Two-Fold Machine Learning Approaches in IoT Botnet Defense: A Review of Detection and Prevention Techniques

[1]Priyanka Giri, [2]Aashish Kumar Tiwari

[1]Mtech Scholar, Department of School of Computer Science and Technology, Sam Global University, Bhopal, India

[2]Assistant professor, Department of School of Computer Science and Technology, Sam Global University, Bhopal, India

[1]priyanka20011013@gmail.com ,[2] aashish.tiwari7898@gmail.com

Abstract: Rapid IoT device proliferation enhanced connectivity amid industries while also posing downside cybersecurity threats, mainly in botnet attacks. Such attacks capitalize on the minimal computational resources and sometimes weak security mechanisms of IoT devices to large-scale disruptions such as Distributed Denial of Service (DDoS) attacks. This work scrutinizes the evolving landscape of IoT botnets and points out the applicability of ML in countering such threats. More specifically, it gives an account of and analyzes the Two-Fold Machine Learning Approach that combines detection and prevention into one unified adaptive defense system. The paper classifies the ML techniques used for botnet mitigation, presents a general architecture of ML-integrated security systems on top of which detection and prevention are contrasted, and highlights challenges regarding scalability, data quality, and adversarial robustness while suggesting future research perspectives including federated learning, explainable AI, and cross-layer security frameworks. It stresses that integrating detection and prevention with ML allows not only for real-time mitigation but also for building long-term resilience in IoT environments.

Keywords: IoT Security, Botnet Detection, Botnet Prevention, Machine Learning, Deep Learning, Two-Fold Approach, Anomaly Detection, Cybersecurity.

1. Introduction

Internet of things is an interconnection of billions of smart devices being able to communicate over the internet. Over the past few years, the number of everyday machines embedded with sensors and can communicate over the internet are rising to a great extent. According to the study published in IoT Business News, Devices connected to the IoT world is increasing day by day which is expected to be around 24.1 billion by 2030. The internet of things makes the world smarter by merging the physical devices with the digital intelligence. International standardization sector (ITUT) defines the Internet of Things as an international structure consisting of interconnected devices based on information and communication technologies [1]. There is large flow of data in between the interconnected devices and the security is the major concern in IoT. Accordingly, the number of attacks that exploit the vulnerabilities of IoT devices has increased as well, which could be critical in keeping patients' data secure. However, since an IoT device is designed for a simple purpose with less processing power and memory like a thermostat and a light bulb, manufacturers and researchers have struggled with satisfying its needs of security. In the meantime, adversaries have taken advantage of its vulnerabilities [2]. the Internet of Things (IoT) has become an influential area in academia and industry. IoT has emerged as a significant technology to provide the basis for the infrastructure of different innovations in smart environments, such as smart homes, smart healthcare and smart everything. The exponential growth of IoT devices and the advances in technology are resulting in its adoption in a variety of applications to enhance services. IoT devices include electronics, software, sensors, actuators and connectivity between them, permitting these devices to connect, interact and exchange data. The low price of the IoT devices is increasing their popularity and growth [3].

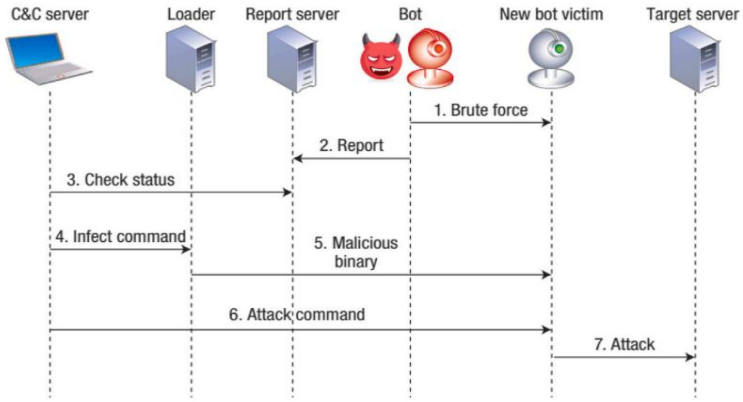

Figure 1 The life cycle of IoT Botnet Mirai [4]

The first IoT Botnet DDoS attack occurred in June 2016, using a malware called LizardStresser. Made mainly for CCTV recorder and IP cameras, this IoT Botnet has hit Brazilian ISPs, financial companies, and governments with a traffic of up to 400 Gbps. Soon after, the IoT Botnet variants exploded with famous names such as Mirai, Psyb0t, Bashlite, Tsunami (Kaiten) changing the concept of Botnet networks. Notably, the Bashlite malware generates a TCP Flood attack of up to 400 Gbps with a network of about 1 million IoT devices limited to infected resources (such as DVRs, IP cameras, and SOHO routers). This malware is considered the precursor to malware Mirai. The Mirai malware generated a record 1.1 Tbps of DDoS attacks, with more than 100,000 SOHO IoT devices infected. In the study describe the life cycle of a typical IoT Botnet (Mirai Botnet) through 7 steps as shown in Fig. 1 [4].

A. Importance of IoT Security

The security of IoT is indispensable in ensuring the security of the massive and still-growing network of interconnected devices that collect, process, and exchange sensitive information. As the number of IoT devices increases in domains such as healthcare, transportation, manufacturing, and smart homes, the potential for security threats also massively increases. If left unprotected, these systems can be targeted by cybercriminals for unauthorized access to confidential data and the outright manipulation of critical operations. Few other threats finish with absolutely devastating consequences of compromised personal privacy, financial losses, disruption of operations, and in some cases, human jeopardy. Strong IoT security is, hence, imperative to guarantee data confidentiality, data integrity, and data availability; maintain user trust; and permit contingently reliable and sustainable use of IoT technologies for both personal and industrial applications [5]. Security in the IoT space is necessary for keeping the user threats away. These threats include unauthorized accesses to data, malware, and system breaches. As the trend of using connected devices in industries and everyday life grows, a solid security apparatus helps individuals to understand the privacy risk involved. This awareness fosters trust in the technology and its providers. Users might feel confident in using IoT services only if they are assured that their data cannot be compromised and that their systems are well protected against any form of compromise. Hence, good security measures will not only prevent adverse events but will also lay a foundation for fostering long-term commitment and reliability in the connected digital world [6].

