

Evaluation of machine learning and deep learning methods for early detection of internet of things botnets

Ashraf Suleiman Mashaleh^{1,2}, Noor Farizah Ibrahim¹, Mohammad Alauthman³, Jamal Al-Karaki^{4,5}, Ammar Almomani^{2,6}, Shadi Atalla⁷, Amjad Gawanmeh⁷

¹School of Computer Sciences, Universiti Sains Malaysia, Pulau Pinang, Malaysia

²Computer Center, Al-Balqa' Applied University, As-Salt, Jordan

³Department of Information Security, Faculty of information technology, University of Petra, Amman, Jordan

⁴College of Interdisciplinary Studies, Zayed University, Abu Dhabi, United Arab Emirates

⁵Department of Computer Engineering, College of Engineering, Hashemite University, Zarqa, Jordan

⁶Research and Innovation Department, Skyline University College, Sharjah, United Arab Emirates

⁷College of Engineering and IT, University of Dubai, Dubai, United Arab Emirates

Article Info

Article history:

Received Jan 18, 2023

Revised Mar 19, 2024

Accepted Apr 2, 2024

Keywords:

Big data

Big data analytics

Healthcare

Internet of things

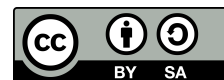
Personalised healthcare

Point-of-care devices

ABSTRACT

The internet of things (IoT) represents a rapidly expanding sector within computing, facilitating the interconnection of myriad smart devices autonomously. However, the complex interplay of IoT systems and their interdisciplinary nature has presented novel security concerns (e.g. privacy risks, device vulnerabilities, Botnets). In response, there has been a growing reliance on machine learning and deep learning methodologies to transition from conventional connectivity-centric IoT security paradigms to intelligence-driven security frameworks. This paper undertakes a comprehensive comparative analysis of recent advancements in the creation of IoT botnets. It introduces a novel taxonomy of attacks structured around the attack life-cycle, aiming to enhance the understanding and mitigation of IoT botnet threats. Furthermore, the paper surveys contemporary techniques employed for early-stage detection of IoT botnets, with a primary emphasis on machine learning and deep learning approaches. This elucidates the current landscape of the issue, existing mitigation strategies, and potential avenues for future research.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Amjad Gawanmeh

Department of Electrical Engineering, College of Engineering and IT, University of Dubai

Dubai, United Arab Emirates

Email: amjad.gawanmeh@ieee.org

1. INTRODUCTION

The internet of things (IoT) has reformed environmental sensing. It can increase life quality by collecting, quantifying, and understanding the environment. The term internet of things, abbreviated as IoT, is becoming a highly appealing buzzword among all individuals associated with practitioners and users of technology, including businesses and their clients. Technology plays a significant role in changing people's lives and significantly influences the workplace, where sensitive information is shared over the Internet. As a result, the attacker's curiosity can be turned into monetary gain. To achieve their objectives, attackers utilize numerous types of malware. Botnets are among the most dangerous forms of malware for unethical Internet activity. IoT device security measures like firewalls and access control mechanisms focus on data confidentiality and authenticity, network access control, security, and privacy policy innovation to build trust [1].

Botnet is robot and network. The Botnet began on internet relay chat (IRC), a text-based chat system that separates conversations into channels, where bots did not always mean evil things [2]. Malware-infested computers, known as bots, are machines infected without the owner's permission.

Attackers frequently alter the configuration of their botnets in order to evade detection, necessitating corresponding updates to detection methods by defenders. However, the detection of botnets typically necessitates substantial intelligence assistance involving the gathering and examining network data from various sources, particularly backbone networks. However, many businesses possess sufficient data on wide-area network traffic to accomplish this task [2], [3].

There are several methods in the literature to detect an IoT botnet. These methods can be grouped based on the botnet stage, such as scanning and spreading. We will analyze the advantages and disadvantages of different approaches, considering the wide range of each. Moreover, the review answers the following questions: i) what are the incentives behind developing IoT botnet attacks? and ii) how have IoT botnet attacks evolved?

To the best of our knowledge, this is the first paper to compare detection methodologies for IoT botnets based on the life-cycle phase of IoT botnets, not botnets in general. Our main contributions include compiling a comprehensive and comparative study of the consequences of IoT botnet attacks to quantify the scope of the problem. In addition, providing a comprehensive overview of recent research on IoT botnet detection and mitigation (2018–2022), including methodology and contributions. We also investigate the most recent datasets used in the IoT security field. This dataset includes both normal and unusual activity. Finally, evaluating emerging IoT botnet risks and new research directions, including future research directions and open research topics for future research.

The rest of the paper is organized as follows: first, we provide a background and overview of IoT and IoT botnets, covering their architecture, applications, and challenges. Then, we discussed the state-of-the-art intrusion detection approaches for the IoT environment. The next section highlights the importance of available datasets for IoT security solutions. A detailed discussion of our comparative study, the new taxonomy of attacks, and the proposed early detection techniques using machine learning and deep learning approaches is presented. Finally, we provide concluding remarks, summarize the contributions of our study, and suggest avenues for further research to improve IoT security.

2. BACKGROUND AND OVERVIEW OF IOT AND IOT BOTNET

The architecture of the IoT comprises three layers: perception, network, and application. Sensors gather data in the perception layer, while gateways facilitate data transmission in the network layer. Finally, in the application layer, user interaction takes place. IoT botnets are remotely controlled networks categorized into centralized, decentralized, peer-to-peer, and hybrid models. This section discusses IoT architecture, IoT botnet architecture, IoT botnet life cycle phases, IoT botnet detection techniques, and features to detect and define IoT botnet phases. In conclusion, we will address every aspect of IoT botnet identification and compare our findings with those of other studies.

2.1. The architecture of IoT Botnet

Traditional botnets have the same structure as IoT botnets, but IoT botnets have a slightly different structure. There are three types of botnets: centralized, peer-to-peer, and hybrid. Centralized botnets are the most common type [4]–[7].

2.1.1. Centralized Botnets

The botmaster oversees and monitors all bots through a centralized server, which minimizes latency. This means all bots receive and report information to a command-and-control server (the C&C server). The Botmaster may control one or multiple central servers within this architectural framework. The server utilizes the HTTP and IRC protocols for communication. A drawback of the botmaster server is its vulnerability as a single point of failure. The Mirai family malware is a prominent instance of centralized IoT botnets.

2.1.2. Decentralized Botnets

Peer-to-peer (P2P) botnets are also a term for it. Every bot connects to at least one other as a client and a server. The commands will only reach each bot if all bots are linked. Because of the varied communication between peers, it is difficult to coordinate between bots in this architecture, but it is also more complicated to

detect. The communication protocol used by this kind of IoT botnet is peer-to-peer. Hajime is one of the most well-known decentralized (P2P) IoT botnets.

2.1.3. Hybrid Botnets

A hybrid botnet comprises two types of bots: servers and clients, with some bots serving as both servers and clients, while others solely function as clients. This design integrates elements from both centralized and decentralized architectures. There is a considerable level of latency in message transmission.

