Proceedings of the Pakistan Academy of Sciences: A Physical and Computational Sciences 59(3): 1-16 (2022)

ISSN (Print): 2518-4245; ISSN (Online): 2518-4253
https://doi.org/10.53560/PPASA(59-3)782

Pakistan Academy of Sciences

Review Article

Machine Learning Methods of IoT Security and Future Application

Aqib Ali[1*], Samreen Naeem[1], Sania Anam[2], and Muhammad Munawar Ahmed[3]

[1]College of Automation, Southeast University, Nanjing, China
[2]Department of Computer Science, Govt Degree College for Women Ahmadpur East, Bahawalpur, Pakistan
[3]Department of Information Technology, The Islamia University of Bahawalpur, Pakistan

Abstract: One of the technologies that are now expanding rapidly is called the Internet of Things (IoT). It is a technology that enables billions of smart devices or things, collectively referred to as "Things," to collect a variety of data about themselves and the environment in which they are located using a variety of sensors. They can then share data with parties who have been permitted to do so for a variety of objectives, such as the management and monitoring of industrial services or the expansion of company services or operations. However, there are presently more security risks associated with the Internet of Things than ever. The field of machine learning (ML) has recently experienced significant advancement in technology, which has resulted in the opening of various new lines of inquiry that may be used to address existing and upcoming issues related to the Internet of Things. Nevertheless, machine learning is a robust technology that can recognize suspicious dangers and activities in smart devices and grids. This paper presents an extensive literature review on Machine Learning methods and the significance of IoT security in the context of various types of potential attacks as well as the comparison of several different ML algorithms regarding the detection of attacks and anomalies. Additionally, many machines learning-based Internet of Things protection systems have been presented.

Keywords: Internet of Things, Cyberattacks, Machine Learning, Security

1. INTRODUCTION

The Internet of things (IoT) is a network of intelligent devices that share data online. In a new context, smart objects gather information and initiate events [1]. Smart cities, houses, transit, agriculture, hospital, supply chain, seismic detection, and smart grid are IoT applications as shown in Figure 1. The Networking, Cloud, and Cybersecurity Solutions (CISCO) predicts 31.3 billion IoT devices by 2025. IoT device growth is rapid and global. IoT devices create massive data. Physical, network, and application architectures make up classical IoT [2]. The gadgets are environmentally conscious and may be wired or wirelessly linked. As in a smart home, the refrigerator may automatically make an order at the registered merchant when the fruit bowl empties and notify home users. Sensors and computers can monitor smart hospital patients in an emergency. Little-end sensors have various features and low computing power. IoT implementation is complex. IoT problems are standardization, interoperability, data storage, processing, trust management, identification, confidentiality, integrity, availability, security, and privacy [3].

IoT devices employ web-enabled sensors and hardware to send, gather, and act on data. Connecting IoT or edge devices to a gateway collects data for cloud analysis. Smart gadgets sometimes communicate with other devices and work on the information delivered between them [4]. Intelligent devices communicate by transferring data packets over a network, saving time and money. IoT gadgets make the network insecure. Unsecured devices abuse the network. Since IoT devices are tightly linked, an attacker can exploit a single weakness to modify all data and damage humans [5]. Several

Received: July 2022; Accepted: September 2022
*Corresponding author: Aqib Ali <aqibcsit@gmail.com>

preventative strategies are explored to avert cyber risks, and a fog security gateway is created. The fog layer's primary purpose is to increase safety and efficiency and minimize cloud data processing, analysis, and archiving [6].

Fog computing explores data's outer edges—the fog layer stores construction data in a customer's cloud or data center. The fog layer improves efficiency and reduces redundancy in cloud data transit, maximizing cloud computing security. Data won't be transferred straight to the cloud layer since it establishes a high-latency network connection between devices and the analytics endpoint and has more bandwidth than the fog layer. In other cases, there's no bandwidth to transport data since it's processed locally [7]. An IDS analyzes data flow to detect and safeguard system information. IDS activities include monitoring, analysis, and detection. The monitoring phase depends on the host-based or network-based sensor, the analysis phase on model identification or feature extraction, and the detection phase on detecting abnormalities or abusive intrusions [8]. IoT is a new technology that has many uses. Many applications struggle with security and privacy. IoT security and privacy have been studied. New technologies can handle IoT security, though [9]. This article identified three prominent security technologies: ML, Blockchain, and AI.

2. LITERATURE REVIEW

This section contains relevant works on anomaly detection using machine learning methods in the IoT network. Using distributed deep learning fog for ML algorithm-based computing in IoT, an NSL-KDD dataset is utilized to compare the model to the surface algorithm. The outcome may be better. As a signature-based IDS [10]. ADFA-LD dataset used with Raspberry pi for a perceptron-based fog IDS. When improving calculating accuracy and efficiency. Traditional intrusion detection systems consist of a host and network-based or hybrid IDS, which may detect cyber-attacks differently. Standard IDS are designed to identify intrusion activity on single or complete network traffic. First, host-based IDS installs antivirus software and identifies suspicious network traffic by scanning and analyzing system calls, application logs, file systems, etc. Some IoT devices have restricted capability and resources [11]. Therefore, this solution fails.

The second kind, network-based IDS, analyzes all network traffic and identifies known and unknown threats (HIDS) using an anomaly-based and signature-based hybrid approach. Signature-based technique uses more resources and doesn't identify attacks, only database records [12]. Anomaly-based NIDS is better at monitoring

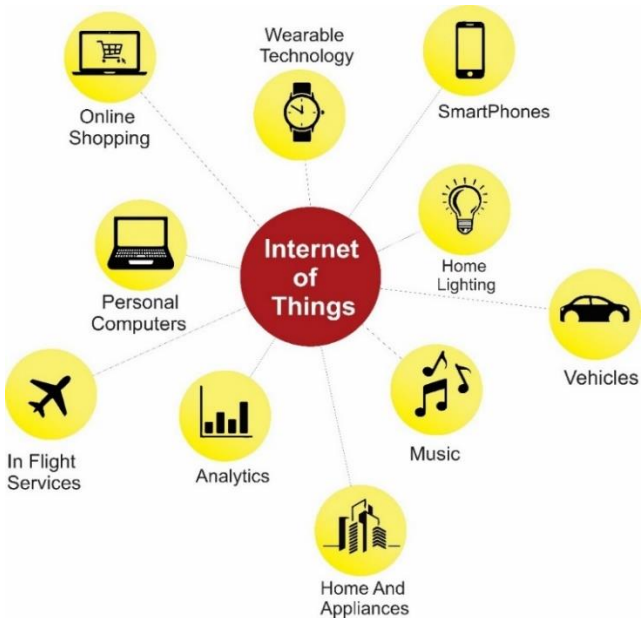

Fig. 1. IoT Applications

network traffic and identifying threats. Anomaly detection promises to identify NIDS attacks.

Random Forest (RF) is utilized to detect malicious activity using the UNSW-NB15 dataset and the AD-IoT detection approach, which uses binary classification to characterize packet behavior as usual or dangerous. Only package behavior limits it—unknown packet attack. AD-IoT hasn't been utilized to designate an attack. Hence this will be the inquiry [13]. Most of the advanced research work done in current days should provide excellent direction for future researchers [14-22].