B. Role of Machine Learning in Botnet Defense

Machine learning stands as a crucial guard against IoT botnet attacks by enabling timely and precise spotting of malicious activities in network traffic. A dual-level scheme has been presented in which deep learning models, ResNet-18-type architectures, are used in two-stage detection: one model detects behaviours related to scanning and reconnaissance activities, which are said to come before botnet deployment, while the other identifies DDoS attacks. It is a two-stage technique for increasing detection capabilities, the first stage concentrating on early reconnaissance and the next on attack. By generating and training on various datasets with several types of scanning and DDoS attack patterns, the methods promote robustness and good generalization over different scenarios of attacks. Corresponding to this, the approach shows a very high precision and recall value, along with equally high accuracy, thus making it a dependable framework for on-the-fly identification and prevention of IoT-based botnet threats [7]. A typical role of machine learning in botnet defense is detecting and classifying malicious behaviors into the IoT network traffic with very high accuracy and efficiency. Machine learning algorithms identify patterns and anomalies indicative of botnet activity, including both the scanning and DDoS phases, by analyzing huge volumes of data. Especially with deep learning structures such as CNNs and RNNs, these models learn to distinguish between legitimate traffic and attack traffic and, therefore, detect any attack suspiciously early, minimize false positives, and support real-time defense mechanisms. The adaptability and learning capability of machine learning with increasing data forms a very strong backbone for securing the IoT and mitigating the botnet threats that keep evolving [8].

2. IoT Botnet Threat Landscape

The growing interconnection of resource-constrained devices that oftentimes lack strong security measures shapes the IoT botnet threat landscape. These devices present easy targets for attackers who infect them with a form of malware and thereafter form extensive networks called botnets. Once compromised, these are used by the attackers to remotely control these devices to carry out malicious activities such as phishing, spamming, malware distribution, and distributed denial-of-service (DDoS) attacks. Keeping this in mind, a botnet may be constructed as peer-to-peer, client-server, or hybrid model, making it rather versatile as well as difficult to destroy. As IoT devices gain massive traction without standardized security protocols, the attack surface, and consequently the impact of botnet attacks, is bound to rise, thereby posing severe threats to users, services, and critical infrastructure [9]. Depending on what is going in homes, industries, or public infrastructure, the delivery of billions of interconnected devices acts as one of the factors making the threat world increasingly complex and dangerous. Many of those devices have processing capabilities with no security provisions, rendering them susceptible to malware infection. Weaknesses are exploited by attackers to develop botnets or compromise legitimate ones of free devices to arbitrarily launch massive cyberattacks such as DDoS attacks. These are interference services with stealing data and building mistrust in digital systems. The botnet threat-scope continues

to increase as the number and types of IoT devices do; this requires aggressive defense mechanisms and tough device management [10].

A. Overview of IoT Architecture and Vulnerabilities

This section discusses the threats at various layers of generic IoT, as depicted in Figure 4. The components of an IoT System include different types of sensors and actuators, a smartphone with an associated application installed in it, the web interface for the smart environment, the servers the IoT devices interact with, and the requisite communications within the IoT system. Table 2 summarizes the threats (TH) imposed on various layers of IoT architecture along with their impact and successfully launched attacks [11]. It is observed that the IoT devices are easy to get control of and thus leading to all the DoS attacks these days. Like the generic architecture, the proposed threat architecture also includes three layers: (i) perception layer, (ii) network layer, and (iii) application layer. The description of each layer is as follows [12].

