Library Progress International
Vol.44 No.3, Jul-Dec 2024: P.6295-6315

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

A Comprehensive Review on Security of Internet of Things using Machine Learning: Threats, Recent Advancements and Challenges

Muskan Garg[1,*] and Dr. Sima[2]

Research Scholar, Computer Science (FPA), DLCSUPVA, Rohtak, Haryana, India[1]
garg04muskan@gmail.com
Associate Professor, Faculty of Planning and Architecture, DLCSUPVA, Rohtak, Haryana, India[2]
simasingh.2009@gmail.com
(garg04muskan@gmail.com)

How to cite this article: Muskan Garg, Sima (2024). A Comprehensive Review on Security of Internet of Things using Machine Learning: Threats, Recent Advancements and Challenges. *Library Progress International,* 44(3), 6295-6315

ABSTRACT

As technology has advanced, Internet of Things (IoT) devices have become more prevalent in daily life. However, as more people use IoT devices, their security becomes a bigger concern for both manufacturers and users. Despite considerable efforts from the researchers, improving the detection accuracy while minimizing false positives and effectively identifying new types of security breaches remain critical issues. Recently, techniques such as deep learning and machine learning have been explored as potential solutions to improve the security of Internet of Things devices. This study offers an approach for safeguarding IoT environments based on major ML and DL techniques. It categorizes selected studies according to the specific ML/DL algorithms applied. Additionally, this review comprehensively examines the latest advancements in ML and DL approaches by detailing their methodologies, evaluation metrics, and choice of datasets. By identifying the limitations of current methods, this work outlines research challenges and suggestions for future investigation to improve the security of IoT devices.

Keywords: Internet of Things (IoT); Security; Threats; Machine Learning (ML); and Deep Learning (DL).

1. INTRODUCTION

Internet of Things defines a network of interconnected components that are integrated with sensors and actuators that may communicate and share data with other objects and networks. Its popularity has surged recently, significantly influencing everyday living[1]. Given the swift expansion of IoT, linking billions of devices that communicate through the internet, these devices are now present in homes, workplaces, transportation, alarm systems, healthcare, telecommunications, agriculture, and various other environments. As the IoT ecosystem is not just a singular network of computing devices [2], its integration across various devices heightens concerns regarding security and privacy. IoT devices lack inherent security measures, rendering them susceptible to potential attacks. Moreover, the transition from physically isolated systems to Internet-connected, remotely managed devices have broadened the attack surface, increasing vulnerability compared to traditional networks. This increased susceptibility to the IoT is attributed to its distinctive characteristics and the utilization of layered protocols, making it challenging to comprehend underlying security issues. Security requirements within the IoT systems vary across applications, resulting in diverse security solutions. In recent years, machine learning has developed into a useful tool in many different applications. This evolution is particularly evident in Internet of Things (IoT) systems. ML/DL methods transform security measures beyond essential communication to develop intelligence-based security systems. This research provides an extensive examination of machine learning strategies and the latest advancements in deep learning techniques for improving the security of IoT systems. It also compares current studies to evaluate the effectiveness and practicality of employing ML/DL approaches to enhance IoT security. This

involves addressing challenges and investigating opportunities to identify potential avenues for future research. The document critically analyses existing ML/DL techniques that are currently being used to enhance IoT security, exploring the potential, advantages, and limitations of each technique. The main contributions of this study are:

1. It reviews how ML and DL approaches are used to strengthen IoT system security.
2. It offers a detailed examination of different ML and DL models, providing a comparative analysis to outline their features and applications.
3. It discusses the significant challenges in applying ML and DL algorithms safeguarding IoT environments to unlock new research directions.

The paper is structured as follows: The methodology used in this study is discussed in section 2. Section 3 provides an introduction to the structure of IoT systems, highlighting the security concerns. An extensive survey of the literature is presented in section 4. In Section 5, previously proposed methods are analyzed and the potential for applying ML and DL methodologies to improve the security of IoT systems is examined. Section 6 elaborates on the findings and outlines directions for future investigations. Section 7 concludes the key points of this study.

2. METHODOLOGY

IoT security has recently experienced notable expansion owing to the increasing number of researchers intrigued by this particular domain. This study classifies the relevant studies based on IoT security. A comprehensive examination of the existing literature reveals that ML and DL based approaches significantly enhance IoT security. Initially, an extensive literature survey was conducted by using the AND OR operators, about topics such as IoT, cyberattacks, security, machine learning, deep learning, threats, and vulnerabilities from various scientific databases: IEEE, Scopus, Springer, Wiley, Web of Science, and Science Direct. This screening yielded 17,700 records, as identified by the literature search. To gain further insights into the utilization of ML in improving IoT security, this research focused on publications centred around machine-learning-based approaches. A limited number of articles were reviewed, and this review aimed to establish standards for ML and DL research criteria and methodology. After the initial search, papers published between 2015 and the present were selected, reducing the selection to 14,900. During the systematic selection phase, , a systematic selection process was carried out to select studies based on criteria such as their relevance to ML/DL application in enhancing IoT security, the reputation of the publishing journal, the originality of the work, and the length of the study. After thorough reading and careful examination, 64 studies were deemed suitable for the review. The chosen papers' distribution across different years is depicted in Figure 1. These selected studies were thoroughly analyzed and synthesized to create an comprehensive review, providing a thorough analysis of the relationship between ML/DL and IoT security.

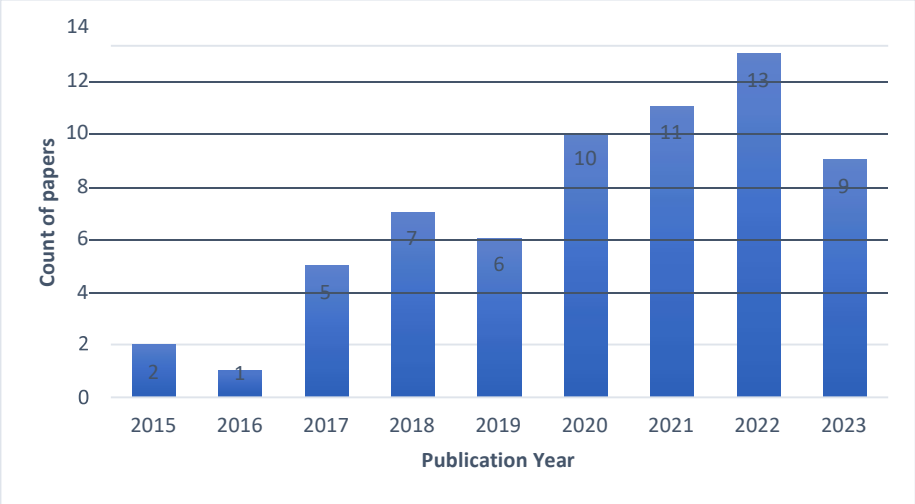

Figure 1 Year-wise distribution of papers

3. BACKGROUND

This segment provides an introduction to the structure of IoT systems, highlighting the security concerns and

necessities associated with the different layers of IoT, aiming to facilitate the readers' comprehension and enhance their understanding of IoT security issues.

3.1 IoT System

A fundamental IoT architecture is structured around three layers: physical layer, network layer, and application layer, as depicted in figure 2.

The physical layer consists of concrete components like sensors and actuators, which are crucial for gathering live data via various communication tools .

The network layer bears the responsibility of establishing secure connections among network devices. Furthermore, it facilitates transmitting and manipulating the data captured by sensors.

The purpose of the application layer is providing application-specific services, like those found in smart cities, smart healthcare, and smart home settings. Security risks can especially affect this layer. To counteract this, a machine learning technique can be incorporated to guarantee the IoT network's dependability and security [3]. Furthermore, additional networking support technologies like network processing, external middleware, and distributed technology are frequently incorporated into Internet of Things solutions, adding an additional layer of data handling.

3.2 IoT Security Threats

The IoT architecture is vulnerable to attacks at every layer. IoT provides users with useful and effective services, but because of device vulnerabilities and the diversity of network systems, it also raises serious issues related to privacy and security. When creating a successful IoT security solution, the following key security aspects need to be taken into consideration:

Confidentiality: Confidentiality means that no unauthorized parties can access the sensitive data on IoT devices. However, maintaining confidentiality is challenging due to the massive volumes of data generated by the widespread use of IoT devices, especially as data moves from the perception layer to cloud storage, exposing system data to potential breaches.

Authentication: Verifying the identity of users or devices before granting access is essential. The authentication process can vary significantly across IoT systems, depending on their security vs. flexibility needs. Designing an authentication system requires a careful balance between meeting system needs and adhering to security constraints, considering the specific characteristics of the devices involved.

Authorization: This involves granting access rights to an IoT system, which could be to services, humans, ormachines. Actions should only be performed with the proper authorization of the requester. The challenge in IoT settings is to effectively manage access rights, especially for physical sensor devices that need to interactwith the system.

Integrity: There are different integrity requirements for IoT systems. Integrity features are essential for an efficient checking method to identify any alterations made during communication over an unsecured wireless network. Restricting data access to authorized entities can enhance the integrity of the device information. Since a significant amount of data is transferred via wireless networks, cyberattacks can more easily target the Internet of Things [4]. Integrity guarantees a quick and easy verification procedure for identifying communication changes using an unsecured wireless network. If integrity breaches are not identified early on, it can hinder devices' primary functionalities.

Availability: IoT systems must constantly make their services available to authorized entities. Both hardware and software are necessary for data availability in Internet of Things systems. Hardware availability refers to the ease with which IoT devices can access the data. In contrast, software availability deals with the requirement that services offered to end users be approved before being accessed. Threats like denial-of- service attacks or active jamming can severely impact IoT devices and systems, making it critical to ensure uninterrupted access to IoT services for users.