3. CURRENT RESEARCH GAPS IN IOT SECURITY

Understanding the underlying privacy and security problems is critical to properly implementing the IoT. In the past, the IoT was built on top of existing technology [23]. As a result, it's critical to determine if the IoT's security concerns are novel or a revolution in the security challenges experienced by previous technologies. Several characteristics, such as incorporating apps, networks, hardware, and software, are comparable to the last security issues [24]. The fundamental problem with the IoT is resource limits, which make it challenging to employ present advanced IoT security solutions. In addition, IoT privacy and security issues necessitate optimal algorithms and layered architecture. IoT systems, for example, require more robust cryptographic optimization and new algorithms to handle privacy and security owing to IT limits. On the other hand, various IT gadgets bring new problems to existing security methods [25]. ML approaches may be used to increase the security of text data by automated organizing in this situation. These methods will be addressed in more detail later in the paper.

4. IOT LAYERS

The Internet of Things architecture functions as a portal to a variety of different hardware applications [26]. This allows for the establishment of a connection as well as the extension of IoT services to each gateway. When transmitting and receiving information or data from different levels of Internet of Things architecture [27], several network protocols are used. Some examples of these protocols are Bluetooth, Wi-Fi, RFID, narrow and wide band, ZigBee, and LPWAN. A typical Internet of Things architecture consists mostly of three layers: the physical layer, the network layer, and the application layer as shown in Figure 2 [28].

- **The Physical Layer:** This layer is characterized by sensing and knowledge gathering and collection about the world in which intelligent

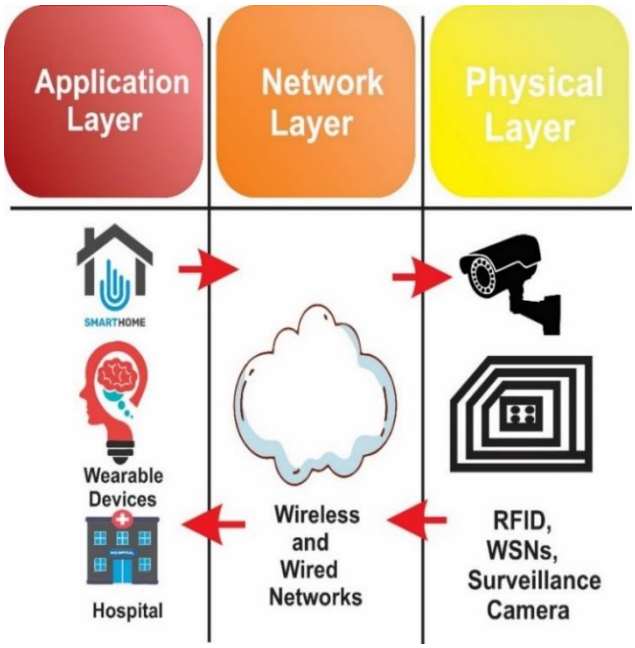

Fig. 2. IoT Layers: The Architecture

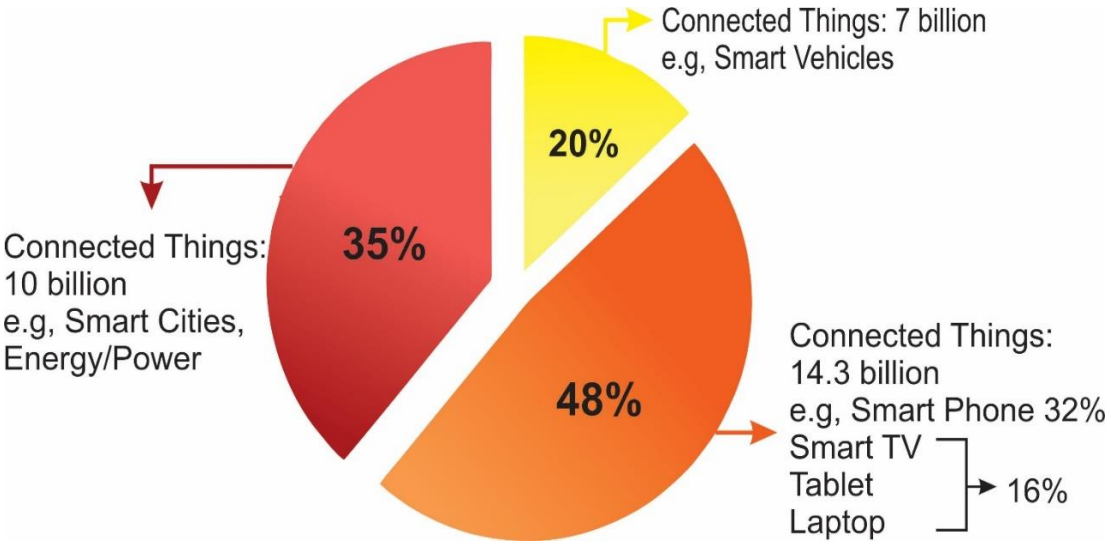

Fig. 3. Users of IoT devices Estimated by the year 2025.

things are available [29].

- **The Network Layer:** The layer feature allows data to be delivered and processed utilizing various devices' internet connections [30].
- **The Application Layer:** Its primary purpose is to give a specific application-based service to the user [30].

4.1 Security in the IoT

21st-century IoT device security is a prominent subject. IoT connects the universe. It opens several doors for attacks [31]. IoT apps running on an open network make gadgets easier to use. The Internet of Things endangers human life by exposing it to various hazards and threats. Still, it also makes compliance more straightforward. [32] Internet of Things devices may be accessed from any location without user authentication. Several security measures will need to be developed to ensure the safety of IoT devices. Because of their physical construction, Internet of Things devices has limited computing capabilities, which makes it impossible to devise an all-encompassing security protocol. A reliable IoT must have security qualities. Standard IoT security criteria include confidentiality, integrity, and authentication [33]. An estimated percentage of IoT device users by 2025 is presented in Figure 3.

- Confidentiality involves prudence through concealing information. Sensitive sensors need concealment, such as with military data. WSN is a highly-requested feature. If WSN reports could be altered, the enemy may be misled. Social and industrial uses need secrecy [34].
- To preserve IoT data integrity, the recipient must confirm no messages were modified during transmission or delivery. The data integrity check ensures that the information provided has not been modified. This is very important because even if intruders cannot get the data, the network may still fail to function correctly if any of the nodes have been infiltrated and altered the data. Data may be modified automatically without human involvement if the connection is unstable. Integrity check detects unintentional and purposeful message modifications [35].
- The authentication procedure verifies a message's origin. Sensor nodes assess the peer node's identification and validity. Authenticity ensures a simple message. The Message Authentication Code (MAC) offers message integrity and authenticity [36].

5. IOT ATTACKS

In recent years, the IoT has been attacked, raising awareness among businesses and consumers. Describes IoT attacks, impacts, and surfaces. Cyber and physical attacks against IoT [37]. Figure 4 shows IoT security threats, including different types of attacks, effects of the attack, anomaly detection,

