on advanced practices of knowledge distillation and multi-branch architecture have been suggested for detecting botnet activities in encrypted DNS traffic while protecting the privacy of a person [9], [13]. Furthermore, smart architectures adapted for AI-powered IoT environments are trying to integrate proactive mitigation capabilities, along with detecting the phenomenon, thereby making the system resilience go up before coordinated botnet attacks [10]. On the other front, reliable and trustworthy deep-learning frameworks have been designed for industrial IoT systems, aimed at

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 |

proving their reliability and stability, thus countering adversarial attacks in mission-critical environments [11].

It is attentively drawn upon advanced insights to explicitly argue that among the deficits have been left with class imbalance, interpretability, large-scale operations, and operation in real-time. Emerging agile paradigms, on the other hand, like quantum machine learning for anomaly detection, are foreseen to bring a fresh way for processing complex security data from IoT with twin fuel efficiency [12]. Moreover, ensemble-based setups have demonstrated better generalization and robustness across diverse attack scenarios, emphasizing the urgency of adaptive and scalable machine learning solutions for securing IoT networks against threats of botnet [13]. Emerging paradigms such as quantum machine learning have been explored for anomaly detection, indicating potential future advancements in processing complex IoT security data more efficiently [14]. Additionally, ensemble-based anomaly detection techniques continue to demonstrate improved generalization and robustness across diverse attack scenarios, reinforcing the importance of adaptive and scalable machine learning solutions for securing IoT networks against botnet threats [15].

Table 3: Machine Learning and Deep Learning–Based IoT Botnet Detection Research

Ref.	Research Aspect	Technique / Approach	Key Contribution	Major Outcome
[1]	ML-based botnet detection	Machine learning–driven anomaly detection and alerting	Intelligent analysis of IoT traffic behavior	Accurate detection with timely alert generation
[2]	Hybrid learning models	Spatial–temporal hybrid ML/DL architecture	Captures dynamic attack behavior and traffic dependencies	Improved detection accuracy and probabilistic risk assessment
[3]	Feature engineering	Hybrid feature selection with DL-based IDS	Reduced feature dimensionality and computation cost	Maintained accuracy in resource-constrained IoT environments
[4]	Deep learning optimization	Optimized CNN architecture	Efficient discriminative feature extraction	Higher accuracy and reduced false positives
[5]	Network-based security	DL integrated with Software-Defined Networking (SDN)	Centralized monitoring and scalable mitigation	Improved response time and network scalability
[6]	C2 communication analysis	Deep learning–based automation	Detection of command-and-	Early-stage and automated botnet detection

			control communications	
[7]	Comparative analysis	Ensemble ML and DL models	Evaluation across multiple threat scenarios	Superior accuracy and robustness
[8]	Feature learning	Autoencoder-based latent feature extraction	Detection of stealthy IoT botnets	Improved detection in high-dimensional data
[10]	AI-powered IoT security	Intelligent detection and proactive mitigation architecture	Integration of detection and response mechanisms	Enhanced resilience to coordinated attacks
[11]	Industrial IoT security	Trustworthy deep learning framework	Focus on reliability and stability	Secure operation in mission-critical environments
[15]	Ensemble anomaly detection	Voting-based and ensemble ML techniques	Improved generalization across attack types	Robust and adaptive botnet detection

III. DEEP LEARNING–BASED DETECTION MODELS

Recent achievements in Internet of Things(IoT) security research have been moving towards more intelligent and thoughtful approaches for such challenging tasks since these groups contend with the harsh attacks of large botnets. Quantum Machine Learning(QML) techniques seem another exploration trajectory that has been much inspired by the fact that quantum computing greatly enhances both learning algorithms for faster pricing and pattern recognition in such very complex IoT environments [16]. Along with it, research among deep learning-based techniques for intrusion detection systems has suggested the effectiveness of Convolutional, Recurrent, and hybrid neural networks in identifying IoT botnets.

However, the review papers discussed challenges in terms of the scalability, data imbalance problem, and real-time deployment [17]. The key to increasing intrusion detection efficiency in resource-constrained Internet of Things (IoT) networks is dimensionality reduction. They make particular choices: The deep learning–based feature reduction in combination with classification techniques has produced notable improvements in detection accuracy with a decrease in computational complexity and lessened memory usage [18]. Again, few-shot learning and deep reinforcement learning models become attractive due to their capacity to detect botnet attacks with limited labeled data and provide an answer to the lack of diverse and real IoT attack datasets [19]. These methods are in essence strong on how they can adapt to the new threat scenarios and hence are well-suited for dynamic IoT environments.