2.2. The IoT Botnet life cycle phases

While the IoT Botnet life cycle Phases are usually divide them into several phases, it is more common to be divided into three phases. According to many studies [4] it is divided into three phases: the scanning phase, the propagation phase, and the attack phase. Illustrated in Figure 1, which shows the types of attacks in every phase.

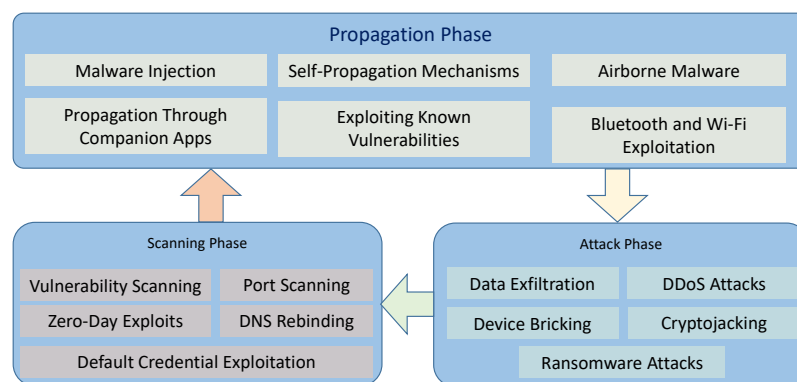


Figure 1. IoT life cycle integrated attacks

2.2.1. Scanning phase

Scanning activity detection is the first stage of the detection process, as bots scan considerably quicker than C&C servers, which causes scanning to be discovered rapidly [8]. A bot or malicious software conducts scanning and reconnaissance activities to identify a device susceptible to exploitation. The Botmaster seeks out vulnerable IoT devices for potential exploitation. After identifying a target, the malware infects it through brute force or exploiting vulnerabilities. The compromised device has transformed into a bot communicating with the master robot. The Mirai malware family utilizes fingerprint packets to scan for pseudo-random IPv4 addresses to identify IoT devices that may be vulnerable through the Telnet service on port 23 or 2323. The bot targets new victims by exploiting weak passwords through brute-force attacks or capitalizing on well-known vulnerabilities in IoT devices [9], [10].

2.2.2. Propagation phase

The bot is installed and activated through the device's architecture. The bot terminates the service process to eliminate any existing malware and restricts access to its ports [4]. The malicious code rapidly recruits and spreads additional bots to enlarge the IoT botnet. During this stage, the bots remain idle as they await directives from their botmaster.

2.2.3. Attack phase

Malicious activities are perpetrated, including minimum data loss occurs (DDoS) attacks, cryptocurrency mining, and spam. The attacker begins the attack by sending minimum data loss occurs commands to the distributed bots through the C&C server, triggering the attack [4]. Consequently, the bots initiate the attack promptly upon receiving identical commands. Communication and control are established throughout all stages of the Botnet's design. Furthermore, this is the point at which the bot and the controller host communicate and exchange commands.

3. INTRUSION DETECTION SYSTEM FOR THE IOT

DDoS attacks are one of the most dangerous threats posed by botnets nowadays. The DDoS has significant destructive potential due to the enormous number of participants in a Botnet network [11]. The botmaster utilizes the Botnet network to bring the victim's control system to a screeching halt by flooding it with requests from the Botnet members. Furthermore, some large-scale botnets can risk internet service providers (ISPs). IoT botnet-driven DDoS attacks and their corresponding protections against them were examined in [12]. They explained why DDoS attacks on IoT devices are so common and showed the most common strategies for defending against DDoS attacks.

An intrusion detection system (IDS) detects attempts to illegally access a computer system or disrupt and modify it over a network like the Internet. These attacks can break copyright, use malware, or disgruntle company staff. Due to the high cost of cyberattacks and the growing number of internet-connected devices and the IoT, identifying botnet networks of compromised devices is crucial to defeating attackers [12]. Early botnet detection is difficult owing to constant mutation, complexity, and enormous data volume, especially from sensor networks and IoT.

IDS can be classified based on sensor type, location, and alert generation methods. In many simple intrusion detection systems, all these devices are combined. Cybercrime has shown how easy it is for cyber threats to spread worldwide, as even a small breach can hurt a company's most essential services or infrastructure. Many cybercriminals steal information and make illegal money around the world; hence, classifications for these types of attacks are necessary in the literature [13].

3.1. Intrusion detection using machine learning

Due to its efficacy, machine learning is crucial to AI. It is used in data mining, pattern recognition, and medicine. Machine learning algorithms detect hidden patterns and rules, enabling prediction and categorization models [2]. Machine learning develops data-learning systems. The algorithms are supervised, unsupervised, or reinforcement learning. The model can identify unlabeled data after supervised learning techniques trained on labeled data. The categorization process is "supervised" because it can repeat a manager's help with data sorting in the future. Unsupervised learning algorithms don't need labeled datasets for training. Unsupervised learning divides unlabeled datasets into subgroups using specified parameters. An agent learns through trial and error in RL. Reinforcement learning agents adjust to maximize long-term rewards.

According to Nguyen *et al.* [14] which states that IoT botnet attacks can be identified by monitoring temporal aberrations in IoT devices. Researchers assess a device's packet count and use the isolation forest technique to find anomalies. Examining device evolution can distinguish normal from abnormal behavior. Isolation forest, a model-free anomaly detection approach with linear time complexity and low memory needs, is used. They also detect anomalies shallowly. The authors also advise feeding an anomaly detection system a IoT device behavior feature set. This shallow anomaly detection method. uses multiscale ordinal template alterations.

Nomm and Bahsi [15] proposed an anomaly detection technique based on unsupervised learning and feature selection, focusing on feature selection. Before the data was supplied to a classifier, this method explored different feature selection strategies to reduce the dimensionality of the data. One hundred fifteen unique numerical features produced by 9 IoT devices are included in an actual Mirai botnet dataset used in the study. The characteristics describe many network attributes, including source and destination IP addresses, jitter, and socket data. The authors employed entropy, variance, and Hopkins statistics to minimize the data's dimensionality. Then, three classifiers were used: local outlier factor (LOF), support vector machine (SVM), and an isolation forest (IF). The findings revealed that combining feature reduction via entropy with the IF classifier made it possible to reach 90% accuracy results with only five features. This technique detects anomalies at the network level but ignores irregularities in the content of packets sent by IoT devices.

Regan *et al.* [16] attempted to address two of the most prevalent issues in IoT systems: security and privacy. The researchers employed a federated technique based on a deep autoencoder to analyze on-device decentralized data and identify botnet attacks at the edge layer. To maintain privacy, it is imperative to prevent the transfer or relocation of data from the device beyond the network edge. In contrast, machine learning algorithms are extended to the edge layer, where the data originates. This means that the data can be kept safe. They reported that their approach could detect anomalies in IoT botnet datasets with a 98% accuracy rate. Both inbound and outbound Botnet cyberattacks can be prevented using a two-fold machine learning strategy presented by the researchers in [17]. The initial goal was to build a cutting-edge deep learning model,

ResNet-18, for identifying (pre-attack stage) scanning activities to safeguard the IoT network against botnet attacks. An added ResNet-18 model for identifying DDoS attacks carried out by intruders following breaches of weakly secured IoT devices was trained in the second stage of the training process. Nmap, a network traffic generator, generated 33 types of scanning and 60 types of DDoS attack traffic. The authors asserted that the proposed approach achieves a level of precision of 98.89%. Table 1 provides a summary of the various studies that have been conducted recently on DDoS using machine learning, the used dataset, attack types, and the used techniques.