Non-repudiation: Securing the data exchanged between two systems is ensured by non-repudiation. Since non-repudiation offers evidence of the data's origin, dependability, and integrity, it ensures that the validity of the data cannot be disputed. All these security attributes should be considered for an efficient IoT security

solution. The vulnerabilities ateach layer of the IoT architecture give rise to these security challenges, which can be mitigated using variousstrategies detailed in Section 6 of this document.

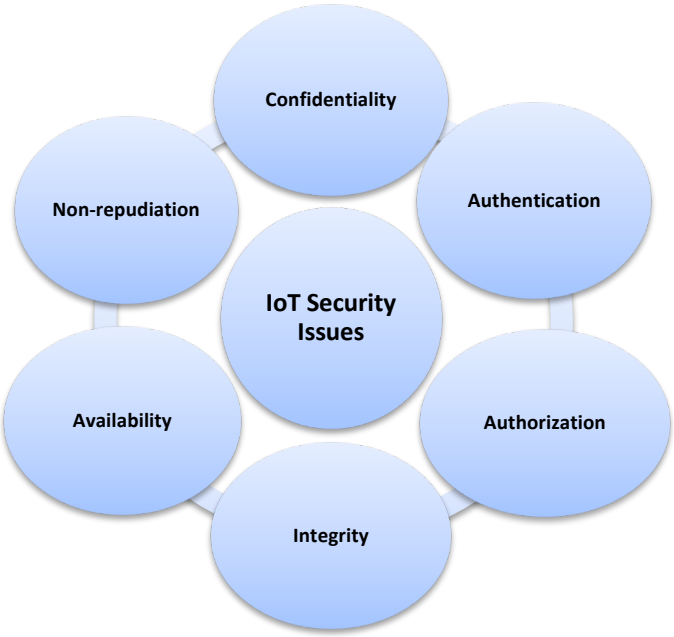

Figure 2 IoT Security Issues

3.3 Security Attacks and IoT Layers

The security attacks in Internet of Things architecture vary depending upon the layer. Researchers conducted rigorous analyses to assess the most prevalent security concerns [5]. Table 1 demonstrates the major security attacks and challenges that each layer faces. Various machine learning algorithms are being employed to meet the security requirements listed in the table, which are covered in depth in Section 7 of the paper. Each layer in the IoT architecture has its own set of functions. The perception layer, consisting of various sensors and devices, mainly employs access control, basic encryption, and node verification to protect IoT environments. The network layer, responsible for data transmission, is vulnerable to various security threats including phishing for sensitive information like passwords, denial of service assaults, routing attacks, data breaches, identity verification challenges, and encryption needs [6]. The user is provided with services by the application layer. It handles various security issues, including programming, malicious code, data leaks, attacks on access control, service disruptions, and software defects. Table 1 shows the layers and attacks associated with each layer.

4. RELATED LITERATURE

[7] Proposed a deep learning method for detecting anomalies that combined deep belief network (DBN) and Restricted Boltzmann Machine (RBM) with a single hidden layer for the purpose of unsupervised feature diminution. This strategy successfully identified anomalies with a 97.9% accuracy rate on the DARPA KDDCUP'99 dataset.

Table 1 Security Attacks based on IoT layers

Layer	Attacks	Description	Security Challenges
Physical	Eavesdropping[8]	To intercept and collect data over the network	Data confidentiality, Integration
	Tampering	Manipulating hardware, Altering software or modification of data.	Authorization, Integration, Privacy

	Malicious Node Injection Attack[9]	Introduction of malicious nodes into the network	Integrity, Confidentiality, Availability
Network	DoS/DDoS Attack [10]	Making the target unavailable by flooding it with illegitimate traffic	Availability, reliability, Network Congestion, Authorization, Access control, and Heterogeneity
	Sinkhole Attack	Malicious nodes redirect network traffic.	Authorization, Confidentiality, Traffic Manipulation
	Packet Sniffing	Intercepting and monitoring packets over the network	Confidentiality, Access control
	Replay Attack	Intercept data packets over the network, save them for later use and replay them back to the network.	Authentication, Data Integrity, Availability
	Sybil attack	Fake identities or Sybil nodes are used to take control of the peer network.	Data integrity, Trust Establishment
Application	Malware [11]	Malicious software or programs are deployed into a device or network with the content of causing harm.	Confidentiality, Integration, Availability
	Phishing Attack	A fraudulent email, message, or website that appears to be from a legitimate source gains credentials and access to the victim and damages data.	Data confidentiality, Integrity breach
	Malicious Code Injection	Untrusted data is injected into the target system through vulnerable entry points.	Authorization, Data breaches
	Web/DoS/DDoS Attack	Sending numerous random packets at a high speed to the intended IoT device, hence impeding the system's services.	Confidentiality, Integrity, Availability
	Man-in-the-middle attack	A malicious entity intercepts between two communicating parties.	Confidentiality, Integration, Authentication

[12] Designed a deep learning framework for detecting cyberattacks in mobile cloud environments, demonstrating a high accuracy of 97.11%.

[13] Presented an intrusion detection system utilizing deep belief networks. After fifty cycles and only 40% of the entire dataset utilized for training, the proposed DBN-based intrusion detection system achieved a testing accuracy of approximately 97.5%, outperforming the current DBN-SVM-based system.

[14] Proposed a framework using recurrent neural network to identify intrusions (RNN-IDS). When assessing its effectiveness against traditional machine learning strategies for both binary and multiclass categorization, the RNN-IDS method proved to be superior, delivering more accurate classification models in both scenarios.

[15] Developed an innovative, multi-tiered intrusion detection framework that blends extreme learning machines and support vector machines. This method aims to enhance the detection of both existing and emerging cyber threats. A key feature of this approach is the development of an optimized training dataset, achieved through a refined K-means algorithm. This optimization not only improves the detection system's accuracy but also reduces the time required for classifier training. Utilizing the KDD Cup 1999 dataset for evaluation, this model demonstrated a accuracy rate of 95.75% and superior attack detection capabilities when compared to other models evaluated with the same dataset.

[16] Presented a Naïve Bayes algorithm-based drone cybersecurity solution for the Internet of Things. Through network, drone, and IoT sensor data analysis, the system can identify security patterns that help detect attacks. This approach was validated on two different datasets, where it achieved a 96.3% success rate in detecting

attacks in real-time, outperforming existing machine learning methods. Despite its successes, it's important to note that the Naïve Bayes algorithm's assumption of data independence may limit the model's effectiveness.

[17] Developed three-tiered IDS that uses supervised learning to find intrusions on IoT networks. The three primary tasks of this framework is to classify each connected IoT device's typical behaviour, detect malicious packets during an attack, and categorize the kind of assault carried out. Eight well-known, commercially available devices are used in a smart home testbed where the system is assessed. The system's efficacy is evaluated by implementing 12 attacks from four major categories and four multistage attack scenarios with intricate sequences of events. The system's ability to automatically distinguish between malicious and benign network traffic and identify successful assaults on connected devices is demonstrated by an F-measure of 96.2%, 90.0%, and 98.0%.

[18] Presented a security framework named Intrusion Detection Tree (IntruDTree), focusing on enhancing security via minimizing the feature dimensions, thus cutting down computational expenses and boosting predictive accuracy. As part of this, cybersecurity data is used to analyse the performance using ROC, accuracy, precision, f-score, and recall metrics. The model's efficacy is then confirmed by comparing it to other well established algorithms such as LR, KNN, SVMs, and the Naive Bayes classifier. [19] proposed a new approach for detecting wormholes in IoT networks, utilizing federated deep learning alongside a Dynamic Trust Factor (DTF) and employing CNN and LSTM models for ensuring security of the data at the node level. This method not only reaches a 96% success rate but also benefits from being lightweight due to its cascaded and federated learning structure.

[20] Highlighted the use of machine learning to improve DDoS attack detection accuracy using the CICIDS 2017 and CICDDoS 2019 datasets. After choosing pertinent features, the researchers input them into machine learning algorithms using the MI and RFFI techniques. Compared to previous approaches, the findings demonstrated improved accuracy for RF with utilizing 16 features and and another method using 19 features. For future DDoS and other threat detection, the researchers advised employing wrapper feature selection techniques like sequential feature selection using neural networks.

This study stands out in the IoT field by covering all three dimensions: ML/DL approaches, specific measures and functions, and IoT difficulties, setting it apart from previous works. It provides an extensive review of recent studies from 2015 to 2023, making it a comprehensive source for understanding the latest trends in IoT security and the role of the ML/DL techniques in this. This makes the study a significant resource to grasp the current landscape of IoT research, offering a thorough and contemporary overview of new methodologies.

5. MACHINE LEARNING AND DEEP LEARNING POTENTIAL FOR IOT SECURITY

Devices and networks can be effectively protected against known threats by using conventional security methods. Though growing more frequently in IoT systems, they fail to recognize and react to new risks and zero-day assaults. Furthermore, due to the dynamic and complex nature of Internet of Things systems, standard security techniques may be resource-intensive and unsuitable. Significant advancements across multiple sectors have been made possible by Machine Learning. These algorithms manage the development of machines that advance autonomously with experience. The development of low-cost techniques, the widespread availability of large datasets, and the development of new algorithmic methodologies have all contributed greatly to the advancement of learning algorithms. The domains of deep learning (DL) and machine learning (ML) have advanced substantially in the last few years, moving from experimental stages to indispensable tools with a wide range of applications. Although DL is a subfield of ML, this discussion

differentiates between traditional ML techniques, which requires engineered features and DL techniques. Deep learning represents a modern approach in learning methodologies, utilizing several layers of non-linear processing for the extraction and transformation of features for pattern recognition in a more discriminative or generative manner.

