Journal of Reliable Intelligent Environments
https://doi.org/10.1007/s40860-024-00226-y

ORIGINAL ARTICLE

A survey: contribution of ML & DL to the detection & prevention of botnet attacks

Yassine EL Yamani[1] · Youssef Baddi[2] · Najib EL Kamoun[1]

Received: 30 November 2023 / Accepted: 11 June 2024

Abstract
Machine Learning (ML) and Deep Learning (DL) are transforming the detection and prevention of botnets, significant threats in cybersecurity. In this survey, we highlight the shift from traditional detection methods to advanced ML and DL techniques. We demonstrate their effectiveness through case studies involving classification algorithms, clustering techniques, and neural networks. We also explore innovative strategies like federated learning and meta-learning models that enhance proactive defenses, including predictive analytics, real-time systems, and automated responses. Our paper discusses challenges such as data privacy, model overfitting, and the need for adaptability to sophisticated botnet structures. We emphasize the importance of ongoing research and collaboration across disciplines to keep pace with fast-evolving cyber threats, offering insights for developing intelligent cybersecurity defenses.

Keywords Botnet · Machine learning · Deep learning · Cybersecurity · IoT · Artificial intelligence in security

1 Introduction

The digital world faces increasing threats from botnets, which are networks of hijacked devices controlled by cybercriminals to carry out various cyberattacks. These attacks threaten both personal and corporate data, as well as the stability of essential services. Botnets have evolved from simple spam tools to complex entities capable of large-scale Distributed Denial-of-Service (DDoS) attacks, highlighting the limitations of traditional security measures and the need for more adaptable solutions [1].

As botnet structures become more complex, incorporating devices from the Internet of Things (IoT) to cloud technologies, traditional cybersecurity methods are no longer sufficient. This gap has led to the adoption of Machine Learning (ML) and Deep Learning (DL) in cybersecurity. These technologies enhance the detection and prevention of botnets by analyzing large datasets to predict and counteract threats more effectively than traditional methods [2, 3]. Additionally, advanced communication frameworks in IoT environments support these efforts by providing scalable and efficient data transfer mechanisms [4]. However, implementing ML and DL also presents challenges, such as high computational demands and concerns about data privacy and model overfitting [5–7].

Our paper is organized as follows. Section 2 provides a detailed overview of botnets, discussing their definition, functionality, and recent developments, along with a review of recent incidents and their impacts. Section 3 examines traditional methods for detecting botnets, their limitations, and how ML and DL are beginning to address these issues. Section 4 explores the application of ML and DL in cybersecurity, describing various algorithms like classification, clustering, and neural networks, and evaluating how advanced techniques like deep learning can strengthen cybersecurity defenses. This section also highlights the importance of datasets, the challenges in applying ML and DL, and the evaluation of these models in the cybersecurity field.

Section 5 details the specific roles and contributions of ML and DL in detecting botnets, categorizing different machine learning techniques and deep learning approaches, and highlighting hybrid and innovative detection methods. Section 6 covers proactive measures for preventing botnet attacks using ML and DL, outlining strategies such as incremental learning, meta-learning, and real-time detection to improve

✉ Yassine EL Yamani
elyamani.y@ucd.ac.ma

1 STIC Lab, FSJ, Chouaib Doukkali University, El Jadida, Morocco

2 STIC Lab, ESTSB, Chouaib Doukkali University, El Jadida, Morocco

Published online: 24 June 2024

cybersecurity. Finally, Section 7 discusses the current challenges and future directions for using ML and DL in botnet detection and prevention, emphasizing the need for adaptability and continuous model updates. Section 8 concludes with a summary of the findings and suggestions for future research.

2 Botnets: an overview

2.1 Definition and functioning of botnets

What are Botnets? Botnets, a blend of "robot" and "network," are intricate networks of devices compromised by cybercriminals. These devices range from personal computers to Internet of Things (IoT) gadgets, all infected with malware that turns them into tools for malicious activities. Botnets are commonly used for various harmful operations, including Distributed Denial-of-Service (DDoS) attacks, data theft, and spreading additional malware [8, 9].

Command-and-control architecture: The operation of a botnet revolves around its command-and-control (C&C) architecture. This system allows cybercriminals to control the compromised devices. Through C&C servers, cybercriminals send commands that organize complex attacks or quietly steal data. Understanding this central command mechanism is essential for knowing how botnets work and finding ways to disrupt them [8, 9].

Challenges posed by Botnets: As botnets become more sophisticated, they present ongoing challenges to traditional cybersecurity measures, which often struggle to adapt quickly enough to address such dynamic threats effectively. The increasing complexity of botnets shows the need for continually developing cybersecurity strategies to keep up with these advanced threats [9].

Additionally, insights from the detection mechanisms of ransomware attacks, which are discussed extensively in [10], highlight the importance of adaptive and robust detection systems in countering botnet threats.

2.2 Trends in botnet evolution

Botnets have significantly evolved, mirroring technological advancements and expanding their influence across the digital landscape. Originally simple tools for spamming and basic Distributed Denial-of-Service (DDoS) attacks, botnets have transformed into complex systems capable of executing sophisticated cybercrimes.

Early Botnets to advanced DDoS attacks: Initially used for spamming, botnets like Gameover Zeus have developed into complex peer-to-peer (P2P) networks, showing significant improvements in their capabilities [11]. This evolution highlights their adaptation to better cybersecurity defenses and the ongoing need for advancements in security strategies.

IoT device vulnerability and the Mirai Botnet: The Mirai botnet exploited vulnerabilities in IoT devices to launch massive DDoS attacks in 2016 [1, 12, 13]. This incident demonstrated the potential for large-scale disruptions and marked a shift towards targeting the widespread but often insecure IoT devices, often managed by less experienced developers.

Emergence of mobile Botnets: With the rise of smartphones, mobile botnets like Andbot have emerged, using mobile-specific command and control tactics to increase stealth and resilience [14]. This development highlights the expanding threat landscape as cybercriminals exploit the widespread use of mobile devices.

Vehicular ad hoc networks (VANETs) and Botnet threats: The advancement of VANETs brings new security challenges, posing risks to both digital and physical safety. Efforts like SHIELDNET aim to mitigate these threats, showing the continuous evolution of botnet challenges in vehicular contexts [15].

Complexity of P2P Botnets: P2P botnets, such as Gameover Zeus, present considerable challenges due to their decentralized command structures that blend with legitimate traffic, making detection more difficult [11]. This complexity requires more advanced detection techniques to effectively identify and counter these threats.

Social network Botnets (SnBs): SnBs exploit social networks to manipulate information and spread malware. This trend illustrates how cybercriminals leverage social platforms to reach large audiences, posing unique challenges for detection and management [16].

2.3 Recent botnet incidents and their evolving impact

Botnets continue to evolve and pose increasing threats to cybersecurity. For instance, the Trickbot botnet highlights the vulnerabilities of Internet of Things (IoT) devices, exploiting them to conduct DDoS attacks, identity theft, and large-scale data breaches. This botnet has significantly impacted the financial sector, demonstrating the urgent need for better detection and prevention methods [17].

Additionally, the emergence of the Meris botnet marked a substantial increase in attack severity. In September 2021, it caused unprecedented DDoS incidents affecting major platforms like Yandex and Cloudflare [13]. This situation further exposed critical weaknesses in IoT security, especially the unencrypted nature of most IoT traffic, leading to significant security breaches [18].

3 Detection of botnets: traditional approaches

3.1 Conventional methods for botnet detection

The fight against botnets uses a range of established detection techniques, each targeting different aspects of these cyber threats. Key methods include signature-based detection, anomaly detection, and network traffic analysis. These strategies are the pillars of traditional cybersecurity defenses. Table 1 below outlines how each method functions and the challenges they face, providing a clear perspective on how they contribute to securing networks from botnet intrusions.

3.2 Limitations of traditional techniques

Traditional botnet detection techniques, while foundational, face considerable challenges in addressing the sophistication of modern threats, especially in IoT and complex networks.

Adaptability to new threats: Traditional approaches like signature-based detection often fall short in recognizing new and unknown botnet behaviors. This is a major limitation in IoT settings where botnet activities are unique and rapidly changing [19, 20]. Research highlights the dynamic and decentralized nature of IoT botnet threats, pointing to the need for more flexible detection frameworks [22, 23].

High false positive rates: Systems based on anomaly detection frequently encounter high false positive rates, incorrectly flagging unusual but non-malicious activities as threats. This problem is worse in complex scenarios, such as distinguishing between benign and malicious DNS queries, which remains a significant challenge [21, 28, 29].

Reactive nature: Traditional methods, which are predominantly reactive, struggle against new or rapidly evolving botnet strategies. Their effectiveness diminishes in a landscape where botnet structures and attack techniques are constantly evolving [25, 30, 31].

Resource intensity and scalability: Anomaly-based detection requires continuous monitoring, which is resource-intensive and often does not scale well in large or complex networks, especially those with numerous IoT devices [24, 32].

