Asian Journal of Research in Computer Science

9(2): 30-46, 2021; Article no.AJRCOS.69410
ISSN: 2581-8260

Attack and Anomaly Detection in IoT Networks using Machine Learning Techniques: A Review

Saad Hikmat Haji[1*] and Siddeeq Y. Ameen[1]

[1]Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2021/v9i230218
Editor(s):
(1) Dr. Dariusz Jacek Jakóbczak, Koszalin University of Technology, Poland.
Reviewers:
(1) Sanjaya Kumar Behera, Utkal University, India.
(2) K. Parvathavarthine, Manonmaniam Sundaranar University, India.
Complete Peer review History: http://www.sdiarticle4.com/review-history/69410

Received 25 March 2021
Accepted 01 June 2021
Published 02 June 2021

Review Article

ABSTRACT

The Internet of Things (IoT) is one of today's most rapidly growing technologies. It is a technology that allows billions of smart devices or objects known as "Things" to collect different types of data about themselves and their surroundings using various sensors. They may then share it with the authorized parties for various purposes, including controlling and monitoring industrial services or increasing business services or functions. However, the Internet of Things currently faces more security threats than ever before. Machine Learning (ML) has observed a critical technological breakthrough, which has opened several new research avenues to solve current and future IoT challenges. However, Machine Learning is a powerful technology to identify threats and suspected activities in intelligent devices and networks. In this paper, various ML algorithms have been compared in terms of attack detection and anomaly detection, following a thorough literature review on Machine Learning methods and the significance of IoT security in the context of various types of potential attacks. Furthermore, possible ML-based IoT protection technologies have been introduced.

Keywords: Internet of Things (IoT); IoT attack; machine learning; anomaly detection.

**Corresponding author: E-mail: saad.hikmat91@gmail.com;*

1. INTRODUCTION

IoT interconnects electrical equipment with a server and shares information without human interference [1-4] [5,6]. Users can remotely control computers from anywhere, making them vulnerable to a range of threats. As a result, the security of the IoT system is very concerned about the growing number of intelligent devices today, as the devices contain private and valuable user information [1,4,6]. In his research presentation in 1999, Kevin Ashton first used the term IoT. IoT has been employed in different connectivity protocols to create a relation between the person and the virtual world through various smart devices and their services [7,8]. Smart home and portable products, for example, provide information about the position of the buyer, contact details, health details, etc., that must be safe and confidential [9]. As most IoT devices are resource-constrained (i.e., batteries, bandwidth, storage, and calculation), extraordinarily configurable and sophisticated protection strategies based on algorithms are not available [10-12].

Machine learning and deep learning approaches were widely used for various tasks, including classification, regression, and IoT applications such as intrusion detection, image analysis, and recommendation systems [13,14].

Machine learning (ML) approaches are an excellent solution to stable IoT programs. ML is an innovative tool for artificial intelligence, which cannot be complicated and can surpass complex networks [11][15]. A wide range of attacks and a safety plan is developed using the ML methods to train a machine. Furthermore, Machine Learning developments appear promising in detecting and intelligent handling of new threats via learning skills. Future IoT device security protocols would also make ML algorithms more reliable and accessible than before [16,17].

The remainder of this article has the following structure: Section 2 provides an overview of IoT and its security, layers, and IoT security importance; Section 3 provides IoT attacks, impact and various attack surfaces, anomaly detection in IoT, ML in IoT security, including various types of learning algorithms and IoT security solutions; Section 4 provides an overview of published papers on ML-based IoT security; Section 5 presents an overview and discussion of the reviewed papers; Finally, Section 6 presents the conclusion of the survey.

2. INTERNET OF THINGS (IOT)

The Internet of Things or IoT means the trillions of physical devices connected to the Internet and the worldwide storage and data exchange. With the emergence of cost-effective computer chips and a broad-based wireless network, anything from a pill to an aircraft can now be transformed into a part of the IoT [19-22]. By connecting and attaching sensors to all these different things, artificial intelligence can be applied to otherwise dumb devices so they can share real-time data without needing a human. The Internet of things makes our society more intelligent and adaptive and fuses the

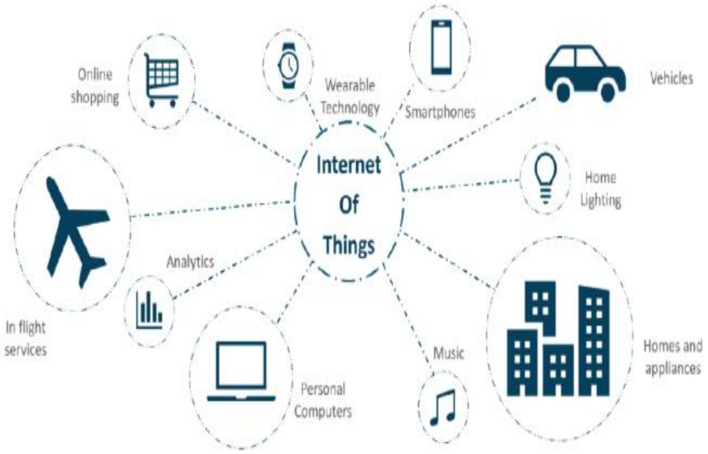

Fig.1 IoT in Action [18]

digital and physical worlds [18, 23-25].

2.1 Internet of Things (IoT) Layers

To create a connection and extend IoT's services at each doorway, the IoT architecture is a portal to different hardware applications [26]. Different networking protocols such as Bluetooth, Wi-Fi, RFID, narrow and broadband, ZigBee, LPWAN are followed to transmit and receive information/data from different layers of the IoT architecture [23,27].

A typical IoT architecture mainly comprises three layers: physical, network, and application layers [28,29].

2.2 Security in the Internet of things (IoT)

IoT device security in the 21st century has been a burning issue. On one side, IoT binds the whole universe and takes it close. On the other, it opens different windows for attacks of various kinds [30-32].

IoT apps are used across an open network for different purposes, making their devices more user-friendly [33]. On the one hand, IoT places human life at higher risk because of various risks and attacks; on the other hand, IoT makes it simpler and more obedient in technical terms [34,35]. IoT device protection is becoming a burning concern because specific IoT devices can be accessed from anywhere without user consent [35,36]. To secure IoT products, a wide variety of security systems have to be deployed. However, IoT devices' physical structure limits their computer functionality, limiting the implementation of a complex security protocol [37,38].