5.1 Machine Learning (ML) in IoT Security

Based on the traits that define them, machine learning may be divided into multiple categories. These include the following, each with its unique approach: 1) Supervised learning, 2) Unsupervised learning, 3) Semi-supervised learning, and 4) Reinforcement learning.

5.1.1 Supervised Machine Learning

In supervised learning, a model is trained on labelled dataset, enabling it to accurately make predictions or judgments on new, unlabeled data. The main goal these models is to correctly classify new data under the appropriate categories using a variety of techniques and algorithms. This segment covers various supervised machine learning techniques, including benefits, drawbacks, and uses in IoT security. These are a few techniques used in supervised learning.

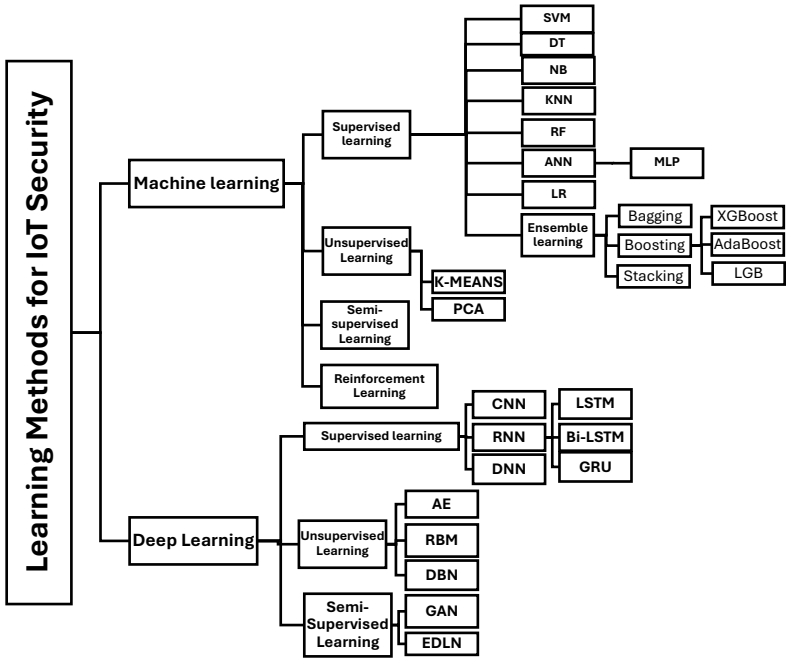

Figure 3 Classification of learning methods used in IoT systems security

Support Vector Machines (SVMs)

Supervised learning techniques, such as SVMs, are appropriate for solving problems related to both regression and classification. They work by creating a multidimensional hyperplane that separates the data points into different groups. Primarily used for binary classification, SVMs can also handle multi-class scenarios by either pairing each class for binary classification or setting one class against all others. The efficiency of SVMs, with a time complexity of $O(N2)$, N being the sample size, makes them a preferred choice for memory storage. Their application is widespread across various security domains, like intrusion detection[21].

[22] to detect impersonation attacks using SVM for feature extraction, showing high effectiveness in both semi-distributed and fully distributed intrusion detection systems (IDS). Moreover, [23] found SVMs to be advantageous in exploiting device security, offering a more effective approach than traditional methods in breaking cryptographic devices, with machine learning techniques further enhancing this capability.

Decision Trees (DTs)

DTs are a type of supervised machine learning algorithm that classifies or makes estimates of outcomes according to a series of decisions or rules based on the attributes of the data. The structure of a DT includes

nodes representing attributes, branches indicating decisions, and leaves denoting outcomes or class labels. DTs are known for their ability to automatically identify and prioritize the most informative features for tree construction, while also trimming non-essential branches to avoid overfitting. Popular DT variants include CART, C4.5, and ID. [24] used feature selection strategies that reduced the total number of features and improve accuracy. They assessed k-nearest neighbour and decision tree as two machine learning techniques for classification. The decision tree approach outperformed the k-nearest neighbour technique, which achieved 94.97% accuracy, with a 98.97% accuracy rate. A simulated Internet of Things network with nine devices— including a doorbell, webcam, baby monitor, thermostat, and security camera—was utilized in the study. The dataset included 502,605 normal packets, 2,835,317 Bashlite packets, and 2,935,131 Mirai packets.

Naïve Bayes (NB)

Bayes' theorem is a statistical principle that uses previous information about an incident to determine the likelihood of the same incident happening again. Naïve Bayes, a simple algorithm for machine learning that assesses the probability of a particular outcome based on the attributes of unlabeled examples, is based on this theorem. In the context of NB classification, it is assumed that each attribute independently influences the likelihood of the outcome being either normal or abnormal. This method has proven effective for identifying network intrusions and anomalies [25]. One key advantage of NB classifiers is their simplicity and ease of implementation. They are versatile, suitable for both binary and multiclass classification, and they don't require a large dataset for training. Moreover, they perform well even when some features are not relevant.

k-Nearest Neighbour (KNN)

This algorithm predicts a data sample's category based on the similarity of its features to those of its neighbours. The choice of k, the number of neighbours to consider, is crucial as it can affect the model's accuracy; too small a value may lead to overfitting, while too large a value can cause misclassification. [26] evaluated different machine learning techniques with a multiclass classifier that employs the looking-back technique to detect denial-of-service (DoS/DDoS) attack. The Bot-IoT dataset has been used to assess the accuracy of this method, which is found to be 99.93% for KNN without the Looking-Back approach and 99.81% for RF with the Looking-Back approach.

Random Forest (RF)

It is another widely used method known for its simplicity and versatility in both regression and classification tasks. This method involves building a collection of decision trees, using the bagging technique to train them, and creating a "forest" of trees. [27] investigated that RF can effectively identify various cyber threats in software-defined networks for the Internet of Things (IoT), with certain features enhancing detection precision. The algorithm's performance slightly decreases with smaller forests but it has the benefit of less computational overhead, which makes it suitable for IoT applications with limited resources.

Artificial Neural Network (ANN)

ANN mimic the human brain's structure with interconnected nodes or neurons and are adept at handling large datasets and complex non-linear relationships. Despite their ability to learn intricately, the complexity of ANNs can slow down the training process. [28] proposed a new approach utilizing KNN, Naive Bayes, and Multi-layer Perceptron, a variant of ANN for detecting DDoS attacks on internet of things network, showing promising results in both balanced and imbalanced datasets in terms of accuracy and AUC scores.

Logistic Regression (LR)

Mostly used for binary classification, logistic regression (LR) uses a logistic function to estimate the probability of an outcome. [29] demonstrated high accuracy in detecting packet-level attacks on IoT networks, utilizing LR, along with five other machine learning classifiers, SVM, RF, DT, KNN, NB indicating its effectiveness in distinguishing between normal and malicious traffic patterns.

Ensemble Learning

Ensemble learning integrates the results from various fundamental classification approaches to generate a combined outcome, enhancing classification accuracy. This technique is predominantly utilized to boost a model's effectiveness. By leveraging multiple models' diversity and complementary attributes, ensemble learning strives to perform better than any individual model could. Methods such as bagging, boosting, and stacking are examples of ensemble learning approaches.

Bagging is primarily used in both classification and regression tasks. It enhances model precision by employing decision trees, significantly reducing variance. This decrease in variance leads to improved accuracy by mitigating the issue of overfitting, a common problem in many predictive models.

Boosting leverage the mistakes made by prior models to improve the accuracy. It does this by integrating several simple models, often called weak learners, to form a robust combined model

Different types of boosting exist, such as Adaptive Boosting(ADB), gradient boosting, Extreme Gradient Boosting (XGB), and Light Gradient Boosting(LGB). In the case of gradient boosting, models are added one after the other to correct the errors of preceding models, with each new model focusing on the residual errors left by its predecessors. This approach uses the gradient descent method to identify and rectify inaccuracies in the learners' predictions.

Adaptive gradient boosting enhances the gradient boosting method by adjusting the learning rate based on the performance of past iterations. This enables the model to learn more efficiently and find the optimal solution more quickly. [30] proposed a method that combines machine learning and feature selection techniques. Their approach employs recursive feature elimination to select features from the NSL-KDD and NBaIoT datasets. The accuracy rate of 99.98% was attained by this hybrid approach, which was higher than the accuracy rate of 99.30% by the independent gradient-boosting classifier.

Extreme Gradient Boosting is a technique that uses Gradient Boosting based on decision trees, where the approach is to create short and simple decision trees iteratively. These trees are called "weak learners" due to their high bias. The process begins by building the first bare tree, which has poor performance, followed by building another tree that can predict what the first tree cannot. This procedure continues until a specified condition, such as reaching a set number of trees, is achieved. An efficient IoT botnet attack detection method is presented by [31] which employs a combination of Fisher-score for selecting relevant features and a genetic algorithm-enhanced extreme gradient boosting (GXGBoost) technique. [32] Presented a predictive model using machine learning and explainable AI (XAI) to identify security threats in HVAC log data. Various machine learning methods, such as Gradient Boosting, ADB, DT, RF, LGB Boosting, XGB, and CatBoost, have been evaluated. With an AUC of 0.9999, accuracy of 0.9998, recall of 0.9996, precision of 1.000, and an F1 Score of 0.9998, the XGBoost classifier performed the best.