Lack of comprehensive solutions: Existing methods tend to target specific elements of botnet threats and do not provide a holistic approach to comprehensively tackle the full range of botnet activities, particularly within the diverse IoT environment [20, 26, 27].

3.3 Bridging traditional gaps: the emergence of ML and DL

Traditional botnet detection methods face challenges such as adaptability issues, high false positive rates, and a reactive approach. Machine Learning (ML) and Deep Learning (DL) provide a transformative upgrade by learning from complex datasets and shifting cybersecurity from a reactive to a proactive stance.

Revolutionizing detection with ML and DL: By analyzing real-time data, ML and DL enhance the accuracy of traditional detection methods and significantly reduce false positives, greatly improving cybersecurity effectiveness.

Enhancing conventional methods: Integrating ML and DL with traditional techniques refines detection accuracy. For example, ML algorithms enhance anomaly-based systems to better distinguish between legitimate anomalies and actual threats. In network traffic analysis, they help uncover complex botnet patterns that conventional methods might miss.

Confronting IoT challenges: In the diverse and decentralized IoT environment, ML and DL are particularly effective. Their ability to adapt and learn from varied data makes them powerful tools against the dynamic threats in IoT contexts.

Integrating ML and DL with traditional detection methods not only addresses existing challenges but also establishes a proactive, dynamic cybersecurity framework. Subsequent sections will delve into the specific roles and contributions of ML and DL, highlighting their transformative potential in cybersecurity strategies.

4 ML and DL in cybersecurity

4.1 Harnessing ML algorithms in cybersecurity

Machine Learning (ML) plays a crucial role in strengthening cybersecurity. In this subsection, we explore how ML algorithms enhance digital defenses by providing adaptive intelligence that evolves in response to emerging cyber threats. These algorithms transform cybersecurity strategies by leveraging data-driven insights to detect and mitigate vulnerabilities effectively. Batta Mahesh's comprehensive analysis [33] highlights the significant impact of ML in developing resilient and intelligent cybersecurity measures.

4.1.1 Classification algorithms

Classification algorithms, essential to supervised learning, analyze labeled data to classify and predict the nature of new, unseen data. They are crucial in cybersecurity for distinguishing between normal operations and malicious activities. These algorithms range from simple decision trees to complex neural networks, accommodating different data complexities to tailor solutions for specific cybersecurity challenges [34, 35].

Table 1 Overview of conventional methods for Botnet detection

Method	Effective against	Approach	Challenges and advancements
Signature-based detection [19]	Well-documented threats and known botnet types	Matching network traffic and system activities with known malicious signatures	Requires more nuanced approaches due to advancements in botnet strategies [20]
Anomaly-based detection [21]	Previously unknown botnet activities and new or evolving botnet strategies	Clustering similar network flows and activities to pinpoint bot-infected hosts	Struggles with high false positive rates but shows significant advancements in accurately identifying botnet activities [21]
Honeypots [22]	Botnet attacks in IoT and Smart Factory environments	Attracting botnet attackers for close monitoring and logging of their activities	Effective in studying real-world attack activities in IoT and IoMT settings, though not using AI, ML, or DL [23]
Network Traffic Analysis [24]	Botnet Command and Control (C&C) and attack traffic through TCP, UDP, and DNS protocols	Classifying network traffic to distinguish between malicious botnet traffic and legitimate network activities	Critical in spotting distinct traffic patterns associated with botnets, primarily not involving AI, ML, or DL [24]
Behavioral Analysis [25]	Both known and emerging botnet threats	Analyzing traffic patterns and flow intervals to detect botnets during various lifecycle phases	Demonstrates potential in identifying botnet activities based on network behavior, even in encrypted communications [25]
IP and Domain Blacklisting [26]	Known malicious sources and botnet communications using DNS	Maintaining and utilizing “blacklists” of known malicious IP addresses and domains to filter out harmful traffic	Essential for quickly identifying threats from known malicious sources but challenged by the rapidly changing landscape of botnet domains and IPs [26]
Log Analysis [27]	Botnet activity in extensive network or cloud environments	Applying heuristics to large-scale logs to detect behavioral anomalies indicative of botnets	Effective in analyzing interaction patterns and deviations in log data, identifying botnet activity in large-scale networks [27]
DNS Traffic Monitoring [28]	Botnet activities related to C&C servers, migrations, commands, and malware updates	Identifying anomalies such as repeated queries to specific domains or queries to known malicious domains	Effective in various network sizes, focusing on detecting changes in C&C servers and abnormal DNS query behaviors [29]

- *Versatility in applications*: These algorithms range from simple decision trees to complex neural networks, accommodating different data types and complexities. They offer tailored solutions for specific cybersecurity challenges [34, 35].
- *Robust anomaly detection*: Classification algorithms are effective at identifying unusual patterns, making them vital for systems such as botnet detection, intrusion detection systems (IDS), and malware identification [36, 37].
- *Algorithm varieties*: Common types include Decision Trees, Support Vector Machines (SVM), Naive Bayes, K-Nearest Neighbors (KNN), and Neural Networks [35].
- *Adaptability and continuous learning*: Many algorithms support incremental learning, allowing them to adapt to new threats and evolve with the dynamic cybersecurity environment [38].
- *Challenges and considerations*: Challenges include dealing with imbalanced datasets and the need for extensive, accurately labeled training data. Addressing these issues often involves techniques like synthetic data generation to enhance model accuracy and robustness [39].

4.1.2 Clustering algorithms

Clustering algorithms, essential in unsupervised learning, organize data into groups based on similarity and play a crucial role in cybersecurity [40]. They help identify patterns and anomalies within large datasets using techniques like K-Means, Hierarchical clustering, and DBSCAN, which are tailored for specific data distributions and applications.

- *Anomaly and pattern detection*: Clustering algorithms are vital for anomaly detection in cybersecurity. By grouping similar data points, they help identify unusual patterns such as unrecognized botnet behaviors and new malware signatures [36].
- *Application in cybersecurity*: These algorithms are essential for detecting botnet communication patterns and isolating suspicious network traffic. They are particularly effective when attack signatures are not well-defined or are constantly evolving [41, 42].
- *Challenges and considerations*: Challenges include selecting the optimal number of clusters and the appropriate distance measure. The effectiveness of clustering depends on data characteristics and algorithm parameters, which are crucial for successful anomaly detection in cybersecurity [40].

4.1.3 Neural networks

Neural Networks are fundamental in Machine Learning for modeling complex data relationships and significantly enhancing cybersecurity. These networks, mimicking the human brain's structure, consist of interconnected nodes that process and learn from input data, excelling in identifying complex patterns crucial for detecting sophisticated cyber threats [43].

- *Foundation for advanced models*: They underpin specialized architectures such as Convolutional Neural Networks (CNNs) for image-related tasks [44] and Recurrent Neural Networks (RNNs) for processing sequential data [45].
- *Cybersecurity applications*: Neural networks help build systems that effectively detect and respond to cyber threats, enhancing overall security measures [46].
- *Deep learning foundations*: They form the basis for Deep Learning, involving networks with multiple layers that model complex processes to improve cybersecurity defenses [43].
- *Data and computational demands*: Their effectiveness relies on substantial data and computational power, necessitating high-quality data management and resource allocation [47].
- *Network security*: Protecting neural networks against adversarial attacks is crucial to prevent manipulations that compromise their functionality [47].

4.1.4 Ensemble methods

Ensemble Methods enhance machine learning predictions by combining multiple models, known as "weak learners," into a collective framework. This approach surpasses the accuracy and robustness of any single model. These methods leverage the strengths of various models through techniques like bagging and boosting, which merge predictions to reduce errors and stabilize outcomes [48].

- *Varieties of ensemble methods:*
  - *Bagging:* Reduces variance by combining outputs from models trained on different data subsets.
  - *Boosting:* Increases accuracy by focusing on instances misclassified by previous models.
- *Cybersecurity applications:* Ensemble methods excel in detecting complex threats like botnet attacks. They identify subtle malicious patterns that single models might miss [49].
- *Challenges:* Despite their effectiveness, ensemble methods require significant computational resources and a diverse array of models to optimize performance [50].
- *Botnet detection:* Their ability to enhance network security against advanced botnets demonstrates their

effectiveness in countering sophisticated evasion tactics, thereby strengthening cybersecurity defenses [49].

4.1.5 Reinforcement learning (RL)

Reinforcement Learning (RL) stands out in Machine Learning for its unique decision-making process, which involves interacting with an environment to achieve specific goals. This method uses a reward system that reinforces optimal behaviors, making it particularly effective for tasks requiring sequential decisions, such as navigation and real-time strategy games [51].