Privacy and decentralization have become crucial aspects of recent IoT security solutions. It has been proposed that Federated learning–based botnet detection frameworks being introduced can enable collaborative model training across distributed IoT devices without sharing raw data, and thus preserving privacy and maintaining competitive performance in detection [20]. Deep learning architectures such as stacked autoencoder–gated recurrent unit (SAE-GRU) models have been used for scalable botnet detection on smart city infrastructures and showed good performance under large-scale and heterogeneity networks [21]. Additionally, stacked ensemble learning techniques combining multiple classifiers have outperformed isolated classifiers in terms of high detection accuracy and generalization while also displaying good resilience for different attack patterns [22].

Domain-specific IoT environments have been widely explored. Several bio-inspired deep learning techniques have been used to develop an intrusion detection scheme for IoMT networks that ensure high sensitivity in the detection of botnet attacks while guaranteeing the reliability of healthcare systems [23]. Deep learning-based intrusion detection on optical networks has further broadened the scope of IoT botnet detection frameworks to high-speed communication environments [24]. With edge-based detection that capitalizes on modular neural network designs for botnet detection in its infancy, early results show low-latency and light computational overhead that renders it suitable for real-time applications for the IoT [25].

Explainability and trustworthiness of AI models have gained recent attention in the field of IoT security research. Explainable AI techniques have been integrated into botnet detection models to enhance transparency, interpretability, and user trust—with detection accuracy as an exception [26]. Deep learning frameworks for secure communications meanwhile enhance the role of AI in the improved reliability and resilience of IoT networks [27], [28]. Advanced machine learning techniques for rapidly changing threat landscapes highlight adaptability and robustness under zero-day incident circumstances [29]. Additionally, in lightweight stacked models have shown results with better efficiency in bot contained detection with low resource consumption, suggesting their suitability for deployment in resource-constrained IoT environments [30].

Table 4: DEEP LEARNING–BASED DETECTION MODELS

Ref.	Research Focus / Technique	Key Contribution	Major Outcome / Advantage
[16]	Quantum Machine Learning (QML)	Introduced quantum-driven ML algorithms for intrusion detection in IoT environments	Faster learning, enhanced pattern recognition, improved detection in complex IoT systems
[17]	Deep learning–based IDS (Review)	Comprehensive review of CNN, RNN, and hybrid DL models for IoT botnet detection	High effectiveness identified; challenges noted in scalability, data imbalance, and real-time deployment

[18]	Dimensionality reduction with DL	Combined deep feature reduction with classification techniques	Improved detection accuracy with reduced computational and memory overhead
[19]	Few-shot learning & Deep Reinforcement Learning	Botnet detection with limited labeled data	Strong adaptability to evolving threats and suitability for dynamic IoT environments
[20]	Federated Learning–based botnet detection	Privacy-preserving decentralized model training across IoT devices	Maintained high detection performance while preserving data privacy
[21]	SAE-GRU deep learning model	Scalable botnet detection for smart city infrastructures	Robust performance in large-scale and heterogeneous IoT networks
[22]	Stacked ensemble learning	Combined multiple classifiers for botnet detection	Higher accuracy, improved generalization, and resilience to diverse attack patterns
[23]	Bio-inspired deep learning (IoMT)	Botnet detection tailored for medical IoT environments	High sensitivity and reliability for healthcare-critical systems
[24]	DL-based IDS for optical IoT networks	Detection of IoT intrusions over high-speed optical networks	Extended applicability to high-bandwidth communication environments
[25]	Edge-based modular neural networks	Early-stage botnet detection at the network edge	Low latency, lightweight computation, suitable for real-time IoT applications
[26]	Explainable Artificial Intelligence (XAI)	Integration of explainability into botnet detection models	Improved transparency, interpretability, and user trust
[29]	Advanced machine learning for evolving threats	Robust ML models for dynamic and zero-day attack scenarios	High adaptability and resilience to emerging botnet threats
[30]	Lightweight stacked ensemble models	Efficient botnet detection with reduced resource usage	High detection efficiency suitable for resource-constrained IoT environments

IV. COMPARATIVE ANALYSIS OF EXISTING STUDIES

Table 5 presents analysis from selected high-performance studies in botnet detection for IoT comparing which detection technique was used, datasets were applied, and finally to what extent the accuracy was achieved. A ML-based botnet detection and alerting framework by [1] was evaluated on real-time IoT network traffic, achieving a 95 percent accuracy, and demonstrated that traditional ML methods become very efficient when supported by intelligent alerting mechanisms. Analysis in [2] used the hybrid architecture combining Graph Neural Networks and Long Short-Term Memory networks in benchmark datasets of IoT botnets, with

