The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 3, June 2025
https://doi.org/10.33022/ijcs.v14i3.4853

Machine Learning-Based Security Algorithms for Detecting and Preventing DDoS Attacks on the IoT: State-of-the-Art, Challenges, and Future Directions

Coster Baloyi[1], Topside Mathonsi[2], Deon Du Plessis[3], Tonderai Muchenje[4], Tshimangadzo Tshilongamulenzhe[5]
costbal@gmail.com[1], mathonsite@tut.ac.za[2], danieldp@uj.ac.za[3], muchenjet@tut.ac.za[4], tshilongamulenzhetm@tut.ac.za[5]
[1,2,4,5] Tshwane University of Technology
[3] University of Johannesburg

Article Information

Received : 24 Apr 2025
Revised : 18 May 2025
Accepted : 9 Jun 2025

Keywords

IoT, DDoS, ML, DT, LR

Abstract

The Internet of Things (IoT) represents a vast network of interconnected devices equipped with software, sensors, and other technologies that enable data exchange and autonomous operation with other devices and systems without human intervention over the internet. IoT applications span across various sectors, including agriculture, education, healthcare, and communication. However, Distributed Denial of Service (DDoS) attacks continue to pose significant risks to the IoT network due to current challenges of classification efficiency and response times by the existing algorithms, such as Decision Tree (DT), Linear Regression (LR), and K-means. This paper provides a comprehensive review of DDoS attack types within the IoT networks. Secondly, the paper critically examines and analyses the challenges and opportunities inherent in leveraging Machine Learning (ML) algorithms for detecting, preventing, and mitigating these attacks. Finally, it presents the categories of IoT performance metrics, and their statistics found in the literature over the past decade.

A. Introduction

The Internet of Things (IoT) is regarded as one of the fastest-growing technologies, along with big data and Artificial Intelligence (AI). IoT covers the data communication framework [1, 2]. IoT includes a set of correlated devices that have the ability to connect without any human intervention [3, 4]. Many devices equipped with sensors, such as printers, lights, coffee machines, and CCTV cameras, are increasingly integrated with IoT across various sectors, including agriculture, education, and healthcare, enabling them to connect to the internet for enhanced functionality and automation [5, 6, 7].

The introduction of IoT in the agricultural sector has transformed the traditional farming way with enhanced soil monitoring and water management [7]. In 2018, there were a total of 22 billion IoT devices interconnected worldwide, which also projected an increase to 38.6 billion in the year 2025 and 50 billion in the year 2030 [5]. In 2020, it was recorded that roughly 127 new devices are connected to the internet every second, and it is estimated that the overall number of associated devices will increase by more than 27 billion by 2025 [1].

With the continued growth of IoT devices, cybersecurity attacks such as Denial of Service (DoS), Distributed Denial of Service (DDoS), spoofing, and Structured Query Language (SQL) injections, among others, have increased, turning the IoT network environment into a hotspot for malicious activities [7]. There is always a risk posed by these IoT devices since they can also connect systems such as database servers and cloud storage for collecting, processing, and monitoring IoT system data, which can be utilized to hack into many other critical components of the IoT infrastructure [5].

A large number of IoT networks introduce the latest issues such as volume of data, management of these devices, storage and communication issues as well as privacy and security concerns amongst others [8]. These devices handle sensitive data, and any security breach might seriously jeopardize privacy and vital infrastructure systems [9]. Additionally, IoT devices may operate as entry points for hackers, increasing the potential effect of security breaches by enabling them to access larger networks [10, 11, 12].

The review of the literature has indicated that researchers have designed and implemented security algorithms to detect and prevent DDoS attacks in the IoT network [1, 6]. However, there is still a gap in improving accuracy and precision in the classification of cyberattacks under large network traffic in IoT devices. This led to unacceptable classification efficiency and response times, leading to inaccuracy in detection, low precision rate, and poor network performance. Therefore, this paper conducts a systematic literature review on existing techniques for detecting and preventing DDoS attacks in IoT networks. This paper reviews the performance metrics mainly used in the field of IoT environments. This was achieved by making use of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) approach. PRISMA was used to identify the reviewed articles, screened for selection, and checked for fitness and inclusion. The methodology is described in detail in the methodology in section IX.

The rest of the paper is structured as follows: The paper contributions are presented in Section II. An overview of IoT is presented in Section III. Furthermore, the paper discusses an overview of DDoS attacks in IoT in Section IV. The paper

presents the related work in Section IV. The ML Techniques to detect and prevent DDoS attacks on IoT networks is in Section V. In Section VI, the paper presented the rated work section. In section VII, the paper discusses categories of IoT performance metrics. Section VIII demonstrated the methodology. Section IX presents the results and lessons learnt. Section X presents the conclusion.

B. Contributions

The key contribution of this paper is outlined below:

- An in-depth review of Distributed Denial of Service (DDoS) attacks within the context of Internet of Things (IoT) networks, highlighting their evolving nature, common attack vectors, and the significant impact they pose on resource-constrained IoT environments.
- A comprehensive evaluation of machine learning (ML) algorithms used for the detection and mitigation of DDoS attacks in IoT networks, outlining their strengths, limitations, and applicability to real-world deployment scenarios.
- An analytical synthesis of IoT performance metrics commonly used in the literature over the past decade, offering a structured classification and discussion on how these metrics are employed to assess the effectiveness of DDoS detection models and overall network performance.

C. Overview of IoT

IoT has increasingly become the most useful technology in education, in agriculture, and in everyday life. This is due to its ability to connect different devices, such as printers, smart refrigerators, and smart TVs, allowing them to collect and exchange data over the internet. The IoT characteristics are clearly summarized in Table 1 below.

Table 1. Properties of IoT

Properties of IoT	Description
Architecture	Hybrid, heterogeneous, and compatible with different device manufacturing products
Scalability	Device network connectivity is increasing daily, hence the ability to handle such a load
Connectivity	Availability, guaranteed device network connectivity
Identity and Intelligence	Collected data is accurately interpreted
Safety	Security of the day, the ability to secure data, including personal information
Dynamic and self-adaptive	Ability to operate in different locations regardless of the time of day or night

1. IoT architecture

IoT architecture consists of four main components that differ in terms of performance, application, and area of functionality, namely: sensors, network gateway, management service layer, and application layer [13].

a) Sensors

Network devices that generate, receive, deliver, and execute over the network. These devices have the ability to receive input from different environments and respond accordingly [13].

b) Network gateway

To be able to connect and exchange data, IoT devices require a stable and fast network connection, such as stable WIFI connections [13].

c) Management service layer

These are the network devices that receive and transfer data to the cloud. This data is first stored in the local device and then transferred to the cloud through IoT benefit [13].

d) Application layer

Multiple applications in fields such as robotics, traffic monitoring systems, health, and agriculture are built based on IoT. These applications can simplify communication through IoT [13].

The components of IoT are shown below.

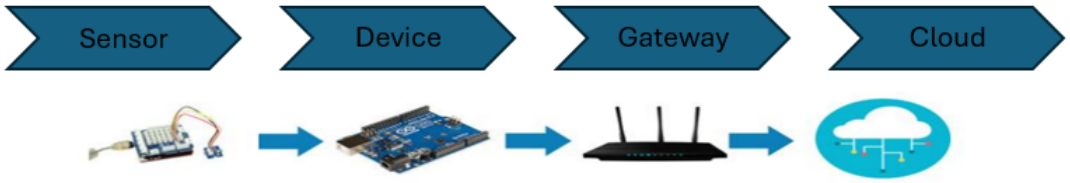

Figure 1. Components of IoT

The architecture of IoT in Figure 1 demonstrates different layers of functionalities from a sensor layer, which is an internal component of a device that receives input and provides output. The device layer will receive and transmit data, while the gateway layer enables transmission to the cloud layer, which is the storage layer [13].

D. Overview of DDoS attacks in IoT

DDoS attacks are among the major risks to the security of IoT networks as attackers utilize multiple compromised nodes to flood the target by creating considerable network traffic that depletes the target's resources [14]. Below are examples of different types of DDoS attacks in the IoT network, as well as their impact.

1. Types of DDoS attacks and their impact on IoT

a) IoT Volume-based DDoS attacks.