LGBM implements a gradient-based one-sided sampling technique for tree splitting, enhancing memory efficiency and accuracy. It opts for leaf-wise development over conventional level-wise expansion, accelerating the process compared to traditional depth-wise expansion methods. [33] used XGB and LGBM for detecting DDoS attacks in IoT networks using BoT-IoT, IoT-23, and CIC-DDoS2019 datasets. Techniques like principal component analysis (PCA) and analysis of variance (ANOVA) were used for feature extraction and selection. The findings demonstrated that these boosting techniques significantly outperformed CDF in terms of accuracy by at least 16%, with LGBM standing out for its efficiency, achieving an accuracy rate of up to 94.79% in less than 54 seconds.

5.1.2 Unsupervised Machine Learning

This section discusses common unsupervised machine learning methods such as principle component analysis (PCA) and k-means clustering, and looks at their benefits, drawbacks, and applications for enhancing the security of IoT systems.

K-Means Clustering

This technique is designed to discover groupings within a dataset based on similar characteristics. It achieves this by determining k number of clusters and assigning each data point to the nearest cluster, with 'k' representing the total clusters to form. The process involves calculating the mean of all points in a cluster to find the centroid and reallocating each point to the cluster closest to it, based on the squared Euclidean distance. This procedure is repeated until points no longer switch clusters, providing a final grouping. Although k-means shows promise, it is found less effective than supervised methods for recognizing previously identified threats.

Principal Component Analysis (PCA)

With the help of PCA, a dataset's number of variables can be decreased while maintaining the majority of the original data's information in a fewer number of variables. The process of reducing potentially correlated variables to a small set of uncorrelated variables known as principle components allows for this reduction. In IoT frameworks, this method is particularly helpful for feature selection involving real-time intrusion detection.

5.1.3 Semi-supervised Machine Learning

A combination between supervised and unsupervised methods is semi-supervised learning. It solves the problem of not having a fully labelled dataset by using both labelled and unlabelled data throughout the training process. It improves the process of learning and may produce better results, although it might not reach the accuracy levels of fully supervised learning methods. Consequently, semi-supervised learning has been less frequently adopted for securing IoT environments.

5.1.4 Reinforcement Learning (RL)

A unique approach in machine learning known as reinforcement learning, involves learning optimal behaviors through trial and error interactions with their environment. Drawing inspiration from behavioral psychology and neuroscience, RL focuses on teaching agents to associate situations with actions that maximize rewards, without pre-existing knowledge of the best actions. RL distinguishes itself by learning from direct engagement and experimentation, making it suitable for scenarios where optimal actions are not immediately evident. This makes RL an appealing choice over supervised methods for complex problem-solving tasks.

5.2 Deep Learning

DL has recently gained significant attention in the research community, particularly in IoT systems. Compared to traditional ML, DL demonstrates enhanced efficacy in managing extensive datasets. This characteristic renders DL methodologies well-suited for IoT frameworks that generate vast data. Furthermore, DL is adept at autonomously discerning and delineating complex data interrelations, which is a significant advantage. DL a specific segment of ML employs multiple processing layers to handle non-linear data, thus aiding in feature abstraction and transformation for pattern analysis. This section delves into IoT security strategies leveraging deep learning techniques.

5.2.1 Supervised Deep Learning

The following section outlines the common supervised deep learning methods.

Conventional Neural Network (CNN)

The adaptability of Convolutional Neural Networks (CNNs) has made them a popular choice for a variety of tasks, particularly due to their proficiency in feature extraction. A key feature of CNNs is the sharing of weights across several layers of computation, enhancing their efficiency. Typically, a CNN structure includes convolutional, activation, pooling, and fully connected layers, organized in a certain configuration. The complexity of the features extracted by the network is influenced by its depth, with potential to identify both simple and intricate patterns. [34] Proposed an efficient feature extraction method using CNNs for detecting intrusions in IoT networks, demonstrating higher accuracy over existing techniques when evaluated on well-known datasets including KDDCup-99, NSL-KDD, CICIDS-2017 and BoT-IoT.

Recurrent Neural Networks (RNNs)

RNNs are feed-forward neural networks optimized for sequential data processing. Comprising input, hidden, and output layers, RNNs utilize the outputs from previous inputs combined with current inputs to make decisions, with hidden layers serving as a form of memory. Despite their capabilities, RNNs struggle with long sequence data due to their limited memory span. To overcome this, variants like Long Short-Term Memory (LSTM), Bidirectional LSTM (Bi-LSTM), and Gated Recurrent Unit (GRU) are used.

Deep Neural Network (DNNs)

DNNs are characterized by their multiple interconnected layers, enabling them to discern complex patterns through a succession of non-linear transformations. [35] developed a specific DNN model, designed with four hidden layers to enhance IDS, focusing on the classification of data from the KDD Cup'99 and NSL-KDD datasets. It uses a softmax classifier in the output layer and rectified linear units in hidden layer. While the

model exhibits high efficacy in detecting various types of attacks, it faces challenges with the U2R class due to dataset constraints. The authors mentioned that a more complex structure with additional nodes and layers may lead to longer computing times and increased resource consumption. To address these issues, they suggest using optimization algorithms and automatic tuning.

5.2.2 Unsupervised deep learning

In this section, various unsupervised deep learning techniques are discussed, focusing on autoencoders, restricted Boltzmann machines, and deep belief networks.

Auto Encoder (AE)

The essence of autoencoders is their capacity to detect and emphasize the most important characteristics by ensuring that the output resembles the input as closely as possible. Structurally, autoencoders consist of input and output layers of identical dimensions, with hidden layers usually more compact than the input layer. This symmetric method functions through an Encoder-Decoder mechanism. [36] proposed an approach for network intrusion detection that employs a conditional variational autoencoder with a distinctive design that incorporates intrusion labels into the decoder layers, outperforming the effectiveness of conventional classifiers. This technique is adept at reconstructing incomplete features from partial datasets, effectively handling categorical features with numerous unique values. Its high reconstruction accuracy holds the potential to significantly improve intrusion detection accuracy.

Restricted Boltzmann Machine (RBM)

RBMs serve as unsupervised learning models aimed at generating deep structures. In an RBM, the model is completely unguided, and there are no links between nodes that are on the same level. The architecture of RBMs includes visible layers for input data and hidden layers for latent variables. Through hierarchical feature extraction from data, the initial layer's features act as latent variables for subsequent layers. [37] utilized the Restricted Boltzmann Machine to enhance the IoT architecture security in Software Defined Networks. The results of the tests demonstrated a notable precision rate exceeding 94%, showcasing its effectiveness.

Deep Belief Network (DBN)

DBNs leverage layers of Restricted Boltzmann Machines (RBM) followed by a softmax classification layer, creating a robust deep learning model. DBNs allow for bidirectional data flow between the input and hidden layers. The unique aspect of DBNs is their pre-training process, which adopts a greedy layer-wise learning technique without supervision, followed by supervised fine-tuning phase to enhance feature learning. [38] used DBN to significantly boost the accuracy of IDS and optimized the system through various algorithms like particle swarm, fish swarm, and genetic algorithms, particularly in identifying U2R and R2L class intrusions, as evidenced by tests conducted with the NSL-KDD dataset.

5.2.3 Semi-Supervised deep learning

In this segment the highly effective hybrid deep learning techniques: Generative Adversarial Networks (GANs) and Ensemble of Deep Learning Networks (EDLNs) are discussed.

Generative Adversarial Network (GAN)

The core of GANs involves the parallel training of generative model and discriminative model in a competitive setting. The generative model is tasked with understanding the distribution of data and creating new data instances, while the discriminative model evaluates whether a given sample originates from the actual training dataset or has been produced by the generative model. This process is depicted in figure 4, where the generator takes in initial data and transforms it into an output that resembles real-world data, and discriminator then assesses whether the input data is real or fake.

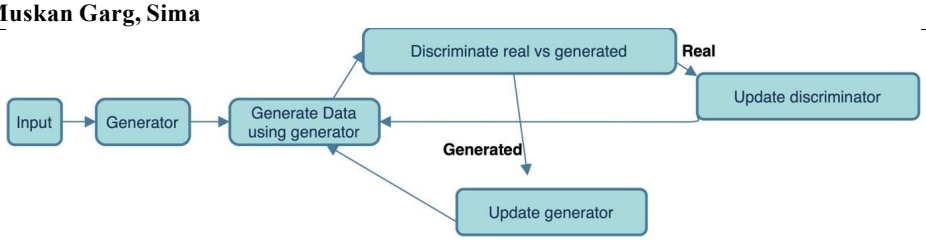

Figure 4 Generative Adversarial Network(GAN)

Ensemble of DL Network (EDLN)

Integrating multiple deep learning (DL) algorithms can yield superior outcomes compared to operating each algorithm independently. Ensemble Deep Learning Networks (EDLNs) effectively combine various model types—generative, discriminative, or a mix of both—to tackle complex problems characterized by uncertainties and complex, high-dimensional data.. EDLNs have demonstrated their effectiveness across several fields, notably in recognizing human activities. Nevertheless, there's a need of investigating how lightweight classifiers, whether homogenous or heterogeneous, might be deployed within distributed frameworks to boost the accuracy and performance of IoT (Internet of Things) security systems, whilst also addressing the computational challenges inherent in such systems.

In this segment, recent advancements in ML and DL methodologies aimed at enhancing IoT device security have been discussed. A comparative study of these advancements, as summarized in Table 2, which outlines year wise the AI approach, learning approach, specific algorithms utilized, datasets for evaluation, achieved accuracy rates, and the primary goal of each technique.