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 |

reported accuracy being an outstanding 96%--showing the pooling of both spatio-temporal network traffic characteristics. An optimized hybrid feature deep-learning intrusion detection system in [3] reached an excellent detection accuracy rate of 95%, indicating the effectiveness of feature optimization in capacity building and loss of computational overhead in its role in this direction. After the deep learning models, the major advance toward the use of these deep learning methods in IoT network security/IoT botnet detection research. These are new strategies for detecting adversarial environments: autoencoders have been used for feature learning on benign Mozi malware botnet packet data in [8], with an accuracy rate of over 96%, thus indicating its capability to detect botnet behaviors through (stealth) latent feature representation. Multi-branch deep learning, by knowledge distillation in [9], achieved 95% accuracy on encrypted DNS traffic (thus doing away with the need for inspecting payloads in such an analysis), along with addressing privacy issues and encryption challenges. The most reliable deep learning method for classifying raw packet data on industrial IoT datasets in [11] claimed a huge 97% accuracy, emphasizing robustness and suitability for mission-critical applications. A voting-based ensemble machine learning approach used on many IoT anomaly detection datasets in [15] achieved an accuracy rate of almost 96%, showing an improved generalization power and resistances against differentiating attack scenarios. In summary, the comparison underscores the fact that hybrid, ensemble, or deep learned models, when optimized, astoundingly outperform all the other developed models in IoT botnet identification.

Table 5: COMPARATIVE ANALYSIS OF EXISTING STUDIES

Ref.	Technique Used	Dataset Used	Reported Accuracy
[1]	Machine learning–based botnet detection and alerting framework	Real-time IoT network traffic dataset	95%
[2]	Hybrid Graph Neural Network (GNN) and LSTM architecture	Benchmark IoT botnet traffic datasets	96%
[3]	Optimized deep learning IDS with hybrid feature selection	Public IoT intrusion detection datasets	95%
[8]	Autoencoder-based feature learning and hashing	Mozi IoT botnet dataset	96%
[9]	Multi-branch deep learning with knowledge distillation	Encrypted DNS traffic dataset	95%
[11]	Trustworthy deep learning framework (Alpha-Net)	Industrial IoT (IIoT) datasets	97%
[15]	Voting-based ensemble machine learning approach	Multiple IoT anomaly detection datasets	96%

V. CONCLUSION AND FUTURE WORK

This paper presents an exhaustive study on the latest machine-learning and deep-learning-based methods for detecting IoT botnets, wherein the methods have been found to be helping solve the escalated security needs faced in the IoT ecosystem heterogeneous platforms and resource constraints. Studies cited have shown that deep, hybrid, or ensemble learning techniques can maintain consistently high levels of detection accuracy (often exceeding 95%). Techniques like hybrid GNN-LSTM architectures, autoencoder-based feature learning, and voting-based ensemble classifiers can capture complex space-, time- and behavior-centric patterns inherent in IoT network traffic. Deep-learning techniques benefit feature selection, encrypted-traffic analysis, industrial IoT frameworks while enhancing robustness in detection in addition to broader coverage against scalability and privacy concerns. Comparative results show that optimized and hybrid learning methods outperform traditional-specific models in accuracy, generalization, and adaptability against changing botnet threats. Many of these pressing issues continue to be unaddressed. The traditional approaches still rely on centralized architectures in handling static datasets. It ultimately limits an approach's functionality when exposed to the real-world IoT deployment scenario. High computational complexity, non-understood decisions, and real-time, edge-based detection supportability combine to reduce a model's practical implementation. Although various deep learning models have shown prevailingly good accuracies in detection, most research centers on false-positive rates and false-negative rates, with sniffles towards latency, energy efficiency, and adaptability to zero-day attacks. Future research should focus on developing lightweight and adaptive detection frameworks that can operate efficiently at the edge while maintaining high accuracy.

REFERENCES

1. Happy, Rita Chhikara, and Neeti Kashyap. "ML-BoTDAM: machine learning driven botnet detection and alerting mechanism." *Memetic Computing* 18.1 (2026): 13.
2. Babenko, Tetiana, et al. "Hybrid GNN–LSTM Architecture for Probabilistic IoT Botnet Detection with Calibrated Risk Assessment." *Computers* 15.1 (2026): 26.
3. 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.
4. Ram, Raja, and Sanjay Pal. "Optimization Analysis of CNN-based Deep Learning System for Autonomous Detection of IoT Botnet Attacks." *International Journal of Research & Technology* 14.1 (2026): 28-32.
5. Reddy, K. Sudhakar, et al. "An Effective Software defined Network for Botnet Attack Detection and Mitigation using Deep Learning Approaches." *Adaptive Technologies for Sustainable Growth*. CRC Press, 2026. 224-228.
6. Aljammaz, Nouf, Mohammed Elaffendi, and Suliman Fati. "C2 communications and botnet detection: Exploring the potential of deep learning for automating the detection process." *Cybersecurity, Cybercrimes, and Smart Emerging Technologies*. CRC Press, 2026. 32-43.
7. Gilliland, Joshua, et al. "Comparing Machine Learning Algorithms for Detection and Prevention of Cyber-Attacks on IoT Devices: A Literature Review." *Leadership, Business and Management in STEM* (2026): 94-104.