The volume-based DDoS attacks cause a system to halt by overloading the communication lines used to access the victim's network nodes. Unlike the resource exhaustion application layer attack that comprises volume-based or protocol exploitation, which are much more expressive in the amount of traffic made during execution in the IoT network [14]. Another example of the volume-based DDoS attacks is the amplification attack that instructs the web servers to change the source address entry to that of the victim's IP address, resulting in the victim's server bandwidth being depleted [15, 16].

b) IoT Protocol-based DDoS attacks.

The Protocol-based DDoS attacks focus on the server resources, unlike the volume-based attacks that deplete the IoT network bandwidth. They are known for targeting the load balancers and firewalls by flooding them with bogus requests to deplete the resources available [14]. In this instance, hardware resources such as central processing unit (CPU), storage, and memory are targeted through the network layer with the purpose of exhausting the available resources [15].

c) IoT Application-based DDoS attacks.

The application-based DDoS attacks take advantage of the vulnerabilities in the application or a network service, thereby causing instability and making it impossible for authorized users to have access to the IoT network system [14]. These types of attacks are always mistaken for technical errors, causing the system to slow down by using the least amount of bandwidth possible to ensure its effectiveness [17, 18].

Below is a summary of the categories of DDoS attacks and their examples.

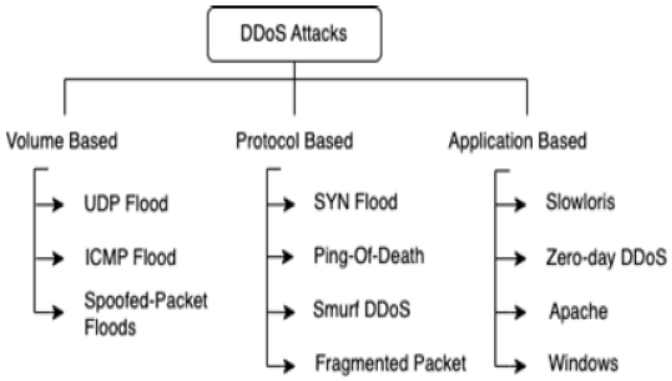

Figure 2. DDoS attack types [13]

2. DDoS Attack Scenarios

A DDoS attack is a type of DoS attack that originates from multiple sources to make it more effective than a single-source attack [18]. The complete intention is to flood the target device with a large number of meaningless and forged packets. With

the evolution of network communication and computer devices, the impact of DoS attacks became less effective as a result of the development of DDoS attacks [18, 19].

An example of a DDoS attack is a botnet that comprises two or more managed devices situated remotely from each other to launch a DDoS attack on the same target in order to halt the server network services, as shown in Figure 3.

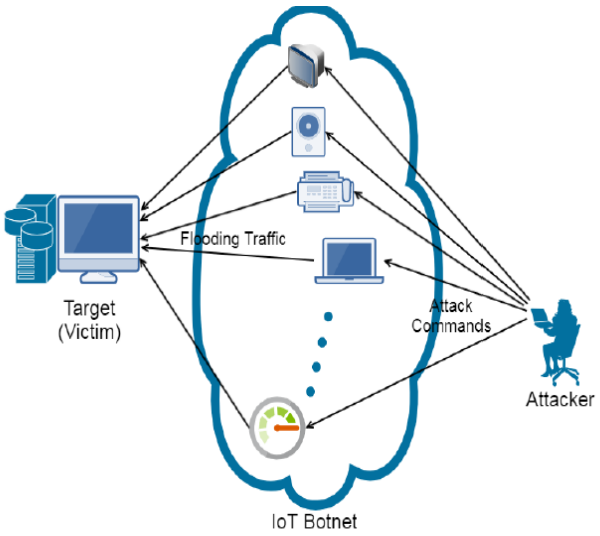

Figure 3. Botnet in IoT network [18]

IoT botnet enables the attacker to control a collection of several malicious devices referred to as zombies to remotely instruct these devices to launch a malicious attack making use of attack commands [18]. The botnet attack commands, and control techniques determine the way the bot can be orchestrated, this can be done through Hypertext Transfer Protocol (HTTP), Domain Name System (DNS), Internet Relay Chat (IRC), and Peer-to-Peer (P2P) based. Attackers use the botnet type of attack to commit malicious activities such as theft of personal information, sending spam emails, and phishing activities.

DDoS attacks can occur in two ways, namely, network bandwidth consumption and system resources consumption.

2.1. Network Bandwidth Consumption DDoS attacks

In order to frequently block the target device, the botnet transmits large network packets to consume network bandwidth, as shown in Figure 3. The details of network bandwidth consumption from DDoS attacks are discussed below:

a) User Datagram Protocol (UDP) flood attack

UDP is a transport protocol that is connectionless. This type of attack does not require authentication when transmitting packets [18]. UDP can send a large number of packets to the target device to consume bandwidth, causing inaccessible normal services, as shown in Figure 4.

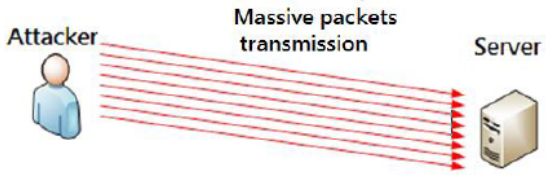

Figure 4. UDP flood attack [18]

b) Internet Control Message Protocol (ICMP) flood attack

Under normal circumstances, a ping command is used to send an ICMP echo request header packet to the master, and the mast will send an ICMP echo reply to the heard packet to the client confirming if the connection between them can be transmitted properly [18]. The ICMP will send a large number of ping commands to the attached server in a short period of time, consuming severe resources and causing services to halt immediately, as shown in Figure 5.

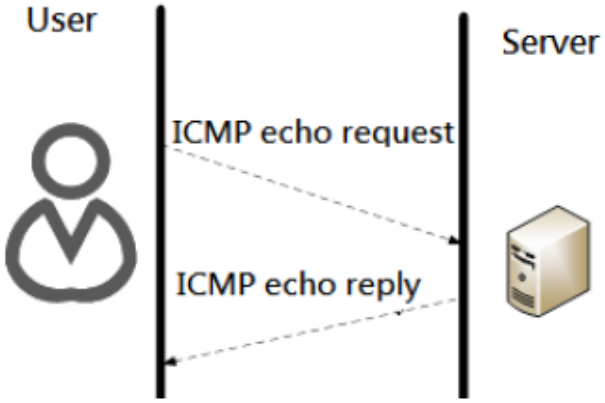

Figure 5. ICMP before attacks [18]

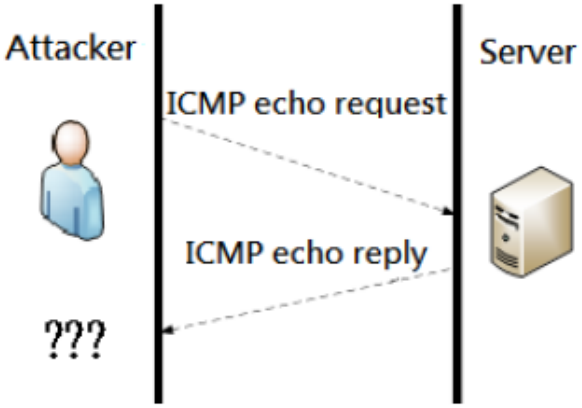

Figure 6. ICMP attack [18]

c) Teardrop Attack

The teardrop attack achieves its attack by segmenting each packet and shifting before transmission. It uses this method of attack to mimic shift information, so it

becomes difficult to reassemble the packet, thereby causing errors and recording the processing information for future packet reassembly [18].

2.2. DDoS Attacks on System Resource Consumption

System vulnerabilities or forged IPs cause system resource consumption in IoT networks. Service suspension is usually caused by CPU resources and system memory exhaustion. The examples of this type of DDoS attack in IoT networks are discussed below:

a) IoT Synchronized (SYN) Flood Attack

This type of attack looks for vulnerabilities in the three-way handshake between the sender and the receiver in the Transmission Control Protocol (TCP) in the IoT network [18]. In this attack, an attacker may deliberately not return ACK information or use a forged IP address to make the server send SYN + ACK packets to a forged IP address in the SYN flood. Since it is a forged IP address, the server cannot receive an ACK packet I response, as a result of a continuous sending of SYN + ACK packets by the server until it times out, thereby consuming server bandwidth and memory resources as shown in Figure 7.