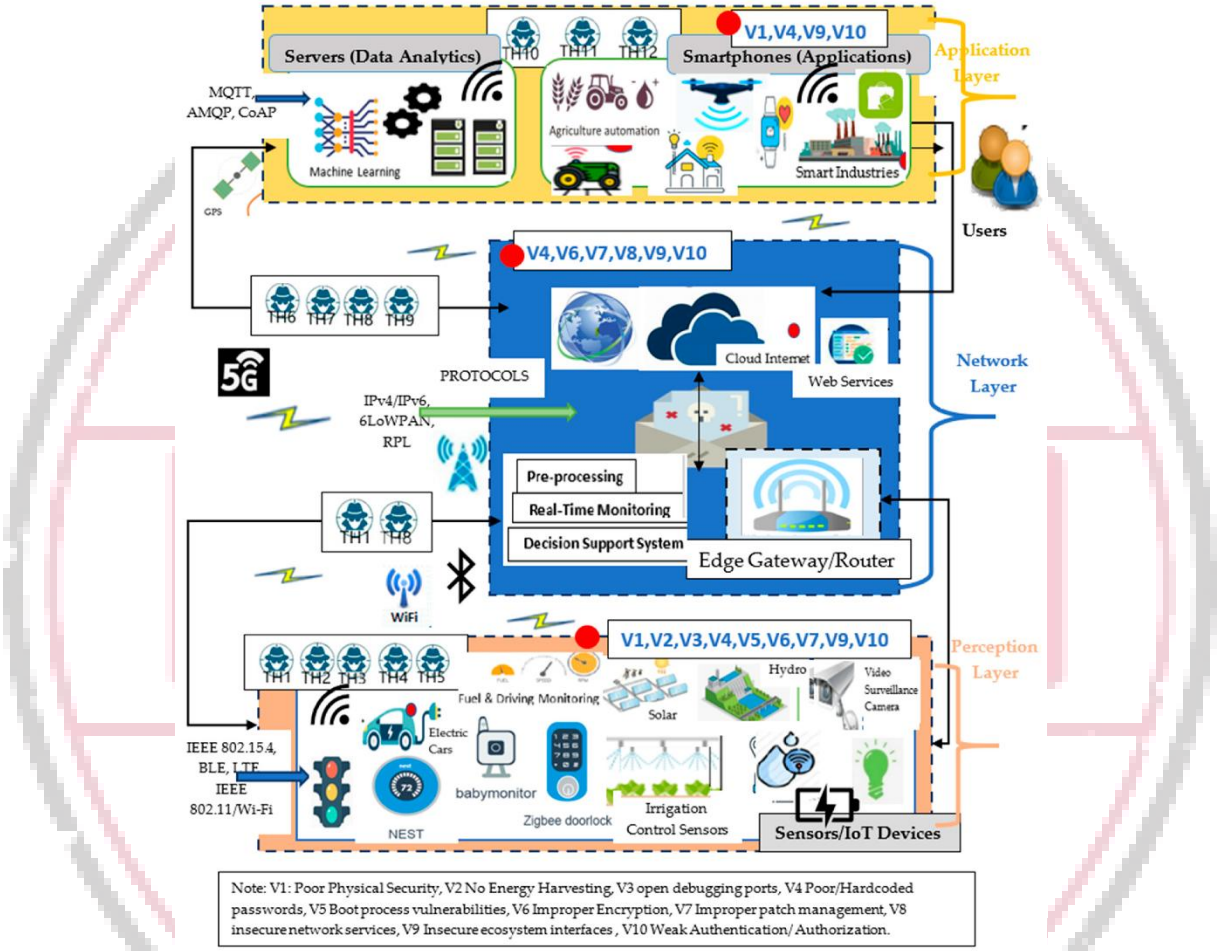

Figure 2. Threat Architecture of Internet of Things [12].

The Internet of Things is built on a layered architecture that was created to meet the demands of various industries, businesses, and societies. Ageneral layered architecture for the IoTconsists of five levels, which are described below: [13]

1. Physical Layer: This is a hardware layer that includes embedded systems, RFID tags, sensor networks, and other sensors. This hardware layer may collect data from a system or environment, process data, and facilitate communication.
2. Gateway layer: This layer manages data and is responsible for publishing and subscribing to the "Things" services, message routing, and platform communication.
3. Internet layer: The Internet layer is where routing occurs. Its primary function is to move packets across networks, and it enables network-to-network communication.
4. Middleware layer: This layer is responsible for collecting and filtering data from hardware devices, performing information discovery, and regulating application access.
5. Application layer: This layer delivers application services. The middleware layer provides these services to various applications and users in IoT-based systems. These services may be utilized in industries including logistics, retail, and healthcare

B. Fundamentals of IOT Botnet

The fundamentals of an IoT botnet involve understanding its architecture, infection ways, and the intended malicious functions. An IoT botnet, in essence, is a network of malware-infected Internet-connected devices such as smart cameras, routers, sensors, and household appliances, which are voluntarily at their own attest by an attacker. These devices tend to be targeted due to their limited computational power and meagerly implemented security measures, such as weak or hardcoded passwords, outdated firmware, and open ports [14]. The general structures of IoT botnets consist of several crucial components: the bots (infected devices), C&C servers for the attackers to issue orders, loaders to place malware on new victims, and scanners or reporters to discover and log vulnerable targets. The life cycle of an IoT botnet initiates with scanning the Internet for insecure devices, exploiting the vulnerabilities to illegally access them, deploying the bot malware into those devices, and finally orchestrating the bots for nefarious activities [15]. IoT botnets are generally used to launch Distributed Denial of Service (DDoS) attacks, sending huge amounts of traffic towards the victim system to make it incapable. Now they do a greater number of cybercrime activities such as spam attacks, credential stuffing, data theft, espionage, cryptocurrency mining, and proxying wet compromised devices for anonymous communication. Botnet detection and mitigation are highly difficult due to the decentralized nature and huge scale of the IoT deployments. As the number of IoT devices exponentially grows in every sector, the threat from botnets also gains its importance and demands urgent attention toward security-by-design, continuous monitoring, and automated threat detection systems [16].

C. Prominent IoT Botnet Attacks (e.g., Mirai, Hajime, Mozi)

Several botnet incidents of high-profile nature have brought forth the crucial vulnerabilities to the IoT ecosystems and brought forth a notion about the increasing sophistication of these threats. One of the most famous instances being the Mirai botnet that came forth in 2016. It used a hardcoded list of default usernames and passwords to infect thousands of IoT devices that were then used to conduct very large-scale Distributed Denial of Service (DDoS) attacks [17]. The most famous DDoS attack was against the DNS provider Dyn, a victory that caused large-scale outages for popular services like Twitter, Netflix, and Reddit. Another big case is that of Hajime-a peer-to-peer botnet, well established-end in the middle of a command-and-control server, and seems advanced architecture. While not expressly malicious, it clearly shows evolutions in the creation of more resilient and stealthy botnet architectures. Likewise, Mozi also helps exhibit how attackers combine known working vulnerabilities and propagation techniques for rapid threat expansion [18]. Combining hybrid C&C architecture, Mozi botnet is among those capable of a varied array of attacks-a Prolonged DDoS, DNS spoofing, and logical data exfiltration being some of them. In sum, such gradual showcasing of more advanced IoT botnet architecture contrasts with the traditional cybersecurity defense initiatives [19].

3. Machine Learning in IoT Security

An IoT network keeps expanding here and gets more complex. Traditional mechanisms usually are ill-suited, given the vastness and diversity of data they generate. An ML system, therefore, provides a robust alternative. It enables systems to recognize patterns, react to new threats, and make intelligent decisions based on data fed into them, with little need for explicit programming. Since machine learning systems evolve as time passes, they become more proficient on security, especially against botnet attacks and botnet mitigation measures, thereby making ML techniques essential in cyber security wise [20].