- *Agent–environment interaction*: RL involves an agent learning decision-making by interacting with its environment to maximize cumulative rewards [51].
- *Reward feedback*: At the core of RL is the reward signal, which guides the agent's actions to maximize the total received rewards [51].
- *Sequential decision making*: RL excels in tasks requiring sequential decisions, such as navigation and real-time strategy games [51].
- *Exploration vs. exploitation*: RL balances trying new strategies (exploration) with using known successful strategies (exploitation) [51].
- *Policy and value functions*: RL involves learning policies for action selection and value functions to estimate future rewards, which are critical for guiding decisions [51].

4.2 DL in cybersecurity: fortifying digital bastions

Deep Learning (DL) is reshaping cybersecurity by introducing advanced models that identify complex patterns and anomalies with remarkable accuracy. This shift towards predictive and proactive defense strategies is highlighted in the comprehensive survey by Pouyanfar et al. [52]. DL's role is crucial in adapting to the rapidly changing cyber threat environment.

4.2.1 Convolutional neural networks (CNNs)

Convolutional Neural Networks (CNNs) excel in processing visual data, automating feature extraction to enhance accuracy in tasks such as identifying important features for image-based tasks [44].

- *Convolutional layers:* These layers apply filters to capture spatial relationships in data.
- *Pooling layers:* These layers follow convolutional layers to reduce the size of feature maps while preserving essential information.
- *Fully connected layers:* These layers perform high-level reasoning in the network after the convolutional and pooling layers.
- *ReLU activation function:* This function adds nonlinearity to the network, allowing it to learn complex patterns.
- *Applications in cybersecurity:* CNNs are effective for malware classification, anomaly detection, and network intrusion detection, efficiently recognizing malicious activities [53, 54].

4.2.2 Recurrent neural networks (RNNs)

Recurrent Neural Networks (RNNs) are highly effective for processing sequential data, such as in natural language processing and time series analysis. Their architecture retains information for analyzing temporal behaviors [45].

- *Memory:* RNNs maintain an internal state to incorporate historical context into their predictions [55].
- *Parameter sharing:* They use the same parameters across different inputs, reducing the model's complexity and enhancing its ability to handle various sequence lengths [43].
- *Sequential data processing:* Designed specifically for sequential input, RNNs are ideal for tasks where order and context matter [56].
- *Advanced variants:* Modifications like LSTMs [45] and GRUs [17] help manage long-range dependencies and mitigate issues like the vanishing gradient problem.
- *Cybersecurity applications:* RNNs analyze network traffic dynamics to detect anomalies and cyber threats, such as botnets [3, 17, 57]. They minimize the need for manual feature engineering by learning from raw data like network packets and system logs, making them versatile against various attack types [58].

4.2.3 Generative adversarial networks (GANs)

Generative Adversarial Networks (GANs), developed by Goodfellow et al. [59], use two neural networks—the generator and the discriminator—in adversarial training to enhance their ability to detect complex patterns, such as those in botnet activities.

- *Data simulation by the generator:* The generator creates data that mimics network traffic associated with botnets, generating varied examples of potential threats.
- *Authenticity assessment by the discriminator:* The discriminator learns to distinguish between genuine and simulated traffic, continuously improving its ability to identify real threats.

- *Adversarial training:* The ongoing competition between the generator and the discriminator sharpens the system's ability to detect botnet activities [60, 61].

4.2.4 Deep Boltzmann machines (DBMs)

Deep Boltzmann Machines (DBMs) extend traditional Boltzmann Machines by adding multiple layers, enhancing their ability to model complex data representations unsupervised. This is valuable in cybersecurity for capturing high-level data abstractions [62].

- *Multiple layers:* Facilitate the modeling of complex data structures and hierarchical representations [63].
- *Stochastic units:* Both visible and hidden units in DBMs operate based on probabilistic distributions, adding a fundamental probabilistic nature to the model [62].
- *Energy-based framework:* DBMs employ an energy-based framework where the goal is to minimize the system's energy to stabilize observed data configurations [63].
- *Undirected connections:* These connections allow the model to capture bidirectional relationships in data [62].
- *Complex inference and learning:* The processes are computationally intensive, often requiring techniques like Markov chain Monte–Carlo (MCMC) and variational methods [64].

4.2.5 Deep belief networks (DBNs)

Deep Belief Networks (DBNs) are advanced neural network models that excel in learning multi-level data representations, making them highly effective in cybersecurity for detecting complex patterns and potential threats [65].

- *Layered architecture:* DBNs consist of multiple layers of hidden units, allowing them to abstract data representations at different levels [65].
- *Greedy layer-wise training:* This method initializes weights effectively, providing a strong foundation for additional fine-tuning [66].
- *Generative model:* DBNs can generate new data samples that resemble the training data. This is achieved through their deep architecture and ability to learn the joint probability distribution of input data [65].
- *Fine-tuning with supervised learning:* DBNs are initially trained in an unsupervised manner, then fine-tuned with supervised methods to improve performance on specific tasks [67].
- *Wide application:* Their robust learning capabilities make DBNs suitable for a variety of applications, from image recognition to cybersecurity [65–67].

4.2.6 Variational autoencoders (VAEs)

Variational Autoencoders (VAEs) combine the architecture of traditional autoencoders with variational inference, excelling in data compression and generation. This makes them highly effective for anomaly detection in cybersecurity [68, 69].

- *Probabilistic latent space:* VAEs encode inputs into distributions, providing a probabilistic approach to handling data variability and uncertainty [68, 69].
- *Reconstruction and regularization:* They balance accurate input reconstruction with regularizing the latent space to ensure generalization [68].
- *Generative capabilities:* VAEs can generate new data similar to the input data, which is useful for data augmentation and simulation [68, 69].
- *Handling imbalanced datasets:* They are effective in creating synthetic samples to improve performance in scenarios with imbalanced data, such as intrusion detection tasks [69].

4.3 Importance of datasets in ML/DL for cybersecurity

In cybersecurity, the success of Machine Learning (ML) and Deep Learning (DL) relies heavily on the quality and breadth of the datasets used for training. These datasets are fundamental because they determine the ability of these technologies to accurately detect, classify, and predict cyber threats. Data quality, diversity, and representation are critical to developing models that are accurate and robust against continuously evolving cyber threats.

Dataset diversity and quality: A diverse dataset that includes various attack vectors, normal behaviors, and anomalies is essential for training models that perform effectively in real-world scenarios. The quality of the data—its cleanliness, relevance, and accuracy—directly influences the learning process of models, impacting their performance in identifying and mitigating threats [70, 71].

Challenges in dataset procurement and preparation: Collecting comprehensive and balanced datasets is challenging in cybersecurity. Novice developers, in particular, may struggle with these tasks, impacting the effectiveness of ML and DL models [12, 72]. Additionally, the sensitive nature of cybersecurity data complicates its collection and use, demanding strict data handling and processing standards to address privacy and ethical concerns [73].

The role of public and synthetic datasets: Public datasets like NSL-KDD, CICIDS2017, and CTU-13 are vital for research and benchmarking within the cybersecurity community, allowing for the assessment and comparison of various models [74, 75]. Synthetic data generation can also supplement datasets, particularly for rare attack types, enhancing the models' ability to generalize and adapt to new threats [39].

4.4 Challenges in application within cybersecurity

While Machine Learning (ML) and Deep Learning (DL) have revolutionized cybersecurity, their implementation faces significant challenges.

Data privacy and ethical concerns: The use of ML and DL in botnet detection raises significant data privacy and ethical issues. Ensuring data security and addressing concerns such as bias and discrimination are crucial. Ethical governance is necessary to prevent ML and DL models from perpetuating societal inequities or infringing on privacy, especially for novice developers who may struggle with these complexities [5, 12, 76]. Incorporating frameworks like ISO 27001 and NIST CSF provides standardized guidelines and controls to enhance these efforts [77].

Computational resource demands: ML and DL models require significant computational resources, which can be a barrier for smaller organizations. These models increase complexity and may strain system resources, necessitating a balance between performance and resource allocation [7].

Overfitting and model generalization: Overfitting is a major challenge in cybersecurity. ML models often perform well on training data but fail to generalize to new, unseen datasets. This limitation is critical in cybersecurity, where adaptability to evolving threats is essential [6, 78, 79].

Adapting to evolving threats: Cyber threats, especially sophisticated botnets like Gameover Zeus, are continually evolving. ML and DL models need to be regularly updated to keep pace with new tactics and resistances [11].

Advanced ensemble techniques for complex IoT data: In IoT environments, complex and voluminous data require advanced techniques for effective threat detection. Meta-learner models that integrate various deep learning and machine learning approaches can enhance detection accuracy and address the diverse challenges of IoT security [80].

4.5 Evaluating ML and DL models in cybersecurity

In cybersecurity, the deployment of Machine Learning (ML) and Deep Learning (DL) models is increasingly critical. However, their effectiveness relies on rigorous evaluation, as shown in Table 2. These evaluations are essential not only for understanding the models' capabilities in detecting and mitigating cyber threats but also for guiding their continuous improvement.