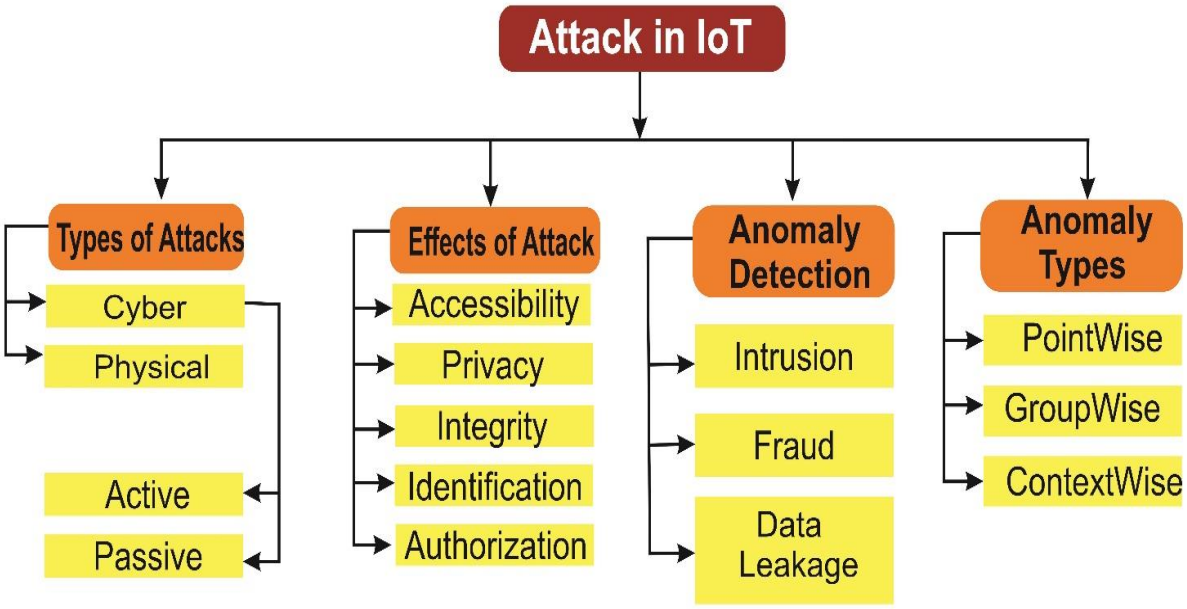

Fig. 4. Graphical representation of IoT security threats, including different types of attacks, effects of the attack, anomaly detection, and anomaly types.

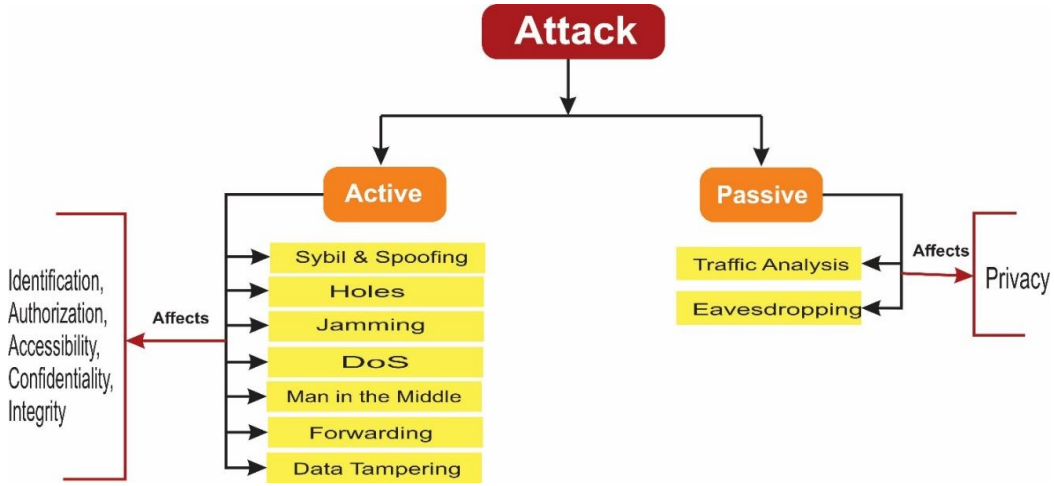

Fig. 5. Types of attacks and their effects

and anomaly types. Many different Internet of Things devices is the target of cyberattacks, which involve hacking into wireless networks and stealing, deleting, altering, or destroying user data.

Physical attacks destroy IoT devices. The gadget may be attacked without a network. Mobile devices, cameras, sensors, routers, etc., can also be attacked [38]. The following subsections focus on cyber-attacks based on their severity on active and passive IoT devices as shown in Figure 5.

5.1 Active IoT Attacks

An active assault is carried out by a network attacker who, after gaining access to the interface settings, then disconnects certain services from the IoT devices they target. Interruptions, interventions, and changes are all examples of active assaults that may occur in several different ways. Attacks such as denial of service, middle hand, Sybil and spoofing, hole attacks, jamming, selective forwarding, and data manipulation are shown in Figure 6 [39].

5.1.1 Denial of Service (DoS) Attacks

DoS attacks disable system services by sending repeated requests, as seen in Figure 5. The user cannot navigate or connect to the IoT device, which prevents them from making informed decisions. DoS attacks force Internet of Things devices to remain active, which causes battery drain. Repeated

attacks from various IP addresses create multiple requests to overwhelm a server in a DDoS attack. It's tough to tell natural from hazardous traffic. An IoT botnet malware has been responsible for disruptive DDoS attacks in recent years [40].

5.1.2 Sybil and Spoofing Attacks

These exploits obtain unwanted access to IoT systems using user identification (RFID and MAC address). The TCP/IP lacks a comprehensive security protocol, making IoT devices vulnerable to phishing. These two attacks also launch man-in-the-middle and DoS attacks [41].

5.1.3 Jamming Attacks

Continuous wireless network communication by broadcasting undesired signals to IoT devices causes user issues by keeping the network busy (Figure 6). This exploit affects IoT system performance by requiring more memory, bandwidth, etc. [42].

5.1.4 Man in Middle Attacks

Network participants carry out man-in-the-middle attacks directly connected to another user interface. False information may easily disrupt conversations. Bad data to hack original data [43].

5.1.5 Forwarding Attacks

Figure 5 illustrates how a broadcast attack node may be dropped in the middle of a transmission, resulting in a networking system hole. Malicious inbound assaults include Trojans, rootkits, worms, adware, and viruses that may cause financial harm, power dissipation, and corrupt wireless network output [44]. This attack is difficult to detect.

5.1.6 Holes Attacks

Black Hole and Gray Hole attacks are active attacks since they influence network performance and create crashes [45].