A. ML Techniques Used in Cybersecurity

Machine learning techniques in cybersecurity can essentially be divided into various classes, each serving particular objectives in the detection and defense against threats. Supervised learning involves the training of a model on a labeled dataset, wherein the model detects relationships between input features and labels supplied in the training set and classifies them for known outcomes such as 'benign' against 'malicious' traffic [21]. Typical algorithms for supervised learning include Decision Trees, Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), Random Forests, and Logistic Regression. In comparison, unsupervised learning is promoted when there is little or no labeled data present for the modeling task at hand. Models under this category try to find some hidden pattern or anomaly in the data with the application of k-Means Clustering, DBSCAN, Autoencoders, and Principal Component Analysis (PCA) [22]. Semi-supervised learning serves as a combination of a minuscule amount of labeled data with a vastly more substantial number of unlabelled data for improved classification.

Reinforcement learning is another sophisticated technique wherein an agent learns to optimize its decision-making policy via trial and error in a dynamic environment, granting an adaptive and real-time mitigation capability [23]. Deep learning, a subset of machine learning, utilizes neural networks, especially Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), to extract complex hierarchical features from the raw data, suitable for time-series analysis and deep packet inspection. These machine-learning techniques are sometimes considered the backbone of cybersecurity solutions: IDS, malware detection, phishing detection, and botnet traffic analysis, etc., which renders these tools significantly more efficient and more accurate in the detection of threats in IoT environments [24].

B. Benefits of ML for IoT Botnet Mitigation

Among the primary advantages of employing machine learning to counterbotnet threats in IoT networks is its ability to perform automated threat detection by training models to identify new or evolving attacks based on their behavioral patterns rather than on known attack signatures. This helps to take preemptive and intelligent measures against unfolding risks. Then, scalability allows ML techniques to process huge amounts of data coming from various IoT devices and monitor large and complex networks in real time [25]. Additionally, ML will have adaptive learning irrespective of the training data used and thus can allow models to be retrained and updated as new threats evolve, fitting the dynamic cybersecurity landscape. Other detection capabilities of ML include discovering anomalies through unsupervised and deep learning techniques that might detect the more subtle variations in device behavior signifying a botnet infection. It goes farther than mere detection; it is able to predict and prevent attacks by identifying the early signs of malicious behavior so that defenses can be deployed ahead of the attack being fully realized [26]. With these capabilities working together, they greatly enhance the intelligence, responsiveness, and efficacy of any IoT security system, particularly in cases where conventional cyber defenses are weak.

C. Categories of ML-Based Defense Detection vs. Prevention

There are two complementary defense strategies to detect and prevent IoT botnets using ML techniques: detection and prevention. Detection-based techniques are used for monitoring after the attack has been initiated, i.e., to detect malicious activity or compromised devices. Examples of such techniques include traffic classification, device behavior profiling, botnet command and control (C&C) detection, and botnet C&C communications [27]. The entire purpose is to raise real-time alerts about suspicious activity and contain the threats before they propagate and/or cause heavy damages. Some examples of detection mechanisms are traffic anomaly detection employing CNN and botnet-related signature classification using SVM.

Prevention attempts to thwart attacks from affecting the system in any way, while detection gives way to an attack by concept of identification and subsequent alerting of its presence. It works in a manner adaptive toward predictive modeling from historical threat data with reinforcement learning for firewall rules, integrated with ML-mechanized access control and authentication. Often these are coupled with real-time threat intelligence feeds and early warning systems so as to block suspicious behaviors as fast as possible [28]. For instance, ML models may be able to detect scanning activities or other exploitation attempts that usually precede full-blown infections. Thus, detection and prevention-based methods provide a dual-layer protection; essentially, they equip the systems to respond in different instances of a botnet lifecycle, and with accurate and agile defenses [29].

4. Two-Fold Machine Learning Approach: Concept and Framework

IoT botnets, very complex and adaptive in nature, force us to have an alphabetically integrated countermeasure system. The classic measures tend to separate detection and prevention, often limiting their efficiency against these very fastly changing threats. In line with this, the Two-Fold Machine Learning Approach has evolved as a strategic framework with the recommended merger of reactive detection and proactive prevention into a single adaptive system [30]. The philosophy explains that when both layers are combined, security posture is greatly enhanced. Detection is concerned with intrusion, anomaly, or device compromise after it has occurred, while prevention is concerned with thwarting these actions by predicting them, so they never occur in the first place [31]. The rationale for such an approach originated from the cyber kill chain methodology, which shows where disrupting an attack in different stages of reconnaissance, exploitation, and command-and-control provides value in minimizing damage and response time, with the attack information being fed back into the system to help with prevention information, and vice versa, allowing both the detection and prevention information to work together in a feedback loop to increase the accuracy, adaptability, and speed of the security system as a whole [32].