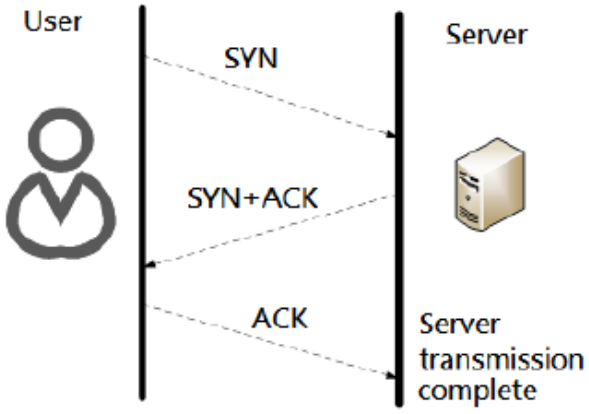

Figure 7. TCP three-way handshake [18]

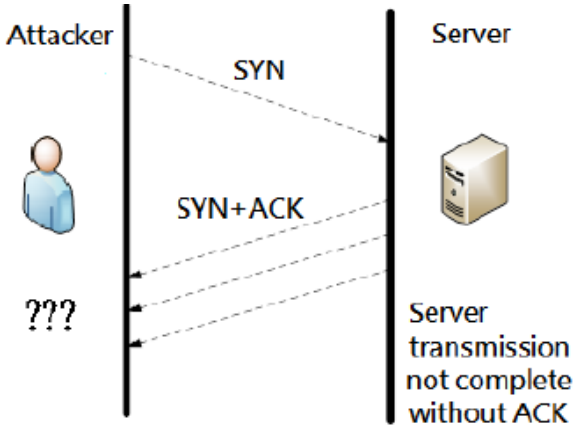

Figure 8. SYN flooding attack [18]

b) IoT Local Area Network Denial attack

In this type of attack, a forged IP address is converted to the same IP as the attacked host IP as a result, the host continues sending SYN + ACK packets back to itself, causing a continuous loop and consuming its resources in the IoT network [18].

c) IoT DNS flood attacks

This type of attack uses a botnet to attack the DNS by sending randomly generated DNS requests to the DNS server, causing the DNS service Interruption in the IoT network [18].

E. ML Techniques to Detect and Prevent DDoS Attacks on IoT Networks

This section focuses on different ML techniques employed to detect and prevent DDoS attacks in the IoT networks, including their functionalities and characteristics, namely:

1. AdaBoost

AdaBoost stands for Adaptive Boosting, which is a useful ensemble learning technique used in IoT security for classification activities [20, 21]. Its quality feature is in the ability to increase capacity to improve the performance of weak learners sequentially by assigning misclassification instances with higher weight values in each iteration [20]. In the IoT networks security context, AdaBoost iteratively trains weak learners to identify misclassified instances and form a strong classifier that is able to identify with accuracy complex attack patterns. Its strong feature is in the ability to withstand different types of attacks in the IoT network. However, AdaBoost's challenge is in its sensitivity to noisy data, and when the dataset is noisy and complex, it degrades the performance of its weak learners.

2. Random Forest

The RF techniques are an effective and robust tool in the classification activities in IoT networks. This uses a decision tree that is generated during the training phase. RF is good at detecting and identifying different cybersecurity threats that target IoT networks [20]. RF uses a decision tree generated during the training phase. RF technique demonstrates a strong handling of high-dimensional datasets, by offering strong detection capabilities for different types of attacks such as SYN flooding, Port Scan, and other complex DDoS attacks. Its advantage lies in its ability to provide randomness to mitigate overfitting. However, its disadvantage is its potential difficulties in interpreting the decision-making process and its increased computational complexity [20].

3. Decision Trees

The Decision Tree technique plays a crucial role in the decision-making process by improving the analysis of the identified attack matrix in the IoT network [20, 22]. It recursively divides the input space according to features and creates a tree-like structure of decision nodes and leaves. In the Decision Trees, classification is optimized by selecting features at the decision nodes. Decision Trees are known

for their adaptability, interpretability, and effectiveness in classifying and detecting DDoS attacks [23]. However, even though Decision Trees are easy to follow and provide a clear representation of the decision logic, they may be prone to overfitting when the sequence is complex.

4. KNN

KNN stands for K-Nearest Neighbors. KNN is a useful technique in the IoT networks responsible for regression and classification activities [20, 24]. KNN offers prediction based on the KNN average value or the main class in the feature space. KNN provides an easy and simplified interpretation of different classification scenarios. KNN is sensitive to the distance metric employed and performance parameter "k" including a trade-off between accuracy rate and computational cost that is useful in the IoT network security application [24].

5. SVM

SVM is short for Support Vector Machine, which is a useful technique for regression, text categorization, bioinformatics, and classification in IoT networks. SVM plays an important role when there is a need to identify a hyperplane that effectively distinguishes data points belonging to different features in classes [20]. The optimization of the margins between the hyperplane and the data nearest point of each class is offered by SVM. SVM contributes to stabilizing the IoT security environment by offering resilience generalization to unknown data [25]. However, SVM has computational complexity challenges in constrained resources for IoT network devices.

6. Naïve Bayes

Naïve Bayes is a useful technique in the IoT network environment due to its efficiency and simplicity, used mainly for probabilistic classification [26]. This is achieved by applying Bayes' model and through the assumption of feature independence. Naïve Bayes presents effectiveness in the categorization and classification of different types of DDoS attacks in IoT networks. Naïve Bayes offers real-time applications and computational resources due to its computational efficiency and easy implementation [26]. However, its independence assumption challenges may not always align with the desired real-time dataset.

7. Logistic Regression

LR stands for Logistic Regression and is a useful ML technique in the IoT network environment for binary classification activities. This is achieved by computing the likelihood of the instances of a particular class utilizing the logistic function [27]. LR stands out for its efficiency, simplicity, and interpretability [28]. LR uses algorithmic weights for each feature. The linear combination of weights and input features is transformed by the logistic function in a range between 0 and 1. However, LR may be less effective when working with relationships that are non-linear between features and the target variable.

This section presented an overview of DDoS attacks in IoT. The categories of DDoS attacks, such as volume, protocol, and application-based based were discussed, and their impact on the IoT network was highlighted. Volume-based

attacks can cause the system to stop functioning by flooding the victim's network bandwidth, while the protocol-based attacks focus on depleting server resources, and application-based based take advantage of open vulnerabilities in IoT applications. Different ML techniques are also presented in this section. The next section will present the related work.

F. Related Works

This section provides a critical review of existing literature on machine learning algorithms proposed for detecting DDoS attacks in IoT networks, with a particular focus on their methodologies, performance, and identified limitations.

Shire et al. [29] proposed an IoT malware traffic analysis technique in order to improve the protection of IoT devices at the gateway level by detecting unknown malware. The techniques comprise three segments, the first is the collection of network traffic using files that have pre-captured network traffic through TCP replay, and processed by the TensorFlow module. The second segment is the visualization segment, which converts the collected traffic into 2D images. All the files collected were from real-world network environments. The algorithm used was called the visual representation algorithm, which collected data that was based on Binvis represented in different American Standard Code for Information Interchange (ASCII) values, color classes blue, red, and green. The third segment is the malware traffic analysis, where a machine learning model, utilized on a larger scale called TensorFlow, is used to analyze the images against its in-depth training. The simulation was performed on an Ubuntu 18.0.4 workstation; the dataset used contained 100 pcap samples collected from external repositories with 30 normal and 70 malware traffic samples. Wireshark testing was conducted, and the TensorFlow algorithm was trained in 500 iterations. The results were presented as follows: the accuracy rate was 91.32%, the precision rate was 91.67%, and the recall rate was 91.03%. The limitation of the study is that none of the results exceeded 92%, showing room for more research.

Khedr et al. [30] proposed a four-model DDoS attack detection and mitigation (FMDADM) framework for the purpose of detecting DDoS attacks at high and low rates and classifying traffic attacks and flash crowds while protecting local and remote IoT nodes at the same time, preventing infections from propagating to the ISP level. Firstly, the module implemented an Average Drop Rate (ADP) for an early detection process. Secondly, utilised a double-check mapping function (DCMF) for early attack detection at the data plane level. Thirdly, the module was ML-based detection that included training and testing, feature extraction, data preprocessing, and classification. The fourth module introduced an attack mitigation process. Three test cases were proposed, namely: one single-node attack, a multi-node attack, and all with real IoT traffic generated and deployed. The dataset used was called Eddge-IIoTset. The simulation was conducted through sFlow-RT. The results were 99.79% accuracy, 99.43% precision, 99.77% F-measure, 99.79% recall, 99.95% specificity, 00.21% negative predictive value, 00.91% false positive rate, 00.23% false negative rate, and 2.64 average detection time benchmarks. The limitation of this study is that further research is required to detect more types of attacks on the SDN-based IoT network.