Quantitative evaluation metrics: The effectiveness of ML and DL models in cybersecurity is measured using several key metrics. These metrics include accuracy, precision, recall, and F-measure, each providing insights into different aspects of model performance. Table 2 details these metrics, explaining how they are calculated and their relevance in model evaluation.

Limitations and real-world application: While these metrics provide fundamental insights, they can be misleading in imbalanced datasets where threat instances are much rarer than normal events. Metrics like accuracy might not fully capture the model's performance under such conditions [81]. Balancing precision and recall is particularly crucial; focusing too much on reducing false positives can lead to high rates of missed detections, which is critical in cybersecurity [82].

5 Contribution of ML and DL in botnet detection

In this section, we explore various ML strategies, illustrating their application through selected studies that reflect recent advances and innovative approaches in combating cyber threats.

5.1 Machine learning techniques in botnet detection

Machine Learning (ML) plays a pivotal role in enhancing cybersecurity by providing a variety of algorithms adept at processing complex datasets. These techniques are crucial for detecting and mitigating botnet activities, effectively adapting to evolving cyber threats. The following Table 3 offers a detailed overview of the key ML techniques applied in recent studies to combat botnet threats.

5.2 Deep learning techniques in botnet detection

Deep Learning (DL) has dramatically shifted the landscape of botnet detection with its advanced capabilities in analyzing and modeling complex data structures. This section presents a series of deep learning techniques that have been instrumental in identifying and countering botnet threats, highlighting the significant impact of these technologies in strengthening cybersecurity.

The following Table 4 encapsulates the scope and depth of DL applications in botnet detection, providing a clear view of the innovations and methodologies that are shaping modern cybersecurity strategies.

5.3 Hybrid and combined detection techniques

In the rapidly evolving field of cybersecurity, hybrid and combined detection techniques integrate Machine Learning (ML) and Deep Learning (DL) with other computational strategies. This sophisticated amalgamation enhances the

Table 2 Metrics used to quantify model performance [72, 81]

Metric	Definition	Formula
True positive	Instances where the model correctly identifies a cyber threat	TP
False positive	Occurs when the model incorrectly identifies normal activity as a threat	FP
True negative	Cases where the model correctly identifies an activity as benign	TN
False negative	When the model fails to detect an actual cyber threat	FN
Precision	The ratio of correctly predicted positive observations to total predicted positives	$\frac{TP}{TP+FP}$
Recall	The model's ability to detect all relevant instances of threats	$\frac{TP}{TP+FN}$
F-measure	Balances precision and recall, useful when false negatives and positives have different costs	$\frac{2\times\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}}$
Accuracy	Overall effectiveness of the model in classifying both threats and non-threats	$\frac{TP+TN}{TP+FP+TN+FN}$

Table 3 Comprehensive overview of ML techniques in Botnet detection

Category	ML technique	Year	Key findings and contributions
Classification algorithms	Decision trees for efficient IoT Botnet detection [83]	2018	Demonstrated the efficacy of decision trees in IoT botnet detection with a reduced feature set, achieving high accuracy
	Tree-based models in Mirai detection [2]	2021	Showcased Kitsune NIDS's proficiency with 'Coarse Tree' models in efficiently identifying Mirai botnet attacks
	KNN and SMOTE for IoT Botnet detection [84]	2021	Illustrated the combined use of KNN and SMOTE in enhancing detection accuracy, underlining the importance of dataset balance
Clustering algorithms	K-means and K-medoids clustering [41]	2016	Showcased the proficiency of K-means and K-medoids in segregating botnet traffic from regular activities
	Hierarchical clustering for DGA-based Botnet detection [42]	2021	Applied hierarchical clustering with ML techniques to identify DGA-based botnets effectively
Neural networks	Mirai botnet detection using AA-dense RNN [85]	2021	Introduced a neural network-based approach, primarily trained on normal traffic, for highly accurate botnet attack detection
	Enhanced Mirai malware detection using ANN and random forest [86]	2021	Highlighted the integration of ANN with ensemble methods, particularly random forest, for Mirai malware detection
Ensemble methods	Smart anomaly-based intrusion detection using GWO-PSO-RF [87]	2021	Combined Grey Wolf optimization and particle swarm optimization for feature selection with random forest classifier, achieving high detection accuracy in IoT networks
	Precision-driven botnet detection with combined forest model [88]	2021	Introduced a 'Combined Forest' model for distinguishing various botnet activities through traffic-flow analysis
Reinforcement learning	Detection zero-day malware attacks on IoT with reinforcement learning [89]	2022	Presented a novel intrusion detection model that synergizes supervised and adversarial learning for zero-day attack detection
	Evasion generative adversarial network for botnet detection [90]	2023	Introduced RELEVAGAN, integrating deep reinforcement learning with generative adversarial networks for botnet detection

Table 4 Summary of deep learning techniques in botnet detection

Category	DL technique	Year	Key findings and contributions
Convolutional neural networks	Anomaly detection in IoT networks using CNN [91]	2022	Addressed vulnerabilities in IoT networks to botnet attacks using CNNs enhanced by regularization techniques
	Detecting android botnet applications using CNN [92]	2023	Highlighted the efficacy of CNNs in addressing botnet threats on Android platforms, analyzing colored images transformed from application byte code files
Recurrent neural networks	BLSTM-RNN and word embedding for IoT botnet detection [57]	2018	Combined BLSTM-RNN with word embedding techniques to significantly enhance packet-level botnet detection in IoT devices
	Advanced classification of DGA domain names [3]	2019	Utilized LSTM with attention mechanisms for advanced classification of DGA domain names
	Detection of IoT botnets with GRU networks [17]	2023	Explored GRU networks for precise botnet detection in IoT devices, demonstrating proficiency in managing sequential data
Deep neural networks	Deep autoencoder-based IoT botnet detection [93]	2018	Introduced deep autoencoders for efficient network traffic analysis and anomaly identification in IoT devices
	LS-DRNN: memory-efficient deep learning method for botnet attack detection [94]	2021	Showcased a memory-efficient deep learning method, integrating LAE, SMOTE, and DRNN for botnet attack detection in IoT networks
	DNNBoT: DNN-based botnet detection and classification [95]	2022	DNNBoT models, optimized through advanced techniques, exhibited exceptional accuracy in detecting and classifying botnet attacks
Generative adversarial networks	CL-GAN: GAN for generating and detecting AGDs [60]	2023	Introduced CL-GAN, employing a GAN for identifying algorithmically generated domains, emphasizing continuous adaptability to new DGA patterns
	Anomaly detection using DCGAN in the internet of things [61]	2023	Introduced a pioneering ensemble model combining DCGAN with Bi-LSTM networks for identifying a range of botnet-driven attacks in IoT
Deep belief networks	DBN-based framework for malware detection in android systems [67]	2018	Presented a DBN-driven framework that adeptly combines high-level static and dynamic analyses for feature extraction
	Intrusion detection based on DBNs [65]	2022	Highlighted the use of DBNs for botnet detection, particularly in NIDS, emphasizing their prowess in identifying complex data representations
	Chronological salp swarm algorithm based dbn for intrusion detection [66]	2022	Introduced a novel approach combining deep learning with optimized algorithms for enhanced intrusion detection in cloud environments

Table 4 continued

Category	DL technique	Year	Key findings and contributions
Deep Boltzmann machines	Malware attack detection using EDRBM [64]	2023	Investigated the application of deep Boltzmann machines for botnet detection in large networks, leveraging statistical features from flowsets
Variational autoencoders	Detecção de Ataques de Botnets em IoT via VAE [68]	2022	Employed variational autoencoders to detect botnet attacks in IoT devices, focusing on the N-BaIoT dataset
	ML with VAE for Imbalanced datasets in intrusion detection [69]	2022	Introduced a machine learning framework combining a VAE with a multilayer perceptron model for intrusion detection

Table 5 Comprehensive overview of hybrid and combined techniques in botnet detection

Technique	Year	Key findings and contributions
Enhancing botnet detection with SVM and AFSA [96]	2014	Introduced a hybrid system that utilizes SVM and the Artificial Fish Swarm Algorithm to optimize feature selection, significantly enhancing botnet detection in LAN environments
Enhanced P2P botnet detection using decision trees and neural networks [97]	2018	Combined decision trees with multilayer neural networks to analyze TCP control packet headers, offering a refined method for detecting decentralized P2P botnet activities
Hybrid decision tree and random forest approach for IoT DDoS attack detection [98]	2020	Merged decision tree and random forest algorithms to improve accuracy in detecting DDoS attacks in IoT networks, highlighting the effectiveness of using multiple ML techniques
XGBoost and advanced ML algorithms [99]	2022	Explored the integration of XGBoost with DL models like RNNs, LSTMs, and CNNs to provide adaptable and highly effective solutions for IoT network security

detection capabilities against diverse botnet threats by leveraging the strengths of multiple methodologies to effectively tackle the complexities of modern cyber threats.