The success of the Two-Fold Machine Learning Approach implementation is highly dependent on the integration of detection and prevention models. There is a number of integration strategies that may be utilized. One of the models can initiate the system when integrated sequentially. ML models would detect anomalies in network traffic, or behavior on a device, and upon confirmation of an anomaly, prevention actions such as isolating the compromised device from the rest of the network or blocking suspicious IP addresses would be initiated [33]. Conversely, a preventive integration first can be established where an ML model would also monitor high-risk behavior and enforce protective controls based on its observation, with some detection mechanism to ascertain the correctness of these actions after the fact to enhance threat intelligence. A more powerful setup is granted when parallel integration is employed: the detection engine and prevention engine work in tandem, looking at the same input from different angles [34]. For instance, the supervised model might be on the lookout for known attack signatures, whereas the unsupervised one is searching the wild for unseen anomalies. Being enhanced by a feedback-driven loop, this ensures that a natural environment continues to retrain both detection and prevention models, reducing false positives and increasing the level of resilience over time [35]. The general architecture of a Two-Fold Machine Learning system for IoT botnet defense is composed of several interconnected modules. It starts with the data collection module that procures diverse inputs such as traffic flow data, packet-level details, device telemetry, and even contextual network behavior. This raw data passes through the preprocessing plus feature engineering phase, where the data are cleaned, normalized, and then transformed into features appropriate

for ML model training, such as packet sizes, frequencies, protocol types [36]. The detection engine then applies a set of supervised, unsupervised, or deep learning models to identify botnet activities of both known and unknown variants and generate alerts for the suspicious activities. Simultaneous to the prevention engine working with predictive modeling or reinforcement learning to predict attacks and respond by deploying mitigation tactics such as access control policies, sandboxing, or IP filtering. The two engines connect to a centralized decision module capable of applying logic, rules, and security policies to coordinate responses, including logging and alerting. Lastly, a continuous feedback-and-model-update loop allows the system to evolve with emerging threats by retraining models with new data and real-time feedback and, thus, provide a highly adaptive and intelligent defense for the IoT environment [37]. This figure 2 illustrates a layered ML-based system where IoT data undergoes feature extraction and is processed simultaneously by detection and prevention engines. A decision engine coordinates response actions based on analyzed threats, while a feedback loop continuously refines the model for adaptive and real-time defense.

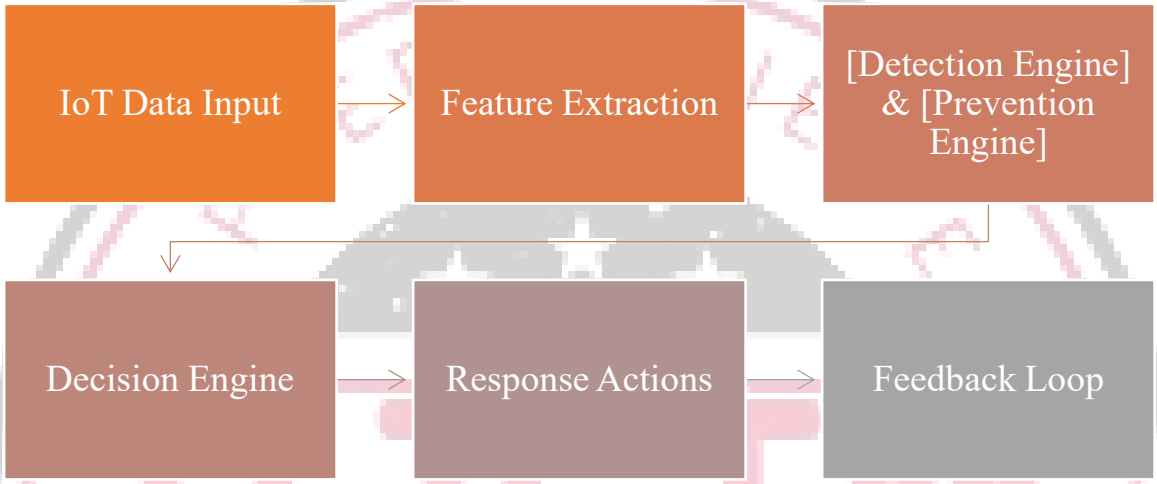

Figure 2 Architecture of Two-Fold Machine Learning Framework for IoT Botnet Defense

5. Detection Techniques in IoT Botnet Defense

Detection of IoT botnets is a critical first line of defense in near-real-time discovery of compromised devices and malicious network behavior. Machine learning-based detection methods work by analyzing large volumes of network data, device behavior, and traffic patterns to uncover anomalies that may characterize botnet infection [38]. Common supervised learning methods include SVM, Decision Trees, or Random Forests-based classification applied on labeled datasets discriminating benign and malicious traffic, whereas unsupervised techniques such as k-Means Clustering or Autoencoders come of use when no labeled data exist, as these discover outliers in network behavior deviating from learned norms [39]. Another new trend in botnet detection is to use deep learning algorithms such as CNNs and RNNs that process raw packet-level and time-series traffic data with a possibility of high accuracy in detecting intricate botnet behaviors. Since such models exhibit the ability to detect known threats together with previously unreported or rapidly evolving attack vectors, the problem lies in leveraging ML-based detection systems to handle encrypted traffic, imbalanced datasets, and false positives. Yet, detection is a standing pillar of botnet defense before mitigation and prevention strategies can be invoked [40].

6. Prevention Techniques Using Machine Learning

While detection warns of threats in progress, prevention tries to acutely and reactively focus on a blocking technique before any damage is done to even a fast-spreading IoT botnet. Machine learning aids prevention through predictive and adaptive security mechanisms that identify anticipated behavior used for malicious purposes on either historic trends or real-time information. Reinforcement learning is, for instance, suited to dynamic environments where the agent learns to carry out actions (such as isolation of devices or modification of firewall rules) that best minimize long-term risk [41]. Others consider enhancement of these methods through predictive modeling for infection-like scenarios from past traffic that could predict where to harden nodes considered at risk. Prevention mechanisms may also be linked to an access control system, where the ML method should calculate trust scores for behavior and allow device connections in response. Anomaly prediction could start countermeasures like traffic shaping or throttling when scanning or propagation is identified. This set of powers reduces the attack surface, while in early stages of the botnet lifecycle, like reconnaissance and initial infection, it creates disruptions [42]. Although challenges such as false alarms and high processing costs do exist, prevention methods involving ML are a turning point from reactive to proactive IoT security and are essentially the backbone of a sturdy two-tiered defense model.