Bukhowah et al. [31] proposed an ML technique for developing an efficient and robust solution for detecting DoS attacks in the Information Centric Network (ICN) - IoT environment. The study explored the different ML techniques in literature that include Decision Trees (DT), Neural Network (NN), Deep Neural Network (DNN), Back propagation (BP), XGBoost, J48, and Multilayer Perceptron (MLP) to compare their detection rate using classification metrics such as accuracy. This approach was carried out on the NDN architecture. The study utilized the ndnSIM simulation tool to evaluate the results. The dataset utilised was called the synthesis dataset for detecting DoS attacks in the ICN-IoT environment. The results. The results showed that KNN achieved 98.35%, SVM achieved 99.4%, and RF provided good performance in precision, accuracy, and recall. Furthermore, the SVM, RF, and KNN performed well compared to other techniques. The limitation of the study is that further research is required to explore additional attacks, threats, and types through enhanced ML technology.

Sanjeevini et al. [32] proposed a technique that focused on ML algorithms such as Naïve Bayes, KNN, RF, XGBoost, Support Vector Machine, and AdaBoost for classification purposes to distinguish the network system from attack conditions and normal conditions in the IoT environment. The RF algorithm resulted in good performance over other algorithms. The dataset used to train the algorithm was called the CICDDoS2029 dataset and contains ten different attacks on an IoT environment. The limitation of the study is that the dataset used only contains 10 different attacks and may not consider new attacks.

Seyed et al. [33] proposed an interactive technique that split modelling into two layers in order to optimize the detection of intrusion attacks to learning algorithms by integrating algorithmic methods and reduction of learning costs: The Cost-Sensitive Learning algorithm was used for cost discrimination, and the Meta-Learning was dedicated to metadata management. This model optimizes the automation detection of intrusions into IoTs using self-learning. The algorithm used is called the One-R algorithm. The study utilized the Weka tool for the simulation of the model, which is an ML algorithm set for data mining. The dataset utilised is called One-R. The parameters trained include clustering, data preparation, classification, visualization, regression, and association rule mining. The result showed a classification quality rate of approximately 93.66%, a consistency rate of 0.883, the false positives of 0.2 and 4.2%. The sensitivity was between 77.8% and 97.3%, the specificity was between 95.8% and 99.8%, and the precision was 0.951. The limitation of this study shows that the classification rate still requires further improvement.

Williams et al. [34] proposed a standard approach to deal with different threats and attacks in IoT devices by using strong encryption techniques such as the SHA-256 hashing function to protect data at rest and data in transit. Their technique included authentication techniques, namely identity or device authentication, procedural authentication, and token-based authentication that verify the identity of an entity accessing the network service. The algorithm used for blockchain to perform effectively is called the consensus algorithm. The algorithm helped to decrease the complexity of the block, network instability, and latency; however, the proposed solution was not innovative and did not proactively detect unknown attacks, which can lead to further malicious attacks. Furthermore, there is still a

concern about the data at rest for further research due to the emergency and integration of various technologies into IoT systems.

Seyed et al. [35], proposed a new intrusion detection optimization (NIDO) model that allowed choosing among machine learning methods, namely supervised, reinforcement, and unsupervised, to effectively detect intrusions in IoT devices. The optimal method choice for the model was based on the cost-sensitivity and the ability to minimize the learning impact of the attacks. The study utilized the latest DDoS attacks dataset called CICIDS2018 with up-to-date real-world data. A Confusion Matrix, which is also known as an error matrix, is utilized to evaluate the performance of a machine learning technique based on the classification of attacks. Weka Tool was utilized for simulation. The algorithmic policy for Meta-learning was used. The results showed a classification rate of 93,66%, a Precision rate of 96%, and a False Positive rate of 0,3%. Their proposed solution was to improve the detection rate; however, the study still intends to utilize other methods to compare the results and deduce the best in terms of performance and quality of intrusion detection.

Ravi & Shalinie [36] proposed a security framework called learning-driven detection mitigation (LEDEM) that uses a semi-supervised machine-learning algorithm to mitigate DDoS attacks in an IoT environment. This framework leverages software-defined network (SDN) and cloud paradigm. The LEDEM test was done in the testbed and emulated topology. The results achieved an accuracy rate of 96.28% in detecting DDoS attacks and were compared with the state-of-the-art solutions. The limitation of the study is adaptability issues since it only uses one classification method and is incapable of dealing with different types of DDoS attacks.

Bagaa et al. [37] proposed a unique machine learning (ML) based security algorithm that automatically deals with developing security features related to the IoT environment. This is a supervised learning algorithm that leverages both Network Functions Virtualization (NFV) and Software Defined Network (SDN), enabling them to mitigate DDoS attacks on the IoT environment. A neural network and distributed mining system were employed for effective DDoS detection. The dataset used was called the NSL KDD dataset. The experiments were conducted using a real Smart building scenario using one-class SVM. The results showed 99.71% accuracy in detection. The limitation of this algorithm is that the cost of misclassification is higher than the processing time.

Abdallah et al. [38] proposed a mixed Intrusion Detection System that combines Long Short-Term Memory Network (LSTM) and Convolution Neural Network (CNN) algorithms to obtain the spatial and temporal features of the network traffic. This approach uses two regularization models, namely: dropout model and L2 Regularization (L2Reg), to resolve the issues of overfitting. The proposed model improved the detection performance of zero-day attacks. The dataset utilized was called the InSDN dataset. The integration of CNN and LSTM algorithms has improved intrusion detection and achieved 96.32% accuracy. The limitation of this approach is that it cannot handle real-time datasets.

Elsayed et al. [39] proposed a unique mixed Deep Learning (DL) approach that is based on a Convolutional Neural Network (CNN) that classifies traffic flow to determine whether the traffic is normal or malicious attacks in the SDN

environment. The proposed framework combines CNN with ML algorithms such as KNN and SVM to improve anomaly detection. The framework uses a regularization model called SD-Reg that was based on a weight matrix of normal deviation to resolve the problem of overfitting and improve the capability of detecting unknown attacks. The framework used the latest SDN dataset to train and evaluate the performance of the proposed framework. The results showed 97,47% accuracy for CNN-RF and 97,37% classification. The limitation of the study is that accuracy can still be improved.

Najafimehr [40] proposed an ML-based model that reviewed the mixed approach, the supervised, and the unsupervised, as well as analyzing the challenges related to it for detecting DDoS attacks. This was achieved by comparing the ML models, namely: the Random Forest (RF) and the Support Vector Machine (SVM), as well as the Deep Learning models, namely: Convolutional Neural Network (CNN) and the Long Short-term Memory (LSTM). The approach has proved that the compared models are effective in detecting attacks in the IoT environment. The study utilized the following datasets, namely: KDDCup99, NSL-KDD, UNSW-NB15, CICDS2017, CICDDoS2019, and Edge0IIoTset. The results showed KDDCup99 and NSL-KDD datasets were outdated with no innovation for advanced attacks, CICDS2017 and Edge-IIoTset lack novel types of DDoS attacks. CICDDoS2019 is not suitable for detecting low-rate and slow attacks. The limitation of the study is that the datasets used failed to show efficiency in the detection of new attacks.

Dash et al. [41] proposed two approaches, namely: one using Principal Component Analysis (PCA) and the other without PCA in order to improve the DDoS attack detection technique for IoT devices utilizing a suitable dataset, rigorous model evaluation, different classifiers, efficient preprocessing, and feature selection. The study utilized the NSL-KDD dataset, which contained different network traffic data. The encoding model and RobustScaler are used as preprocessing phases. The results displayed significant improvement by integrating a robust scaler and PCA. The accuracy performance for RF was 99.87%, and for KNN classifiers was 99.14%, Naïve Bayes displayed a low accuracy of 87.14%. The limitation of the study is the inconsistency with the success rate through Naive Bayes.