Table 1. Machine learning-based IoT intrusion detection research

Paper	Used Dataset	Attack Stage and Type	Used Technique
[18]	A real IoT data traffic	IoT botnet attacks	An Adaptive online ensemble learning
[19]	BoT-IoT	DDoS attack	Combined machine learning, feature engineering, and SMOTE resampling with K-nearest neighbors.
[20]	N-BaIoT	poisoning attacks	Federated learning
[21]	IoT POT, VirusShare	DDoS attack	combined deep and machine learning with PSI rooted sub-graph features CNN, RNN
[14]	Own dataset	DDoS attack	collaborative machine learning model
[22]	Own dataset	DDoS attack	Supervised classification algorithms like naive Bayes, decision trees, and support vector machines
[23]	public botnet dataset (N-BaIoT)	IoT botnet attacks	Fisher score based feature selection and GXGBoost genetic-based extreme gradient boosting model
[24]	NSL-KDD dataset, UNSW-NB15 dataset, and the BoT-IoT	Denial-of-service, malware, and botnet attacks	SVM and RF models
[25]	UNSW-NB15	DDoS attack, malware	ensemble learning and feature selection
[26]	The TON_IoT	DDoS attack, malware	SVM model
[27]	UNSW-NB15	DDoS attack, malware	SVM and Boruta algorithm
[28]	NSL-KDD, the UNSW-NB15, and the BoT-IoT	DDoS attack, malware	SVM and RF models

3.2. DDoS attack studies using deep learning

It is necessary to know the distinction between deep learning and machine learning. Machine learning is well-suited to small datasets and yields good results [29]; deep learning techniques, on the other hand, have recently attracted considerable attention due to their capacity to deal with big datasets. Many research topics, including image, sound, speech identification, signal processing, natural language processing, and IDS, are investigated using deep learning. Also, one of the essential characteristics of deep learning is automated feature development to determine which features are most important in an attack. Compression also makes it possible for deep learning to be used in networks with limited resources, like IoT networks, which makes it possible to use deep learning even in networks with limited resources. As an example, [30], [31], and [32] used deep learning to find DDoS attacks and activities. Some authors are also researching how to make attacks less harmful.

Akgun *et al.* [30] suggested a method that uses a deep learning model and preprocessing stages to identify DDoS attacks. The study investigates the real-time performance of models utilizing deep neural networks, convolutional neural networks, and long short-term memory for detecting purposes. The authors evaluated the suggested model using the CIC-DDoS2019 dataset. The preprocessing of the CIC-DDoS2019 dataset involved feature deletion, random subset selection, feature selection, duplication removal, and normalization. Using a random partitioning technique, researchers partitioned the large CIC-DDoS2019 dataset into smaller sub-datasets, each including a benign class. The authors employed preprocessing techniques such as feature removal and selection. Out of the initial 88 features, 40 crucial ones were selected.

Defense methods applied at the source alone are insufficient for present DDoS solutions because they lack visibility into ongoing attacks. In study Myneni *et al.* [31] SmartDefense was created for edge computing to identify and address DDoS attacks at their source. SmartDefense reduces DDoS attacks by minimizing bandwidth consumption and eliminating duplicate traffic from residential edge networks to the ISP edge network. SmartDefense demonstrates how internet service providers can identify botnet devices within their customers' networks by transmitting data from intelligent edge devices to a botnet detection system located at the network edge of the provider. The researchers utilized two detection engines: fast neural network (FNN) and the other based on incoming traffic forecasted by the FNN, which underwent training on a labeled dataset (CICDDoS2019) containing various DDoS attack types. An LSTM-based neural network processes the other engine's traffic from the evaluating engine. After being trained on a labeled dataset of many different DDoS attacks, the LSTM module can predict how likely future attacks will be. These results show that two stage edge computing is a good way for ISPs to avoid wasting bandwidth and time because of harmful traffic

at the provider edge.

A novel technique entitled detecting attack using live capture neural network (DALCNN) is proposed by [32] for detecting DDoS attacks in IoT based on the notion of recurrent neural networks and creating a software-defined network (SDN) utilizing the OpenDayLight platform. The recurrent neural network (RNN) technique was used in the study to handle this problem and prevent losses for the proposed solution. The RNN analyzes past measurements and current input at each input stage. These model training methods can guarantee that minimum data loss occurs and that all data information is kept. Compared to other RNN approaches, the conventional RNN approach is simple and requires less training time. Additionally, a three-tier architecture is proposed to categorize DDoS attacks. The method classifies the types of attacks that use a novel activation function and deep learning concepts for machines. Failure to identify large-scale attacks like DDoS makes networks susceptible and endangers human lives if vital, lifesaving medical and industrial equipment fails. In addition, while proposing an IDS solution, researchers often select a single model and a single dataset [33]. One disadvantage of using a single dataset is that it creates biased results by focusing solely on limited network traffic patterns and attack classes. Also, some datasets, such as NSL-KDD and KDD CUP 99, are not IoT. Therefore, using several individuals and hybrid deep learning classifiers, the technique in [33] assesses many datasets (ancient, recent, non-IoT, and IoT-specific). The authors [33] intended to provide a standard against which to compare various classification models. The data was split into two sets of DL classifiers for analysis. Initially, individual classifiers were executed on datasets to gather crucial data such as training time, parameters, model settings, and performance indicators. Various hybrid classifiers were used to collect the data. Two experiments were conducted using the NSL-KDD and UNSW NB15 datasets. Securing the IoT network layer is crucial for technical reasons. In the same way, [34] suggested using a DL-based model to find the IoT routing protocol. The DL model was trained and evaluated using a dataset through simulations using Cooja IoT simulator. The simulations included up to 1,000 nodes spread across 16 networks to detect three types of assaults: decreased rank, hello flood, and version number attacks. The deep neural network efficiently identified all three attacks effortlessly. The dataset created by the authors did not provide the quantity of normal and aberrant samples. However, evaluation criteria like accuracy, recall, and f-measure may not accurately reflect a model's performance when working with imbalanced datasets.

Both inbound and outbound Botnet cyberattacks can be prevented using a two-fold machine-learning strategy presented by the researchers in [17]. The main goal was to create an advanced deep learning model, ResNet-18, to detect scanning activity in the pre-attack stage and safeguard the IoT network from botnet attacks. During the second training round, a ResNet-18 model was developed to identify DDoS attacks caused by intruders exploiting vulnerabilities in insecure IoT devices. Nmap, a tool for generating network traffic, offers 33 scanning techniques and 60 DDoS attacks. Hussain *et al.* [17] asserted that the proposed approach achieves a level of precision of 98.89%. Reinforcement learning (RL) is considered one of the best options for safeguarding IoT against adversarial learning environments that integrate the environment's actions into the learning process at the same time. Therefore, Caminero *et al.* [35] suggests a basic GAN-based intrusion detection approach. In the paper, the authors use a classifier to predict the samples correctly, and then another adversarial configuration, a normal GAN model, makes the prediction more difficult. RL provides IoT security for adversarial learning environments where many heterogeneous IoT devices create a large volume of bandwidth data or a full data stream.