Table 2 Machine Learning/Deep Learning algorithms used in IoT security

Reference	Year	AI-based approach	Type of learning	Classifier	Dataset	Performance Rate
[39]	2023	DL	Supervised	LSTM	ToN-IoT and InSDN	ToN-IoT:Accuracy (96.35%) and precision (98.4%). InSDN : Accuracy(99.73%) and precision(98.9%)
[40]	2023	Hybrid	Supervised	DT + GB	NSL-KDD, BoT-IoT, IoT-23, Edge-IIoT	Accuracy and precision are highest for Edge-IIoT(100%) and lowest for IoT-23(99.98%). Recall is also highest for Edge-IIoT(100%) and lowest for IoT-23(99.99%).
[41]	2023	DL	Supervised	FMI-DNN, FDL	IoT-Botnet 2020	Accuracy (99.4%), Reduced error rate is 0.142.
[42]	2023	ML	Supervised	AdaBoost	IoT-23, Edge-IIoT, BoT-IoT,	Edge-IIoT Dataset: Accuracy (99.9%), Precision (100%), F1-score (100%) and Recall (100%), BoT-IoT Dataset: Accuracy (99.99%), Precision (99.99%) Recall (100%), F1-score(99.99%).IoT-23: Accuracy(99.98%), Precision (99.98%), Recall (99.91%), and F1-score (99.99%).
[43]	2023	Hybrid	Semi-supervised	DNN+GAN	UNSW-NB15	Accuracy (90.9%). Average (precision, recall, and F1 Score) is

						84%.
[44]	2022	Hybrid	Supervised	XGB+RF	N-BaIoT	Accuracy(99.9426%), F1 score (99.94%), balanced accuracy (99.9683%), and error score (0.06%).
[45]	2022	ML	Supervised	RF, XGBoost	UNWS-NB15	Average Accuracy(90%), Recall (90%), F1-Score (90%) Precision (90%),
[46]	2022	ML	Supervised	SVM, KNN, RF	Kaggle banking dataset	Highest Accuracy(99.8%), F1-Score (98.5%), Precision (99.07%), Recall (98.32%),
[47]	2022	Hybrid	Semi-supervised	KNN+PCA	Bot-IoT, NSL-KDD	Highest Accuracy(99.10%) , Detection rate(98.4%), and False alarm rate(2.7%) on the NSL-KDD dataset.
[48]	2022	DL	Supervised	CNN	NID and BoT-IoT	NID Dataset: Accuracy (99.51%) and BoT-IoT: Accuracy (92.85%)
[49]	2022	DL	Supervised	CNN, LSTM, GRU(RNN)	Bot-IoT dataset	Accuracy LSTM(99.8%), CNN(99.7%), and GRU(99.6%). LSTM outperformed CNN and GRU. LSTM: Precision (99.7%), Recall (100%) and F1 score (99.8%). LSTM and GRU recall is 100%, CNN is 99.9%, and F1 score is 99.8% for all three.
[50]	2022	ML	Supervised	LR, NB, DT, ensemble learning	CICIDS2017	Highest Accuracy(99.67 %)RF in both classifications.
[51]	2021	Hybrid	Supervised	CNN+LSTM	IoT-23	Accuracy(96%)
[52]	2021	Hybrid	Supervised	RF+CNN(RCNN), XGBoost+ CNN(XCNN)	CCD-INID-V1, Balot, DoH20	RCNN model AUC(95.6%) on CCD-INID-V1, (99.9) on Balot, and (9.86%) on DoH20. XCNN model AUC(99.8%) on CCD-INID-V1, (99.9%) on Balot, and (99.9%) on DoH20.
[53]	2021	ML	Supervised	XGBoost	N/A	Accuracy(95.56%)
[54]	2021	ML	Supervised	KNN, SVM, DT, NB, RF, ANN, LR	Bot-IoT	Accuracy RF(99.00%) is best in binary classification, KNN(99.00%) is best in multiclass classification.
[55]	2021	Hybrid	Semi-supervised	INB+PCA	UNSW-	Accuracy(92.48%), Detection Rate(95.35%), precision(81.95%),

					NB15	recall(95.35%), and F1-Score(91.64%).
[56]	2020	DL	Supervised	RNN	NSL-KDD	Accuracy(92.18%)
[57]	2020	ML	Supervised	XGBoost	NSL-KDD	Accuracy(97.00%), Matthews correlation coefficient (90.5%) and Area Under the Curve (99.6%).
[58]	2020	DL	Supervised	RNN-based LSTM	N/A	Precision(72.44%), Recall (70.78%), F1 score(71.18%).
[59]	2020	ML	Supervised	LR, SVM, DT, RF, ANN, and KNN, Bagging, Boosting, Stacking	UNSW-NB15 and CICIDS2017	The highest Accuracy for the UNSW-NB15 dataset is 81.77% (RF), and the lowest is 71.49% (SVM). The highest Accuracy for CICIDS2017dataset is 99.7% (RF) and(KNN), and the Lowest is 92% (DT). The accuracy of ensemble methods on UNSW-NB15 and CICIDS2017 datasets are 82.36% and 99.7%, 83.30% and 99.8% and 83.84% and 99.9%, respectively.
[60]	2019	ML	Supervised	KNN, RF	N-BaIoT	Accuracy KNN(95.36%), RF(99.85%)
[61]	2019	DL	Supervised	LSTM	NSL-KDD , CIDDS-001 and UNSWNB15	NSL-KDD dataset: Accuracy (99.5%), CIDDS-001 dataset: Accuracy (99.3%) and UNSWNB15 dataset Accuracy (99.1%).
[62]	2018	ML	Supervised	SVM	ISCX	Accuracy (93.47%)
[63]	2018	DL	Supervised	DNN, CNN, RNN	Real	Accuracy DNN(96.3%), CNN(94.7%), LSTM(76%)

6. DISCUSSION AND FUTURE DIRECTIONS

This segment explores the findings from existing studies, highlighting prevalent trends in research and identifying opportunities for further investigation. However, for larger datasets, ML becomes only feasible if the data is pre-labelled, a costly and time demanding process. As a result, Deep Learning (DL) methods are preferred for managing large datasets because they possess the capability to identify and learn valuable patterns from raw data. Due to the extensive dataset requirements and the depth of DL algorithms, they demand significant computational resources and time. The effectiveness in detecting intrusions increases with more extensive training. A Sunburst chart presented in Figure 5 illustrates the distribution of the literature reviewed, organizing it from the center outward by categories, learning types, and the algorithms used in the outermost layer. It is observed from the diagram that ML algorithms were used more than DL during the period reviewed. Furthermore, it notes that the most commonly utilized algorithms are SVM and RF, which are ML algorithms. The most commonly used DL-based algorithm is LSTM. Some methodologies combine multiple algorithms to increase detection accuracy but at the expense of greater complexity and computing resource requirements. These methodologies are shown under hybrid models in Figure 5. Many algorithms still need to be addressed, such as Gradient Boosting, Categorical Boosting algorithm, Classification and Regression Trees. The survey highlights the limited application of evolutionary computing and rule-based AI in network intrusion detection, with only a few studies adopting GA and FL, indicating a vast area ripe for further exploration. The analysis further discusses the performance metrics researchers utilize in evaluating their methodologies, as depicted in

Figure 6. The most prevalent metrics are Detection Accuracy and Recall, underscoring the necessity for high accuracy and detection rates for adequate network security. In addition to accuracy and recall, precision and F-measure are equally essential performance metrics to showcase the effectiveness of network security enhancements.