Pandey & Mishra [42] proposed two approaches, namely: Pearson correlation coefficient and Extra Tree classifier, to analyse the performance of ML-based classifiers that include boosting and bagging techniques for classification of DDoS attacks in the IoT environment. For analysis, the CICDDoS2019 dataset was used for types of attacks. Performance was evaluated for the following techniques: AdaBoost, ML classifiers, eXtreme Gradient Boosting (XGBoost), Random Forest (RF), Naïve Bayes (NB), Gradient Boosting (GB), and support vector machine (SVM) techniques. The results showed that the RF demonstrated better performance compared to other techniques, with the least training time and the least training of 99.99% recall, 100% precision, 99.99% f1-score, and 99.99% accuracy. The limitation of this study is that during training, the records of data files were partially included, meaning not all the data files were included, which opens room for misclassification of attacks.

Signh & Jain [43] proposed a Gini-Impurity-based technique for the detection and mitigation of DDoS attacks in the IoT environment. The Gini-Impurity-based technique was used as a metric for software-defined networks (SDN) to measure the

homogeneity of network traffic in the IoT environment. This approach has been demonstrated to be efficient and effective, and it requires less computational power. For classification, Decision Tree (DT), Logistic Regression (LR), Multi-Layer Perceptron (MLP), and K-Nearest Neighbors (KNN) algorithms are used in their approach. The study used real-world network traffic datasets called NSL KDD and CICFlowMeter datasets. The results showed 99.98% DT, 99.98% KNN, 99.99% LR, and 99.99% MLP for the NSL KDD dataset and 99.93% DT, 99.82% KNN, 91.69% LR, and 98.47% MLP for the CICFlowMeter dataset. The limitation of this study is the high computational cost.

Saiyed & AL-Anbagi [44] proposed a Deep Ensemble learning with pruning (DEEPShield) model by integrating a Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN) network with a network traffic analysis system to improve the detection of both high- and low-volume DDoS attacks in IoT with resource-constrained environments. The LSTM model focuses on detecting sequences in network traffic flows and temporary patterns. The CNN model specializes in identifying spatial patterns and relationships between features, which helps in distinguishing various DDoS attacks. The dataset used includes CICIDS-17, ToN-IoT, ISCX-12, and HL-IoT. The results showed over 90% accuracy for both DDoS attack types. The limitation of the study is that it requires more time to collect the data to be used during experimental evaluation.

Ravi et al. [45] proposed a deep learning-based framework that extracts internal feature categories from gated recurrent unit (GRU) layers to detect DDoS attacks and classify them into their attack categories. The Kernel principal component analysis (Kernel PCA) was used to extract the optimal features, which are then fused together. Furthermore, DDoS attack detection and its classification are done using a fully connected network. This framework can be used in real-time to effectively detect DDoS attacks in IoT environments and classify them into their respective categories. The dataset used in this study was called SDN-IoT datasets, and the simulation was done using the Mininet tool. The proposed GRU feature fusion model showed 99% accuracy with 99% macro precision, 99% macro recall, and 99% macro F1-score. For attack classification, the proposed GRU feature fusion model showed 99% accuracy with 99% macro precision, 99% macro recall, and 99% macro F1-score. The limitation of this study is that the datasets used were insufficient for analyzing the behaviors of IoT network traffic.

Kumar & Sharma [46] proposed an inverted hour-glass-based layered network classifier for classification and a hybrid intelligent system for feature selection to enhance accuracy in the detection of DDoS attacks. This framework utilised three types of datasets, namely: KDD-Cup99 database, NSL-KDD Database, and UNSW-NB15 database, for identifying new and old DDoS attacks. The framework achieved the goal by using the inverted hour-glass-based network by sampling the data with an increase in the number of layers for effective training. The results of the proposed model showed 99.97% of NSL-KDD, 99.57% of KDD-CUP99, and 99.73% of UNSW NB15 in accuracy detection. The limitation of this model is that it can only handle one classification method.

The above ML algorithms were summarized based on the qualities of the proposed solution and their limitation as presented in Table 2.

Table 2. Summary of ML algorithms

Summary of the ML algorithms	Advantages of the proposed solution	Limitations of the solution
Shire et al. [29] proposed a visual representation algorithm	Improved the protection of IoT devices on the gateway level by detecting unknown malware	None of the results exceeded 92%, showing room for more research
Khedr et al. [30] proposed a FMDADM framework	Improved accuracy	Further research is required to detect more types of attacks on the SDN-based
Bukhowah et al. [31] compared ML techniques, namely: DT, NN, DNN, BP, XGBoost, J48, and MLP	An efficient and robust solution for detecting DoS attacks	Further research is required to explore additional attack threats and types through an enhanced ML technology
Sanjeevini et al. [32] proposed an RF algorithm	Uses CICDDoS2029 dataset	It contains 10 different attacks and may not consider new attacks.
Seyed et al. [33] proposed a One_R algorithm	Optimizes automation detection of intrusions into IoTs	The classification rate requires further improvement
Williams et al. [34] proposed a consensus algorithm	Decreased the complexity of the block, network instability, and latency	Not being innovative and proactively detecting unknown attacks can lead to further malicious attacks.
Seyed et al. [35] proposed an algorithmic policy for Meta-learning-based	latest DDoS attack dataset CICIDS2018 with up-to-date real-world data	Intend to utilize other methods to compare the results
Ravi & Shalinie [36] proposed the LEDEM framework	Achieved a good accuracy rate	Uses only one classification method
Bagaa et al. [37] proposed NFV and SDN algorithm	The best accuracy detection rate	The cost of misclassification is higher
Abdallah et al. [38] proposed CNN and LSTM algorithms	Improved the intrusion detection and accuracy rate	It cannot handle real-time datasets
Elsayed et al. [39] proposed a CNN with ML algorithms such as KNN and SVM	Used the latest SDN dataset to train and evaluate the performance	Accuracy can still be improved
Najafimehr [40] compared ML algorithms, namely: RF, SVM, CNN, and LSTM	Effective in detecting attacks in the IoT environment	The datasets used failed to show efficiency in the detection of new attacks
Dash et al. [41] proposed two approaches, namely PCA and without PCA	Improved accuracy performance	Inconsistency with the success rate through Naive Bayes

Pandey & Mishra [42] evaluated AdaBoost, ML classifiers, eXtreme, XGBoost, RF, NB, GB, and SVM techniques	RF demonstrated better performance	The data files were partially included
Signh & Jain [43] proposed DT, LR, MLP, and KNN algorithms	Uses real-world network traffic datasets	High computational cost
Saiyed & AL-Anbagi [44] proposed a DEEPShield	Improve the detection of both high- and low-volume	More time to collect the data
Ravi et al. [45] proposed a deep learning-based framework	Real-time detection of DDoS attacks in an IoT environment	The datasets used were insufficient for analysing the behaviour of IoT network traffic
Kumar & Sharma [46] proposed an inverted hour-glass-based layered network classifier for classification and a hybrid intelligent system	Sampling the data with the increase in the number of layers for effective training	It can only handle one classification method

G. Categories of IoT Performance Metrics

In this section, different aspects and parts that affect IoT overall performance are presented [47, 48]. These performance metrics are categorized into ten different metrics, namely: data privacy and inference metrics, software metrics, security metrics, experience quality metrics, information quality metrics, system quality metrics, test metrics, network metrics, anomalies and attack prediction metrics, and hardware metrics.

1. Data Privacy and Inference Metrics

The data privacy and inference metrics include the following: information loss, information privacy, trustworthiness, identifiability, utility, mutual information, and differential privacy [47].

2. Software Metrics

The software metrics include the following: Code redundancy and complexity, Code readability, code, cohesion, Duplicated blocks, Density of comment lines, Method, Number of comment lines, Primary Training, Number of lines, Unit interface size, Quality of code, and secondary practice [47].

3. Security Metrics

The security metrics include the following: Password strength, Successful Attack Percentage, Inbound and Outbound Connection, Risk, Cost of Attack, Mean Time to compromise, rate of compromise, and probability of successful attack [47].

4. Experience Quality Metrics

This includes a survey and Mean Opinion Score.

5. Information Quality Metrics

This includes timeliness, Artificiality, concordance, and completeness [47].

6. System Quality Metrics

The system quality metrics include the following: reliability, recoverability, recoverability, functional correctness, conformance, efficiency, portability, availability, flaws over time, rate of user error, integrity, confidentiality, functionality, functionality, maturity, safety, and rate of user error [47].