The following Table 5 provides a succinct overview of key hybrid and combined detection techniques, outlining their significant contributions to advancing botnet detection strategies.

Table 6 Cutting-edge innovations in botnet detection techniques

Innovative approach	Year	Key findings and contributions
Backtracking for botnet detection in wired networks [100]	2018	Introduced a backtracking method evaluating network parameters to effectively distinguish legitimate from malicious traffic in wired networks
Federated learning for botnet detection in IoT [101]	2023	Implemented federated learning in IoT networks to enhance privacy and efficiency, allowing local data processing while integrating host and network intrusion detection systems for comprehensive security enhancements

5.4 Innovative approaches in botnet detection

In this subsection, we explore recent innovative research in Machine Learning (ML) and Deep Learning (DL) applied to botnet detection. It focuses on adaptive learning and federated learning models, which promise to advance cybersecurity with their adaptability and privacy-preserving capabilities, effectively tackling sophisticated botnet threats.

The following Table 6 provides a comprehensive overview of pioneering studies that push the boundaries of botnet detection through innovative ML and DL techniques, indicating the year of implementation and summarizing their core innovations and significant contributions.

5.5 Discussion and conclusions

This chapter highlights the extensive research in Machine Learning (ML) and Deep Learning (DL) for botnet detection, focusing on innovative methodologies that enhance cybersecurity strategies. The insights discussed provide a comprehensive view of the cutting-edge techniques and significant advancements that shape modern cybersecurity measures.

Innovations and synergies in botnet detection: ML and DL have broadened the scope of cybersecurity, particularly in detecting and neutralizing sophisticated botnet activities. Classification algorithms [84] and neural networks [44, 45] play key roles in extracting complex patterns and distinguishing between benign and malicious activities. Ensemble methods [87, 88] integrate various algorithms to improve accuracy and adaptability, addressing the dynamic and complex nature of cyber threats, especially in IoT environments.

Challenges: evolving threats and technological demands: The continuous evolution of botnet tactics requires that ML and DL models adapt swiftly to maintain effectiveness. The reliance on comprehensive and high-quality data for training these models introduces challenges related to data privacy, ethical considerations, and computational demands. Ensuring the integrity and confidentiality of data while managing the logistical aspects of deploying sophisticated models in real-time scenarios is crucial.

Collaborative research and interdisciplinary approaches: Addressing the multifaceted challenges of botnet detection demands a collaborative approach that spans multiple disciplines. By integrating expertise from various fields, including computer science, data analysis, and ethics, cybersecurity strategies can be robust, innovative, and ethically sound. Interdisciplinary collaborations enrich the development process and foster holistic solutions.

Ethical considerations and the path forward: As ML and DL technologies become integral to cybersecurity, addressing ethical concerns is imperative. Practices that ensure data privacy, model transparency, and responsible AI usage are essential. These ethical practices must be woven into the fabric of cybersecurity strategies to align technological advancements with societal values and norms [34, 52].

The exploration of ML and DL in botnet detection showcases a domain characterized by innovation and adaptability. The integration of advanced analytical techniques, alongside a commitment to ethical practices and interdisciplinary collaboration, is vital for developing effective defenses that align with both technological needs and ethical standards.

6 Proactive botnet defense with ML & DL

Building on the insights from Sect. 5 on ML and DL in botnet detection, Sect. 6 advances into proactive measures for botnet prevention. It emphasizes how these technologies extend beyond mere detection to predict and prevent threats, showcasing a shift from traditional reactive measures to a proactive cybersecurity approach. In this chapter, we explore how predictive modeling and real-time monitoring are essential in today's digitally integrated world, highlighting various studies that underline the critical role of ML and DL in actively shaping cybersecurity defenses.

6.1 Machine learning as a vanguard in botnet defense

Machine Learning (ML) plays a crucial role in cybersecurity, equipping systems with the necessary tools to proactively counter and mitigate evolving botnet threats. By integrating various ML techniques such as classification algorithms, neural networks, and ensemble methods, cybersecurity frameworks are strengthened, enhancing both threat prediction and prevention capabilities. This strategic deployment of ML not only addresses current cybersecurity challenges but also anticipates potential threats, ushering in a new era of advanced digital defense mechanisms.

The following Table 7 encapsulates a selection of ML techniques pivotal in the proactive prevention of botnet attacks. It highlights the implementation years and summarizes the core achievements and contributions of each technique, illustrating how ML has become an indispensable asset in enhancing network security.

6.2 DL: deciphering and disarming advanced threats

Deep Learning (DL) stands at the forefront of cybersecurity, utilizing sophisticated models like Recurrent Neural Networks (RNNs) and Deep Neural Networks (DNNs) to analyze and neutralize complex cyber threats. These advanced DL techniques play a pivotal role not only in detecting but also in predicting and preemptively countering botnet strategies. This approach highlights DL's crucial role in evolving cybersecurity defenses, shifting from reactive responses to proactive threat management and prediction.

The following Table 8 encapsulates key DL approaches in botnet threat mitigation, illustrating the transformative impact of these technologies in fortifying digital infrastructures against sophisticated cyber-attacks.

6.3 Frontier technologies in proactive defense

Exploring the frontier of cybersecurity, we delve into advanced technologies that are reshaping proactive defense strategies. This section highlights how Meta-Learning, Incremental Learning, and Online and Real-Time Detection Techniques are advancing cybersecurity, setting new standards for dynamic and effective threat mitigation.

The following Table 9 encapsulates the innovative techniques transforming the landscape of botnet prevention. It illustrates cutting-edge approaches that not only react to threats but also predict and neutralize them in real-time, thereby significantly bolstering cybersecurity infrastructure.

Table 7 ML-driven strategies for botnet attack prevention

Category	ML technique	Year	Key findings and contributions
Classification algorithms	Random forest for DNS query analysis [102]	2018	Employed random forest to analyze DNS queries, leading to a sophisticated classifier with over 90% accuracy in real-time monitoring
Neural networks	ARNN for collective classification [103]	2023	Introduced ARNN, demonstrating unparalleled accuracy in predicting botnet activities and adaptability to both traditional and incremental learning
Ensemble methods	Combined forest approach [88]	2021	Amalgamated pre-processed decision trees into a 'Combined Forest' model for identifying botnet communication patterns and early detection
	Optimized ML models for Kitsune NIDS [2]	2021	Explored the efficacy of ensemble machine learning algorithms in optimizing Kitsune NIDS for Mirai Botnet malware detection

Table 8 DL innovations in botnet attack mitigation

Category	DL technique	Year	Key findings and contributions
RNNs	GRU for IoT PdM systems [104]	2019	Utilized gated recurrent unit models to predict the remaining useful life of machinery, demonstrating resilience against FDIA
DNNs	DBoTPM for botnet attack prediction [105]	2023	Introduced DBoTPM, a deep neural network model for predicting botnet attacks in IoT infrastructures with high accuracy and computational efficiency

6.4 Discussion on effectiveness and challenges

In the dynamic realm of cybersecurity, ML and DL have initiated a transformative era in preemptively countering botnet threats. This section evaluates the effectiveness of these technologies and the challenges they encounter, emphasizing their pivotal role in advancing cybersecurity.

Unveiling the efficacy of ML and DL in botnet prevention: ML and DL have proven effective in botnet prevention, as evidenced by various empirical studies. Classification algorithms and neural networks, such as those described in [102] and [103], excel in detecting and preventing threats by analyzing extensive data sets with high precision. These advanced methodologies not only detect but also predict potential threats, facilitating a shift from traditional reactive measures to proactive security strategies.

Confronting the challenges: technological and ethical implications: The application of ML and DL in cybersecurity faces significant challenges. The evolving nature of cyber threats requires these models to continually adapt, demanding ongoing enhancements to maintain efficacy. The effectiveness of these systems heavily relies on the quality and breadth of the training data, which brings additional ethical concerns regarding privacy and data integrity. Technological challenges include the need for sophisticated algorithm tuning and the integration of these systems within

Table 9 Advanced techniques in botnet attack prevention

Category	ML technique	Year	Key findings and contributions
Incremental learning techniques	AA-dense RNN with incremental online learning [106]	2022	Revolutionized botnet prevention in IoT networks through AA-dense RNN equipped with incremental online learning capabilities
Meta-learning	Meta-learning with deep learning models [80]	2023	Harmoniously integrated RNN, LSTM, and CNN supported by LR, MLP, SVM, and XGBoost for high accuracy in detecting botnets
Online learning techniques	AADRNN with online learning [107]	2023	Introduced AADRNN mastering both offline and online learning, providing a comprehensive solution to cybersecurity challenges
Real-time detection techniques	ML for real-time network monitoring [108]	2023	Employed advanced ML methodology for expedited network traffic analysis, achieving substantial detection accuracy within one-second intervals

existing cybersecurity infrastructures without compromising operational integrity or privacy.