Roopak *et al.* [36] suggested and assessed four deep-learning methods for identifying DDoS attacks in IoT networks. They proceeded to compare these methods with traditional machine learning algorithms. Each model has an input layer with 82 units, representing the flow-level features in CIC2017. The output layer calculates the likelihood of a flow being linked to a DDoS assault. The researchers discovered that the hybrid LSTM-CNN method outperformed previous deep learning and machine learning techniques, obtaining a 97.16% accuracy rate. Deep learning models surpass machine learning models. Modifications were implemented in the dataset to rectify the imbalance in the data distribution. Additionally, a restricted set of criteria, such as accuracy, precision, and recall, were used to assess the models. Fuzzy logic method was also discussed in [37].

Due to the IoT's restricted hardware resources, researchers must carefully choose their data analysis tools and algorithms. As in Meidan *et al.* [38] used one-class classification algorithms to detect specific botnet threats. They studied the detection of attacks in the IoT network and proposed a new technique to overcome the problem of attacks initiated by IoT devices. Afterward, an autoencoder was used to identify anomalies in IoT traffic. In their study, IoT-based Bashlite and Mirai botnet attacks were employed as the data set for evaluating

their proposed approach. However, the utilized data sets are also on several corrupted IoT devices. The research showed that the proposed method could be used to find cyberattacks on IoT network devices. Table 2 presents an overview of the various studies that have been undertaken recently on DDoS using deep learning, as well as the approach that was applied and the limitations of those studies.

Table 2. Deep learning-based IoT intrusion detection research

Referece	Used Dataset	Attack Stage and Type	Used Technique
[34]	Custom simulated IoT Net	Attack simulation, DDoS, routing attacks	Deep neural network
[35]	NSL-KDD	Attack simulation, DoS, Probe, R2L, U2R	Reinforcement learning
[36]	CICIDS2017	Attack simulation, DDoS	Deep neural network
[38]	Custom IoT botnet	Real botnet attacks	Deep autoencoder
[39]	ToN-IoT	Attack simulation, DoS, Recon, Infiltration, Escalation	RNN-GRU hybrid deep learning
[40]	CICIDS2017	Attack simulation, DoS, DDoS, Heartbleed, Web attacks, Botnet attacks, Brute force, XSS, SQL injection	Deep neural network
[41]	CICIDS2017, N-BaIoT, CI-CIoT2023	Attack simulation, DoS, DDoS, Brute force, XSS, SQL injection, Infiltration, Botnet attacks	Attention-based deep learning
[42]	NSL-KDD	Attack simulation, DoS, Probe, R2L, U2R	Knowledge transfer deep learning
[43]	CIDDS-001, UNSW-NB15, NSL-KDD	Attack simulation, DoS	Deep learning ensemble

4. AVAILABLE DATASETS FOR IOT

Obtaining a valuable dataset of network traffic for ML purposes can be difficult. We need a reliable, up-to-date dataset that includes normal and unusual activities to determine how well an IDS works. The following briefly explains the most popular datasets used to evaluate IDS.

4.1. MQTTset dataset

The MQTTset dataset was created by [44]. It was developed to train ML-based IDSs in an IoT scenario. The MQTTset's specific goal is to focus on the MQTT protocol, and the hazards associated with IoT nodes. The authors used eight sensors and an MQTT broker to generate the dataset in their lab. The collecting period corresponds to a one-week time window, resulting in more than 11 million network packets with a data size of more than 1 GB. The MQTTset contains genuine and malicious traffic. The dataset has 33 features, including 3 TCP and 30 MQTT. Attacks against MQTT brokers created malicious traffic. Slow DoS against IoT environments (SlowITe), MQTTSa malformed data attack, and MQTTSa brute force authentication

The authors [1] used machine learning to validate the data. They contrasted balanced and imbalanced data sets. An unbalanced data set had good accuracy due to many innocuous records. IoT Intrusion Detection models extensively utilize MQTT protocol communication datasets. MQTT dataset features are unidirectional, bidirectional, and packet-based. The dataset's features are extrapolated from raw communication data to get MQTT protocol communication characteristics. A smart home with 10 IoT sensors creates the MQTTset dataset testbed. Five attack categories make up MQTTset. Denial of service attacks make up most of the attacks in the dataset.

4.2. MQTT-IoT-IDS2020 dataset

The MQTT-IoT-IDS2020 dataset was created by [45]. The dataset comprehensively examines the message queuing telemetry transport (MQTT) network architecture. The system is vulnerable to four specific types of attacks: aggressive scanning, user datagram protocol scanning, MQTT brute force, and SSH brute force. The network comprises 12 MQTT sensors, a broker, a video feed replicating device, and an intruder. Under normal circumstances, the twelve sensors send occasional messages. The dataset includes scenarios for testing practical devices and typical MQTT attacks. The dataset MQTT-IoT-IDS2020 contains four attack categories. The dataset includes an MQTT brute force attack and traditional networking scanning attacks.

4.3. N-BaIoT dataset

As part of their research on IDS for online networks, the authors [46] made a dataset evaluating IDS for IoT networks. The researchers generated and gathered network traffic from two distinct networks. The first network consisted of an IP camera video surveillance system, on which they conducted eight distinct attacks. These attacks targeted the availability and integrity of the video uplinks. The second network was an IoT network comprising three PCs and nine IoT devices. Among these devices, one was infected with the Mirai botnet malware.

Their published papers [47] fully explain the attacks and network topologies. The authors gathered a series of feature vectors for the nine attacks. Various attack types include OS scan, fuzzing, video injection, ARP MiTM, active wiretap, SSDP flood, SYN DoS, SSL renegotiation, and Mirai.

4.4. MedBioT dataset

In 2020, the Tallinn University of Technology gave the MedBioT dataset [48]. The dataset was generated within an IoT setting comprising a mix of real and simulated IoT devices, amounting to 83. BashLite, Mirai, and Torii are prominent malware that were utilized. Using the original MedBioT pcap files with the Argus program generates the network flow. The malicious traffic of BashLite and Mirai involves disseminating malware commands and enabling communication between servers and bots. Torii's harmful traffic is only linked to the initial infection on the device. Upon activation, the malware collects legitimate network data. There are a total of 23,340,359 distinct network packets in the collection.

4.5. UNSW-NB15 dataset

UNSW Canberra researchers created a dataset for IDS evaluation [49]. The researchers utilized the IXIA perfectStorm program at the Australian Center for cyber security (ACCS) to generate malicious and harmless network traffic. The task was completed in two days, with sessions of 16 and 15 hours each. They compiled a 100 GB collection with several new features from pcap files. NB15 was intended to be a more advanced version of the KDD99 dataset we previously talked about. There is one positive goal and nine negative ones. The malicious types include denial of service (DoS), exploits, analysis, fuzzers, worms, reconnaissance, generic, shell code, and backdoors. The dataset was created by simulating attacks in a fictional environment. We have analyzed the abovementioned datasets and summarized their essential properties in a Table 3.