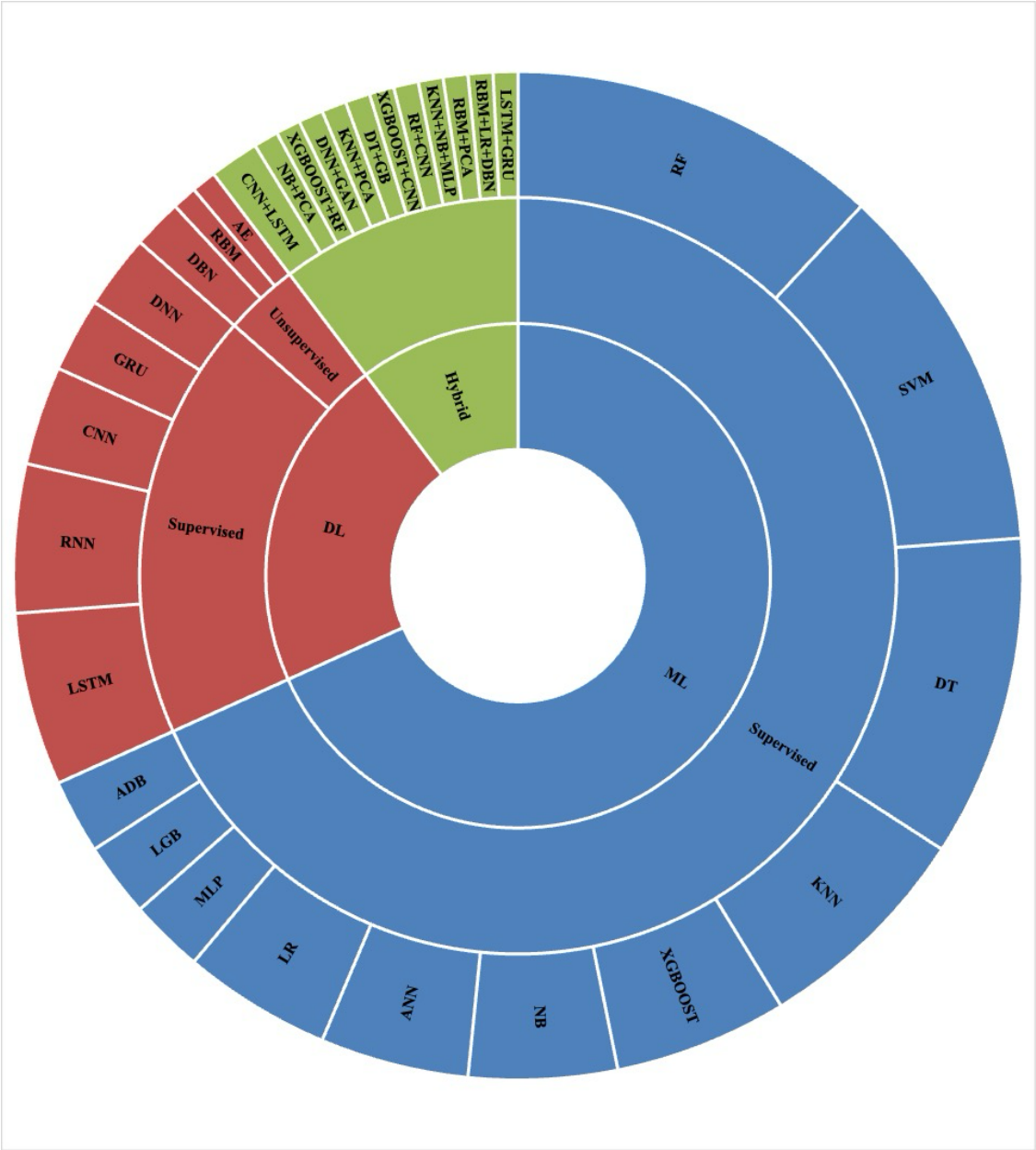

Figure 5 Recent ML/DL-based studies

Most of the studies reviewed claimed to achieve high levels of accuracy in their methods. However, there was no presentation of evidence to support these claims. Making the implementations available could prove these reported accuracies and enable other researchers to verify and enhance the approaches. Radar diagrams in Figure 7 exhibit the reported accuracy rates, showing a scale from 84% to 100% and indicating potential for enhancement in detection accuracy. Benchmarking is crucial for advancing research. Figure 8 illustrates the frequency of datasets utilized in the literature based on their adoption rate. Among these, NSL-KDD and BoT-IoT emerge as the datasets most frequently employed within the timeframe analysed. The NSL-KDD is suggested as a solution for problems found in the KDD CUP 99 dataset.

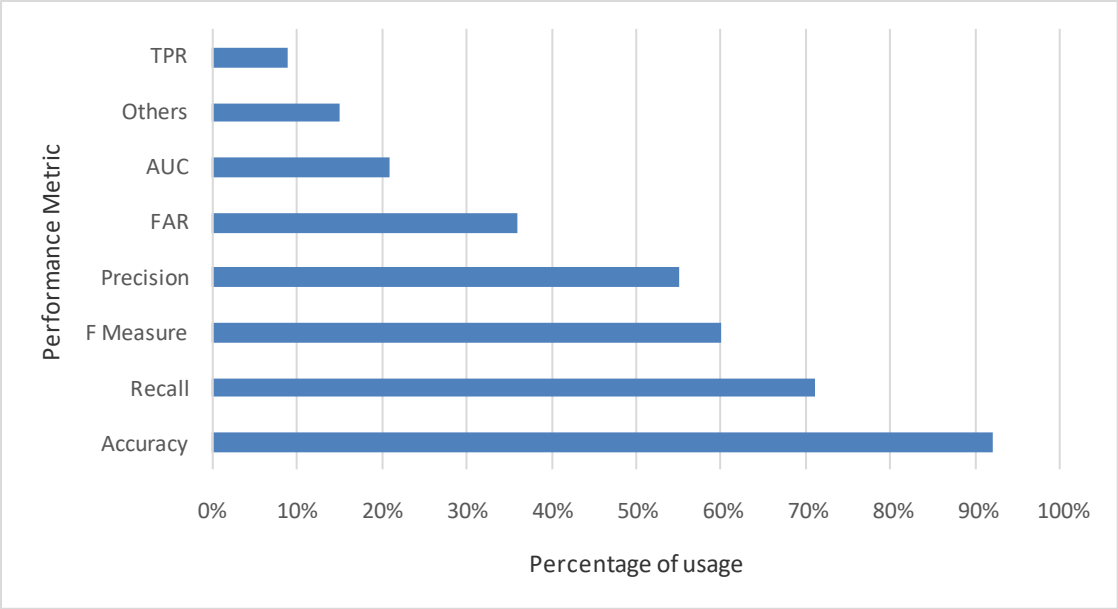

Figure 6 Evaluation Metrics used in studies

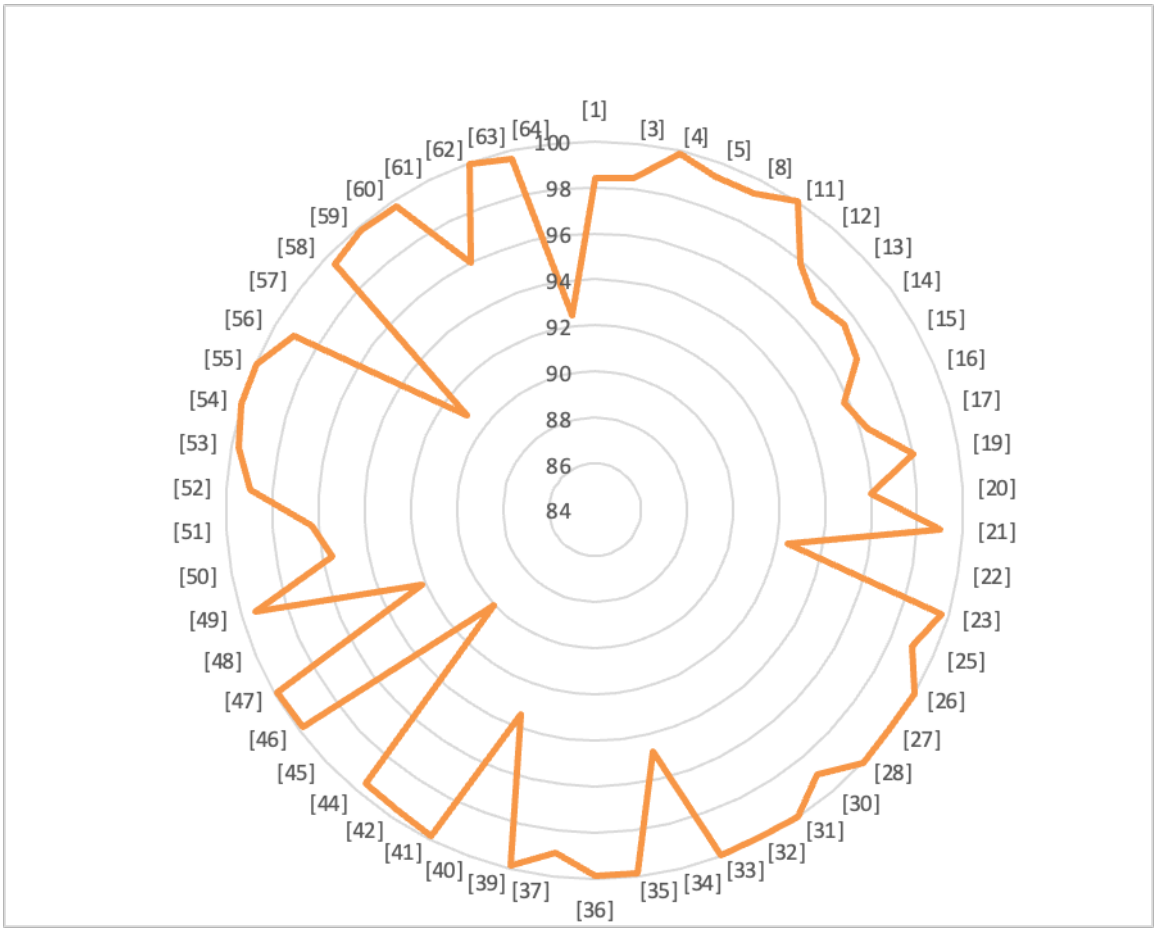

Figure 7 Reported accuracy

Meanwhile, the Bot-IoT dataset is frequently used as it contains large amounts of malicious and benign traffic. However, it also suffers from intense class imbalance, with less than 1% of the traffic being benign. This can lead to a significant contrast, as over 99% of the traffic is malicious. Many of the presented methods were tested using simulated datasets. However, other widely used benchmark datasets are UNSW-NB15, NBaIoT,

IoT-23 and CICIDS2017. However, evaluating these proposed methods through real-world datasets has become a priority. However, the process of constructing a dataset is a costly undertaking that requires significant resources and expert knowledge. Therefore, an important research challenge in this field is to systematically build a current dataset that includes sufficient instances of almost every kind of attack. The NSL-KDD dataset is suggested as a remedy for specific problems found in the KDD CUP 99 dataset. Meanwhile, the Bot-IoT dataset is frequently utilized due to its extensive collection of both malicious and legitimate traffic.