8. Saxena, Nitesh Kumar, and Bhupender Singh Rawat. "Detection of Mozi IoT Botnet Using Autoencoder-Based Feature Learning and Hashing." *Journal of Recent Innovations in Computer Science and Technology* 3.1 (2026): 64-73.
9. Qin, Zhipeng, et al. "A Botnet Detection Method for Encrypted DNS Traffic Based on Multi-branch Knowledge Distillation." *Computer Networks* (2026): 112060.
10. Memos, Vasileios A., et al. "A Novel Architecture for Mitigating Botnet Threats in AI-Powered IoT Environments." *Sensors* 26.2 (2026): 572.
11. Nandanwar, Himanshu, and Rahul Katarya. "Alpha-Net: A dependable and trustworthy deep learning framework for securing industrial internet of things networks against botnet attacks." *Computers and Electrical Engineering* 131 (2026): 110919.
12. Zahid, Mohammad, and Taran Singh Bharati. "Leveraging Machine Learning and Deep Learning in IoT Security: A Review." *Security and Privacy* 9.1 (2026): e70144.
13. Qin, Zhipeng, et al. "A Botnet Detection Method for Encrypted DNS Traffic Based on Multi-branch Knowledge Distillation." *Computer Networks* (2026): 112060.
14. Ahmad, Ishtiaq, et al. "Quantum Machine Learning for Anomaly Detection: The Future of Smarter and Safer IoT Networks." *IEEE Network* (2026).
15. Maroof, Mediha, Ayesha Maroof, and Ayesha Bano. "Anomaly Detection in IoT Using Machine Learning Techniques: A Comparative Study and Voting-Ensemble Approach." *The Asian Bulletin of Big Data Management* 6.1 (2026): 1-16.
16. Bharathi, Indira, Veeramani Sonai, and Sridevi S. "Quantum-driven enhanced machine learning algorithm for intrusion detection in Internet of things environment." EPJ Quantum Technology (2026).
17. Al-Shurbaji, Tamara, et al. "Deep learning-based intrusion detection system for detecting IoT botnet attacks: a review." IEEE Access 13 (2025): 11792-11822.
18. Abbasi, Fereshteh, Marjan Naderan, and Seyed Enayatallah Alavi. "Dimensionality reduction with deep learning classification for botnet detection in the Internet of Things." Expert Systems with Applications 267 (2025): 126149.
19. Alexander, R., and K. Pradeep Mohan Kumar. "BOTSIAM-DRL-Botnet detection using a few shot active matching siamese network deep reinforcement learning in IoT networks." Cluster Computing 28.10 (2025): 665.
20. Hossain, Md Alamgir, and Md Samiul Islam. "Towards decentralized cybersecurity: a novel privacy-preserving federated learning approach for botnet attack detection." Blockchain: Research and Applications (2025): 100355.
21. Tariq, Usman, and Tariq Ahamed Ahanger. "Employing SAE-GRU deep learning for scalable botnet detection in smart city infrastructure." PeerJ Computer Science 11 (2025): e2869.
22. Ali, Mudasir, et al. "Botnet detection in internet of things using stacked ensemble learning model." Scientific Reports 15.1 (2025): 21012.
23. Haq, Baseer Ul, et al. "Botnets Attack Detection Using Bio-Inspired Deep Learning Techniques in Internet of Medical Things (IoMT)." Security and Privacy 8.1 (2025): e493.
24. Imtiaz, Nouman, et al. "A deep learning-based approach for the detection of various internet of things intrusion attacks through optical networks." Photonics. Vol. 12. No. 1. MDPI, 2025.
25. Alqattan, Duaa, et al. "Modular neural network for edge-based detection of early-stage iot botnet." High-Confidence Computing 5.1 (2025): 100230.

26. Saied, Mohamed, and Shawkat Guirguis. "Explainable artificial intelligence for botnet detection in internet of things." Scientific Reports 15.1 (2025): 7632.
27. Salama, Ramiz, et al. "Deep learning technology: enabling safe communication via the internet of things." Frontiers in communications and networks 6 (2025): 1416845.
28. Salama, Ramiz, et al. "Deep learning technology: enabling safe communication via the internet of things." Frontiers in communications and networks 6 (2025): 1416845.
29. Polam, Ram Mohan, et al. "Advanced Machine Learning for Robust Botnet Attack Detection in Evolving Threat Landscapes." Available at SSRN 5515384 (2025).
30. Esmaeilyfard, Rasool, Zohre Shoaei, and Reza Javidan. "A lightweight and efficient model for botnet detection in IoT using stacked ensemble learning: R. Esmaeilyfard et al." Soft Computing 29.1 (2025): 89-101.