Recent AI advancement in ML and DL with more-enhanced and timely detection and prevention of cyber threats, medical diagnoses, and data security in various fields are involved. In healthcare, DL methods like pretrained lightweight models and MobileNets have become highly accurate for detecting Parkinson's disease from hand sketches [43], whereas ML models have outshined traditional risk prediction methods for cardiovascular disease in Australian cohort studies [47]. In network security, multivariate LSTM autoencoders have been developed to enhance MAC-layer spoofing detection under realistic RSSI traces [45], and the ML-based encrypted traffic classification has become important for monitoring modern IoT networks [46]. Meanwhile, blockchain-integrated AI methods such as AI-Hybrid chains with advanced encryption and fuzzy logic promote an enhanced level of secure access control for the cloud-based IoT systems [48]. Interpretable ML models have identified the principal variables affecting wheat yields such as nitrogen use and solar radiation in agriculture [50], whereas two-fold feature selection has improved the classification accuracies of clinical and lifestyle risk factors for diabetes studies [51]. Lastly, in networking, self-attentive models (SAM) were presented to enhance real-time traffic classification by improving interpretability at the packet level [52].

Table 1 Comparative Studies of AI Applications in Security and Healthcare

Ref.	Focus Area	Key Methods	Approach	Performance Metrics	Outcome
[43]	PD Detection via Hand Sketches	Pretrained Lightweight DL (PLDL), MobileNets, Two-Fold Training	Pattern Recognition in Medical Images	Accuracy	100% accuracy with KNN
[44]	DL Survey in Medical Imaging & Object Detection	Survey of DL approaches, DL for Object Detection	Review Paper	Coverage, Advances, Trends	Summarized DL growth and challenges
[45]	RSSI-Based Spoofing Detection	Multi-model LSTM Autoencoder	Experimental Network Analysis	Detection Rate, Adaptability	Outperformed existing spoofing detection methods
[46]	Encrypted Traffic Classification	ML-based Traffic Classification	Survey and Methodological Review	Classification Accuracy, Interpretability	Comprehensive review and future insights
[47]	CVD Risk Prediction (Australia)	ML Models vs Framingham Model	Predictive Modeling in Healthcare	AUC, NRI, Accuracy	Up to 5.1% improvement over Framingham model
[48]	Cloud-IoT Access Control & Intrusion Detection	AI-Hybrid Blockchain, TL-DDQN, Con-ResNet	Secure Access Control via ML & Blockchain	Attack Detection Rate, Throughput, Delay	Effective, secure model with layered defense
[49]	AI in IoT Botnet Detection and Prevention	Review of ML/DL models, Datasets, Evaluation Methods	Systematic Literature Review	Dataset Variety, Detection Efficacy	Identified gaps in IoT botnet mitigation methods
[50]	ML for Wheat Yield Prediction	Random Forest, Tree-based Models, Interpretability Tools	Data-Driven Yield Analysis	R^2, RMSE, MAE	Identified key yield drivers and interactions
[51]	Diabetes Risk Prediction with Feature Selection	Two-fold Feature Selection (PCA, IG), ML Classifiers	Predictive Modeling with Feature Eng.	Accuracy, AUC	Identified glucose as most relevant predictor
[52]	Online Traffic Classification using SAM	Self-Attentive Mechanism (SAM), Packet-level Deep Learning	Packet-Level DL for Real-Time Classification	Protocol/Application Accuracy Gains	Improved classification and interpretability

7. Conclusion

Botnet threats are becoming more common, increasingly sophisticated, and more damaging with every passing second produced from the exponential growth of IoT devices. Thus, these demands intelligent and dynamic mechanisms functioning against security. This article has considered the Two-Fold Machine Learning Approach as an effective framework, combining detection and prevention capabilities for securing IoT ecosystems. With the Two-Fold Machine Learning Approach, ML models are prepared for real-time monitoring and prediction so that the approach helps expedite threat detection, keep down false positives, and act against malicious behaviors beforehand. Detection models reveal botnet activities once the device is infected, while prevention models seek to stop possible threats before they exist: By combining them, a strong layered security system is built. Yet how to face real-world challenges such as data scarcity, adversarial attacks, and system scalability is the next room for improvement. Distributed learning, explainable models, and standardized protocols will further secure the approach. In essence, the Two-Fold approach offers a hopeful key to deploying more secure, resilient, and intelligent IoT environments thus.

References

[1] Pokhrel, S., Abbas, R., & Aryal, B. (2021). IoT security: botnet detection in IoT using machine learning. *arXiv preprint arXiv:2104.02231*. https://doi.org/10.48550/arXiv.2104.02231

[2] Jung, W., Zhao, H., Sun, M., & Zhou, G. (2020). IoT botnet detection via power consumption modeling. *Smart Health*, *15*, 100103. https://doi.org/10.1016/j.smhl.2019.100103

[3] Wazzan, M., Algazzawi, D., Bamasaq, O., Albeshri, A., & Cheng, L. (2021). Internet of Things botnet detection approaches: Analysis and recommendations for future research. *Applied Sciences*, *11*(12), 5713. https://doi.org/10.3390/app11125713

[4] Nguyen, G. L., Dumba, B., Ngo, Q. D., Le, H. V., & Nguyen, T. N. (2022). A collaborative approach to early detection of IoT Botnet. *Computers & Electrical Engineering*, *97*, 107525. https://doi.org/10.1016/j.compeleceng.2021.107525

[5] Rekha, S., Thirupathi, L., Renikunta, S., & Gangula, R. (2023). Study of security issues and solutions in Internet of Things (IoT). *Materials Today: Proceedings*, *80*, 3554-3559. https://doi.org/10.1016/j.matpr.2021.07.295

[6] Koohang, A., Sargent, C. S., Nord, J. H., & Paliszkiewicz, J. (2022). Internet of Things (IoT): From awareness to continued use. *International Journal of Information Management*, *62*, 102442. https://doi.org/10.1016/j.ijinfomgt.2021.102442

[7] Srikanth, T., Mamatha, K., & Kumar, S. A Two-Fold Machine Learning Method for Identifying and Preventing IoT Botnet Attacks. Vol 13 Issue 04, Dce 2023. ISSN NO: 0364-4308.