7. Test Metrics

The testing metrics include the following: Defect Fix vs Defect Discovery, Test Case Review Defect Density, Defect Re-Open Rate, Defect Rejection Rate, Defect Leakage, Effective Density Defect, Executive Production Test, Coverage Requirement, and Scripting Production Test [47].

8. Network Metrics

The network metrics include the following: reliability, delay end to end, delay average link, packet delay, data loss rate, code rate expected transmission delay, network stability delay, package latency, availability, control overhead, network size, implementation complexity, network overload, latency, processing speed, connection rate, memory space, bandwidth, size of the network, Temperature message size, rate of data, and throughput [47].

9. Anomalies and Attachment Prediction Metrics

The anomalies and attack prediction metrics include the following: Accuracy, Recall, Confusion Matrix, F1 score, and precision [47].

10. Hardware Metrics

This includes the accuracy of the sensors, energy consumption, sensor time duration, and camera resolution [47].

Figure 9 presents the summary of the IoT Performance Metrics found in the Literature over the Past decade.

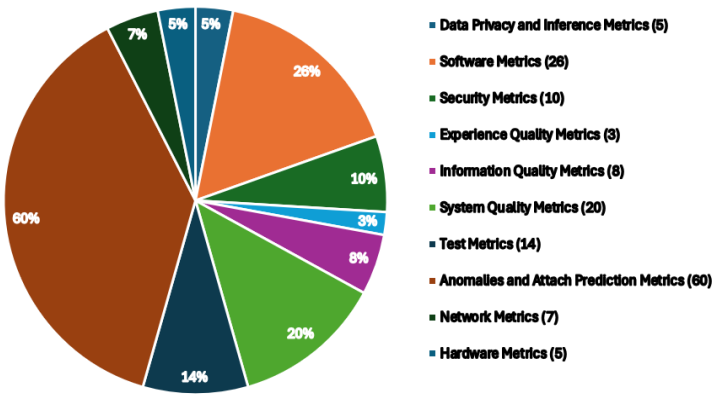

Figure 9. Statistics of IoT Performance Metrics over the past decade

In Figure 9, the classification of anomalies and attack prediction metrics, software metrics, and system quality metrics have the highest number with 60, 26, and 20 percent, respectively. While the experience quality metrics, hardware metrics, data privacy and interference metrics, and the network metrics are lowest with 3, 5, and 7 percent, respectively.

From the reviewed articles, the anomalies and attack prediction metrics such as Accuracy, Recall, Confusion Matrix, F1 score, and precision are mostly used for their ability to assess efficiency and efficacy for ML algorithms and provide reasonable comparisons across different ML algorithms [49, 50, 51].

The information quality metrics were used less from the reviewed articles due to the reason that the study was focused on accuracy and precision, and therefore, the focus was on articles with anomalies and attack prediction metrics.

H. Modelling Techniques and Performance Metric

There are a variety of techniques that can be utilized for modelling purposes in IoT. In order to determine how well detection and prevention techniques can perform, we need to highlight the performance metrics that are used. We begin our discussion by defining the performance metrics used for accuracy and precision detection.

1. Performance Metrics

For every machine learning problem, we require a set of performance metrics for performance evaluation. In this paper, we discussed the categories of IoT performance metrics and their classifications. However, for the purpose of this study, we selected the anomalies and attack prediction metrics that include accuracy, recall, precision, F1-score, and confusion matrix [49].

1.1. Accuracy

Accuracy can be a measure of correctly labelled instances in a dataset relative to the overall total number of instances in the dataset. This matrix is mostly utilized to evaluate algorithm performance in classification problems [49, 50, 51]. This is defined as shown in equation (1):

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

Which is the ratio of accurately classified data instances against the total number of observations.

1.2. Recall

Recall can be a measure of relevant data instances selected in a specific class. In actual fact, recall determines how many of the actual positives have been predicted by the algorithm [49, 50, 51]. Recall is defined as shown in equation (2):

$$Recall = \frac{TP}{TP + FN} \quad (2)$$

Which is equal to the number of true positives divided by true positives plus false negatives

1.3. Precision

Precision determines what number of data selected instances that are relevant. How many of the data instances observed by an algorithm are actually correct is referred to as precision [49, 50, 51]. Precision is defined as shown in equation (3):

$$Precision = \frac{TP}{TP + FP} \quad (3)$$

Which is equal to true positives divided by true positives plus false positives.

1.4. F1 Score

F1-Score which is also referred to as f-measure focuses in both recall and precision in order to determine the performance of an algorithm. It computes the harmonic mean of both recall and precision utilizing false negatives and positives [49, 50, 51]. F1-Score is defined as shown in the equation (4).

$$F1 - Score = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (4)$$

1.5. Confusion matrix

The confusion matrix determines the correct and incorrect predictions observed by the algorithm. It assists in evaluating algorithm performance. The algorithm's effectiveness may be evaluated by its time, meaning "how quickly the algorithm can take to compute a given model [49].

These metrics display quantitative instruments of how well the algorithms are able to detect and prevent DDoS attacks in IoT [51].

I. Methodology

This systematic literature review of IoT ML algorithms was compiled by making use PRISMA approach. Keywords such as IoT ML algorithms were used in a search in reliable databases such as IEEE Xplore, Web of Science, Scopus, and Google Scholar. Google Scholar was mostly utilized for its ability to generate more articles that are easy to open and download [52]. Previous research papers that are not older than 2018 were reviewed. The research papers from 2020 to 2024 contributed 95% of this work, and this is due to their most updated level of contribution on the topic of ML algorithm challenges for detecting and preventing DDoS attacks in IoT networks.

An initial total of 830 articles were identified through database searches. After removing duplicates and screening titles and abstracts for relevance, 311 articles were retained for full-text assessment. Following a rigorous eligibility review based on inclusion and exclusion criteria, a final set of 55 articles was included in the synthesis, as depicted in the PRISMA flow diagram (see Figure 10).

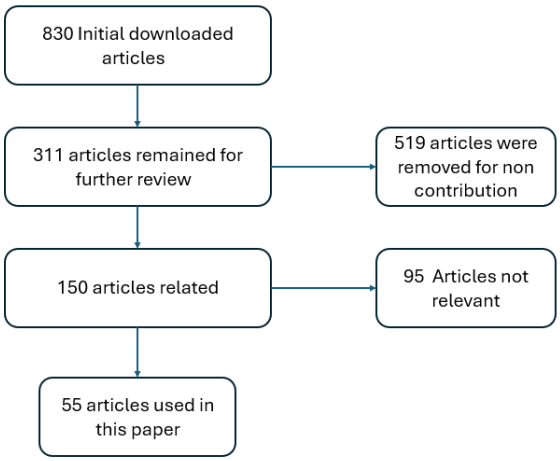

Figure 10. Article Selection Process

J. Results and Lessons learnt

The performance metrics measure the effectiveness of the mechanism to detect and prevent DDoS attacks in IoT networks [49]. Anomalies and attack prediction metrics such as accuracy, recall, precision, F1-score, and confusion matrix are relevant in evaluating performance for machine learning techniques to detect and prevent DDoS attacks in IoT.

The PRISMA approach assisted in the exclusion and selection of relevant articles used in this paper. There are 55 articles selected for further analysis in this research, as shown in Figure 10. These are articles from 2018 to 2024.

1. ML algorithms used in IoT networks

Several articles proposed ML techniques to detect DDoS attacks in IoT networks as summarized in Table 2 [29, 30, 31, 35, 42]. The algorithms used include the following: DT, NN, DNN, BP, XGBoost, J48, MLP, CNN, LSTM, eXtreme, RF, NB, GB, and SVM, DT, LR, MLP, and KNN. The KNN is leading in several studies and is followed by CNN, while the lowest one is the DT.

2. DDoS attacks: Datasets used in IoT networks

The selected articles have shown different datasets used in the past to implement DDoS attacks simulation in IoT networks. The choice was to select between private and public datasets, with public datasets being mainly selected due to their ease of access. The private datasets are normally not freely available due to the security concerns they come with.

In the selected articles, the following datasets are used, namely: Eddge-IIoTset, synthesis dataset, CICDDoS2029, One-R, CICIDS2018, NSL KDD, InSDN, latest SDN dataset, KDDCup99, UNSW-NB15, CICIDS2017, CICDDoS2019, CICFlowMeter, ToN-IoT, ISCX-12, and HL-IoT and UNSW-NB15 [30, 35, 38, 40].