Table 1. Role and functionality of Iot layers

IoT Layers	Role and functionality
Sensor/Physical Layer	The characteristics of this layer are sensing, and knowledge about the world in which intelligent objects are available is gathered and collected [1,4,6]
Network Layer	The layer functionality enables the data to be transmitted and processed using the internet access of the different devices [1,4,6]
Application Layer	Its crucial function is to provide the user with a particular application-based service [1,4,6]

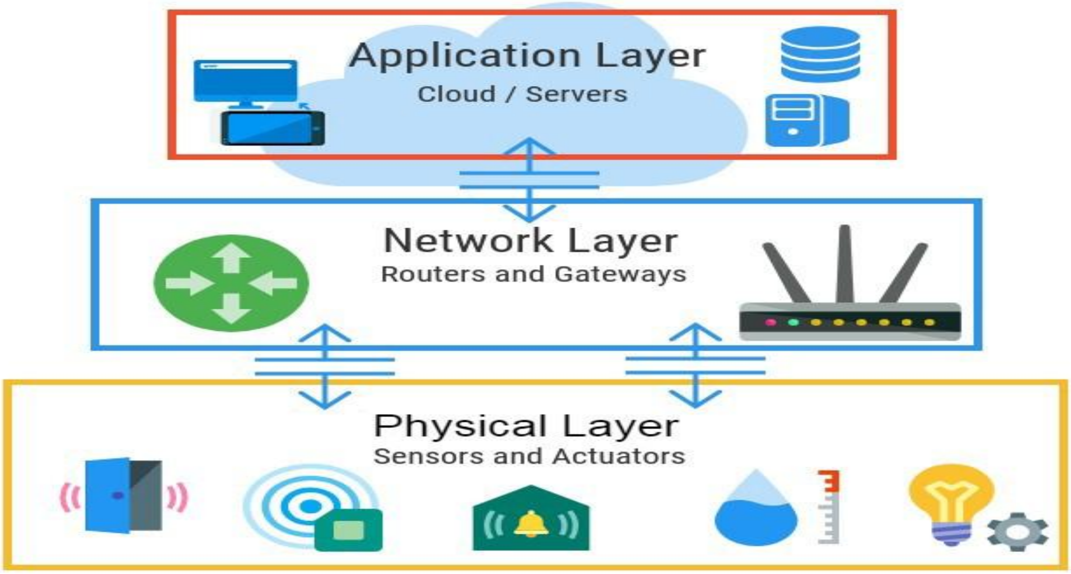

Fig. 2. The architecture of IoT Layers [30]

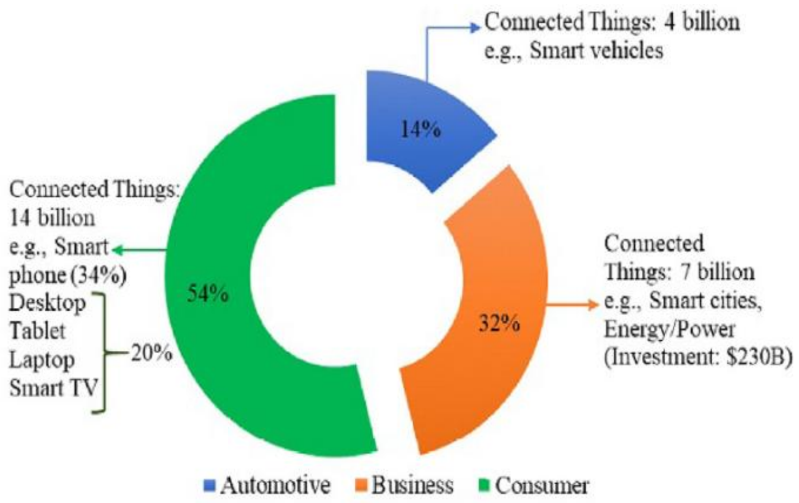

Fig.3 IoT device users estimated by 2021 [20]

It is essential to consider the properties that characterize protection when defining a stable IoT. In a standard IoT program, security specifications are grouped into three major categories: (I) confidentiality, (ii) integrity, and (iii) authentication [39].

- In keeping information concealed from third people, confidentiality means discretion. Sensitive sensors demand secrecy, for example, with crucial military information. The Wireless Sensor Network (WSN) system is one of the most often requested qualities. If a WSN's reports could be manipulated, forces may be misled, which might benefit the adversary. In vital social and industrial applications, confidentiality is equally critical [39].
- The communication receiver must ensure that messages received during transmission or delivery have not changed to protect the integrity of IoT data. The integrity of the data confirms that the sent data is not altered or distorted. It is particularly significant because even when intruders cannot obtain data, the network may not perform effectively if compromising nodes damage the sent data. Indeed, data may be modified without an intruder if the communication connection is not dependable. Integrity control guarantees that accidental and deliberate changes in the message are detected [39].
- The authentication process determines if a communication comes from where it is claimed or what it is proclaimed to be. The sensor nodes shall determine the identification and authenticity of the peer node they are conveying. Authenticity ensures an authentic message. Message Authentication Code (MAC) is brief information used for message authentication and provides the message's integrity and validity [39,40].

3. IOT ATTACKS

IoT system has seen various attacks over the past few years, making manufacturers and consumers more aware of IoT products [41,42]. This section outlines multiple types of attacks, effects, and IoT surfaces.

The Attacks in IoT are divided into two types: cyber and physical. Cyberattacks include both passive and active attacks, as shown in Fig.4. A cyber-attack threat targets multiple IoT device by hacking and operations in a wireless network (stealing, erasing, changing, or destroying) the user's data. Physical assaults, on the other hand, cause physical harm to IoT devices [30].

Here, no network is required to attack the device. Such attacks are also subject to physical IoT devices, such as mobile devices, cameras, sensors, routers, etc. [30 43].

According to their severity in Active and Passive IoT devices, the following subsections concentrate primarily on the various cyberattack forms as two majors cyberattack types [30].

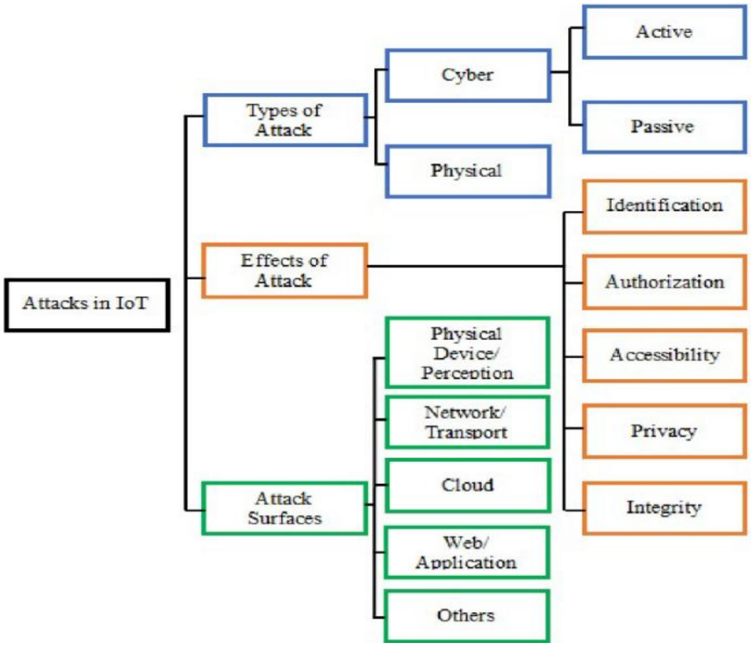

Fig.4 complete list of IoT attacks, including various attacks, attack surfaces and attack effects [30]

3.1 Active IoT Attacks

An active attack happens when a network attacker accesses the interface settings and disconnects certain services [44,45]. Protection of IoT devices may be attacked in various ways, including interruption, interventions, and changes in active attacks. Fig.5 describes active attacks, e.g., DoS, middle-hand attacks, Sybil attacks, spoofing, hole attacks, jamming, selective Forwarding, malicious inputs, data tampering, etc. [30].