Forging the path forward: a multidisciplinary approach: Addressing the complexities of utilizing ML and DL in cybersecurity necessitates a comprehensive approach that spans technological innovation, ethical considerations, and regulatory compliance. This approach should include refining algorithmic accuracy, ensuring robust data protection practices, and fostering a culture of ethical AI use. Collaboration across sectors and disciplines is crucial to develop resilient, effective, and ethically responsible cybersecurity solutions.

As we advance, it's evident that enhancing cybersecurity measures against botnets with ML and DL involves a balanced approach that aligns technological advancements with ethical and societal values.

7 Challenges and prospects in botnet defense

7.1 Current challenges in utilizing ML & DL against botnets

Machine Learning (ML) and Deep Learning (DL) are crucial in the fight against botnets, yet they face several challenges that demand constant innovation and adaptation.

Adapting to sophisticated botnet structures: Contemporary botnets, such as Mirai, have grown increasingly complex, requiring continual advancements in ML and DL models to keep pace. The development of advanced models like DBoTPM [105] is essential for matching the sophistication of modern botnets.

Data privacy and ethical concerns: The use of ML and DL in cybersecurity introduces significant data privacy and ethical issues [5, 76]. Balancing technological effectiveness with privacy protection remains a critical challenge.

Computational resource demands: High computational demands limit the deployment of sophisticated ML and DL models, especially for resource-constrained organizations [7]. Efficiently managing these resources is crucial for effective technology deployment.

Overfitting and model generalization: Overfitting is a major concern where models excel on training data but fail on unseen data. Enhancing model generalization to effectively handle new and diverse threats remains a significant challenge [6, 78].

Real-time detection and adaptability: Models must detect threats in real-time and adapt quickly to changing botnet tactics, as demonstrated by AA-Dense RNN [106] and various meta-learner models [80].

Balancing detection accuracy and false positives: It is vital to maintain high detection accuracy without triggering false alarms, ensuring models differentiate effectively between normal and malicious activities [102].

Addressing evolving threats: Continual updates to ML and DL models are necessary to address the rapid evolution of botnet strategies [11].

7.2 Future prospects and potential for innovation

The future of botnet detection and prevention using ML and DL holds great potential for breakthroughs and novel methodologies. As cyber threats become more sophisticated, our defensive strategies must evolve concurrently, leveraging advanced models and incorporating emerging technologies to stay ahead.

Innovative model development: Future research will focus on developing innovative ML and DL models tailored to modern botnet challenges. Investigations into models like DBoTPM and AADRNN [105, 107] pave the way for sophisticated solutions capable of adapting to complex botnet behaviors.

Enhanced IoT security: The proliferation of IoT devices increases the need for robust security solutions. Emerging research, employing GRU networks [104] and meta-learning [80], emphasizes fortifying IoT ecosystems against botnets, with prospects for developing specialized models to efficiently manage the diverse data landscape of IoT devices.

Cross-domain collaborations: Collaborative efforts across various fields, as exemplified by Khetani et al. [109], promise innovative botnet countermeasures by harnessing advancements from domains such as healthcare and finance. This interdisciplinary approach could significantly enhance cybersecurity, offering fresh perspectives and technologies to counteract botnet threats.

Ethical AI and privacy considerations: The advancement of ML and DL must prioritize ethical concerns, especially regarding data privacy. Upholding high ethical standards [5, 76] will be essential for the successful integration of these technologies into cybersecurity practices.

7.3 Adaptability and model updates in cybersecurity

In the fast-evolving field of cybersecurity, the adaptability and regular updating of ML and DL models are crucial. As botnets become more sophisticated, adopting adaptive ML and DL models is vital for maintaining effective defenses.

Adaptability to emerging threats: The dynamic nature of cyber threats, particularly botnets, requires models that can evolve with new and changing tactics. Studies on models like AA-Dense RNN [106] and DBoTPM [105] demonstrate the ability of these technologies to adjust to shifting attack patterns. Ongoing development is essential for effective preemption and response to future threats.

Continuous model updates for effectiveness: The rapid evolution of botnet strategies necessitates constant updates to detection models. Research on real-time IoT botnet detection using Auto-Associative Deep Random Neural Networks (AADRNN) [107] underscores the importance of continually updating learning algorithms to keep pace with emerging botnet tactics.

Integrating new data sources: As botnet attacks grow in complexity, enriching ML and DL models with diverse data sources becomes increasingly important for improving detection capabilities. Research integrating DNS query analysis and the 'Combined Forest' method [88, 102] shows how varied data types can enhance the comprehensiveness and effectiveness of threat detection.

Challenges in continuous learning: Continuous model updating is essential but challenging, requiring substantial computational resources and continual data collection. The computational demands of advanced ML and DL models necessitate efficient resource management to support ongoing learning, as discussed in [7].

Future directions: The focus should shift towards developing self-updating models that operate in real-time, utilizing the latest AI and data processing technologies. The potential of federated learning, highlighted in [101], offers promising decentralized learning capabilities that can swiftly adjust to changes in network conditions.

8 Conclusion

The integration of Machine Learning (ML) and Deep Learning (DL) into cybersecurity has transformed how we tackle botnet threats, offering significant advancements while facing challenges like evolving tactics, data integrity, and high computational demands. Research focusing on autonomous and adaptive ML/DL models, such as those discussed in [105] and [107], promises to further enhance cybersecurity measures. Collaborative efforts across different sectors are vital for a holistic defense strategy, combining technological and methodological innovations to effectively counter emerging threats [77].

Ethical considerations and data privacy, crucial for the responsible application of AI, must be addressed to maintain public trust and ensure effective deployment, as noted in references [5] and [76], particularly by supporting novice developers in their roles [12]. The increasing frequency and severity of botnet incidents, highlighted by attacks like the Meris [13], underscore the urgency for continuous innovation and vigilance.

As the landscape of cyber threats evolves, particularly with botnets, the need for ongoing innovation, collaboration among academia, industry, and government, and public awareness about cybersecurity grows increasingly important. By strengthening these areas, we can enhance our defensive measures and maintain the integrity of our digital infrastructures. The path forward in cybersecurity is marked by a commitment to innovation and cooperation, ensuring robust defenses against the sophisticated cyber threats of tomorrow.

Author Contributions All authors of this work participate equally to produce the paper.

Funding Not applicable.

Availability of data and materials Not applicable.

Declarations

Conflict of interest Not applicable.

Ethical approval Not applicable.