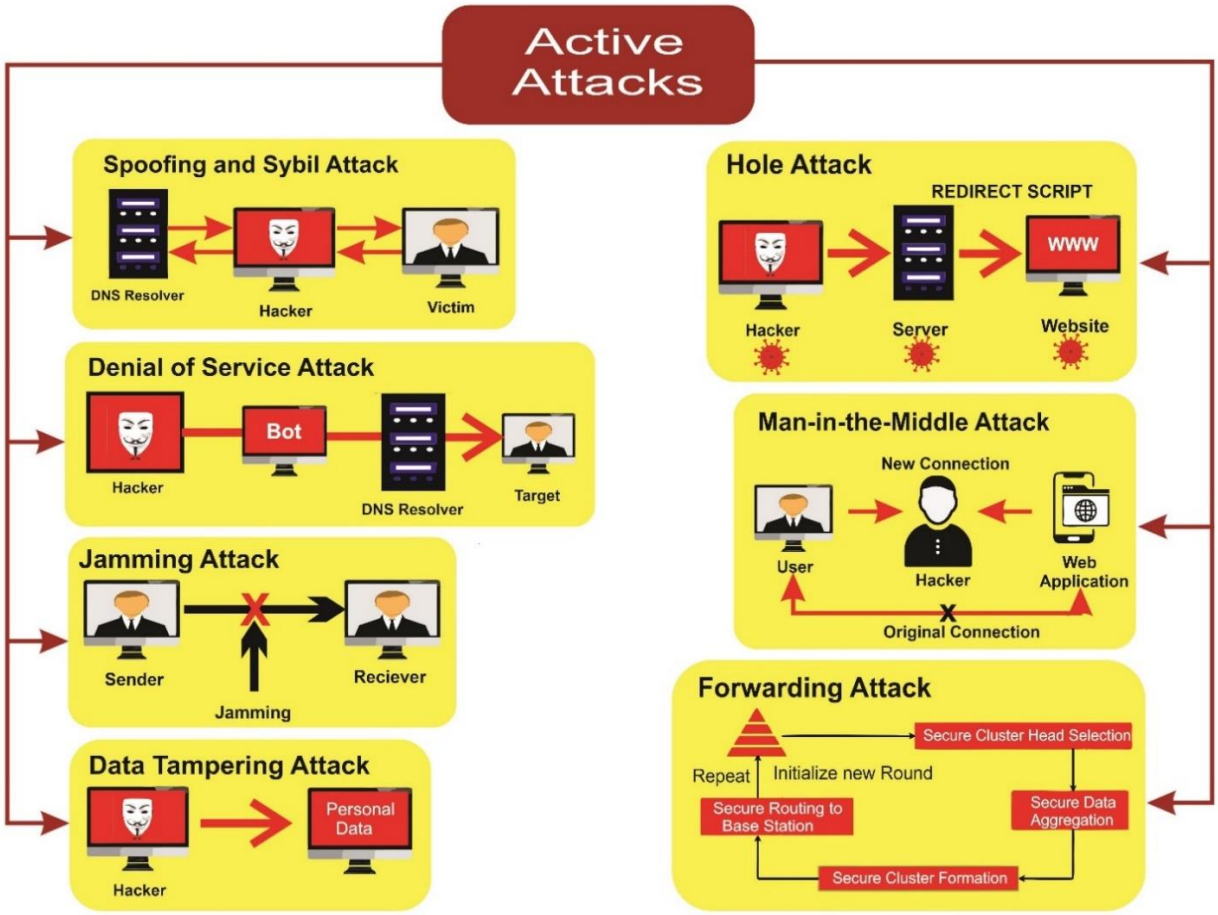

Fig. 6. Types of active attacks

5.1.7 Data Tampering Attacks

Data tampering threatens businesses, lives, and property. Companies must avoid such attacks and mitigate their harm [46].

5.2 Passive Attacks

Passive attacks capture user data without their awareness. Listening and traffic monitoring are prominent passive attack approaches [47].

- **Eavesdropping:** an attacker listens to two parties' messages. Attack works without encrypted traffic. The attacker can access unencrypted information, such as a password [48].
- **Traffic analysis:** the attacker analyses the traffic's metadata to learn about the traffic, such as the entities involved (speed, duration, etc.). Traffic analysis can lead to attacks if encrypted data is utilized, allowing an attacker to access decrypted information [49].

5.3 IoT Attacks Affect

IoT threats threaten network privacy, authentication, and authorization. Figure 6 lists the attacks and their consequences on IoT devices. When creating an IoT security protocol, consider the following.

5.3.1 Accessibility

Provides IoT device services to authorized users. DoS attacks and jamming make nonsensical requests and keep the network busy, undermining the IoT network. A solid security protocol is needed to keep IoT accessible to user clients [50].

5.3.2 Privacy

Privacy is the only IoT element attacked actively and passively. Today, secret papers, medical information, and national security data are securely encrypted and delivered over the Internet by various IoT devices. Hackers can follow the IoT computer's position and decode third-party data [51].

5.3.3 Integrity

To safeguard IoT data integrity, the recipient must verify that transferred or distributed messages have not been changed. Data integrity ensures that supplied data isn't altered. Even if intruders can't steal data, the network won't work if the susceptible nodes corrupt the delivered data. Insecure interaction channels can modify data without an attacker. Integrity check detects unintentional and purposeful message modifications [52].

5.3.4 Identification

Identification is essential for the authorization of IoT networks. Customers are required to register before they can connect to the Cloud Server. The commercialization of IoT and its resilience are both hindered by identification problems. Phishing and Sybil attacks lower the network's security level and allow unauthorized access to servers. Therefore, it's essential to find an efficient IoT system identification that offers excellent safety [53].

5.3.5 Authorization

Authorization is the user's IoT access. Authorized clients can enter, track, and use IoT data. Admins' directives are also performed. Preserving all user data and offering them information-based access is hard since users are sensors, devices, and services. Identification is IoT user authorization. Clients must register to use the cloud server. IoT trade-offs and resilience make detection challenging. Sybil and phishing attacks impair network security, and attackers get server access without proper identification. A suitable IoT system identification technique is essential to safeguard system restrictions [54]. User permission is accomplished by identification in the IoT. To utilize the cloud server, clients first need to register. The internet of things' resilience and trade-offs compound the detection challenges. Attacks such as spoofing and Sybil weaken the security of a network and make it easier for attackers to access a server without the necessary ID. When protecting system limits, having an appropriate identification method for IoT systems is vital [55].

5.4 IoT Anomaly Detection

There are unconventional real-world datasets. Identifying anomalies implies detecting unusual phenomena compared to typical nodes. Intrusion

Prevention Systems, Fraud Detection, and Data Leakage generate abnormalities. Smart cities, network security, and industries employ anomaly detection [56].

5.4.1 Detection of Intrusion

IoT devices are connected to the Internet and are nevertheless vulnerable to cyber-attacks. DoS and DDOS attacks, for example, do severe harm to the IoT network. Detecting and preventing these threats is the most challenging difficulty in IoT systems [57].

5.4.2 Detecting Fraud

During online logins or payments, IoT networks are vulnerable to intercepting credit card information, banking information, or other personal information [57].

5.4.3 Data Leakage

The disclosure of confidential information from databases, file servers, and other information sources by external entities may lead to the loss of data and jeopardize the confidentiality of the information. Such losses may be prevented using suitable encryption algorithms [56].

5.5 Anomalies Types

It can be identified as a contextual or communal point in the form [57].

5.5.1 Anomalies in Points

Anomalies are used to identify points that are considerably different from the rest of the data points when the evolution of the sequence is unexpected. Frequently used in the identification of fraud [57].

5.5.2 Anomalies in Groups

Many IoT devices exhibit typical time series patterns, such as recurring patterns or shapes. However, a joint audit and review are necessary if several delays occur in the supply chain [56].

5.5.3 Anomalies in Context

The kind of meaning of past information, such as the day of the week, is used to detect it. The circumstances practically cover the whole domain [56].

6. IOT SECURITY BASED ON MACHINE LEARNING

IoT systems must adopt a defensive posture while identifying the primary parameters in security protocols to adjust for dynamic and diverse networks as intelligent attacks and MLs become more common. This is a difficult endeavor since the IoT device's limited resources make it difficult to precisely estimate the current network and attack condition. Reinforcement learning supervised learning, and unsupervised learning are three machine learning approaches used to improve network security in the IoT. Through malware identification, downloaded anti-jamming, access control, and authentication, these strategies serve to increase security [58]. These methods are outlined below in Figure 7.

6.1 Reinforcement Learning

Deep Q networks, post-decision states, Dyna-Q, and Q-learning are examples of reinforcement learning approaches. Through trial and error, these strategies assist IoT devices in selecting security protocols and important parameters for various threats. Q-learning, for example, is utilized as a model-free approach to improve malware detection, downloaded anti-jamming, and authentication performance. Dyna-applicability Qs in malware detection and authentication can also be considered by IoT devices. Finally, malware is detected using the post-decision state [59].