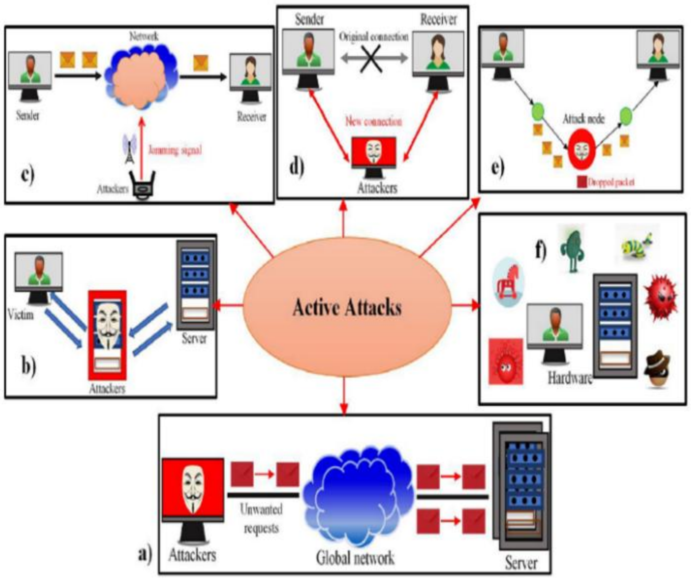

Fig. 5. Different forms of cyber-attacks

- **Denial of Service Attacks (DoS):** DoS attacks are primarily responsible for disabling system services by generating many repetitive demands, as shown in Fig.5. As a result, the user cannot navigate and connect to the IoT device, making informed decision-making impossible. Furthermore, DoS attacks keep IoT devices turned on all the time, reducing battery life[46-48]. A distributed denial of service (DDoS) attack occurs as several attacks are initiated from different IP addresses to generate various requests to hold the server busy. This makes distinguishing between natural and malicious traffic impossible [49,50]. In recent years, a specific IoT botnet virus known as Mirai has been responsible for initiating disruptive DDoS attacks, causing thousands of IoT computers to malfunction due to interferences [30,51].
- **Spoofing and Sybil attacks:** these types of attacks are mainly used to gain unauthorized access to IoT systems by targeting user identification (RFID and MAC address), as seen in Fig.5. The TCP/IP suite lacks a robust security protocol, making IoT devices more vulnerable, mainly spoofing attacks. Furthermore, these two attacks initiate additional extreme attacks, such as man-in-the-middle attacks and denial-of-service (DoS) [30,52].
- **They were jamming attacks:** Continuous communication in a wireless network through transmitting undesirable signals to IoT devices, causing problems for users by keeping the network constantly busy, as shown in Fig.5. Furthermore, this type of attack reduces the performance of IoT systems by using more memory, bandwidth, and so on [30].
- **Man-in-the-middle attacks:** Man-in-the-middle attacks are carried out by network members directly linked to another user interface, as shown in Fig. 5. As a result, it is simple to disrupt communications by adding bogus and incorrect data to hack original data [30,53,54].
- **Selective Forwarding attacks:** The transmission attack functions as a node of the communication device, which can be dropped to create a networking hole, as seen in Fig.5 during transmission. It is hard to detect and stop this kind of attack [30].
- **Malicious Input attacks:** Malicious input attacks include malicious attacks by malware, including Trojans, rootkits, worms and adware, and viruses that cause financial damage, dissipation of power, and deteriorating IoT systems' wireless network output, as seen in Fig.5 [30].
- **Hole Attacks:** Blackhole and Grayhole attacks are classified as Active assaults since they affect network performance and cause the network to collapse as shown in Fig.5 [51].
- **Data Tampering:** Data tampering is a severe threat not just to corporations but also to people's lives and property. As a result, companies must take precautions to avoid such assaults and reduce whatever damage they may inflict as seen in Fig.5 [30].

3.2 Passive IoT Attacks

Passive attacks are designed to collect information about the user without their knowledge and decode their private, encrypted data [55,56]. Eavesdropping and traffic monitoring are the two most popular techniques for conducting a passive attack on an IoT network [57].

- **Eavesdropping:** The attacker listens in on messages sent and received by two entities. The traffic must not be encrypted for the attack to be effective. The attacker can obtain any unencrypted information, such as a password supplied in response to an HTTP request [57,58].
- **Traffic analysis:** The attacker examines the metadata transmitted in traffic to derive traffic information, e.g., exchanged traffic and the involved entities (rate, duration, etc.). If encrypted data is employed, traffic analyses can also lead to cryptanalysis assaults, leading to the attacker obtaining information or successful traffic unencrypted [57].

3.3 Affects of Attacks in IoT

To protect users' privacy, authentication, and permission, the impact of IoT attacks is threatening for the network. Fig. 6 provides a complete list of various forms of attacks, including their effects on IoT devices. When designing a security protocol for the IoT device's attacks, the following features must be considered [30,59].

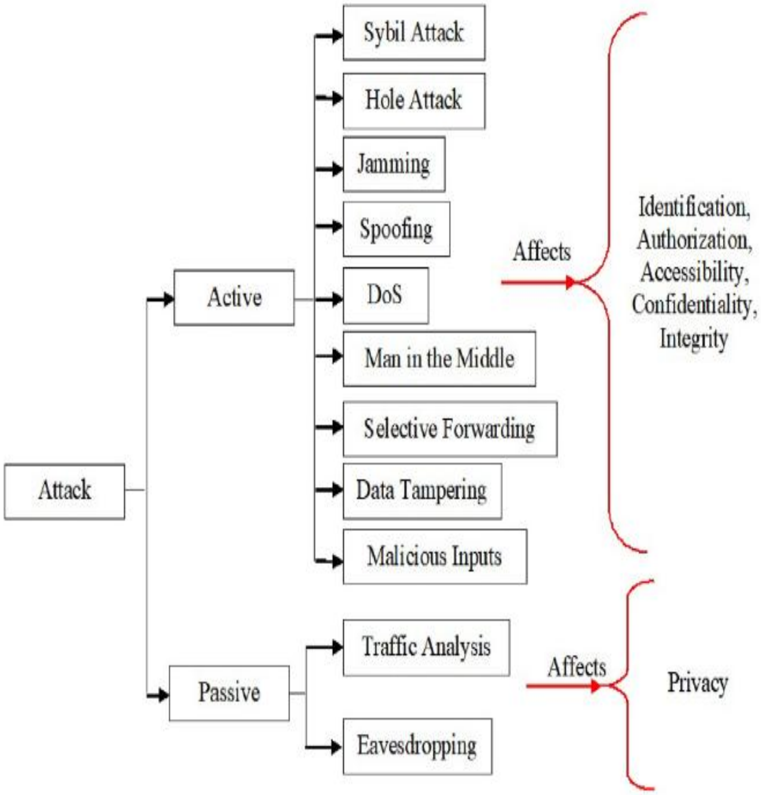

Fig. 6. Active and passive attacks with their effects [30].