Table 3. Datasets comparison

Dataset	Year	Features	Testbed	IoT devices	Threats
N-BaIoT	2018	23	2 Layers	9 types	10-attacks
MQTTset	2020	33	2 layers	8 types	5 attacks
X-IIoTID	2021	59	3 layers	Industrial & IoT devices	18 attacks
MedBioT	2020	100	3 layers	83 types	3 attacks
UNSW-NB15	2022	49	3 virtual servers	N/A	9 attacks
MQTT-IoT-IDS2020	2021	44	12 MQTT sensors	2 types	3 attacks

5. DISCUSSION

Deep learning and machine learning are two different methods to use artificial intelligence to solve problems. It is important to know the difference between the two. Most of the time, deep learning is used when the dataset is large because it helps people learn more than traditional machine learning algorithms. On the other hand, machine learning is appropriate for the small dataset, giving good results. Deep learning techniques have recently been getting attention due to their ability to deal with massive datasets. Deep learning is extensively studied in various research domains, including image and sound recognition, speech recognition, signal processing, natural language processing, and IDS [50]. Figure 2 shows the summary of available methods for botnet detection in IoT.

Restrictive Boltzmann machines, deep belief networks, auto-encoders, and recurrent neural networks are popular IDS methods. We analyzed the dataset using the restricted Boltzmann technique to reveal correlations among the features. It is utilized for reconstructing the inputs and selecting the optimal combination of these attributes. Also, DBN is a deep neural network class. It is an algorithm comprising several RBMs (restricted Boltzmann machines) connected (the first outputs of the RBM are input to the second RBM, and so on), so it's appropriate for real-life scenarios and technologies.

However, these models are trying to discover new inputs; accordingly, helping the system classify the dataset into different categories is the main objective of a deep belief network to identify the features in an unlabeled dataset and extract the essential features. The feature will be cons these technologies have not answered. The entropy score is sufficiently large, and its correlation scores are small enough. This would mean that the feature does not contain any redundant data shared with other features and is as irrelevant as possible to each other. For example, in studies [50]–[52] utilizes deep learning to detect malicious activities. Also, the essential thing about deep learning is that one does not have to develop the features by hand to know the most critical attacks. This means one can use deep learning even in networks with limited resources, like IoT

networks. Other unsupervised learning methods were discussed in [53]–[57], rule-based methods [58], [59], and graph-based methods [60], [61].

Users must monitor and secure network connections to prevent attackers from accessing critical data. Although we have addressed IoT solutions incorporating machine learning and deep learning, this part highlights difficulties these technologies have not addressed. Choosing the proper machine learning or deep learning method for IoT security is challenging. Machine learning or deep learning techniques require the proper dataset and algorithm to build an IoT security solution. IoT devices create a lot of redundant or unnecessary data. This creates issues for the researchers, who must cope with outliers and unclear data. In this study, many IoT device attacks were explored and covered. Many IoT solutions for these attacks, including machine and deep learning, were also examined. There are still many problems with security in IoT, as IoT devices do not have many resources. Machine learning and deep learning bridge a high level of security with low computational complexity.

As previously indicated, there are three stages to the life cycle of an IoT botnet: scanning, propagation, and attack. The bots, the C&C, and the bots communicate now. After the botnets had launched their attacks, it is evident that most research did not develop strategies to identify IoT botnets. This means that if an attacker begins to scan or spread their network, they may be able to locate botnets quickly. As a result, researchers need to understand more about detecting IoT botnets before attacks are launched against those networks.

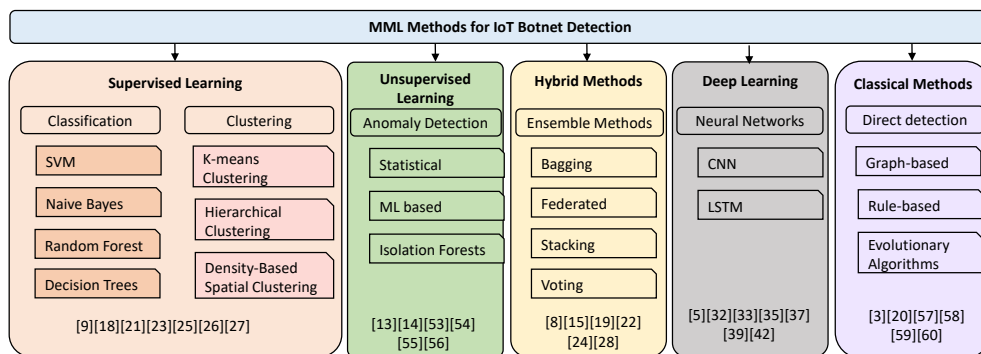


Figure 2. Taxonomy of Botnet detecting methods in IoT

Most of the work done to find IoT botnets is focused on developing ways to find DoS/DDoS, scanning, or IoT malware as attacks by IoT botnets, mostly Mirai, rather than finding ways to find the other attacks, in particular in big data context within complex operations, such as CPS [62]. In addition, incorporating spam detection methods into IoT botnets may raise more complex issues [63]. A current attack trend that the studies have not considered is the unauthorized use of IoT device resources for computing operations. This was due to a lack of datasets, difficulty executing experiments connected with various suspicious activities, and a lack of simulations.

On the other hand, the datasets used do not have enough types of suspicious bot network activities. As a result, the datasets did not accurately represent IoT ecosystems or were not obtained from IoT devices. They were taken from IoT devices and can only be used for certain things or places, like the home system. As a result, many proposed solutions may run into problems when used in other ecosystems or devices. More IoT botnet datasets are needed, and researchers should investigate building more datasets and finding ways to extract real datasets [64].

6. CONCLUSION

IoT devices are popular because they convert various application domains into Internet hosts. Also, the IoT needs stronger security because attacks are expensive, and more and more devices are connecting to the Internet. IoT security is ensured using machine- and deep learning-based intrusion detection systems. This study surveys ML and DL-based IDS approaches for IoT networks and devices. We have addressed IoT architecture, protocols, vulnerabilities, and protocol-level attacks. In addition, this article discusses the numerous datasets available for use in research about the security of the IoT. Numerous studies and research

initiatives have focused on the IoT. There are still a lot of open research questions about applying machine learning and deep learning to IoT security. We strongly recommend that research in the future focus right away on finding botnets early to get a leg up on attackers. Still, botnets are hard to find early on because they are constantly changing, very complicated, and create a lot of data.

Future directions in this domain include refining the accuracy and efficiency of both machine and deep learning-based intrusion detection methods by exploring each algorithm's unique features. In addition, new methods must adapt to the dynamic nature of evolving botnets and, hence, develop new methods that can effectively identify and mitigate emerging threats and possibly apply them in a real-time context.