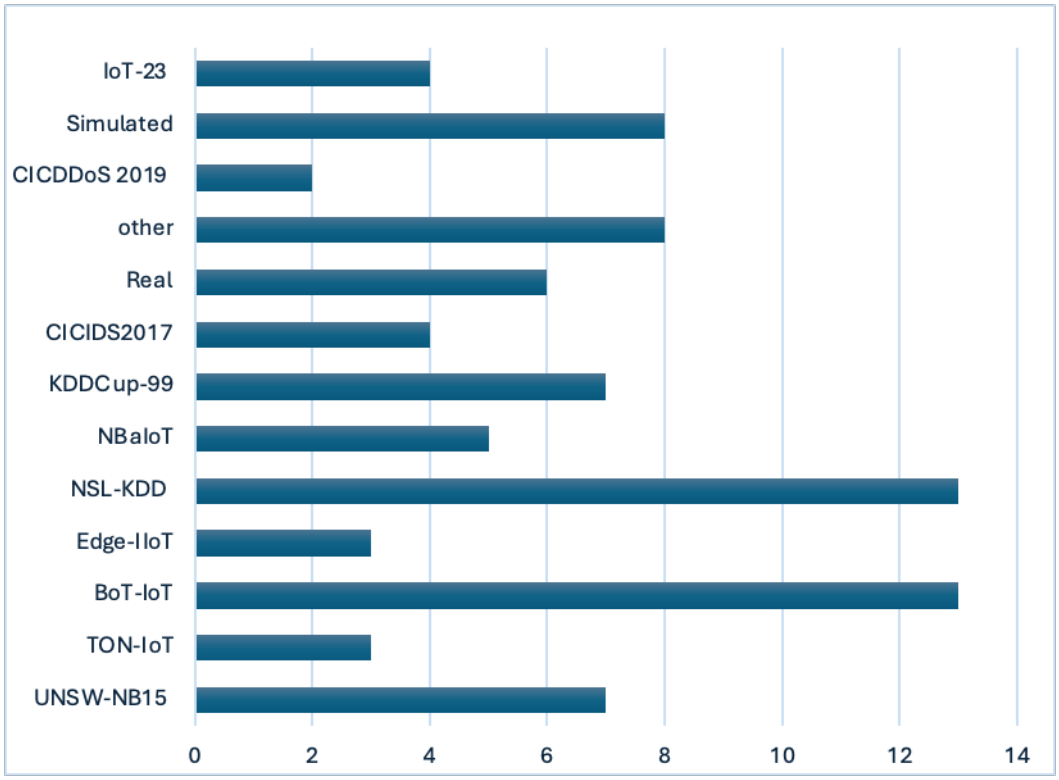

Figure 8 Datasets distribution

7. CONCLUSION

The security of IoT devices has become a growing research area with increasing application of IoT devices. This paper studies application of machine learning and deep learning methods in this field. Various ML/DL-based approaches have been explored in the literature for this purpose. In the studies reviewed, a selection was made of papers published from 2015 to 2024, sourced from prestigious platforms such as IEEE Xplore, MDPI's Open Access Journals, Science Direct, ACM, Springer, Scopus, Wiley, and Web of Science. A classification system was then introduced to categorize these papers based on the artificial intelligence category and the learning method employed, whether supervised, semi-supervised, or unsupervised learning. The study also looked into the most commonly chosen performance assessment metrics by researchers when evaluating their techniques, where it was found that detection accuracy and recall are the most common metrics. The research indicates that while many proposed methods achieve high rates of detecting attacks, they often rely on outdated datasets for testing due to the extensive results these datasets offer. However, these datasets need to encompass zero-day attacks, thus limiting the effectiveness of these methods in real-world situations. To develop a truly efficient model, it must undergo testing and validation using datasets that include both old and new types of attacks.dditionally, newer datasets, such as BoT-IoT, face issues like class imbalance. Therefore, a significant challenge in research is the creation of a modern, balanced dataset that encompasses a wide range of attack types with sufficient instances of each. This study highlights the need for additional investigation to improvethe capability of models in identifying infrequent attacks in real-world situations and to create simpler solutions for the proposed models. This insight will be leveraged in future research to create an innovative, lightweight,and efficient ML/DL-based methodology capable of accurately identifying intrusions within a network.

Acknowledgment

I would like to express my gratitude towards my husband for the encouragement which helped me in completion of this paper. I would like to express my special gratitude and thanks to my guide Dr. Sima for imparting her knowledge and expertise in this study.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] W. Ding, M. Abdel-Basset, and R. Mohamed, "DeepAK-IoT: An effective deep learning model for cyberattack detection in IoT networks," *Inf Sci (N Y)*, vol. 634, pp. 157–171, Jul. 2023, doi: 10.1016/j.ins.2023.03.052

[2] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," Computer Networks, vol. 141. Elsevier B.V., pp. 199–221, Aug. 04, 2018. doi: 10.1016/j.comnet.2018.03.012.

[3] J. G. Almaraz-Rivera, J. A. Perez-Diaz, and J. A. Cantoral-Ceballos, "Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models," Sensors, vol. 22, no. 9, May 2022, doi: 10.3390/s22093367.

[4] M. Hasan, M. Milon Islam, M. Ishrak Islam Zarif, and M. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," 2019, doi: 10.1016/j.iot.2019.10.

[5] M. Humayun, M. Niazi, N. Z. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," Arab J Sci Eng, vol. 45, no. 4, pp. 3171– 3189, 2020, doi: 10.1007/s13369-019-04319-2.

[6] P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," Computers and Security, vol. 127. Elsevier Ltd, Apr. 01, 2023. doi: 10.1016/j.cose.2023.103096.

[7] K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," in Proceedings - 2016 15th IEEE International Conference on Machine Learning and Applications, ICMLA 2016, Institute of Electrical and Electronics Engineers Inc., Jan. 2017, pp. 195–200. doi: 10.1109/ICMLA.2016.167.

[8] T. M. Hoang, T. Q. Duong, H. D. Tuan, S. Lambotharan, and L. Hanzo, "Physical layer security: Detection of active eavesdropping attacks by support vector machines," IEEE Access, vol. 9, pp. 31595–31607, 2021, doi: 10.1109/ACCESS.2021.3059648.

[9] K. Chen et al., "Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice," Journal of Hardware and Systems Security, vol. 2, no. 2, pp. 97–110, Jun. 2018, doi: 10.1007/s41635-017-0029-7.

[10] M. H. Aysa, A. A. Ibrahim, and A. H. Mohammed, "IoT Ddos Attack Detection Using Machine Learning," in 4th International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2020 - Proceedings, Institute of Electrical and Electronics Engineers Inc., Oct. 2020. doi: 10.1109/ISMSIT50672.2020.9254703.

[11] W. Yaokumah, J. K. Appati, and D. Kumah, "Machine Learning Methods for Detecting Internet-of-Things (IoT) Malware," International Journal of Cognitive Informatics and Natural Intelligence, vol. 15, no. 4, 2021, doi: 10.4018/IJCINI.286768.

[12] Institute of Electrical and Electronics Engineers, 2018 IEEE Wireless Communications and Networking Conference (WCNC).

[13] O. NAECON-OIS 2015 Dayton et al., Proceedings of the 2015 IEEE National Aerospace and Electronics Conference (NAECON).

[14] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," IEEE Access, vol. 5, pp. 21954–21961, Oct. 2017, doi: 10.1109/ACCESS.2017.2762418.

[15] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," Expert Syst Appl, vol. 67, pp. 296–303, Jan. 2017, doi: 10.1016/j.eswa.2016.09.041.

[16] R. Majeed, N. A. Abdullah, and M. F. Mushtaq, "IoT-based Cyber-security of Drones using the Naïve Bayes Algorithm." [Online]. Available: www.ijacsa.thesai.org

[17] E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," IEEE Internet Things J, vol. 6, no. 5, pp. 9042–9053, Oct. 2019, doi: 10.1109/JIOT.2019.2926365.

[18] I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, "IntruDTree: A machine learning based cyber security intrusion detection model," Symmetry (Basel), vol. 12, no. 5, May 2020, doi: 10.3390/SYM12050754.

[19] R. Alghamdi and M. Bellaiche, "A cascaded federated deep learning based framework for detecting wormhole attacks in IoT networks," Comput Secur, vol. 125, Feb. 2023, doi: 10.1016/j.cose.2022.103014.

[20] M. Alduailij, Q. W. Khan, M. Tahir, M. Sardaraz, M. Alduailij, and F. Malik, "Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method," Symmetry (Basel), vol. 14, no. 6, Jun. 2022, doi: 10.3390/sym14061095.

[21] Y. Liu and D. Pi, "A novel kernel SVM algorithm with game theory for network intrusion detection," KSII Transactions on Internet and Information Systems, vol. 11, no. 8, pp. 4043–4060, Aug. 2017, doi: 10.3837/tiis.2017.08.016.

[22] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A Machine Learning Security Framework for Iot Systems," IEEE Access, vol. 8, pp. 114066–114077, 2020, doi: 10.1109/ACCESS.2020.2996214.

[23] L. Lerman, G. Bontempi, and O. Markowitch, "A machine learning approach against a masked AES: Reaching the limit of side-channel attacks with a learning model," J Cryptogr Eng, vol. 5, no. 2, pp. 123–139, Jun. 2015, doi: 10.1007/s13389-014-0089-3.

[24] 2018 15th International Conference on Control, Automation, Robotics and Vision (ICARCV). IEEE, 2018.

[25] M. Swarnkar and N. Hubballi, "OCPAD: One class Naive Bayes classifier for payload based anomaly detection," Expert Syst Appl, vol. 64, pp. 330–339, Dec. 2016, doi: 10.1016/j.eswa.2016.07.036.

[26] A. Mihoub, O. Ben Fredj, O. Cheikhrouhou, A. Derhab, and M. Krichen, "Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques," Computers and Electrical Engineering, vol. 98, Mar. 2022, doi: 10.1016/j.compeleceng.2022.107716.

[27] Y. Zhang et al., "Efficient and Intelligent Attack Detection in Software Defined IoT Networks," in 2020 IEEE International Conference on Embedded Software and Systems, ICESS 2020, Institute of Electrical and Electronics Engineers Inc., Dec. 2020. doi: 10.1109/ICESS49830.2020.9301591.

[28] S. Pokhrel, R. Abbas, and B. Aryal, "IoT Security: Botnet detection in IoT using Machine learning," Apr. 2021, [Online]. Available: http://arxiv.org/abs/2104.02231

[29] B. B. Gupta, P. Chaudhary, X. Chang, and N. Nedjah, "Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers," Computers and Electrical Engineering, vol. 98, Mar. 2022, doi: 10.1016/j.compeleceng.2022.107726.