- **Accessibility:** Guarantees that IoT device services are always delivered to their permitted users. The development of an efficient IoT network is vital [60]. At the same time, DoS and jamming attacks undermine this service by generating unreasonable demands and keeping the network busy. to keep IoT system services accessible to user clients without interruption, a robust security protocol is needed [59,61].
- **Privacy:** The only element that both active and passive attacks face in the IoT scheme is privacy. Nowadays, everything, including classified and personal documents, medical records, and national security data, is safely encrypted and transmitted over the Internet by various IoT devices that are not meant to be exposed by unauthorized users [62,63]. However, it is challenging to keep most data secret from unwanted third parties because attackers can trace the physical location of the IoT computer and decode the information. [59].
- **Integrity:** The receiver must check to protect the data integrity in the IoT that the messages received during transfer or distribution have not been changed. The integrity of the data confirms that the data sent is neither modified nor manipulated [58,64]. It is incredibly critical since even if intruders cannot obtain data, the network could not run properly if vulnerability nodes corrupt the transmitted data [65,66]. Indeed, data may be changed without an attacker if the contact channel is not secure. Integrity control guarantees that modifications to the message are detected accidentally and intentionally [39,59,67].
- **Identification:** Identification refers to the user's IoT network authorization. To communicate with the Cloud Server, clients must be registered first. However, IoT systems' commercialization and resilience bring identification issues. Sybil and spoofing attacks damage the network security, and the attackers can access the server without appropriate identification. Hence, an efficient IoT system

identification needs to be identified that can offer high protection when the system is restricted [65,68].

- **Authorization:** The authorization concerns the user's access to the IoT system. It only allows authorized customers to enter, track and use IoT network information data. The commands of users with authorization on the system also are executed. It is pretty challenging to keep all user logs and provide them access depending on the information because users are human, but sensors, devices, and services [58,69].

The user's permission in the IoT network is referred to as identification. To interface with the cloud server, clients must first register. The trade-offs and robustness of IoT schemes, on the other hand, make detection difficult [70]. Sybil and spoofing attacks are to blame for weakening network security, and attackers will quickly gain access to the server without sufficient identification. As a result, an appropriate IoT system identification scheme is needed to provide vital protection while applying system constraints [67].

3.4 Anomaly Detection in IoT Attack

3.4.1 Anomalies and sources of anomalies

There are cases of real-world data sets that are exclusive to all others and recognized as anomalies. Identifying anomalies is to find phenomena that are considered irregular in their activity relative to normal nodes. Separate sources of anomalies include the intrusion prevention system, fraud detection, and data leakage. Detection of anomalies is used in various IoT areas, including smart cities, network security, industries, etc. [13,71].

- **Intrusion detection:** IoT devices are Internet-linked and continue to be susceptible to attacks related to security. Threats like DoS and DDOS attacks incur the IoT network's significant harm. The biggest issue in IoT implementations is detecting and avoiding such attacks [13,72].
- **Fraud detection:** IoT networks remain vulnerable during logins or online payment to intercept credit card information, bank information, or other personal information [13, 73].
- **Data leakage:** External organizations can leak sensitive data from databases, file servers, and other sources of information, leading not just to information loss but also to a threat to confidentiality. Proper mechanisms for encryption can avoid such leaks [13].

3.4.2 Types of Anomalies

It is detectable by form such as point-wise, contextual, or collective [74].

- **Point-wise:** When sequence evolution is unpredictable, anomalies are used to identify significantly different points from the rest of the data points. It is commonly used in the detection of fraud [74].
- **Collective Anomalies:** Typical time series models such as repeat patterns or forms from many IoT devices are observed. In shipping delays of the supply chain, however, it requires an audit and joint review if multiple delays occur [74].
- **Contextual Anomalies:** Detected when prior knowledge type or meaning, such as the day of the week, is considered. Contexts are very domain-wide, almost [74]

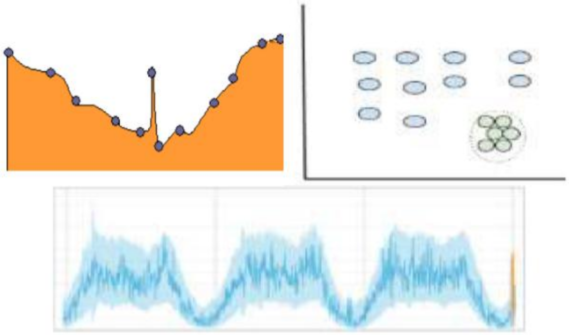

Fig. 7. Pointwise, Collective and Contextual Anomaly Types [74]

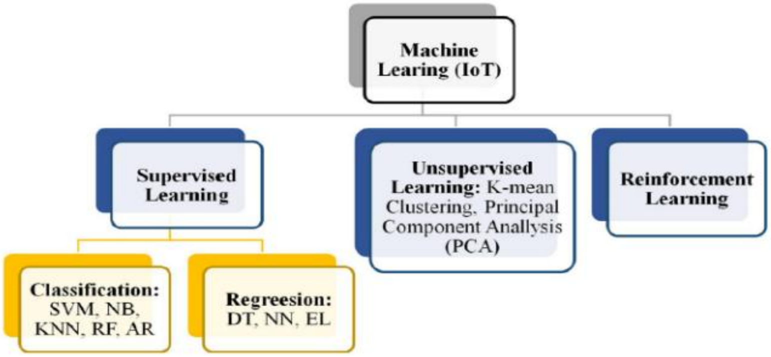
Machine Learing (IoT)
Supervised Learning
Unsupervised Learning: K-mean Clustering, Principal Component Anallysis (PCA)
Reinforcement Learning
Classification: SVM, NB, KNN, RF, AR
Regreesion: DT, NN, EL

Fig. 8. Machine Learning and its Classification [30]

4. MACHINE LEARNING (ML) APPLICATIONS IN IOT ATTACKS DETECTION

ML is a form of artificial intelligence that uses different algorithms to train machines and allows robots to learn from their interactions rather than directly programmed [16]. Human assistance, complex math algorithms, or performing in complex networks are not needed for ML [75,76]. ML strategies for IoT protection have advanced considerably in recent years. Based on an early examination of system behavior, ML approaches can thus forecast different IoT attacks. Furthermore, suitable solutions for resource-limited IoT devices can be provided by combining several ML algorithms. This segment is broken down into two subsections: ML Techniques and ML-based IoT Security Technologies [16].

4.1 Machine Learning (ML) Techniques

ML techniques such as supervised techniques, unsupervised techniques, and reinforcement learning can detect innovative attacks in IoT devices and develop a solid defense strategy. Fig. 7 depicts various machine learning algorithms used for IoT device security [30].

The most popular learning approach in machine learning is supervised learning, in which the output is graded based on the input using a qualified data set and a learning algorithm. Classification and regression learning are two types of supervised learning. While in Unsupervised Learning, there are no output data for such input variables. Most data is unmarked, in which the machine attempts to detect the correlations between this data collection. It classifies them as clusters of various classes [77].