References

1. Antonakakis M, April T, Bailey M, Bernhard M, Bursztein E, Cochran J, Durumeric Z, Halderman JA, Invernizzi L, Kallitsis M et al. (2017) Understanding the mirai botnet. In: 26th USENIX security symposium (USENIX Security 17), pp 1093–1110
2. Alabdulatif A, Rizvi SSH, Hashmani MA (2021) Optimal machine learning models for kitsune to detect mirai botnet malware attack. J Hun Univ Nat Sci 48(6):12
3. Qiao Y, Zhang B, Zhang W, Sangaiah AK, Wu H (2019) Dga domain name classification method based on long short-term memory with attention mechanism. Appl Sci 9(20):4205
4. Baddi Y, Sebbar A, Zkik K, Maleh Y, Bensalah F, Boulmalf M (2024) Msdn-iot multicast group communication in iot based on software defined networking. J Reliab Intell Environ 10(1):93–104
5. Himthani P, Dubey GP, Sharma BM, Taneja A (2020) Big data privacy and challenges for machine learning. In: 2020 Fourth international conference on I-SMAC (IoT in social, mobile, analytics and cloud) (I-SMAC). IEEE, pp 707–713
6. Aburass S (2023) Quantifying overfitting: introducing the overfitting index. arXiv preprint arXiv:2308.08682
7. Wazid M, Das AK, Chamola V, Park Y (2022) Uniting cyber security and machine learning: advantages, challenges and future research. ICT Express 8(3):313–321
8. Eslahi M, Salleh RB, Anuar NB (2012) Bots and botnets: an overview of characteristics, detection and challenges. In: 2012 IEEE International conference on control system, computing and engineering, pp 349–354
9. Walvekar HS, Kanade A, Gautam S, Jagtap S (2022) Bots, botnets and zombies: anatomy, inhibitory measures and threat prevention techniques. Int J Sci Res Comput Sci Eng Inf Technol 8:351–356
10. Maigida AM, Abdulhamid SM, Olalere M, Alhassan JK, Chiroma H, Dada EG (2019) Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. J Reliab Intell Environ 5:67–89
11. Andriesse D, Rossow C, Stone-Gross B, Plohmann D, Bos H (2013) Highly resilient peer-to-peer botnets are here: an analysis of gameover zeus. In: 2013 8th international conference on malicious and unwanted software: "The Americas" (MALWARE). IEEE, pp 116–123
12. Corno F, De Russis L, Mannella L (2022) Helping novice developers harness security issues in cloud-iot systems. J Reliab Intell Environ 8(3):261–283
13. Meris botnet breaks records (2021) Network security 2021(9):3. https://doi.org/10.1016/S1353-4858(21)00098-2
14. Xiang C, Binxing F, Lihua Y, Xiaoyi L, Tianning Z (2011) Andbot: towards advanced mobile botnets. In: 4th USENIX workshop on large-scale exploits and emergent threats (LEET 11)
15. Garip MT, Lin J, Reiher P, Gerla M (2019) Shieldnet: an adaptive detection mechanism against vehicular botnets in vanets. In: 2019 IEEE vehicular networking conference (VNC). IEEE, pp 1–7
16. Boshmaf Y, Muslukhov I, Beznosov K, Ripeanu M (2013) Design and analysis of a social botnet. Comput Netw 57(2):556–578
17. Regisanne W, Kirubavathi G, Sridevi UK (2023) Detection of iot botnet using machine learning and deep learning techniques. Res Square. https://doi.org/10.21203/rs.3.rs-2630988/v1
18. Giess M (2021) Cpaas and sase: the best defences against iot threats. Netw Secur 2021(9):9–12. https://doi.org/10.1016/S1353-4858(21)00103-3
19. Szynkiewicz P (2022) Signature-based detection of botnet DDoS attacks. In: Kołodziej J, Repetto M, Duzha A (eds) Cybersecurity of digital service chains. Springer, Cham, pp 120–135
20. Behal S, Brar AS, Kumar K (2010) Signature-based botnet detection and prevention. In: Proceedings of international symposium on computer engineering and technology, pp 127–132
21. Arshad S, Abbaspour M, Kharrazi M, Sanatkar H (2011) An anomaly-based botnet detection approach for identifying stealthy botnets. In: 2011 IEEE international conference on computer applications and industrial electronics (ICCAIE). IEEE, pp 564–569
22. Wang H, He H, Zhang W, Liu W, Liu P, Javadpour A (2022) Using honeypots to model botnet attacks on the internet of medical things. Comput Electr Eng 102:108212. https://doi.org/10.1016/j.compeleceng.2022.108212
23. Lee S, Abdullah A, Jhanjhi N (2020) A review on honeypot-based botnet detection models for smart factory. Int J Adv Comput Sci Appl. https://doi.org/10.14569/IJACSA.2020.0110654
24. Stevanovic M, Pedersen JM (2015) An analysis of network traffic classification for botnet detection. In: 2015 International conference on cyber situational awareness, data analytics and assessment (CyberSA). IEEE, pp 1–8
25. Zhao D, Traore I, Sayed B, Lu W, Saad S, Ghorbani A, Garant D (2013) Botnet detection based on traffic behavior analysis and flow intervals. Comput Secur 39:2–16. https://doi.org/10.1016/j.cose.2013.04.007
26. Singh M, Singh M, Kaur S (2019) Issues and challenges in dns based botnet detection: a survey. Comput Secur 86:28–52. https://doi.org/10.1016/j.cose.2019.05.019
27. Bottazzi G, Italiano GF (2015) Fast mining of large-scale logs for botnet detection: a field study. In: 2015 IEEE international conference on computer and information technology; ubiquitous computing and communications; dependable, autonomic and secure computing; pervasive intelligence and computing. IEEE, pp 1989–1996
28. Choi H, Lee H, Lee H, Kim H (2007) Botnet detection by monitoring group activities in dns traffic. In: 7th IEEE international conference on computer and information technology (CIT 2007). IEEE, pp 715–720
29. Pomorova O, Savenko O, Lysenko S, Kryshchuk A, Bobrovnikova K (2015) A technique for the botnet detection based on dns-traffic analysis. In: Computer networks: 22nd international conference, CN 2015, Brunów, Poland, June 16–19, 2015. Proceedings 22. Springer, pp 127–138
30. Bertino E, Islam N (2017) Botnets and internet of things security. Computer 50(2):76–79
31. Ogu EC, Ojesanmi OA, Awodele O, Kuyoro S (2019) A botnets circumspection: the current threat landscape, and what we know so far. Information 10(11):337
32. Kolias C, Kambourakis G, Stavrou A, Voas J (2017) Ddos in the iot: Mirai and other botnets. Computer 50(7):80–84

33. Mahesh B (2020) Machine learning algorithms—a review. Int J Sci Res (IJSR) 9(1):381–386
34. Hastie T, Tibshirani R, Friedman JH, Friedman JH (2009) The elements of statistical learning: data mining, inference, and prediction, vol 2. Springer, Berlin
35. James G, Witten D, Hastie T, Tibshirani R et al (2013) An introduction to statistical learning, vol 112. Springer, New York
36. Chandola V, Banerjee A, Kumar V (2009) Anomaly detection: a survey. ACM Comput Surv (CSUR) 41(3):1–58
37. Garcia-Teodoro P, Diaz-Verdejo J, Maciá-Fernández G, Vázquez E (2009) Anomaly-based network intrusion detection: techniques, systems and challenges. Comput. Secur. 28(1–2):18–28
38. Ditzler G, Roveri M, Alippi C, Polikar R (2015) Learning in nonstationary environments: a survey. IEEE Comput Intell Mag 10(4):12–25
39. Chawla NV, Bowyer KW, Hall LO, Kegelmeyer WP (2002) Smote: synthetic minority over-sampling technique. J Artif Intell Res 16:321–357
40. Xu D, Tian Y (2015) A comprehensive survey of clustering algorithms. Ann Data Sci 2:165–193
41. Alejandre FV, Cortés NC, Anaya EA (2016) Botnet detection using clustering algorithms. Res Comput Sci 118:65–75
42. Soleymani A, Arabgol F (2021) A novel approach for detecting dga-based botnets in dns queries using machine learning techniques. J Comput Netw Commun 2021:1–13
43. Goodfellow I, Bengio Y, Courville A (2016) Deep learning. MIT Press, USA
44. Krizhevsky A, Sutskever I, Hinton GE (2012) Imagenet classification with deep convolutional neural networks. Adv Neural Inf Process Syst 25:1097–1105
45. Hochreiter S, Schmidhuber J (1997) Long short-term memory. Neural Comput 9(8):1735–1780
46. Aburomman AA, Reaz MBI (2016) A novel svm-knn-pso ensemble method for intrusion detection system. Appl Soft Comput 38:360–372
47. Szegedy C, Zaremba W, Sutskever I, Bruna J, Erhan D, Goodfellow I, Fergus R (2013) Intriguing properties of neural networks. arXiv preprint arXiv:1312.6199
48. Breiman L (2001) Random forests. Mach Learn 45:5–32
49. Koroniotis N, Moustafa N, Sitnikova E, Slay J (2018) Towards developing network forensic mechanism for botnet activities in the iot based on machine learning techniques. In: Mobile networks and management: 9th international conference, MONAMI 2017, Melbourne, Australia, December 13–15, 2017, Proceedings, vol 9. Springer, pp 30–44
50. Kuncheva LI, Whitaker CJ (2003) Measures of diversity in classifier ensembles and their relationship with the ensemble accuracy. Mach Learn 51:181–207
51. Sutton RS, Barto AG (2018) Reinforcement learning: an introduction. MIT Press, USA
52. Pouyanfar S, Sadiq S, Yan Y, Tian H, Tao Y, Reyes MP, Shyu M-L, Chen S-C, Iyengar SS (2018) A survey on deep learning: algorithms, techniques, and applications. ACM Comput Surv (CSUR) 51(5):1–36
53. Sermanet P, Eigen D, Zhang X, Mathieu M, Fergus R, Le Cun Y (2013) Overfeat: integrated recognition, localization and detection using convolutional networks. arXiv preprint arXiv:1312.6229
54. He K, Zhang X, Ren S, Sun J (2016) Deep residual learning for image recognition. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp 770–778
55. Graves A (2012) Sequence transduction with recurrent neural networks. arXiv preprint arXiv:1211.3711
56. Graves A, Mohamed A-r, Hinton G (2013) Speech recognition with deep recurrent neural networks. In: 2013 IEEE international conference on acoustics, speech and signal processing. IEEE, pp 6645–6649
57. McDermott CD, Majdani F, Petrovski AV (2018) Botnet detection in the internet of things using deep learning approaches. In: 2018 International joint conference on neural networks (IJCNN). IEEE, pp 1–8
58. Kim J, Kim J, Thu HLT, Kim H (2016) Long short term memory recurrent neural network classifier for intrusion detection. In: 2016 International conference on platform technology and service (PlatCon). IEEE, pp 1–5
59. Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, Courville A, Bengio Y (2014) Generative adversarial nets. Adv Neural Inf Process Syst 27:2672–2680
60. Ren Y, Li H, Liu P, Liu J, Zhu H, Sun L (2023) Cl-gan: a gan-based continual learning model for generating and detecting agds. Comput Secur 131:103317
61. Mishra AK, Paliwal S, Srivastava G (2023) Anomaly detection using deep convolutional generative adversarial networks in the internet of things. ISA Trans 145:493–504
62. Hinton G (2007) Boltzmann machine. Scholarped J 2(5):1668
63. Salakhutdinov R, Mnih A, Hinton G (2007) Restricted Boltzmann machines for collaborative filtering. In: Proceedings of the 24th international conference on machine learning, pp 791–798
64. Kumar J, Ranganathan G (2023) Malware attack detection in large scale networks using the ensemble deep restricted Boltzmann machine. Eng Technol Appl Sci Res 13(5):11773–11778
65. Belarbi O, Khan A, Carnelli P, Spyridopoulos T (2022) An intrusion detection system based on deep belief networks. In: International conference on science of cyber security. Springer, pp 377–392
66. Karuppusamy L, Ravi J, Dabbu M, Lakshmanan S (2022) Chronological salp swarm algorithm based deep belief network for intrusion detection in cloud using fuzzy entropy. Int J Numer Model Electron Netw Dev Fields 35(1):2948
67. Saif D, El-Gokhy S, Sallam E (2018) Deep belief networks-based framework for malware detection in android systems. Alex Eng J 57(4):4049–4057
68. Cunha AA, Borges JB, Loureiro AA (2022) Detecçao de ataques de botnets em iot via variational autoencoder. In: Anais do VI Workshop de Computação Urbana. SBC, pp 238–251
69. Lin Y-D, Liu Z-Q, Hwang R-H, Nguyen V-L, Lin P-C, Lai Y-C (2022) Machine learning with variational autoencoder for imbalanced datasets in intrusion detection. IEEE Access 10:15247–15260
70. Xiao H, Xiao H, Eckert C (2012) Adversarial label flips attack on support vector machines. In: ECAI 2012. IOS Press, pp 870–875
71. Barreno M, Nelson B, Sears R, Joseph AD, Tygar JD (2006) Can machine learning be secure? In: Proceedings of the 2006 ACM symposium on information, computer and communications security, pp 16–25
72. Davis J, Goadrich M (2006) The relationship between precision-recall and roc curves. In: Proceedings of the 23rd international conference on machine learning, pp 233–240
73. Mittelstadt BD, Allo P, Taddeo M, Wachter S, Floridi L (2016) The ethics of algorithms: mapping the debate. Big Data Soc 3(2):2053951716679679
74. Sharafaldin I, Lashkari AH, Ghorbani AA (2018) Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp 1:108–116
75. Garcia S, Grill M, Stiborek J, Zunino A (2014) An empirical comparison of botnet detection methods. Comput Secur 45:100–123
76. Stahl BC (2021) Ethical issues of AI. Springer, Cham, pp 35–53
77. Tissir N, El Kafhali S, Aboutabit N (2021) Cybersecurity management in cloud computing: semantic literature review and