REFERENCES





- [1] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015, doi: 10.1016/j.comnet.2014.11.008.
- [2] M. M. Alauthman, "An efficient approach to online bot detection based on a reinforcement learning technique mohammad mansour alauthman a thesis submitted in partial fulfilment of the requirements of the University of Northumbria at Newcastle for the degree of Doctor of Phi," *Northumbria University Newcastle*, 2016.
- [3] T. Khdour, R. Freehat, and A.M. Manasrah, "Botnet detection using artificial intelligence," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, pp. 1–18, 2023.
- [4] M. Wazzan, D. Algazzawi, O. Bamasqa, A. Albeshri, and L. Cheng, "Internet of things Botnet detection approaches: Analysis and recommendations for future research," *Applied Sciences (Switzerland)*, vol. 11, no. 12, 2021, doi: 10.3390/app11125713.
- [5] H. Alzahrani, M. Abulkhair, and E. Alkayal, "A multi-class neural network model for rapid detection of IoT Botnet attacks," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 7, pp. 688–696, 2020, doi: 10.14569/IJACSA.2020.0110783.
- [6] R. Abrantes, P. Mestre, and A. Cunha, "Systematic literature review of social media bots detection systems," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, pp. 1088–1101, 2023.
- [7] B. Dupont and J. Luthaus, "Countering distrust in illicit online networks: the dispute resolution strategies of cybercriminals," *Social Science Computer Review*, vol. 40, no. 4, pp. 892–913, 2022, doi: 10.1177/0894439321994623.
- [8] A. Kumar, M. Shridhar, S. Swaminathan, and T. J. Lim, "Machine learning-based early detection of IoT botnets using network-edge traffic," *Computers and Security*, vol. 117, Jun. 2022, doi: 10.1016/j.cose.2022.102693.
- [9] A. Arshad *et al.*, "A novel ensemble method for enhancing internet of things device security against botnet attacks," *Decision Analytics Journal*, vol. 8, Sep. 2023, doi: 10.1016/j.dajour.2023.100307.
- [10] S. Razaulla *et al.*, "The age of ransomware: a survey on the evolution, taxonomy, and research directions," *IEEE Access*, vol. 11, pp. 40698–40723, 2023, doi: 10.1109/ACCESS.2023.3268535.
- [11] T. J. Holt, "Examining the forces shaping cybercrime markets online," *Social Science Computer Review*, vol. 31, no. 2, pp. 165–177, 2013, doi: 10.1177/0894439312452998.
- [12] M. M. Salim, S. Rathore, and J. H. Park, "Distributed denial of service attacks and its defenses in IoT: A survey," *Journal of Supercomputing*, vol. 76, no. 7, pp. 5320–5363, 2020, doi: 10.1007/s11227-019-02945-z.
- [13] B. Bojarajulu, S. Tanwar, and T. P. Singh, "Intelligent IoT-BOTNET attack detection model with optimized hybrid classification model," *Computers Security*, vol. 126, Mar. 2023, doi: 10.1016/j.cose.2022.103064.
- [14] G. L. Nguyen, B. Dumba, Q.-D. Ngo, H.-V. Le, and T. N. Nguyen, "A collaborative approach to early detection of IoT botnet," *Computers Electrical Engineering*, vol. 97, Jan. 2022, doi: 10.1016/j.compeleceng.2021.107525.
- [15] S. Nomm and H. Bahsi, "Unsupervised anomaly based botnet detection in IoT networks," in *Proceedings - 17th IEEE International Conference on Machine Learning and Applications*, pp. 1048–1053, 2018, doi: 10.1109/ICMLA.2018.00171.
- [16] C. Regan, M. Nasajpour, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and K.-K. R. Choo, "Federated IoT attack detection using decentralized edge data," *Machine Learning with Applications*, vol. 8, Jun. 2022, doi: 10.1016/j.mlwa.2022.100263.
- [17] F. Hussain *et al.*, "A two-fold machine learning approach to prevent and detect IoT botnet attacks," *IEEE Access*, vol. 9, pp. 163412–163430, 2021, doi: 10.1109/ACCESS.2021.3131014.
- [18] Z. Shao, S. Yuan, and Y. Wang, "Adaptive online learning for IoT botnet detection," *Information Sciences*, vol. 574, pp. 84–95, Oct. 2021, doi: 10.1016/j.ins.2021.05.076.
- [19] S. Pokhrel, R. Abbas, and B. Aryal, "IoT security: Botnet detection in IoT using machine learning," *arXiv:2104.02231*, Apr. 2021.
- [20] V. Rey, P. M. Sánchez Sánchez, A. Huertas Celdrán, and G. Bovet, "Federated learning for malware detection in IoT devices," *Computer Networks*, vol. 204, Feb. 2022, doi: 10.1016/j.comnet.2021.108693.
- [21] H.-T. Nguyen, Q.-D. Ngo, D.-H. Nguyen, and V.-H. Le, "PSI-rooted subgraph: A novel feature for IoT botnet detection using classifier algorithms," *ICT Express*, vol. 6, no. 2, pp. 128–138, Jun. 2020, doi: 10.1016/j.ict.2019.12.001.
- [22] A. Kumar and T. J. Lim, "EDIMA: early detection of IoT malware network activity using machine learning techniques," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, Apr. 2019, pp. 289–294, doi: 10.1109/WF-IoT.2019.8767194.
- [23] M. Alqahtani, H. Mathkour, and M. M. Ben Ismail, "IoT Botnet attack detection based on optimized extreme gradient boosting and feature selection," *Sensors*, vol. 20, no. 21, Nov. 2020, doi: 10.3390/s20216336.
- [24] A. Sharma, N. G. Nguyen, S. Natani, and S. Vyas, "Machine learning-based iot intrusion detection: a comprehensive review," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 1, pp. 1–22, 2023.
- [25] S. Saha, A. T. Priyoti, A. Sharma, and A. Haque, "Towards an optimized ensemble feature selection for DDoS detection using both supervised and unsupervised method," *Sensors*, vol. 22, no. 23, Nov. 2022, doi: 10.3390/s22239144.
- [26] M. Arif, M. Imran, and M. Bilal, "IoTprotect: A machine-learning based iot intrusion detection system," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 3, pp. 1–12, 2023.
- [27] S. More, M. Idrissi, H. Mahmoud, and A. T. Asyhari, "Enhanced intrusion detection systems performance with UNSW-NB15 data analysis," *Algorithms*, vol. 17, no. 2, 2024.