In addition, Reinforcement learning helps the machine learn from encounters with its surroundings in the same way as humans do by taking acts that optimize overall feedback. The feedback may be a reward based on the outcome of the assigned mission. There are no predefined behaviors for any given task in reinforcement learning, and the machine uses trial and error methods. The agent may find and apply the best strategy from its knowledge to achieve the highest reward by trial and error [30].

4.2 Machine Learning-Based Solution for IoT Attacks Detection

Over the last few years, the field of ML-based security solutions for IoT devices has emerged as an emerging research area, attracting the interest of today's researchers to contribute more to it. Various ML approaches have been discussed in this section as possible options for protecting IoT devices. These solutions were researched using the three primary architectural layers of an IoT structure: the physical/perception layer, the network layer, and the web/application layer [30].

Traditional authentication mechanisms for protecting the physical surface are insufficient due to the precise threshold value to detect unintended signals that trigger false alarms. As a result, ML-based learning approaches may be used as an option for physical layer authentication [30]. Xiao and Liu, 2016 [78] Recorded that authentication error decreased by about 64.3 percent by QL-based learning methods and demonstrated better performance than standard authentication methods of 12 layers. Other research has been done to establish parameters for the logistical regression model for supervised ML techniques such as Distributed Frank Wolf and Incremental Aggregated Gradient to lower overhead communication and enhance spoofing detection performance [79].

Kiran, 2018 [80] recently proposed a new unified ML-based scheme to protect IoT computers. Essentially, it allows those users with permission to connect with the system and securely archive the information of approved users. Clients in the proposed peer-to-peer encryption protocol framework would first register with the cloud registry before communicating in the IoT framework.

Alam et al., 2018 [81] suggested the Neural and ElGamal algorithms paradigm to prevent attacks and stable IoT devices. The power over its cryptosystem was based on private and public keys here. Data is divided into categories and then correlated with training data. In addition, Baracaldo et al. proposed a new security technique to identify and filter toxic data gathered to form an arbitrary supervised mode [82].

Although the attack is an ordinary phenomenon, network securement is a challenge that connects real life with the virtual world. Therefore, various ML algorithms such as SVM, NN, and KNN can detect an intruder attack [83].

Saied et al., 2016 [84] Proposed a model for detecting DDoS attacks based on an ANN algorithm. Only genuine information packets, rather than forged ones, are permitted to traverse the network under the proposed scheme. Only when educated on modified data sets did ANN do better in detecting DDoS attacks.

4.3 Challenges and Gaps of the existing IoT Networks Security and Machine Learning Techniques

Nowadays, the area of IoT and its importance has reached every doorstep. In addition, the security of IoT has piqued the interest of numerous network and device researchers. The implementation of IoT, its use, and its effect on networks identify various obstacles and weaknesses that will open up new research avenues in the future [85]. Machine learning methods (ML) are a viable solution to stable IoT frameworks. ML is an innovative artificial intelligence technique that does not need explicit scripting and can be exceeded in complex networks [30]. It is crucial to explore the origins of protection and privacy problems for the effective implementation of IoT. In particular, the concept of IoT has been tossed around by the current technology, and therefore the safety problems of IoT are fresh. The legacy of the old technologies must be re-enhanced [77]. Fernandes et al., 2017 [86] concentrated on parallels and disparities between IoT and IT security problems. They have focused on topics relating to privacy. Similarities and variations are driven mainly by software, electronics, networks, and applications. Based on these classifications, the security problems in the classical IT domain are essentially identical to IoT. However, the primary concern of IoT is resource constraints that hinder the adjustment of sophisticated security solutions already available in IoT networks. In addition, IoT protection and privacy technologies need cross-cutting layer architecture and streamlined algorithms. IoT systems can require new breeds of optimized cryptographic and other algorithms for security and privacy, for example, due to computational restrictions.

\

On the other hand, there are other problems with protection protocols in the number of IoT devices. The most complex barriers to defense are not isolated solutions. There is, for instance, a possibility that false-positive results will make the solutions ineffective to such attacks in the event of security problems such as DDoS or intrusion. In addition, market confidence would be reduced, and the efficiency of these solutions deteriorated. A systematic approach towards protection and privacy for IoT would also have applications from current safety technologies and develop new intelligent, stable, evolutionary, and scalable security systems for IoT [77].

5. ASSESSMENT AND RECOMMENDATIONS

As shown in Table 2, researchers used different ML algorithms and techniques in detecting Attacks and Anomaly detection, and they obtained outstanding results in accuracy detection. In studies [95], [88], [89], [90], [87], [77], [94] as the researchers used and compared many ML algorithms and the best results with 99.34%, 99.5%, 99.4%, 99.9%, 99% ,99.5% and 99.9% accuracy have been obtained with the Random Forest (RF) algorithm. While in studies [97]. The results show that DT and KNN worked better than the other algorithms; however, compared to the DT algorithm, the KNN requires considerable time to classify.

Table 2. Performance comparison of ML algorithms for anomaly detection and attacks in IoT networks

Author	Year	Objectives	Datasets	Results and Accuracy	Techniques
Bagui et al., [87]	2021	Intrusion and attack detection for IoT Botnet.	UCI's machine learning repository	Using these three ML classifiers was over 99% in most cases and 100% in many cases.	LR, SVM, RF
Thamaraiselvi et al. [88],	2020	serviceability issues with ML for detecting anomalies in IoT networks	IoT-23	RF algorithm achieved the best results with an accuracy of 99.5 %	SVM, RF, Naïve Bayes, Decision Tree,
Susilo and Sari [67]	2020	Improving IoT Security by using machine learning techniques	BoT-IoT	Random forests and CNN have recorded the highest results in terms of accuracy	Random Forest, CNN, and MLP
Hasan et al., [89]	2019	The efficiency of many machine learning models has been carefully compared to predict attacks and anomalies on IoT networks.	NSL-KDD, Real Traffic, DS2OS	Random Forest has recorded the best accuracy 99.4 %	LR, DT, RF, SVM, and ANN.
Elmrabit et al. [90]	2020	detection of anomalous activities that could be indicative of cyber attacks	CICIDS-2017, UNSW-NB15, ICS Cyberattack	Random Forest (RF) algorithm achieves the best performance, which is 99.9 % for the CICIDS-2017 dataset	LR, GNB, Simple RNN, GRU, CNN-LTSM, CNN, RF, AdaB, DT, KNN, LSTM, DNN
Liu et al., [91]	2020	Enhance IoT security through the experimentation of multiple machine learning methods on the IoT network intrusion dataset.	IoT Network Intrusion Dataset	the accuracy when using KNN algorithms was 99%	LR, SVM, RF, KNN, XGBoost
Aysa et al., [92]	2020	Detect Attack and Anomaly in IoT devices.	Normal and abnormal data from UCI collected from three IoT devices	the merger between random forest and decision tree provided high accuracy	Decision Tree, SVM, Neural Network, Random Forest
Al-Akhras et al., [93]	2020	examine various ML algorithms' effectiveness to detect Attacks and anomaly in IoT Networks	UNSW-NB15	RF and KNN classifiers perform best with 100% accuracy without noise injection and 99% accuracy with 10% noise filtering	RF, KNN, Naïve bayes
Rani and Kaushal, [94]	2020	Improve the security and accuracy of Intrusion Detection System (IDS)	NSL-KDD and KDDCUP99	The proposed simulation has a 99.9 percent accuracy with less time and energy intrusion detection	KNN, NB, Decision Tree, Logistics Regression, RF
Stoian [77]	2020	Anomaly Detections and Attacks in IoT Networks.	IoT-23	The RF algorithm has obtained the best results with 99.5% accuracy	RF, NB, MLP, SVM, and AdaBoost.
Alrashdi et al., [95]	2019	Anomaly Detection and Attack in IoT Networks	UNSW-NB 15	AD-IoT is successful in reaching 99.34%	Random Forest
Alsamiri et al. [96]	2019	Detecting IoT attacks quickly	Bot-IoT	The accuracy for the used ML algorithms was Naïve Bayes was 0.77; the Random Forest was 0.97, ID3 was 0.97; Adaboost had 0.97, MLP was 0.83, QDA was 0.86, and KNN was 0.99.	Naïve Bayes, RF, ID3, Adaboost, MLP, QDA and KNN