6.2 Supervised Learning

Random Forest, Deep Neural Network (DNN), Neural Network, K-Nearest Neighbor (KNN), Naive Bayesian, and SVM (Support Vector Machine) are examples of supervised learning approaches [60]. To construct a classification or regression model, these approaches may be used to label application traces or network data from

IoT devices. SVM may be used by IoT devices to identify phishing attacks and network breaches, for example. A K-NN program to identify malware and network breaches may exist. Then, to identify DoS attacks and network breaches, neural networks are deployed. IoT systems may also employ naive Bayes to identify intrusions, and malware may be detected using the Random Forest Classifier [61]. Finally, DNNs may be used for phishing detection in IoT devices with enough memory and processing capability.

6.2.1 Role of Supervised Learning in IoT Security

Supervised learning approaches are led by a goal that creates a mathematical framework for datasets. This approach employs tagged data to train an algorithm that describes input data best. Inputs and outcomes are offered for learning. These datasets assist machines in discovering outputs for inputs [62]. Supervised learning performance may be achieved when particular targets are specified. For such understanding, it's vital to identify the machine's desired outputs and actual inputs [5]. It identifies rules from datasets and defines classes. Predict criteria, persons, and objects' class memberships. To identify network traffic in an IoT device, you must employ neural networks, KNN, Naive Bayes, and SVM [63]. Classification models can be used if a class or value category has few outputs. Regression can be utilized when the predicted output value is numeric. KNN can identify viruses and networks in IoT systems [64].

Supervised learning techniques use tagged data in IoT networks to solve location, security, adaptive filtering, channel estimation, and spectrum detection. This ML category uses regression and classification. Using classification, supervised learning predicts and models data sets. Regression predicts numerical variables reflecting trends [65]. Decision trees, random forest, naive Bayes, and SVM are classification algorithms. SVM utilizes a kernel to distinguish between classes. SVM models nonlinear decision boundaries. SVM naturally reflects memory intensity; therefore, choosing a kernel may be tricky. This complicates the modelling of massive datasets. IoT users prefer random forests to SVM [65]. Naive Bayes models issues like spam detection and text categorization. Random forest algorithms are naïve, and all input qualities are mutually free, making them better for simulating real-world matters [66]. Random Forest methods are readily developed and adaptable to dataset size. These algorithms demand more training time than Naive Bayes and SVM. It also improves prediction accuracy and precision in less time [66]. It's then linked to a graph with leaves and

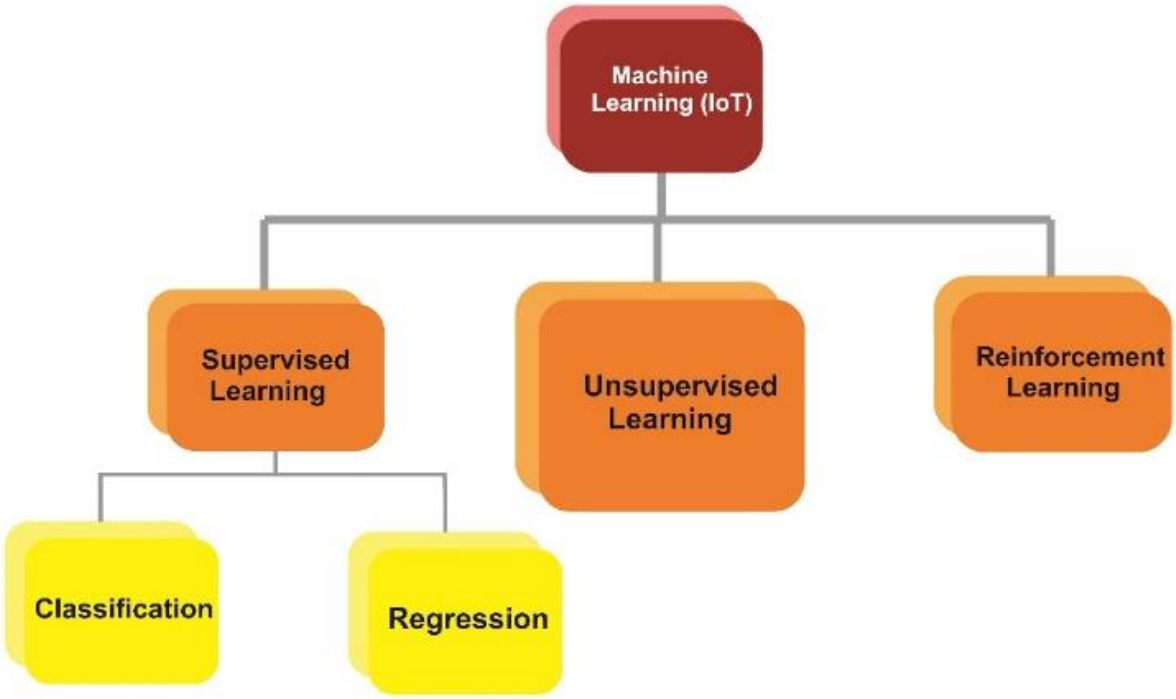

Fig.7. Machine Learning and Its Classification

branches to represent class and choice. A top-down technique traverses the tree to rate an event until a class-specific choice is made. Regression methods include logistic regression and ANN [66]. These are instance-based algorithms. These forecast fresh observations based on training data. Such methods are memory-intensive and perform poorly with substantial data sets.

6.3 Unsupervised Learning

There is no necessity for data labelling, unlike supervised learning. It examines the similarities between unlabeled data to categorize them [67]. IoT systems, for example, might use multivariate correlation analysis to identify DoS attacks. They could also enforce IGMM with PHY-based authentication with privacy protection [67]. While supervised learning focuses on document categorization in the IoT system, unsupervised learning ensures the grouping of documents in the IoT system to increase security. This is in contrast to unsupervised learning providing the set of records in the IoT system.

6.3.1 Role of Unsupervised Learning in IoT Security

Unsupervised learning trains algorithms with unlabeled data. Describing a pattern helps notice a way. If so, incoming data helps the algorithm uncover rules and patterns. Summarizing and combining key points provides meaning and clarity [68]. No output configuration. Unsupervised learning uses association and grouping methods. Clustering involves combining data sets and discovering similarities. This uses K-mean and PCA (principal component analysis). In unsupervised learning, the environment provides input without a purpose. Similarity searches may be done on untagged data. Data may be categorized. Unsupervised learning techniques handle unlabeled data heuristically. Balance loads, group cells, and identify intrusions, faults, and abnormalities. Clustering group data based on similarities and contrasts in unsupervised learning [68]. Unmonitored cluster development means no established performance procedures. Use the displayed data to assess the correctness of the results. If there's an incorrect or correct answer, dataset groupings may be pre-labelled. In this situation, classification methods are preferred. Hierarchical and K-mean clustering are prevalent [69]. K-means is a common technique for categorizing data based on geometric distinctions. Clusters must merge across centroids to become uniformly spherical.

Before clustering, define the cluster size. Clustering does not indicate competence and efficiency. Non-global clusters can cause poor clustering. Most IoT systems and applications use unsupervised learning with limited external environment knowledge. This resembles animal learning. Zero-day attacks on IoT networks are unknown [69].

7. COMPARATIVELY ANALYSIS OF ML ALGORITHMS USED FOR IDS

Table 1 shows that researchers employed ML algorithms and approaches to detect attacks and anomalies with high accuracy. In investigations [70-81], researchers utilized and compared different ML algorithms. The Random Forest (RF) method obtained the best results with 99.34 %, 99.5 %, 99.9 %, 99.59 %, and 99.9 % accuracy. DT and KNN outperformed the other methods. However, KNN takes longer to classify. In addition, combining RF and DT improved attack detection accuracy. RF and KNN obtained 99.9 % attack detection accuracy in experiments.