[8] Mashaleh, A. S., Ibrahim, N. F., Alauthman, M., AlKaraki, J., Almomani, A., Atalla, S., & Gawanmeh, A. (2024). Evaluation of machine learning and deep learning methods for early detection of internet of things botnets. *International Journal of Electrical & Computer Engineering (IJECE)*, *14*(4), 4732-4744. DOI: 10.11591/ijece.v14i4.pp4732-4744

[9] Acharjee, A., Mondal, S., Pipalwa, R., Mitra, A., & Paul, A. (2023). Exploring the evolving landscape of security threats in IoT: Challenges and Countermeasures. *American Journal of Advanced Computing*, *2*(2). https:// doi.org/10.15864/ajac.22013

[10] Jony, A. I., & Hamim, S. A. (2023). Navigating the Cyber Threat Landscape: A Comprehensive Analysis of Attacks and Security in the Digital Age. *Journal of Information Technology and Cyber Security*, *1*(2), 53-67. https://doi.org/10.30996/jitcs.9715

[11] Mathas, C. M., Vassilakis, C., Kolokotronis, N., Zarakovitis, C. C., & Kourtis, M. A. (2021). On the design of IoT security: Analysis of software vulnerabilities for smart grids. *Energies*, *14*(10), 2818. https://doi.org/10.3390/en14102818

[12] Anand, P., Singh, Y., Selwal, A., Singh, P. K., Felseghi, R. A., & Raboaca, M. S. (2020). Iovt: Internet of vulnerable things? threat architecture, attack surfaces, and vulnerabilities in internet of things and its applications towards smart grids. *Energies*, *13*(18), 4813. https://doi.org/10.3390/en13184813

[13] Ramadan, R. (2022). Internet of things (iot) security vulnerabilities: A review. *PLOMS AI*, *2*(1).

[14] Zhao, H., Shu, H., & Xing, Y. (2021, January). A review on IoT botnet. In *The 2nd International Conference on Computing and Data Science* (pp. 1-7).

[15] Alieyan, K., Almomani, A., Abdullah, R., Almutairi, B., & Alauthman, M. (2021). Botnet and Internet of Things (IoTs): A definition, taxonomy, challenges, and future directions. In *Research anthology on combating denial-of-service attacks* (pp. 138-150). IGI Global.

[16] Alqattan, D., Ojha, V., Habib, F., Noor, A., Morgan, G., & Ranjan, R. (2025). Modular neural network for edge-based detection of early-stage iot botnet. *High-Confidence Computing*, *5*(1), 100230. https://doi.org/10.1016/j.hcc.2024.100230

[17] Böck, L., Sundermann, V., Fusari, I., Karuppayah, S., Mühlhäuser, M., & Levin, D. (2023). The End of the Canonical IoT Botnet: A Measurement Study of Mirai's Descendants. *arXiv preprint arXiv:2309.01130*.