Table 3. Summarizes the datasets and algorithms used

Datasets	Number of Studies	Algorithm	Performance Metrics	References

NSL KDD	10	CNN, SVM, RF, PCA, DT, LR, KNN, MLP, LR, NFV	Accuracy, recall, and precision	[20, 22, 23, 25, 27, 31, 32, 37, 40]
Eddge-IIoTset	2	FMDADM	Precision, accuracy, F-Measure, Recall, Negative predictive rate, and false negative rate	[30, 40]
CICDDoS2029	8	Naïve Bayes, KNN, RF, XGBoost, SVM, AdaBoost	Accuracy, Recall,	[20, 25, 31, 40]
One-R	2	One-R	Data preparation, classification, visualization, regression, and association rule mining	[33]
CICIDS2018	3	NIDO	Classification, Precision, False Positive, and Confusion Matrix	[35, 40]
InSDN	3	LEDEM, LSTM, CNN, DL, KNN	Precision, accuracy, and recall	[36, 45]
KDDCup99	5	CNN, SVM, RF	Accuracy, precision, and recall	[25, 37, 38, 40, 46]
UNSW-NB15	5	CNN, SVM, RF, KNN	Accuracy, precision, and recall	[20, 24, 37, 40, 46]
CICDS2017	6	CNN, SVM, RF, LSTM	Accuracy, Precision, and recall	[20, 22, 25, 27, 40]
CICDDoS2019	5	CNN, SVM, RF, AdaBoost, XGBoost, RF, NB, GB	Prediction time, recall, precision, f1-score, accuracy	[20, 27, 31, 37, 40]
ToN-IoT	3	LSTM, CNN, DEEPShield	Accuracy	[31, 40]
HL-IoT	1	LSTM, CNN, DEEPShield	Accuracy	[40]
Synthesis Dataset	2	DT, NN, DNN, BP, XGBoost, J48, MLP, KNN, SVM, RF,	Accuracy, Precision	[31]

Table 3 provides an overview of the performance metrics employed by various researchers in evaluating their proposed models. The most used metrics are the anomalies and attach prediction metrics, namely: Accuracy, Recall, Confusion Matrix, F1-score, and precision. Anomalies and attack prediction metrics are the best performance metrics for DDoS attack prediction.

K. Conclusion and Future Work

This paper presented a review of different types of DDoS attacks and their impact on the IoT network. Literature shows that DDoS attacks are still among the major risks to the security of IoT networks, as attackers are increasing their ways of penetrating the IoT networks by utilizing different compromised nodes to flood the target network with traffic and eventually deplete its resources. We also presented different techniques utilized in the past to detect and prevent DDoS attacks and highlighted their shortcomings when faced with accuracy and precision classification under large network traffic. The categories of IoT performance metrics and their statistics were presented. Future work will focus on conducting a review of different datasets suitable for offering real-time DDoS attack detection.

L. References

[1] Zewdie, T.G. & Girma, A., 2020. IOT Security and the Role of AI/ML to Combat Emerging Cyber Threats in Cloud Computing Environment. 4, 253-263

[2] Chen, Y., 2020. IoT, Cloud, Big data and AI in Interdisciplinary Domains, Simulation Modelling Practice and Theory, 102, 102070

[3] Bobrovnikova, K. Lysenko, S. Hurman, I. Kwiecien, A., 2022. Machine Learning Based Techniques for Cyberattacks Detection in the Internet of Things Infrastructure. 23-25

[4] Seyed, C., Kebe, M., Arby, M.M, Mohmoud, M.B, & Seyidi, C.M.C., 2023. Cybersecurity Mechanism for Automatic Detection of IoT Intrusions Using Machine Learning. Journal of Computer Science, 20, 44-51

[5] Alsamiri, J. & Alsubhi, K., 2019. Internet of Things Cyber Attacks Detection using Machine Learning. International Journal of Advanced Computer Science and Applications (IJICT).12

[6] Seyed, C., Kebe, M., Arby, M.M, Mohmoud, M.B, & Seyidi, C.M.C., 2023. Cybersecurity Mechanism for Automatic Detection of IoT Intrusions Using Machine Learning. Journal of Computer Science, Vol.1, Issue 20.

[7] Mishra, N. & Pandya, S., 2021. Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions. IEEE Access, 9: 59353-59377.

[8] Bharati, S. & Podder, P., 2022. Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions.

[9] Alwahedi, F., Aldhaheri, A., Ferrag, M.A., Battah, A., & Tihanyi, N., 2024. Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. Internet of Things and Cyber-Physical Systems, 4, 167-185.

[10] Sasi, T., Lashkari, A.H, Lu, R., Xiong, P., & Iqbal, S., 2023. A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges, Journal of Information and Intelligence, https://doi.org/10.1016/j.jiixd.2023.12.001.

[11] Tawalbeh, L., Muheidat, F, Tawalbeh, M., & Quwaider, M., 2020. IoT Privacy and Security: Challenges and Solutions,

[12] Alwahedi, F., Aldhaheri, A., Ferrag, M.A., Battah, A., & Tihanyi, N., 2024. Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. Internet of Things and Cyber-Physical Systems, 4, 167-185.

[13] Kuar, R., 2024. Internet of Things: An Overview, International Journal for Multidisciplinary Research (IJFMR), Vol 6. 2.
[14] Alahmadi, A.A., Aljabri, M., Alhaidari, F., Alharthi, D.J., Rayani, G.E., Marghalani, L.A., Alotaibi, O.B., & Bajandouh, S.A., 2023. DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions. https://doi.org/10.3390/electronics12143103
[15] Ismail, S., Hassen, H.R., Just, M & Zantout, H., 2021. A review of amplification-based distributed denial of service attacks and their mitigation. Computers and Security, vol. 109, 102380. https://doi.org/10.1016/j.cose.2021.102380
[16] Lukaseder, T., Stölzle, K., Kleber, S., Erb, B., & Kargl, F., 2018. An SDN-based Approach for Defending against Reflective DDoS Attacks. In Proceedings of the 2018 IEEE 43rd Conference on Local Computer Networks (LCN), Chicago, IL, USA, 1–4 October.
[17] Mohammed, I.K., & Mahdi, N.J., 2021. The Current Trends of DDoS Detection in SDN Environment. 2nd Information Technology To Enhance e-learning and Other Application (IT-ELA).9, 29-34.
[18] Omer, A., Semih, S.A, Merve, O., Abdullar, A.Y., & Erdal, A., 2023. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions, Journal of Information and Intelligence, 12, 1333. https://doi.org/10.3390/electronics12061333
[19] Lee, S.H., Shiue, Y.L., Cheng, C.H., Li, Y.H., & Huang, Y.F., 2022. Detection and Prevention of DDoS Attacks on the IoT. Appl. Sci. 2022, 12,12407. https://doi.org/10.3390/app122312407https://doi.org/10.3390/
[20] Ravi, N., Shalinie, S.M.J, 2020. Learning-Driven Detection and Mitigationof DDoS Attack in IoT via SDN-Cloud Architecture. IEEE Internet Things. 7, 3559–3570.
[21] Simsek, M.M., & Atilgan, E., 2024., DoS and DDoS Attacks on Internet of Things and Their Detection by Machine Learning Algorithm. DUJE (Dicle University Journal of Engineering) 15: 2, 341-353
[22] Wang, F., Jiang, D., Wen, H., & Song, H., 2019. Adaboost-based security level classification of mobile intelligent terminals. J. Supercomput., vol. 75, no. 11, 7460–7478, doi: 10.1007/s11227-019-02954-y.
[23] Douiba, M., Benkirane, S., Guezzaz, A., & Azrour, M., 2023. An improved anomaly detection model for IoT security using decision tree and gradient boosting. J. Supercomput., vol. 79, no. 3, 3392–3411, Feb. 2023, doi: 10.1007/s11227-022-04783-y.
[24] Aamir, M., Rizvi, S.S.H, Guezzaz, A., Hashmani, M.A., Zubair, M., & Usman, J.A., 2021. Machine Learning Classification of Port Scanning and DDoS Attacks: A Comparative Analysis. Mehran Univ. Res. J. Eng. Technol., vol. 40, no. 1, pp. 215–229, Jan. 2021, doi: 10.22581/muet1982.2101.19.
[25] Mohy-eddine, M., Guezzaz, A., Benkirane, S., & Azrour, M., 2021. An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection. Multimed. Tools Appl., vol. 82, no. 15, pp. 23615–23633, doi: 10.1007/s11042-023-14795-2.
[26] Mubarakali, A., Srinivasan, K., Mukhalid, R., Jaganathan, S.C.B., & Marina, N., 2020. Security challenges in internet of things: Distributed denial of service attack detection using support vector machine-based expert systems. Comput. Intell., vol. 36, 4, 1580–159, doi: 10.1111/coin.12293.