The evaluated study indicated that Random Forest ML provided the best attack and anomaly detection. ML is suited for IoT-specific challenges and general cybersecurity applications. ML-based systems balance IoT network risks depending on their speed and adaptability. All ML research is encouraged. ML's importance as an emerging technology is well-established.

8. IOT SECURITY LIMITATIONS OF THE ML APPROACH

Figure 8 shows the number of linked IoT devices, the worldwide IoT market, and forecast predictions through 2025. Since then, electrical and computer engineers have paid much attention to IoT development and security. Machine learning is used to safeguard IoT networks, but it has limits. Uncertainty, fluctuating speed, variety, and volume characterize IoT traffic. Traditional machine-

learning approaches are not scalable enough for IoT data handling [9]. Major field modifications require a precondition. Limitations of ML in IoT networks include energy processing, and data analysis issues as shown in Figure 9.

8.1. Energy Processing

ML algorithms have a sample, computational, and memory complexity. Conventional ML algorithms aren't scalable for small tasks. Traditional ML algorithms aren't fit for resource-constrained IoT. Intelligent IoT devices need real-time data processing for applications. Traditional ML approaches can't handle real-time data streams [82-83].

8.2. Data Analysis

Communication and sensor devices and network-based information systems may generate wireless data. IoT systems value data. To extract sensitive data, do efficient analyses. IoT applications confront a severe issue in managing massive data. IoT data creation is semantical, format-, and type-diverse. Semantic and syntactic heterogeneity. These heterogeneities complicate IoT big data management [84].

9. CONCLUSION

The IoT can revolutionize the globe and solve global challenges. Thanks to innovative IoT services, everyone on the network may access, connect, and store information. While IoT improves our lives through smart gadgets that link us to the virtual world, security is a serious problem. This article reviews Machine Learning-based IoT security literature, encompassing IoT and its architecture, security risks, ML-based methods, and ML-based security solutions. This study focuses on built-in machine learning techniques for IoT security, giving an overview of threats and their implications. In addition, research has been done on machine learning algorithms to identify potential roadblocks, which may be helpful to future researchers as they

Table 1. Summary of Literature Review

Dataset	Feature Optimization Approach	Classifier	Accuracy	Reference
UCI's ML repository	Intrusion and attack detection for IoT Botnet.	SVM, Random Forest	99 %	[70]
IoT-23	ML-based detecting anomalies in IoT networks	Random Forest	99.50 %	[71]
BoT-IoT	Improving IoT Security by ML	Random Forest	99 %	[72]
NSL-KDD, DS2OS	ML Based prediction of attacks on IoT networks.	Random Forest	99.4 %	[73]
CICIDS-2017, Cyberattack	Detection of anomalous activities	Random Forest	99.9 %	[74]
IoT Network Intrusion Dataset	Enhance IoT security through ML methods on the IoT network	KNN	99 %	[75]
UCI	Detect Attacks in IoT devices	Decision Tree	99.20 %	[76]
UNSW-NB15	ML-based detection of attacks and anomalies in IoT	Random Forest + KNN	99 %	[77]
KDDCUP99	Improve the security IDS	KNN, Decision Tree	99.9 %	[78]
IoT-23	Anomaly Detections in IoT Networks.	Random Forest	99.50 %	[79]
UNSW-NB 15	Attack Detection in IoT Networks	Random Forest	99.5 %	[80]
Bot-IoT	Detecting IoT attacks	Random Forest	97.00 %	[81]

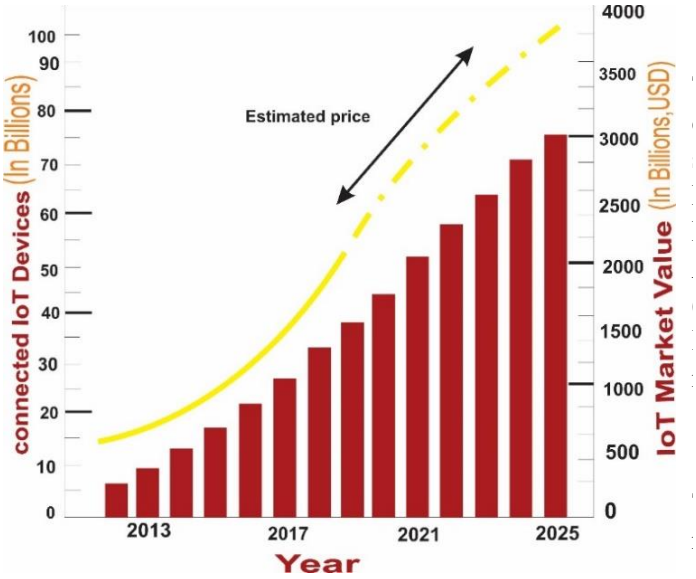

Fig. 8. Total Connected IoT Devices, Global IoT Market, and Future Forecast

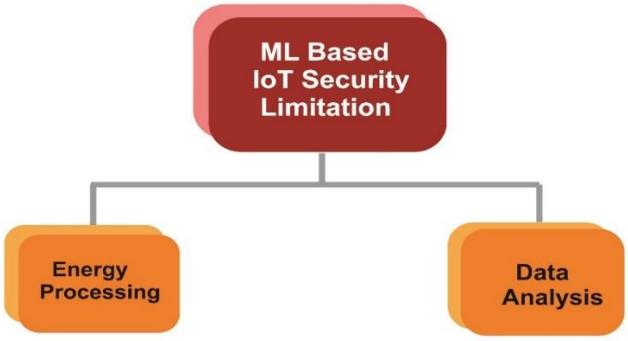

Fig. 9. Machine Learning-Based IoT Security Limitations

choose their ultimate goals.

10. ACKNOWLEDGEMENTS

The authors would like to thank the referees for their careful reading and for their comments, which significantly improved the paper. Additionally, thanks to Dr. Salman Qadri, (Associate Professor, Chairman Department of Computer Science, MNS University of Agriculture, Multan, Pakistan) and Dr. Farrukh Jamal, (Assistant Professor, Department of Statistics, The Islamia University of Bahawalpur, Pakistan) for his motivational support.

11. CONFLICT OF INTEREST

The authors declare no conflict of interest.

12. REFERENCES

1. S.T. Arzo, C. Naiga, F. Granelli, R. Bassoli, M. DevetsikIoTis, and F.H. Fitzek. A Theoretical Discussion and Survey of Network Automation for IoT: Challenges and Opportunity. *IEEE Internet of Things Journal* 8(15):12021-12045(2021).
2. D. Desai, and H. Upadhyay. Security and privacy consideration for internet of things in smart home environments. *International Journal of Engineering Research and Development* 10(11):73-83(2014).
3. M. Boland, F. Alam, and J. Bronlund. Modern technologies for personalized nutrition. *Trends in Personalized Nutrition* 195-222(2019).
4. R. Karthick, A.M. Prabaharan, and P. Selvaprasanth. Internet of things based high security border surveillance strategy. *Asian Journal of Applied Science and Technology* (AJAST) (3):94-100(2019).