[18] Wang, B., Sang, Y., Zhang, Y., Li, S., & Xu, X. (2022, December). A longitudinal measurement and analysis study of Mozi, an evolving P2P IoT botnet. In *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 117-122). IEEE.
[19] Almazarqi, H. (2024). *Profiling IoT botnet activity* (Doctoral dissertation, University of Glasgow).
[20] Ahmad, R., & Alsmadi, I. (2021). Machine learning approaches to IoT security: A systematic literature review. *Internet of Things*, *14*, 100365.
[21] Bharadiya, J. (2023). Machine learning in cybersecurity: Techniques and challenges. *European Journal of Technology*, *7*(2), 1-14.
[22] Salloum, S. A., Alshurideh, M., Elnagar, A., & Shaalan, K. (2020, March). Machine learning and deep learning techniques for cybersecurity: a review. In *The International Conference on Artificial Intelligence and Computer Vision* (pp. 50-57). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-44289-7_5
[23] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies*, *13*(10), 2509. https://doi.org/10.3390/en13102509
[24] Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*, *2*(3), 527-555. https://doi.org/10.3390/jcp2030027
[25] Gopalsamy, M. (2020). Artificial Intelligence (AI) Based Internet-of-Things (IoT)-Botnet Attacks Identification Techniques to Enhance Cyber security. *Int. J. Res. Anal. Rev*, *7*(4), 414-419.
[26] Nookala Venu, D., Kumar, A., & Rao, M. A. S. (2022). Botnet attacks detection in internet of things using machine learning. *NeuroQuantology*, *20*(4), 743-754.
[27] Shang, Y. (2024). Detection and Prevention of Cyber Defense Attacks using Machine Learning Algorithms. *Scalable Computing: Practice and Experience*, *25*(2), 760-769. https://doi.org/10.12694/scpe.v25i2.2627
[28] Alotaibi, A., & Rassam, M. A. (2023). Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense. *Future Internet*, *15*(2), 62. https://doi.org/10.3390/fi15020062
[29] Muthalagu, R., Malik, J., & Pawar, P. M. (2025). Detection and prevention of evasion attacks on machine learning models. *Expert Systems with Applications*, *266*, 126044. https://doi.org/10.1016/j.eswa.2024.126044
[30] Rožanec, J. M., Petelin, G., Costa, J., Cerar, G., Bertalanič, B., Guček, M., ... & Mladenić, D. (2025). Dealing with zero-inflated data: Achieving state-of-the-art with a two-fold machine learning approach. *Engineering Applications of Artificial Intelligence*, *149*, 110339. https://doi.org/10.1016/j.engappai.2025.110339
[31] Miao, H., Liu, Z., Zhao, Y., Guo, C., Yang, B., Zheng, K., & Jensen, C. S. (2024). Less is more: Efficient time series dataset condensation via two-fold modal matching. *Proceedings of the VLDB Endowment*, *18*(2), 226-238. https://doi.org/10.14778/3705829.3705841
[32] Rožanec, J. M., Fortuna, B., & Mladenić, D. (2022). Reframing demand forecasting: a two-fold approach for lumpy and intermittent demand. *Sustainability*, *14*(15), 9295. https://doi.org/10.3390/su14159295
[33] Crovini, C., Ossola, G., & Britzelmaier, B. (2021). How to reconsider risk management in SMEs? An advanced, reasoned and organised literature review. *European Management Journal*, *39*(1), 118-134. https://doi.org/10.1016/j.emj.2020.11.002
[34] Zhang, R., Zhang, B., Li, Y., Zhang, H., Sun, Z., Gan, Z., ... & Yang, Y. (2024). Improve vision language model chain-of-thought reasoning. *arXiv preprint arXiv:2410.16198*. https://doi.org/10.48550/arXiv.2410.16198
[35] Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0. *Applied Sciences*, *13*(6), 3410. https://doi.org/10.3390/app13063410
[36] Weyts, K., Lasnon, C., Ciappuccini, R. *et al.* Artificial intelligence-based PET denoising could allow a two-fold reduction in [^{18}F]FDG PET acquisition time in digital PET/CT. *Eur J Nucl Med Mol Imaging* **49**, 3750–3760 (2022). https://doi.org/10.1007/s00259-022-05800-1
[37] Ying, J. (2020). The importance of the discussion method in the undergraduate business classroom. *Humanistic Management Journal*, *5*(2), 251-278. https://doi.org/10.1007/s41463-020-00099-2
[38] Almseidin, M., & Alkasassbeh, M. (2022). An accurate detection approach for IoT botnet attacks using interpolation reasoning method. *Information*, *13*(6), 300. https://doi.org/10.3390/info13060300
[39] Yamaguchi, S. (2020). Botnet defense system: Concept, design, and basic strategy. *Information*, *11*(11), 516. https://doi.org/10.3390/info11110516
[40] Alothman, Z., Alkasassbeh, M., & Al-Haj Baddar, S. (2020). An efficient approach to detect IoT botnet attacks using machine learning. *Journal of High Speed Networks*, *26*(3), 241-254. https://doi.org/10.3233/JHS-200641
[41] Usmani, S., Saboor, A., Haris, M., Khan, M. A., & Park, H. (2021). Latest research trends in fall detection and prevention using machine learning: A systematic review. *Sensors*, *21*(15), 5134. https://doi.org/10.3390/s21155134

[42] Ma, Z., Mei, G., & Piccialli, F. (2021). Machine learning for landslides prevention: a survey. *Neural Computing and Applications*, *33*(17), 10881-10907. https://doi.org/10.1007/s00521-020-05529-8
[43] Rajinikanth, V., Yassine, S., & Bukhari, S. A. (2024). Hand-sketchs based Parkinson's disease screening using lightweight deep-learning with two-fold training and fused optimal features. *International Journal of Mathematics, Statistics, and Computer Science*, *2*, 9-18. https://doi.org/10.59543/ijmscs.v2i.7821
[44] Kaur, A., Singh, Y., Neeru, N., Kaur, L., & Singh, A. (2022). A survey on deep learning approaches to medical images and a systematic look up into real-time object detection. *Archives of Computational Methods in Engineering*, *29*(4), 2071-2111. https://doi.org/10.1007/s11831-021-09649-9
[45] Madani, P., & Vlajic, N. (2021). RSSI-based MAC-layer spoofing detection: deep learning approach. *Journal of Cybersecurity and Privacy*, *1*(3), 453-469. https://doi.org/10.3390/jcp1030023
[46] Alwhbi, I. A., Zou, C. C., & Alharbi, R. N. (2024). Encrypted network traffic analysis and classification utilizing machine learning. *Sensors*, *24*(11), 3509. https://doi.org/10.3390/s24113509
[47] Sajeev, S., Champion, S., Beleigoli, A., Chew, D., Reed, R. L., Magliano, D. J., ... & Maeder, A. (2021). Predicting Australian adults at high risk of cardiovascular disease mortality using standard risk factors and machine learning. *International journal of environmental research and public health*, *18*(6), 3187. https://doi.org/10.3390/ijerph18063187
[48] Krishnan, S. C. (2024). AI-HybridChain: Picturized authentication and DRL based access control method with secure two fold revocation for ensuring cloud computing security. *Future Generation Computer Systems*, *160*, 389-405. https://doi.org/10.1016/j.future.2024.04.054
[49] Mahi, A. (2023). A comprehensive literature review on machine learning models application in detecting and preventing Botnet attacks on IoT devices.
[50] Nayak, H. S., Silva, J. V., Parihar, C. M., Krupnik, T. J., Sena, D. R., Kakraliya, S. K., ... & Sapkota, T. B. (2022). Interpretable machine learning methods to explain on-farm yield variability of high productivity wheat in Northwest India. *Field Crops Research*, *287*, 108640. https://doi.org/10.1016/j.fcr.2022.108640
[51] Kakoly, I. J., Hoque, M. R., & Hasan, N. (2023). Data-driven diabetes risk factor prediction using machine learning algorithms with feature selection technique. *Sustainability*, *15*(6), 4930. https://doi.org/10.3390/su15064930
[52] Xie, G., Li, Q., & Jiang, Y. (2021). Self-attentive deep learning method for online traffic classification and its interpretability. *Computer Networks*, *196*, 108267. https://doi.org/10.1016/j.comnet.2021.108267