conceptual framework proposal. J Reliab Intell Environ 7(2):69–84
78. Wang Z, Li H, Carpenter C, Guan Y (2020) Challenge-enabled machine learning to drug-response prediction. AAPS J 22:1–6
79. Roelofs R, Shankar V, Recht B, Fridovich-Keil S, Hardt M, Miller J, Schmidt L (2019) A meta-analysis of overfitting in machine learning. Adv Neural Inf Process Syst 32:1–11
80. Rihan SDA, Anbar M, Alabsi BA (2023) Meta-learner-based approach for detecting attacks on internet of things networks. Sensors 23(19):8191
81. Sokolova M, Lapalme G (2009) A systematic analysis of performance measures for classification tasks. Inf Process Manage 45(4):427–437
82. Powers DM (2020) Evaluation: from precision, recall and f-measure to roc, informedness, markedness and correlation. arXiv preprint arXiv:2010.16061
83. Bahşi H, Nõmm S, La Torre FB (2018) Dimensionality reduction for machine learning based iot botnet detection. In: 2018 15th international conference on control, automation, robotics and vision (ICARCV). IEEE, pp 1857–1862
84. Pokhrel S, Abbas R, Aryal B (2021) Iot security: botnet detection in iot using machine learning. arXiv preprint arXiv:2104.02231
85. Nakip M, Gelenbe E (2021) Mirai botnet attack detection with auto-associative dense random neural network. In: 2021 IEEE global communications conference (GLOBECOM). IEEE, pp 1–6
86. Palla TG, Tayeb S (2021) Intelligent mirai malware detection for iot nodes. Electronics 10(11):1241
87. Keserwani PK, Govil MC, Pilli ES, Govil P (2021) A smart anomaly-based intrusion detection system for the internet of things (iot) network using gwo-pso-rf model. J Reliab Intell Environ 7(1):3–21
88. Maudoux C, Boumerdassi S, Barcello A, Renault E (2021) Combined forest: a new supervised approach for a machine-learning-based botnets detection. In: 2021 IEEE global communications conference (GLOBECOM). IEEE, pp 1–6
89. Ngo Q-D, Nguyen Q-H (2022) A reinforcement learning-based approach for detection zero-day malware attacks on iot system. In: Computer science on-line conference. Springer, pp 381–394
90. Randhawa RH, Aslam N, Alauthman M, Khalid M, Rafiq H (2024) Deep reinforcement learning based evasion generative adversarial network for botnet detection. Futur Gener Comput Syst 150:294–302
91. Hairab BI, Elsayed MS, Jurcut AD, Azer MA (2022) Anomaly detection based on cnn and regularization techniques against zero-day attacks in iot networks. IEEE Access 10:98427–98440
92. Arshad M, Karim A, Naseer S, Ahmad S, Alqahtani M, Gardezi AA, Choi J (2023) Detecting android botnet applications using convolution neural network. Comput Mater Contin 77(2):2123–2135
93. Meidan Y, Bohadana M, Mathov Y, Mirsky Y, Shabtai A, Breitenbacher D, Elovici Y (2018) N-baiot-network-based detection of iot botnet attacks using deep autoencoders. IEEE Pervas Comput 17(3):12–22
94. Popoola SI, Adebisi B, Ande R, Hammoudeh M, Atayero AA (2021) Memory-efficient deep learning for botnet attack detection in iot networks. Electronics 10(9):1104
95. Haq MA, Rahim Khan MA (2022) Dnnbot: deep neural network-based botnet detection and classification. Comput Mater Contin. https://doi.org/10.32604/cmc.2022.020938
96. Lin K-C, Chen S-Y, Hung JC (2014) Botnet detection using support vector machines with artificial fish swarm algorithm. J Appl Math. https://doi.org/10.1155/2014/986428
97. Alauthaman M, Aslam N, Zhang L, Alasem R, Hossain MA (2018) A p2p botnet detection scheme based on decision tree and adaptive multilayer neural networks. Neural Comput Appl 29:991–1004
98. Aysa MH, Ibrahim AA, Mohammed AH (2020) Iot ddos attack detection using machine learning. In: 2020 4th International symposium on multidisciplinary studies and innovative technologies (ISMSIT). IEEE, pp 1–7
99. Alissa K, Alyas T, Zafar K, Abbas Q, Tabassum N, Sakib S et al (2022) Botnet attack detection in iot using machine learning. Comput Intell Neurosci. https://doi.org/10.1155/2022/4515642
100. Vidiyala D, Guntupalli B, Alluri BKR (2018) Botnets detection using back tracking in wired networks. In: 2018 Fourteenth international conference on information processing (ICINPRO). IEEE, pp 1–5
101. Caldas Filho FL, Soares SCM, Oroski E, Oliveira Albuquerque R, Mata RZA, Mendonça FLL, Sousa Júnior RT (2023) Botnet detection and mitigation model for iot networks using federated learning. Sensors 23(14):6305
102. Hoang XD, Nguyen QC (2018) Botnet detection based on machine learning techniques using dns query data. Future Internet 10(5):43
103. Gelenbe E, Nakıp M (2023) Associated random neural networks for collective classification of nodes in botnet attacks. arXiv preprint arXiv:2303.13627
104. Mode GR, Calyam P, Hoque KA (2019) False data injection attacks in internet of things and deep learning enabled predictive analytics. arXiv preprint arXiv:1910.01716
105. Haq MA (2023) Dbotpm: a deep neural network-based botnet prediction model. Electronics 12(5):1159
106. Nakip M, Gelenbe E (2022) Botnet attack detection with incremental online learning. In: Gelenbe E, Jankovic M, Kehagias D, Marton A, Vilmos A (eds) Security in computer and information sciences. Springer, Cham, pp 51–60
107. Gelenbe E, Nakip M (2023) Real-time cyberattack detection with offline and online learning. In: 2023 IEEE 29th international symposium on local and metropolitan area networks (LANMAN). IEEE, pp 1–6
108. Velasco-Mata J, González-Castro V, Fidalgo E, Alegre E (2023) Real-time botnet detection on large network bandwidths using machine learning. Sci Rep 13(1):4282
109. Khetani V, Gandhi Y, Bhattacharya S, Ajani SN, Limkar S (2023) Cross-domain analysis of ml and dl: evaluating their impact in diverse domains. Int J Intell Syst Appl Eng 11(7s):253–262