Furthermore, in studies [92], the merge of the two ML algorithms RF and DT, achieved better accuracy for detecting Attacks. While in studies [93], the two ML algorithms RF and KNN, achieved better accuracy in detecting attacks with the accuracy of 99%.

In general, based on the reviewed paper, it is revealed that the Random Forest ML algorithm gives the best performance in detecting Attacks and Anomaly detection.ML has proved its value for general cybersecurity applications and is ideal for dealing with many IoT-specific issues. Based on the speed with which the ML-based systems respond and versatility, they balance a wide variety of IoT network vulnerabilities. ML research for all types of applications is highly stimulated. There are good evidence points that show the value of ML as an emerging technology.

6. CONCLUSION

The Internet of Things has the power to transform the world and put universal subjects in our hands. Consequently, anyone can reach, link, and store information from anywhere on the network through blessing IoT smart services. Although IoT enables our lives by intelligent devices that bind us to the virtual world to make life simpler, easier and faster, IoT technology makes the security of its services a significant concern. This article offers a systematic literature review on Machine Learning-based IoT security, including IoT and its architecture, a comprehensive analysis of various types of security threats, multiple ML-based algorithm categories, and ML-based security solutions. This paper focused on embedded Machine Learning algorithms for IoT security, from which anyone can obtain a general overview of various IoT attacks and their effects. Additionally, Machine Learning algorithms have been studied regarding possible challenges, which can help future researchers determine their ultimate goals and achieve their objectives in this field.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Khan MA, Salah K. "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems. 2018;82:395-411.
2. Chaabouni N, Mosbah M, Zemmari A, Sauvignac C, Faruki P. "Network intrusion detection for IoT security based on learning techniques," IEEE Communications Surveys & Tutorials. 2019;21:2671-2701.
3. Lu Y, Da Xu L. "Internet of Things (IoT) cybersecurity research: A review of current research topics," IEEE Internet of Things Journal. 2018;6:2103-2115.
4. Singh RP, Javaid M, Haleem A, Suman R. "Internet of things (IoT) applications to fight against COVID-19 pandemic," Diabetes & Metabolic Syndrome: Clinical Research and Reviews. 2020;14:521-524,
5. Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. "A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues," IEEE Communications Surveys & Tutorials. 2020;22:1191-1221.
6. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," IEEE Access. 2019;7:82721-82743,
7. Adat V, Gupta B. "Security in Internet of Things: Issues, challenges, taxonomy and architecture," Telecommunication Systems. 2018;67:423-441.
8. Fawzi LM, Alqarawi SM, Ameen SY, Dawood SA. "Two Levels Alert Verification Technique for Smart Oil Pipeline Surveillance System (SOPSS)," International Journal of Computing and Digital Systems. 2019;8:115-124.
9. Al-Sultan MR, Ameen SY, Abduallah WM. "Real Time Implementation of Stegofirewall System," International Journal of Computing and Digital Systems. 2019;8:498-504.
10. Ammar M, Russello G, Crispo B. "Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications. 2018;38:8-27.
11. Chernyshev M, Baig Z, Bello O, Zeadally S. "Internet of things (iot): Research, simulators, and testbeds," IEEE Internet of Things Journal. 2017;5:1637-1647.
12. Vashi S, Ram J, Modi J, Verma S, Prakash C. "Internet of Things (IoT): A vision, architectural elements, and security issues," in 2017 international conference

on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). 2017;492-496.

13. Sharma B, Sharma L, Lal C. "Anomaly Detection Techniques using Deep Learning in IoT: A Survey," in 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE). 2019;146-149.
14. Janaby AO. al, A. Al-Omary, S. Y. Ameen, and H. M. Al-Rizzo, "Tracking High-Speed Users Using SNR-CQI Mapping in LTE-A Networks," in 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT). 2018;1-7.
15. Costa KA. da, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," Computer Networks. 2019;151:147-157.
16. Hussain F, Hussain R, Hassan SA, Hossain E. "Machine learning in IoT security: Current solutions and future challenges," IEEE Communications Surveys & Tutorials. 2020;22:1686-1721,
17. Othman A, Ameen SY, Al-Rizzo H. "Dynamic Switching of Scheduling Algorithm for," International Journal of Computing and Network Technology. 2018;6.
18. Arko AR, Khan SH, A. Preety, M. H. Biswas, "Anomaly detection In IoT using machine learning algorithms," Brac University; 2019.
19. Hassan RJ, S. R. Zeebaree, S. Y. Ameen, S. F. Kak, M. A. Sadeeq, Z. S. Ageed, et al., "State of Art Survey for IoT Effects on Smart City Technology: Challenges, Opportunities, and Solutions," Asian Journal of Research in Computer Science. 2021;32-48.
20. Ameen SY, Ali ALSH. "A Comparative Study for New Aspects to Quantum Key Distribution," Journal of Engineering and Sustainable Development. 2018;11:45-57.
21. Malallah H, Zeebaree SR, R. R. Zebari, M. A. Sadeeq, Z. S. Ageed, I. M. Ibrahim, et al., "A Comprehensive Study of Kernel (Issues and Concepts) in Different Operating Systems," Asian Journal of Research in Computer Science. 2021;16-31.
22. Zebari IM, Zeebaree SR, Yasin HM. "Real Time Video Streaming From Multi-Source using Client-Server for Video Distribution," in 2019 4th Scientific International Conference Najaf (SICN). 2019;109-114.
23. Nižetić S, P. Šolić, D. L.-d.-I. González-de, and L. Patrono, "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future," Journal of Cleaner Production. 2020;274:122877.
24. Khalid LF, S. Y. Ameen, "Secure Iot integration in daily lives: A review," Journal of Information Technology and Informatics. 2021;1:6-12.
25. Alaba FA, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," Journal of Network and Computer Applications. 2017;88:10-28,
26. Yasin HM, Zeebaree SR, M. A. Sadeeq, S. Y. Ameen, I. M. Ibrahim, R. R. Zebari, et al., "IoT and ICT based Smart Water Management, Monitoring and Controlling System: A Review," Asian Journal of Research in Computer Science. 2021;42-56.
27. Singh A, A. Payal, S. Bharti, "A walkthrough of the emerging IoT paradigm: Visualizing inside functionalities, key features, and open issues," Journal of Network and Computer Applications. 2019;143:111-151.
28. Elazhary H. "Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions," Journal of Network and Computer Applications. 2019;128:105-140.
29. Yasin HM, Zeebaree SR Zebari, IM. "Arduino Based Automatic Irrigation System: Monitoring and SMS Controlling," in 2019 4th Scientific International Conference Najaf (SICN). 2019;109-114.
30. Tahsien SM, Karimipour H, Spachos P. "Machine learning based solutions for security of Internet of Things (IoT): A survey," Journal of Network and Computer Applications. 2020;161:102630.
31. Yang Y, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," IEEE Internet of Things Journal. 2017;4:1250-1258.
32. Zeebaree S, S. Ameen, M. Sadeeq. "Social media networks security threats, risks and recommendation: A case study in the kurdistan region," International Journal of Innovation, Creativity and Change. 2020;13:349-365.