[30] E. S. P. Krishna and A. Thangavelu, "Attack detection in IoT devices using hybrid metaheuristic lion optimization algorithm and firefly optimization algorithm," International Journal of Systems Assurance Engineering and Management, 2021, doi: 10.1007/s13198-021-01150-7.

[31] M. Alqahtani, H. Mathkour, and M. M. Ben Ismail, "IoT botnet attack detection based on optimized extreme gradient boosting and feature selection," Sensors (Switzerland), vol. 20, no. 21, pp. 1–21, Nov. 2020, doi: 10.3390/s20216336.

[32] I. U. Khan et al., "A Proactive Attack Detection for Heating, Ventilation, and Air Conditioning (HVAC) System Using Explainable Extreme Gradient Boosting Model (XGBoost)," Sensors, vol. 22, no. 23, Dec. 2022, doi: 10.3390/s22239235.

[33] S. Garg, V. Kumar, and S. Rao Payyavula, "Identification of Internet of Things (Iot) Attacks Using Gradient Boosting: A Cross Dataset Approach," vol. 21, p. 2022.

[34] A. Fatani, M. A. Elaziz, A. Dahou, M. A. A. Al-Qaness, and S. Lu, "IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization," IEEE Access, vol. 9, pp. 123448–123464, 2021, doi: 10.1109/ACCESS.2021.3109081.

[35] Y. Jia, M. Wang, and Y. Wang, "Network intrusion detection algorithm based on deep neural network," IET Inf Secur, vol. 13, no. 1, pp. 48–53, Jan. 2019, doi: 10.1049/iet-ifs.2018.5258.

[36] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, and J. Lloret, "Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in iot," Sensors (Switzerland), vol. 17, no. 9, Sep. 2017, doi: 10.3390/s17091967.

[37] A. Dawoud, S. Shahristani, and C. Raun, "Deep learning and software-defined networks: Towards

secure IoT architecture," Internet of Things (Netherlands), vol. 3–4, pp. 82–89, Oct. 2018, doi: 10.1016/j.iot.2018.09.003.

[38] P. Wei, Y. Li, Z. Zhang, T. Hu, Z. Li, and D. Liu, "An optimization method for intrusion detection classification model based on deep belief network," IEEE Access, vol. 7, pp. 87593–87605, 2019, doi: 10.1109/ACCESS.2019.2925828.

[39] R. A. Elsayed, R. A. Hamada, M. I. Abdalla, and S. A. Elsaid, "Securing IoT and SDN systems using deep-learning based automatic intrusion detection," Ain Shams Engineering Journal, vol. 14, no. 10, Oct. 2023, doi: 10.1016/j.asej.2023.102211.

[40] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, "An improved anomaly detection model for IoT security using decision tree and gradient boosting," Journal of Supercomputing, vol. 79, no. 3, pp. 3392–3411, Feb. 2023, doi: 10.1007/s11227-022-04783-y.

[41] X. Wang, Y. Wang, Z. Javaheri, L. Almutairi, N. Moghadamnejad, and O. S. Younes, "Federated deep learning for anomaly detection in the internet of things," Computers and Electrical Engineering, vol. 108, May 2023, doi: 10.1016/j.compeleceng.2023.108651.

[42] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "lIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning," Cluster Comput, vol. 26, no. 6, pp. 4069–4083, Dec. 2023, doi: 10.1007/s10586-022-03810-0.

[43] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Anomaly based network intrusion detection for IoT attacks using deep learning technique," Computers and Electrical Engineering, vol. 107, Apr. 2023, doi: 10.1016/j.compeleceng.2023.108626.

[44] J. Al Faysal et al., "XGB-RF: A Hybrid Machine Learning Approach for IoT Intrusion Detection," Telecom, vol. 3, no. 1, pp. 52–69, Mar. 2022, doi: 10.3390/telecom3010003.

[45] Ismail et al., "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks," IEEE Access, vol. 10, pp. 21443–21454, 2022, doi: 10.1109/ACCESS.2022.3152577.

[46] U. Islam et al., "Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models," Sustainability (Switzerland), vol. 14, no. 14, Jul. 2022, doi: 10.3390/su14148374.

[47] A. Guezzaz, M. Azrour, S. Benkirane, M. Mohy-Eddine, H. Attou, and M. Douiba, "A Lightweight Hybrid Intrusion Detection Framework using Machine Learning for Edge-Based IIoT Security," International Arab Journal of Information Technology, vol. 19, no. 5, pp. 822–830, Sep. 2022, doi: 10.34028/iajit/19/5/14.

[48] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," Computers and Electrical Engineering, vol. 99, Apr. 2022, doi: 10.1016/j.compeleceng.2022.107810.

[49] A. M. Banaamah and I. Ahmad, "Intrusion Detection in IoT Using Deep Learning," Sensors, vol. 22, no. 21, Nov. 2022, doi: 10.3390/s22218417.

[50] A. Abbas, M. A. Khan, S. Latif, M. Ajaz, A. A. Shah, and J. Ahmad, "A New Ensemble-Based Intrusion Detection System for Internet of Things," Arab J Sci Eng, vol. 47, no. 2, pp. 1805– 1819, Feb. 2022, doi: 10.1007/s13369-021-06086-5.

[51] A. K. Sahu, S. Sharma, M. Tanveer, and R. Raja, "Internet of Things attack detection using hybrid Deep Learning Model," Comput Commun, vol. 176, pp. 146–154, Aug. 2021, doi: 10.1016/j.comcom.2021.05.024.

[52] Z. Liu et al., "Using embedded feature selection and cnn for classification on ccd- inid-v1—a new iot dataset," Sensors, vol. 21, no. 14, Jul. 2021, doi: 10.3390/s21144834.

[53] Z. Shahbazi and Y. C. Byun, "Integration of blockchain, iot and machine learning for multistage quality control and enhancing security in smart manufacturing," Sensors, vol. 21, no. 4, pp. 1– 21, Feb. 2021, doi: 10.3390/s21041467.

[54] A. Churcher et al., "An experimental analysis of attack classification using machine learning in IoT networks," Sensors (Switzerland), vol. 21, no. 2, pp. 1–32, Jan. 2021, doi: 10.3390/s21020446.

[55] S. Manimurugan, "IoT-Fog-Cloud model for anomaly detection using improved Naïve Bayes and principal component analysis," J Ambient Intell Humaniz Comput, 2021, doi: 10.1007/s12652-020-02723-3.

[56] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," Simul Model Pract Theory, vol. 101, May 2020, doi: 10.1016/j.simpat.2019.102031.

[57] J. Liu, B. Kantarci, and C. Adams, "Machine learning-driven intrusion detection for Contiki-NG-based IoT networks exposed to NSL-KDD dataset," in WiseML 2020 - Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning, Association for Computing Machinery, Jul. 2020, pp. 25–30. doi: 10.1145/3395352.3402621.

[58] S. K. Singh, Y. S. Jeong, and J. H. Park, "A deep learning-based IoT-oriented infrastructure for secure smart City," Sustain Cities Soc, vol. 60, Sep. 2020, doi: 10.1016/j.scs.2020.102252.

[59] M. M. Rashid, J. Kamruzzaman, M. M. Hassan, T. Imam, and S. Gordon, "Cyberattacks detection in iot-based smart city applications using machine learning techniques," Int J Environ Res Public Health, vol. 17, no. 24, pp. 1–21, Dec. 2020, doi: 10.3390/ijerph17249347.

[60] A. Guerra-Manzanares, H. Bahsi, and S. Nomm, "Hybrid feature selection models for machine learning based botnet detection in IoT networks," in Proceedings - 2019 International Conference on Cyberworlds, CW 2019, Institute of Electrical and Electronics Engineers Inc., Oct. 2019, pp. 324–327. doi: 10.1109/CW.2019.00059.

[61] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, "Deep learning- based intrusion detection for IoT networks," in Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing, PRDC, IEEE Computer Society, Dec. 2019, pp. 256–265. doi: 10.1109/PRDC47002.2019.00056.

[62] 2018 27th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2018.

[63] IEEE Communications Society, Armed Forces Communications and Electronics Association (U.S.), and Institute of Electrical and Electronics Engineers, MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM) : 29-31 Oct. 2018.

Authors

Muskan Garg is working as an Assistant Professor in the Department of Computer Science and Engineering, Vaish College of Engineering Rohtak affiliated to Maharshi Dayanand University Rohtak. She has received B.Tech and M.Tech in Computer Science and Engineering from Vaish College of Engineering Rohtak. She has published 5 papers in various International/National Journals and Conferences. Her research interests are in IoT security and Machine Learning. Ms. Muskan Garg is currently carrying out Ph.D. research work in association with Dada Lakhmi Chand State University of Performing and Visual Arts Rohtak.

Dr. Sima is working as Director IT and Associate Professor in the subject of Computer Science in Faculty of Planning and Architecture in Dada Lakhmi Chand State University of Performing and Visual Arts Rohtak. She has done Ph.D. in computer science in association with Kurukshetra University, Kurukshetra, India. She is professional Member of CSI INDIA and INTECH India. She has more than 50 research papers to her credit in various International/National Journals and Conferences. Her 3 books have been published in computer science for undergraduate students. Her research interests are in Mobile Ad hoc Networks, and Security. Dr. Sima has chaired various sessions in National Conferences. She is Chief Warden of University, Chairperson Internal Complaints Committee, and Chairperson Women Cell of University, Research Coordinator of University, Member of Purchase Committee, Member of Admission Committee, Member of IQAC and NAAC Committee, Nodal Officer for HSHEC, Digi locker, and various IT related activities.