[27] Mehmood, A., Mukherjee, M., Ahmed, S.H., Song, H., & Malik, K.M., 2018. NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks. J. Supercomput., vol. 74, 10, 5156–5170, doi: 10.1007/s11227- 018-2413-7.

[28] Prathapchandran, K., & Janani, T., 2021. A Trust-Based Security Model to Detect Misbehaving Nodes in Internet of Things (IoT) Environment using Logistic Regression. J. Phys. Conf. Ser., vol. 1850, 1, 012031, doi: 10.1088/1742-6596/1850/1/012031.

[29] Shire, R., Shiaeles, S., Bendiab, K., Ghita, B., & Kolokotronis, N., 2021. Malware Squid: A novelIoT Malware Traffic Analysis Framework Using Convolutional Neural Network and Binary Visualisation. 10.1007/978-3-030-30859-9_6.

[30] Khedr, W.I, Gouda, A.E, & Mohamed, R.E., 2023. FMDADM: A Multi-Layer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks, Vol.11, 20.

[31] Bukhowah, R., Aljughaiman, A., & Rahman, M.M.H.A., 2024. Detection of DoS Attacks for IoT in Information-Centric Networks Using Machine Learning: Opportunities, Challenges, and Future Research Directions, 13, 6 -1031; https://doi.org/10.3390/electronics13061031.

[32] Sanjeevini, S.H., Sreeja, M., Madhuri, S., Mohanty, S.T., & Jhansi, P., 2024. DDoSNET: Detection and Classification of DDoS Attacks in IoT Environment. IRACST-International Journal of Computer Networks and Wireless Communications (IJCNWC). Vol.14, 1

[33] Seyed, C., Kebe, M., Arby, M.M, Mohmoud, M.B, & Seyidi, C.M.C., 2023. Cybersecurity Mechanism for Automatic Detection of IoT Intrusions Using Machine Learning. Journal of Computer Science, Vol.1, 20.

[34] Williams, P., Dutta, I.K., Daoud, H. & Bayoumi, M., 2022. A Survey on Security in Internet of Things with a Focus on the Impact of Emerging Technologies. Journal Homepage: www.sciencedirect.com/journal/internet-of-things

[35] Seyed, C., Roux, J., Ngo, B., & Kebe, M., 2023. Proposal of a Machine Learning-based Model to Optimize the Detection of Cyber-attacks in the Internet of Things. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol, 14. 11.

[36] Ravi, N., & Shalinie, S.M., 2020. Learning-Driven Detection and Mitigation of DDoS attack in IoT via SDN-Cloud Architecture. IEEE Internet Things J., vol. 7, 4, 3559–3570, doi: 10.1109/JIOT.2020.2973176.

[37] Bagaa, M., Taleb, T., Bernabe, J.B., & Skarmeta, A., 2020. A Machine Learning Security Framework for IoT systems,'' IEEE Access, vol. 8, 114066–114077, doi: 10.1109/ACCESS.2020.2996214

[38] Abdallah, M., An Le Khae, N., Jahromi, H., & Jurcut, A.D., 2021. A Hybrid CNN-LSTM Based Approach for Anomaly Detection Systems in SDNs. The 16th International Conference on Availability, Reliability and Security, https://doi.org/10.1145/3465481.3469190

[39] ElSayed, S.M., Le-Khac, N.A., Albahar, M.A., & Jurcut, A., 2018. A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique. Journal of Network and Computer Applications, https://doi.org/10.1016/j.jnca.2021.103160

[40] Najafimehr, M., Zarifzadeh, S., & Mostafavi, S., 2023. DDoS attacks and machine-learning-based detection methods: Department of Computer Engineering. https://doi.org/10.1002/eng2.12697
[41] Dash, S.K., Dash, S., Mahapatra, S., Mohanty, S.N., Khan, M.I., Medani, M., Abdullaev, S., & Gupta, M., 2024. Enhancing DDoS attack detection in IoT using PCA, Egyptian Informatics Journal, https://doi.org/10.1016/j.eij.2024.100450.
[42] Pandey, N. & Mishra, P.K., 2023. Detection of DDoS attack in IoT traffic using ensemble machine learning techniques. Networks and Heterogeneous Media, http://www.aimspress.com/journal/nhm.
[43] Singh, C. & Jain, A.K., 2023. Detection and Mitigation of DDoS Attacks on SDN Controller in IoT Network using Gini Impurity. https://doi.org/10.21203/rs.3.rs-2991752/v1.
[44] Saiyed, M.F, & Al-Anbagi, I., 2024. Deep Ensemble Learning with Pruning for DDoS Attack Detection in IoT Networks. Vol 2.
[45] Ravi, V., Chaganti, R., & Alazab, M., 2022. Deep Learning Feature Fusion Approach for Intrusion Detection System in SDN-based IoT Networks. IEEE Internet of Things magazine, DOI: 10.1109/IOTM.003.2200001.
[46] Kumar, N. & Sharma, S., 2023. A Hybrid Modified Deep Learning Architecture for Intrusion Detection System with Optimal Feature Selection. Electronics, Vol 12, No. 19, 4050; https://doi.org/10.3390/electronics12194050.
[47] Moulla, D.K., Mnkandla, E., & Abran, A., 2023. Systematic Literature Review of IoT metrics. Applied Computer Science, vol. 19, no. 1, pp. 64–81. doi: 10.35784/acs-2023-05
[48] Calderon, G., Campo, G., Saavedra, E., & Santamaria, A., 2023. Monitoring Framework for the Performance Evaluation of an IoT Platform with Elasticsearch and Apache Kafka. Information Systems Frontiers. pp184-191. https://doi.org/10.1007/s10796-023-10409-2
[49] Vakili, M., Ghamsari, M., & Rezel, M., 2020. Performance Analysis and Comparison of Machine and Deep Learning Algorithms for IoT Data Classification. DOI:10.48550/arXiv.2001.09636
[50] Elmahfoud, E., Elhajla, S., Maleh, Y., & Mounir, S., 2024. Machine Learning Algorithms for Intrusion Detection in IoT Prediction and Performance Analysis. International Symposium on Green Technologies and Applications (ISGTA'2023). Procedia Computer Science. pp460-467.
[51] Berqia, A., Bouijij, H., & Merimi, A., 2024, Detecting DDoS Attacks using Machine Learning in IoT Environment, Conference on Intelligent Systems and Computer, DOI:10.1109/ISCV60512.2024.10620122
[52] Hashim, H.S, Hassan, Z.B, & Drus, S.B.M., 2023. Internet of Things: A systematic Literature Review– Overview Paper, Informatica, Vol 46, pp135–146

Appendix A: Glossary

Acronym	Description
ADP	Average Drop Rate
AI	Artificial Intelligence
ASCII	American Standard Code for Information Interchange
CNN	Convolution Neural Network
DCMF	Double-Check Mapping Function
DDoS	Distributed Dineal of Service
DT	Decision Tree
FMDADM	Four-Model DDoS Attack Detection and Mitigating
GRU	Gated Recurrent Unit
IoT	Internet of Things
KNN	K-Nearest Neighbors
LEDEM	Learning-Driven Detection Mitigation
LR	Linear Regression
LSTM	Long Short-Term Memory Network
MATLAB	Matrix Laboratory
ML	Machine Learning
MLBS	Machine Learning-Based Security algorithm
RF	Random Forest
SDN	Software-Defined Network
SQL	Structured Query Language
SVM	Support Vector Machine
TV	Television
HTTP	Hypertext Transfer Protocol
DNS	Domain Name System
IRC	Internet Relay Chat
P2P	Peer-to-Peer
ICMP	Internet Control Message Protocol
TCP	Transmission Control Protocol