33. Ali ZA, Ameen SY. "Detection and Prevention Cyber-Attacks for Smart Buildings via Private Cloud Environment," International Journal of Computing and Network Technology. 2018;6:27-33,
34. Makhdoom I, Abolhasan M, Lipman J, Liu RP, Ni W. "Anatomy of threats to the internet of things," IEEE communications surveys and tutorials. 2018;21:1636-1675.
35. Fawzi LM, Ameen SY, Alqaraawi SM, Dawwd SA. "Embedded real-time video surveillance system based on multi-sensor and visual tracking," Appl. Math. Infor. Sci. 2018;12:345-359.
36. Aziz ZAA, Ameen SYA. "Air pollution monitoring using wireless sensor networks," Journal of Information Technology and Informatics. 2021;1:20-25,
37. Abomhara M, Køien GM. "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," Journal of Cyber Security and Mobility. 2015;65–88-65–88.
38. Benkhelifa E, Welsh T, Hamouda W. "A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems," IEEE Communications Surveys & Tutorials. 2018;20:3496-3509.
39. Oracevic A, S. Dilek, S. Ozdemir, "Security in internet of things: A survey," in 2017 International Symposium on Networks, Computers and Communications (ISNCC). 2017;1-6.
40. Fawzi LM, S. Y. Ameen, S. A. Dawwd, and S. M. Alqaraawi, "Comparative Study of Ad-hoc Routing Protocol for Oil and Gas Pipelines Surveillance Systems," International Journal of Computing and Network Technology. 2016;4.
41. Raghuprasad A, Padmanabhan S, Babu MA, Binu P. "Security Analysis and Prevention of Attacks on IoT Devices," in 2020 International Conference on Communication and Signal Processing (ICCSP). 2020;0876-0880.
42. Farhan FY, Ameen SY. "Improved hybrid variable and fixed step size least mean square adaptive filter algorithm with application to time varying system identification," in 2015 10th System of Systems Engineering Conference (SoSE). 2015;94-98.
43. Amanuel SVA, Ameen SYA. "Device-to-device communication for 5G security: A Review," Journal of Information Technology and Informatics. 2021;1:26-31.
44. Abdullah Ameen DM SY. "Enhanced Mobile Broadband (EMBB): A review," Journal of Information Technology and Informatics. 2021;1:13-19.
45. Othman A, Ameen SY, Al-Rizzo H. "A new channel quality indicator mapping scheme for high mobility applications in LTE systems," Journal of Modeling and Simulation of Antennas and Propagation. 2015;1:38-43,
46. Janaby AOAl, A. Al-Omary, S. Y. Ameen, H. Al-Rizzo, "Tracking and controlling high-speed vehicles via CQI in LTE-A systems," International Journal of Computing and Digital Systems. 2020;9:1109-1119.
47. Othman A, Othman SY, A. Al-Omary, and H. Al-Rizzo, "Comparative Performanceof Subcarrier Schedulers in Uplink LTE-A under High Users' Mobility," International Journal of Computing and Digital Systems. 2015;4.
48. Abdulla AI, A. S. Abdulraheem, A. A. Salih, M. A. Sadeeq, A. J. Ahmed, B. M. Ferzor, et al., "Internet of Things and Smart Home Security," Technol. Rep. Kansai Univ. 2020;62:2465-2476.
49. Hamed ZA, I. M. Ahmed, S. Y. Ameen, "Protecting Windows OS Against Local Threats Without Using Antivirus," relation. 2020;29:64-70.
50. Othman A, Ameen SY, Al-Rizzo H. "An Energy-Efficient MIMO-Based 4G LTE-A Adaptive Modulation and Coding Scheme for High Mobility Scenarios," International Journal of Computing and Network Technology. 2015;3.
51. Syed NF, Baig Z, A. Ibrahim, C. Valli, "Denial of service attack detection through machine learning for the IoT," Journal of Information and Telecommunication. 2020;4:482-503.
52. Mohammed K, S. Ameen. "Performance investigation of distributed orthogonal space-time block coding based on relay selection in wireless cooperative systems."; 2020.
53. Abdulraheem AS, A. A. Salih, A. I. Abdulla, M. A. Sadeeq, N. O. Salim, H. Abdullah, et al., "Home automation system based on IoT,"; 2020.
54. Salih AA, Zeebaree SR, A. S. Abdulraheem, R. R. Zebari, M. A. Sadeeq, and O. M. Ahmed, "Evolution of Mobile Wireless Communication to 5G Revolution," Technology Reports of Kansai University. 2020;62:2139-2151.