- [28] A. A. Alahmadi *et al.*, “DDoS attack detection in IoT-based networks using machine learning models: a survey and research directions,” *Electronics*, vol. 12, no. 14, Jul. 2023, doi: 10.3390/electronics12143103.
- [29] Y. Zhang and C. Ling, “A strategy to apply machine learning to small datasets in materials science,” *npj Computational Materials*, vol. 4, no. 1, 2018, doi: 10.1038/s41524-018-0081-z.
- [30] D. Akgun, S. Hizal, and U. Cavusoglu, “A new DDoS attacks intrusion detection model based on deep learning for cybersecurity,” *Computers and Security*, vol. 118, Jul. 2022, doi: 10.1016/j.cose.2022.102748.
- [31] S. Myneni, A. Chowdhary, D. Huang, and A. Alshamrani, “SmartDefense: a distributed deep defense against DDoS attacks with edge computing,” *Computer Networks*, vol. 209, 2022, doi: 10.1016/j.comnet.2022.108874.
- [32] O. Yousuf and R. N. Mir, “DDoS attack detection in internet of things using recurrent neural network,” *Computers and Electrical Engineering*, vol. 101, Jul. 2022, doi: 10.1016/j.compeleceng.2022.108034.
- [33] R. Ahmad, I. Alsmadi, W. Alhamdani, and L. Tawalbeh, “A comprehensive deep learning benchmark for IoT IDS,” *Computers and Security*, vol. 114, 2022, doi: 10.1016/j.cose.2021.102588.
- [34] F. Y. Yavuz, “Deep learning in cyber security for internet of things,” M.S. thesis, *Fen Bilimleri Enstitüsü*, 2018.
- [35] G. Caminero, M. Lopez-Martin, and B. Carro, “Adversarial environment reinforcement learning algorithm for intrusion detection,” *Computer Networks*, vol. 159, pp. 96–109, Aug. 2019, doi: 10.1016/j.comnet.2019.05.013.
- [36] M. Roopak, G. Yun Tian, and J. Chambers, “Deep learning models for cyber security in IoT networks,” in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2019, pp. 452–457, doi: 10.1109/CCWC.2019.8666588.
- [37] M. Alauthaman, M. Alsaleh, A. Al-Olayan, and M. Al-Qahtani, “A fuzzy logic based feature engineering approach for botnet detection using ann,” *Journal of King Saud University - Computer and Information Sciences*, vol. 33, pp. 1513–1522, 2021.
- [38] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, “N-baiot—network-based detection of IoT botnet attacks using deep autoencoders,” *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018.
- [39] N. W. Khan *et al.*, “A hybrid deep learning-based intrusion detection system for IoT networks,” *Mathematical Biosciences and Engineering*, vol. 20, no. 8, pp. 13491–13520, 2023, doi: 10.3934/mbe.2023602.
- [40] M. Bilal, M. Arif, and M. Imran, “Eidm: deep learning model for IoT intrusion detection systems,” *Security and Privacy*, vol. 6, no. 2, pp. 1–19, 2023.
- [41] Z. Wang, H. Chen, S. Yang, X. Luo, D. Li, and J. Wang, “A lightweight intrusion detection method for IoT based on deep learning and dynamic quantization,” *PeerJ Computer Science*, vol. 9, Sep. 2023, doi: 10.7717/peerj-cs.1569.
- [42] S. Salmi and L. Oughdir, “Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network,” *Journal of Big Data*, vol. 10, no. 1, Feb. 2023, doi: 10.1186/s40537-023-00692-w.
- [43] P. Verma *et al.*, “A novel intrusion detection approach using machine learning ensemble for iot environments,” *Applied Sciences (Switzerland)*, vol. 11, no. 21, 2021, doi: 10.3390/app112110268.
- [44] I. Vaccari, G. Chiola, M. Aiello, M. Mongelli, and E. Cambiaso, “MQTTset, a new dataset for machine learning techniques on MQTT,” *Sensors*, vol. 20, no. 22, Nov. 2020, doi: 10.3390/s20226578.
- [45] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, and X. Bellekens, “Machine learning based IoT intrusion detection system: An MQTT case study (MQTT-IoT-IDS2020 dataset),” in *International Networking Conference*, 2020, pp. 73–84.
- [46] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, “Kitsune: an ensemble of autoencoders for online network intrusion detection,” *arXiv:1802.09089*, 2018.
- [47] Y. M. Pa Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, “IoTPOT: analysing the rise of IoT compromises,” in *9th USENIX Workshop on Offensive Technologies*, 2015.
- [48] A. Guerra-Manzanares, J. Medina-Galindo, H. Bahsi, and S. Nömm, “MedBIoT: generation of an IoT Botnet dataset in a medium-sized IoT network,” in *Proceedings of the 6th International Conference on Information Systems Security and Privacy*, 2020, pp. 207–218, doi: 10.5220/0009187802070218.
- [49] N. Moustafa and J. Slay, “UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),” in *2015 Military Communications and Information Systems Conference (MilCIS)*, Nov. 2015, pp. 1–6, doi: 10.1109/MilCIS.2015.7348942.
- [50] D. Quick, B. Martini, and K.-K. R. Choo, “Chapter 4 - dropbox analysis: data remnants on user machines,” *Cloud Storage Forensics*, pp. 63–93, 2014.
- [51] Z. Li, T. Li, J. He, Y. Zhu, and Y. Wang, “A hybrid real-valued negative selection algorithm with variable-sized detectors and the k-nearest neighbors algorithm,” *Knowledge-Based Systems*, vol. 232, Nov. 2021, doi: 10.1016/j.knsys.2021.107477.
- [52] B. Al-Duwairi, W. Al-Kahla, M. A. AlRefai, Y. Abdelqader, A. Rawash, and R. Fahmawi, “SIEM-based detection and mitigation of IoT-botnet DDoS attacks,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 2, pp. 2182–2191, 2020, doi: 10.11591/ijece.v10i2.pp2182-2191.
- [53] S. A. Najafi, M. H. Asemani, and P. Setoodeh, “Attention and autoencoder hybrid model for unsupervised online anomaly detection,” *arXiv:2401.03322*, Jan. 2024.
- [54] S. K. Jasra, G. Valentino, A. Muscat, and R. Camilleri, “Hybrid machine learning–statistical method for anomaly detection in flight data,” *Applied Sciences*, vol. 12, no. 20, Oct. 2022, doi: 10.3390/app122010261.
- [55] H. Xu, G. Pang, Y. Wang, and Y. Wang, “Deep isolation forest for anomaly detection,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 12, pp. 12591–12604, Dec. 2023, doi: 10.1109/TKDE.2023.3270293.
- [56] Y. Karadayı, M. N. Aydin, and A. S. Öğrenci, “A hybrid deep learning framework for unsupervised anomaly detection in multivariate spatio-temporal data,” *Applied Sciences*, vol. 10, no. 15, Jul. 2020, doi: 10.3390/app10155191.
- [57] A. S. Mashaleh, N. F. Binti Ibrahim, M. Alauthman, and A. Almomani, “A proposed framework for early detection IoT Botnet,” in *Proceedings - 2022 23rd International Arab Conference on Information Technology*, 2022, doi: 10.1109/ACIT57182.2022.9994166.
- [58] W. W. Lo, G. Kulatilleke, M. Sarhan, S. Layeghy, and M. Portmann, “XG-BoT: An explainable deep graph neural network for botnet detection and forensics,” *Internet of Things*, vol. 22, Jul. 2023, doi: 10.1016/j.iot.2023.100747.
- [59] M. Kodys, Z. Lu, K. W. Fok, and V. L. L. Thing, “Intrusion detection in internet of things using convolutional neural networks,” in *2021 18th International Conference on Privacy, Security and Trust (PST)*, Dec. 2021, pp. 1–10, doi: 10.1109/PST52912.2021.9647828.
- [60] M. Catillo, A. Pecchia, and U. Villano, “A deep learning method for lightweight and cross-device IoT Botnet detection †,” *Applied*