5. T. Alam. IBchain: Internet of things and blockchain integration approach for secure communication in smart cities. *Informatica* 45(3)1-14(2021).
6. V. Chang, L. Golightly, P. Modesti, Q.A. Xu, L.M.T. Doan, K. Hall, ... and A. Kobusińska. A Survey on Intrusion Detection Systems for Fog and Cloud Computing. *Future Internet* 14(3):89(2022).
7. C. Butpheng, K.H. Yeh, and H. Xiong. Security and privacy in IoT-cloud-based e-health systems—A comprehensive review. *Symmetry* 12(7):1191(2020).
8. D. Ageyev, T. Radivilova, and O. Mohammed. Traffic Monitoring and Abnormality Detection Methods Analysis. IEEE International Conference on Problems of Infocommunications. *Science and Technology* (PIC SandT) 823-826(2020).
9. H.A. Abdul-Ghani, and D. Konstantas. A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective. *Journal of Sensor and Actuator Networks* 8(2):22(2019).
10. A. Abeshu, and N. Chilamkurti. Deep learning: the frontier for distributed attack detection in fog-to-things computing. *IEEE Communications Magazine* 56(2): 169-175(2018).
11. S. Shamshirband, M. Fathi, A.T. Chronopoulos, A. Montieri, F. Palumbo, and A. Pescapè. Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. *Journal of Information Security and Applications* 55:102582(2020).
12. P.R. Kumar, J.S. Raj, and S. Smys. Analysis of dynamic topology wireless sensor networks for the Internet of Things (IOT). *International Journal of Communication Systems* 34(17):315(2021).
13. I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming. Ad-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* 0305-0310(2019).
14. S.V.N. Santhosh Kumar, M. Selvi, and A. Kannan. A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things. *Computational Intelligence and Neuroscience* (2023).
15. W. Li, Y. Chai, F. Khan, S.R.U. Jan, S. Verma, V.G. Menon, and X. Li. A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system. *Mobile networks and applications* 26:234-252(2021).
16. H. Mliki, A.H. Kaceam, and L. Chaari. A comprehensive survey on intrusion detection-based machine learning for IOT networks. *EAI Endorsed Transactions on Security and Safety* 8(29):e3-e3(2021).
17. M. Imran, U. Zaman, J. Imtiaz, M. Fayaz, and J. Gwak. Comprehensive survey of IoT, machine learning, and blockchain for health care applications: A topical assessment for pandemic preparedness, challenges, and solutions. *Electronics* 10(20):2501(2021).
18. A. Gaurav, B.B. Gupta, and P.K. Panigrahi. A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system. *Enterprise Information Systems* 1-25(2022).
19. M. Zubair, A. Ali, S. Naeem, S. Anam. Traffic Video-Based Parking and Abandoned Object Event Detection. *Proceedings of the MOL2NET'22, Conference on Molecular, Biomedical and Computational Sciences and Engineering 8th ed*. 1–15(2023).
20. M. Zubair, A. Ali, S. Naeem, S. Anam, Image Processing Algorithm. P*roceedings of the MOL2NET'22, Conference on Molecular, Biomedical and Computational Sciences and Engineering 8th ed.* 1–15(2023).
21. M. Zubair, A. Ali, S. Anam. A DDDAS-Based Impact Area Simulation Study of Highway Abnormalities. *Proceedings of the MOL2NET'22, Conference on Molecular, Biomedical and Computational Sciences and Engineering 8th ed*. 1–15(2023).
22. M. Zubair, A. Ali, S. Naeem, S. Anam, Video Streams for The Detection of Thrown Objects from Expressways. P*roceedings of the MOL2NET'22, Conference on Molecular, Biomedical and Computational Sciences and Engineering 8th ed.* 1–15(2023).
23. A. Tewari, and B.B. Gupta. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future generation computer systems* 108: 909-920(2020).
24. S. Rekha, L. Thirupathi, S. Renikunta, and R. Gangula. Study of security issues and solutions in Internet of Things (IoT). *Materials Today: Proceedings* (2021).
25. H. HaddadPajouh, A. Dehghantanha, R.M. Parizi, M. Aledhari, and H. Karimipour. A survey on internet of things security: Requirements, challenges, and solutions. Internet of Things 14:100129(2021).
26. W.Z. Khan, M.H. Rehman, H.M. Zangoti, M.K.

Afzal, N. Armi, and K. Salah. Industrial internet of things: Recent advances, enabling technologies and open challenges. *Computers and Electrical Engineering* 81: 106522(2020).

27. M. Noura, M. Atiquzzaman, and M. Gaedke. Interoperability in internet of things: Taxonomies and open challenges. *Mobile networks and applications* 24(3):796-809(2019).
28. M. Lombardi, F. Pascale, and D. Santaniello. Internet of things: A general overview between architectures, protocols and applications. *Information* 12(2):87(2021).
29. M. Jangjou, and M.K. Sohrabi. A Comprehensive Survey on Security Challenges in Different Network Layers in Cloud Computing. *Archives of Computational Methods in Engineering* 1-22(2022).
30. D. Oliveira, M. Costa, S. Pinto, and T. Gomes. The future of low-end motes in the Internet of Things: A prospective paper. *Electronics* 9(1):111(2020).
31. Z. Shouran, A. Ashari, and T. Priyambodo. Internet of things (IoT) of smart home: privacy and security. *International Journal of Computer Applications* 182(39):3-8(2019).
32. L. Da Xu, Y. Lu, and L. Li. Embedding blockchain technology into IoT for security: A survey. *IEEE Internet of Things Journal* 8(13):10452-10473(2021).
33. G. Han, H. Wang, X. Miao, L. Liu, J. Jiang, and Y. Peng. A dynamic multipath scheme for protecting source-location privacy using multiple sinks in WSNs intended for IIoT. *IEEE Transactions on Industrial Informatics* 16(8):5527-5538(2019).
34. M.Z. Gunduz, and R. Das. Cyber-security on smart grid: Threats and potential solutions. *Computer networks* 169:107094(2020).
35. M. Arulprakash, and R. Jebakumar. People-centric collective intelligence: decentralized and enhanced privacy mobile crowd sensing based on blockchain. *The Journal of Supercomputing* 77(11):12582-12608(2021).
36. K. Kimani, V. Oduol, and K. Langat. Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection* 25:36-49(2019).
37. D.A.S. Resul, and M.Z. Gündüz. Analysis of cyberattacks in IoT-based critical infrastructures. *International Journal of Information Security Science* 8(4):122-133(2020).
38. C. Silpa, G. Niranjana, and K. Ramani. Securing Data from Active Attacks in IoT: An Extensive Study. In Proceedings of International Conference on Deep Learning, Computing and Intelligence, *Springer* 51-64(2022).
39. N.F. Syed, Z. Baig, A. Ibrahim, and C. Valli. Denial of service attack detection through machine learning for the IoT. *Journal of Information and Telecommunication* 4(4):482-503(2020).
40. Y. Tian, S. Chen, and L. Zhang. Unsupervised Detection of Sybil Attack in Wireless Networks. In *IOP Conference Series: Earth and Environmental Science* 693(1):012114(2021).
41. H. Pirayesh, and H. Zeng. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE Communications Surveys and Tutorials* (2022).
42. M. Thankappan, H. Rifà-Pous, and C. Garrigues. Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks: A State-of-the-Art Review. *preprint arXiv*:2203.00579(2022).
43. A. Ali, S. Naeem, S. Anam, M. Zubair. Agile Software Development Processes Implementing Issues and Challenges with Scrum. P*roceedings of the MOL2NET'22, Conference on Molecular, Biomedical and Computational Sciences and Engineering 8th ed.* 1–15(2023).
44. A. TsIoTa, D. Xenakis, N. Passas, and L. Merakos. On jamming and black hole attacks in heterogeneous wireless networks. I*EEE Transactions on Vehicular Technology* 68(11):10761-10774(2019).
45. D. W. Huang, W. Liu, and J. Bi. Data tampering attacks diagnosis in dynamic wireless sensor networks. *Computer Communications* 172:84-92(2021).
46. K. Guha, S. Saha, and A. Chakrabarti. Bypassing Passive Attacks. In Self Aware Security for Real Time Task Schedules in Reconfigurable Hardware Platforms *Springer* 91-110(2021).
47. D. K. Jasim, and S. B. Sadkhan. The Eavesdropping Attack on Security tradeoff for Cognitive Radio Networks. In *2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA)* 223-229(2021).
48. L. Basyoni, N. Fetais, A. Erbad, A. Mohamed, and M. Guizani. Traffic analysis attacks on Tor: a survey. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)* 183-188(2020).
49. P. K. Jena, S. Ghosh, and E. Koley, Design of a coordinated cyber-physical attack in IoT based smart grid under limited intruder accessibility. *International Journal of Critical Infrastructure Protection* 35:100484(2021).