55. Ageed ZS, S. R. Zeebaree, M. A. Sadeeq, M. B. Abdulrazzaq, B. W. Salim, A. A. Salih, et al., "A state of art survey for intelligent energy monitoring systems," Asian Journal of Research in Computer Science. 2021;46-61.
56. Ameen SY. "Advanced Encryption Standard (AES) Enhancement Using Artificial Neural Networks," Int J of Scientific & Engineering Research. 2014;5.
57. Alferidah DK, N. Jhanjhi, "A Review on Security and Privacy Issues and Challenges in Internet of Things," International Journal of Computer Science and Network Security IJCSNS. 2020;20:263-286,
58. Ageed ZS, Zeebaree SR, Sadeeq MM, Kak SF, Z. Rashid N, Salih AA, et al., "A survey of data mining implementation in smart city applications," Qubahan Academic Journal. 2021;1:91-99.
59. Mandal K, M. Rajkumar, P. Ezhumalai, D. Jayakumar, R. Yuvarani, "Improved security using machine learning for IoT intrusion detection system," Materials Today: Proceedings; 2020.
60. Ibrahim IM. "Task scheduling algorithms in cloud computing: A review," Turkish Journal of Computer and Mathematics Education (TURCOMAT). 2021;12:1041-1053.
61. Ameen SY, Nourildean SW. "Firewall and VPN investigation on cloud computing performance," International Journal of Computer Science and Engineering Survey. 2014;5:15.
62. Yahia HS, Zeebaree SR, Sadeeq MA, Salim NO, Kak SF, A.-Z. Adel, et al., "Comprehensive Survey for Cloud Computing Based Nature-Inspired Algorithms Optimization Scheduling," Asian Journal of Research in Computer Science. 2021;1-16.
63. Al-Khayat ON, Ameen SY, Abdallah MN. "WSNs Power Consumption Reduction using Clustering and Multiple Access Techniques," International Journal of Computer Applications. 2014;87.
64. Yazdeen AA, Zeebaree SR, M. M. Sadeeq, S. F. Kak, O. M. Ahmed, R. R. Zebari, "FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review," Qubahan Academic Journal. 2021;1:8-16.
65. Sadeeq MA, Zeebaree S. "Energy management for internet of things via distributed systems," Journal of Applied Science and Technology Trends. 2021;2:59-71.
66. Ameen SY, Yousif MK. "Decode and forward cooperative protocol enhancement using interference cancellation," Int. J. Elect., Comput., Electron. Commun. Eng. 2014;8:273-277.
67. Wang T, M. Z. A. Bhuiyan, G. Wang, L. Qi, J. Wu, T. Hayajneh, "Preserving balance between privacy and data integrity in edge-assisted Internet of Things," IEEE Internet of Things Journal. 2019;7:2679-2689.
68. Abdulrahman LM, S. R. Zeebaree, S. F. Kak, M. A. Sadeeq, A.-Z. Adel, B. W. Salim, et al., "A state of art for smart gateways issues and modification," Asian Journal of Research in Computer Science. 2021;1-13.
69. Ameen SY, S. W. Nourildean, "Coordinator and router investigation in IEEE802. 15.14 ZigBee wireless sensor network," in 2013 International Conference on Electrical Communication, Computer, Power, and Control Engineering (ICECCPCE). 2013;130-134.
70. Abdulqadir HR, Zeebaree SR, Shukur HM, M. M. Sadeeq, B. W. Salim, A. A. Salih, et al., "A study of moving from cloud computing to fog computing," Qubahan Academic Journal. 2021;1:60-70.
71. Cauteruccio F, Cinelli L, E. Corradini, G. Terracina, D. Ursino, L. Virgili, et al., "A framework for anomaly detection and classification in Multiple IoT scenarios," Future Generation Computer Systems. 2021;114:322-335.
72. Smys S, A. Basar, H. Wang. "Hybrid intrusion detection system for internet of Things (IoT)," Journal of ISMAC. 2020;2:190-199.
73. Pai H-T, S.-H. Wang, T.-S. Chang, and J.-X. Wu, "Challenge of Anomaly Detection in IoT Analytics," in 2020 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-Taiwan). 2020;1-2.
74. Mohamudally N, M. Peermamode-Mohaboob, "Building an anomaly detection engine (ADE) for Iot smart applications," Procedia computer science. 2018;134:10-17.
75. Cui J, Wang L, X. Zhao, H. Zhang, "Towards predictive analysis of android vulnerability using statistical codes and machine learning for IoT applications," Computer Communications. 2020;155:125-131.

76. Abdullah SMSA, Ameen SYA, Sadeeq MA, S. Zeebaree, "Multimodal emotion recognition using deep learning," Journal of Applied Science and Technology Trends. 2021;2:52-58.
77. Stoian N-A. "Machine Learning for anomaly detection in IoT networks: Malware analysis on the IoT-23 data set," University of Twente; 2020.
78. Xiao L, Y. Li, G. Han, G. Liu, W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," IEEE Transactions on Vehicular Technology. 2016;65:10037-10047,
79. Xiao L, X. Wan, Z. Han, "PHY-layer authentication with multiple landmarks with reduced overhead," IEEE Transactions on Wireless Communications. 2017;17:1676-1687.
80. Xiao L, X. Wan, X. Lu, Y. Zhang, D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?," IEEE Signal Processing Magazine. 2018;35:41-49.
81. Alam MS, D. Husain, S. Naqvi, P. Kumar, "IOT security through Machine Learning and homographic encryption technique," in International Conference on New Trends in Engineering & Technology (ICNTET), Chennai; 2018.
82. Baracaldo N, B. Chen, H. Ludwig, A. Safavi, and R. Zhang, "Detecting poisoning attacks on machine learning in iot environments," in 2018 IEEE international congress on internet of things (ICIOT). 2018;57-64.
83. Diro AA, Chilamkurti N. "Distributed attack detection scheme using deep learning approach for Internet of Things," Future Generation Computer Systems. 2018;82:761-768.
84. Saied A, Overill RE, Radzik T. "Detection of known and unknown DDoS attacks using Artificial Neural Networks," Neurocomputing. 2016;172:385-393.
85. Ageed ZS, Zeebaree SR, M. M. Sadeeq, S. F. Kak, H. S. Yahia, M. R. Mahmood, et al., "Comprehensive survey of big data mining approaches in cloud systems," Qubahan Academic Journal. 2021;1:29-38.
86. Fernandes E, Rahmati A, Eykholt K, Prakash A. "Internet of things security research: A rehash of old ideas or new intellectual challenges?," IEEE Security & Privacy. 2017;15:79-84.
87. Bagui S, X. Wang, S. Bagui, "Machine Learning Based Intrusion Detection for IoT Botnet," International Journal of Machine Learning and Computing. 2021; 11.
88. Mary DRTaSAS. "Attack and Anomaly Detection in IoT Networks using Machine Learning," Int. J. Comput. Sci. Mob. Comput. 2020;9:95–103.
89. Hasan M, Islam MM, Zarif MII, Hashem M. "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," Internet of Things. 2019;7:100059.
90. Elmrabit N, Zhou F, F. Li, H. Zhou, "Evaluation of machine learning algorithms for anomaly detection," in 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). 2020;1-8.
91. Liu Z, Thapa N, A. Shaver, K. Roy, X. Yuan, 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). 2020;1-5.
92. Aysa MH, Ibrahim AA, Mohammed AH. "IoT ddos attack detection using machine learning," in 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). 2020;1-7.
93. Al-Akhras M, M. Alawairdhi, A. Alkoudari, and S. Atawneh, "Using machine learning to build a classification model for iot networks to detect attack signatures."; 2020.
94. Rani D, Kaushal NC. "Supervised Machine Learning Based Network Intrusion Detection System for Internet of Things," in 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT). 2020;1-7.
95. Alrashdi I, Alqazzaz A, Aloufi E, Alharthi R, Zohdy M, Ming H. "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). 2019;0305-0310.
96. Alsamiri J, Alsubhi K. "Internet of Things cyber attacks detection using machine learning," Int. J. Adv. Comput. Sci. Appl. 2019;10.

97. Fenanir S, Semchedine F, Baadache A. "A Machine Learning-Based Lightweight Intrusion Detection System for the Internet of Things," Revue d'Intelligence Artificielle. 2019;33:203-211.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sdiarticle4.com/review-history/69410