- Sciences (Switzerland)*, vol. 13, no. 2, 2023, doi: 10.3390/app13020837.
- [61] X. Wang *et al.*, "Heterogeneous graph attention network," in *The Web Conference 2019 - Proceedings of the World Wide Web Conference*, pp. 2022–2032, 2019, doi: 10.1145/3308558.3313562.
- [62] K. Biron, W. Bazzaza, K. Yaqoob, A. Gawanmeh, and C. Fachkha, "A big data fusion to profile CPS security threats against operational technology," in *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, Aug. 2020, pp. 397–402, doi: 10.1109/WoWMoM49955.2020.00073.
- [63] A. S. Mashaleh, N. F. Binti Ibrahim, M. A. Al-Betar, H. M. J. Mustafa, and Q. M. Yaseen, "Detecting spam email with machine learning optimized with harris hawks optimizer (HHO) algorithm," *Procedia Computer Science*, vol. 201, no. C, pp. 659–664, 2022, doi: 10.1016/j.procs.2022.03.087.
- [64] A. S. Mashaleh, N. F. B. Ibrahim, M. Alauthman, M. Almseidin, and A. Gawanmeh, "IoT smart devices risk assessment model using fuzzy logic and PSO," *Computers, Materials and Continua*, vol. 78, no. 2, pp. 2245–2267, 2024, doi: 10.32604/cmc.2023.047323.

BIOGRAPHIES OF AUTHORS







Ashraf Suleiman Mashaleh     is a Ph.D. student in cyber security at the University Sains Malaysia, specializes in IoT security. As director assistance of the Computer Center at Al-Balqa Applied University, he holds an M.Sc. in computer information systems and a B.Sc. in computer engineering. With over 23 years of experience at Balqa Applied University, he focuses on network planning, design, and disaster recovery. Mashaleh has contributed to over five national and international projects, including the recent modernization of innovation and research management in neighboring countries (MIMIR). He actively participated in EU training courses on innovation and research management. Holder of a Microsoft Windows Azure certification in cloud technology, Mashaleh is dedicated to advancing cybersecurity knowledge, with a specific emphasis on securing IoT environments. He can be contacted at email: mashaleh@bau.edu.jo.







Noor Farizah Ibrahim     is currently working as a senior lecturer (assistant professor) at the School of Computer Sciences, Universiti Sains Malaysia. She completed her Ph.D. from the University of Bristol, UK. Her research interests revolve around machine learning, natural language processing, time series, and social media studies. Her research has been published in international journals and conferences including computers in human behavior, decision support systems, IEEE Access, Social Science Computer Review, Procedia Computer Science, International Journal on Perceptive and Cognitive Computing, World Academy of Science, Engineering and Technology, and International Journal of Business and Economics Engineering. She can be contacted at email: nfarizah@usm.my.







Mohammad Alauthman     received his Ph.D. from Northumbria University Newcastle, the UK 2016. He received a B.Sc. degree in computer science from Hashemite University, Jordan, in 2002 and an M.Sc. in computer science from Amman Arab University, Jordan, in 2004. He is an assistant professor at the Information Security Department at Petra University, Jordan. His research interests include cyber-security, cyber forensics, advanced machine learning and data science applications. He can be contacted at email: mohammad.alauthman@uop.edu.jo.







Jamal Al-Karaki     Prof. Al-Karaki is currently a full professor at Zayed University, UAE. He received the a PhD degree in electrical/computer engineering with research excellence award from the Iowa State University, USA. He has a vast expertise as a researcher, educator, and academic administrator including leadership positions such as college Dean, director of IT, Co-Founder and division head at various institutes. He led the development some national centers as well as undergraduate program and graduate programs in the general area of computing. He is also serving as accreditation team chair and member for UAE CAA, NQA, and ABET. He published 90+ refereed technical articles in scholarly international journals and conference proceedings. He has been listed among top 2% highly cited researchers worldwide in his domain and also a member of Mohammad Bin Rashed Academy for Scientists. He also attended/gained reputable professional certificates (e.g. CISSP, OSCP, ECSA, GMOB, CHFI, RHCSA, and CCNA security). He also served on the Editorial Board of some international journals and as publicity chair and technical program committee member of several International conferences and workshops. His main research interests include all aspects of computing and technology and their applications for better life. Dr. Al-Karaki is a senior member of IEEE and member of ACM and Tau Beta Pi. He can be contacted at email: jamal.al-karaki@zu.ac.ae.







Ammar Almomani     taught at the School of Information Technology, Skyline University College, and IT Department, Al-Huson University College, Al-Balqa Applied University. He is one of the Top 2% of Global Influential Researchers by Stanford University and the Scopus Index-Oct-2023, over 120+ articles published in reputable journals and conferences, and 8 patents and utility models published as six German utility models and Two Indian granted patents, 20 years of teaching more than 42 topics with various subjects related to cybersecurity, network, and AI. He has published 80 Scopus articles, and garnered over 3,200 citations on Google Scholar. He is actively engaged in the academic community, with a strong online presence and a large readership and following on ResearchGate with about 92,000 readers and followers. He can be contacted at email: ammarnav6@bau.edu.jo, Ammar.almomani@skylineuniversity.ac.ae.



Shadi Atalla     is an associate professor and the director of the computing and information systems program at the University of Dubai. With over 15 years of experience in teaching and research, he is a recognized data science expert and certified big data trainer, highly esteemed in the industry. Dr. Atalla's research focuses on data science algorithms, curriculum development, and artificial intelligence. He has published extensively and is chair of the computer society of IEEE UAE. Furthermore, Dr. Atalla brings a wealth of accreditation experience, having attended three ABET accreditation workshops and contributing to the accreditation process for both 2011 and 2019 CAA standards. His dedication ensures top-quality education and research standards, enhancing the academic excellence of the programs he oversees. He can be contacted at email: satalla@ud.ac.ae.



Amjad Gawanmeh     is an associate professor at the University of Dubai, UAE and Affiliate Adjunct Professor at Concordia University, Montreal, Canada. He received his Ph.D. degrees from Concordia University in 2008; respectively. He has two edited books, 3 book chapters, more than 40 peer reviewed Scopus indexed journal papers, and more than 65 peer reviewed conference papers. He worked at Khalifa University from 2010 until 2019, before joining the University of Dubai on January 2020. He was visiting scholar at Syracuse University, University of Quebec, and Concordia University. He is the editor in chief for the International Journal of Cyber-Physical Systems (IJCPS) IGI, an associate editor for IEEE Access Journal, Springer nature Journal of Reliable Intelligent Environments, and Human-centric Computing and Information Sciences Journal, Springer. He acted as guest editor for several special issues. He is on the reviewer board for several journals in IEEE, Elsevier, Wiley, and many others. He acted as a member of the executive committee for IPCC conference. He has co-chaired several conference workshops and special sessions organized in key conferences including Globecom, ICC, ICDCS, IPCCC, Healthcom, WoWMoM, ISNCC, and WiMob. He is senior IEEE member, IEEE GRSS Chapter chair, and IEEE UAE section conference coordinator. He can be contacted at email: amjad.gawanmeh@ud.ac.ae.