50. M. M. Ogonji, G. Okeyo, and J. M. Wafula, A survey on privacy and security of Internet of Things. *Computer Science Review* 38:100312(2020).
51. H. Xu, W. Yu, X. Liu, D. Griffith, and N. Golmie. On data integrity attacks against industrial Internet of Things. In *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)* 21-28(2020).
52. S. Rizvi, R. J. Orr, A. Cox, P. Ashokkumar, and M.R. Rizvi. Identifying the attack surface for IoT network. *Internet of Things* 9:100162(2020).
53. Y. Zhao, J. Yang, Y. Bao, and H. Song. Trustworthy authorization method for security in Industrial Internet of Things. *Ad Hoc Networks* 121:102607(2021).
54. M.A. Ferrag, L. Maglaras, and A. Derhab. Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends. *Security and Communication Networks* (2019).
55. I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming. Ad-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* 0305-0310(2019).
56. A.A. Cook, G. Mısırlı, and Z. Fan. Anomaly detection for IoT time-series data: A survey. *IEEE Internet of Things Journal* 7(7):6481-6494(2019).
57. I.H. Sarker, A.I. Khan, Y.B. Abushark, and F. Alsolami. Internet of things (IoT) security intelligence: a comprehensive overview, machine learning solutions and research directions. *Mobile Networks and Applications* 1-17(2022).
58. A. Uprety, and D.B. Rawat. Reinforcement learning for IoT security: A comprehensive survey. IEEE Internet of Things Journal 8(11):8693-8706(2020).
59. V. Vijayalakshmi, and K. Venkatachalapathy. Comparison of predicting student's performance using machine learning algorithms. *International Journal of Intelligent Systems and Applications* 11(12):34(2019).
60. E. Toch, B. Lerner, E. Ben-Zion, and I. Ben-Gal. Analyzing large-scale human mobility data: a survey of machine learning methods and applications. *Knowledge and Information Systems* 58(3):501-523(2019).
61. F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris. A review of machine learning and IoT in smart transportation. *Future Internet* 11(4):94(2019).
62. P. Linardatos, V. Papastefanopoulos, and S. Kotsiantis. Explainable ai: A review of machine learning interpretability methods. *Entropy* 23(1):18(2020).
63. A. Aldahiri, B. Alrashed, and W. Hussain. Trends in using IoT with machine learning in health prediction system. *Forecasting* 3(1):181-206(2021).
64. Y. Liu, J. Wang, J. Li, S. Niu, and H. Song. Machine Learning for the Detection and Identification of Internet of Things Devices: A Survey. *IEEE Internet of Things Journal* 9(1):298-320(2021).
65. E.G. Dada, J.S. Bassi, H. Chiroma, A.O. Adetunmbi, and O.E. Ajibuwa. Machine learning for email spam filtering: review, approaches and open research problems. *Heliyon* 5(6):e01802(2019).
66. G. Casolla, S. Cuomo, V.S. Di Cola, and F. Piccialli. Exploring unsupervised learning techniques for the Internet of Things. *IEEE Transactions on Industrial Informatics* 16(4):2621-2628(2019).
67. T.T. Nguyen, P. Krishnakumari, S.C. Calvert, H.L. Vu, and H. Van Lint. Feature extraction and clustering analysis of highway congestion. *Transportation Research Part C: Emerging Technologies* 100:238-258(2019).
68. H. Yang, R. Zeng, F. Wang, G. Xu, and J. Zhang. An unsupervised learning-based network threat situation assessment model for Internet of Things. *Security and Communication Networks* (2020).
69. S. Bagui, X. Wang, X. Wang, and S. Bagui. Machine learning based intrusion detection for IoT botnet. *International Journal of Machine Learning and Computing* 11(6):399-406(2021).
70. S.H. Haji, and S.Y. Ameen. Attack and anomaly detection in IoT networks using machine learning techniques: A review. *Asian journal of research in computer science* 9(2):30-46(2021).
71. T. Wang, M. Z. A. Bhuiyan, G. Wang, L. Qi, J. Wu, and T. Hayajneh. Preserving balance between privacy and data integrity in edge-assisted Internet of Things. *IEEE Internet of Things Journal* 7(4):2679-2689(2019).
72. A. Batool, B. N. Hashmi, A. Ali, S. Naeem, S. Anam. IoT based smart mirror. Proceedings of the MOL2NET'22, Conference on Molecular, *Biomedical and Computational Sciences and Engineering 8th ed.* 1–15 (2023).
73. N. Elmrabit, F. Zhou, F. Li, and H. Zhou. Evaluation of machine learning algorithms for anomaly detection. In *2020 International Conference on*

Cyber Security and Protection of Digital Services (Cyber Security) 1-8 (2020).

74. Z. Liu, N. Thapa, A. Shaver, K. Roy, X. Yuan, and S. Khorsandroo. Anomaly detection on IoT network intrusion using machine learning. In *2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)* 1-5(2020).
75. M.H. Aysa, A.A. Ibrahim, and A.H. Mohammed. IoT ddos attack detection using machine learning. In *2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)* 1-7(2020).
76. A. Batool, B. N. Hashmi, A. Ali, S. Naeem, M. H. Bukhari, M. M. Khan. The Smart Cradle System Basis on Internet of Things. *Proceedings of the MOL2NET'22, Conference on Molecular, Biomedical and Computational Sciences and Engineering 8th ed.* 1–15(2023).
77. D. Rani, and N.C. Kaushal. Supervised machine learning based network intrusion detection system for Internet of Things. In *2020 11th International Conference on Computing, Communication and Networking Technologies* (ICCCNT) 1-7(2020).
78. A. Ali, S. Naeem, S. Anam, and M.M. Ahmed. Entropy in Information Theory from Many Perspectives and Various Mathematical Models. *Journal of Applied and Emerging Sciences* 12(2):158-167(2022).
79. I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming. Ad-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* 0305-0310(2019).
80. J. Alsamiri, and K. Alsubhi. Internet of things cyber-attacks detection using machine learning. *International Journal of Advanced Computer Science and Applications* 10(12):232(2019).
81. S. Naeem, and A. Ali. Bees Algorithm Based Solution of Non-Convex Dynamic Power Dispatch Issues in Thermal Units. *Journal of Applied and Emerging Sciences* 12(1):35(2022).
82. A. Ali, and S. Naeem. The Controller Parameter Optimization for Nonlinear Systems Using Particle Swarm Optimization and Genetic Algorithm. *Journal of Applied and Emerging Sciences* 12(1):56(2022).
83. A. Bhargava, G. Salunkhe, S. Bhargava, and P. Goswami. A Comprehensive Study of IoT Security Risks in Building a Secure Smart City. *Digital Cities Roadmap: IoT-Based Architecture and Sustainable Buildings,* 401-448(2021).
84. D. Li, L. Deng, M. Lee, and H. Wang. IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. *International journal of information management* 49:533-545(2019).