Journal on
Internet of Things

Tech Science Press

DOI: 10.32604/jiot.2023.039391

ARTICLE

A Novel IoT Architecture, Assessment of Threats and Their Classification with Machine Learning Solutions

Oliva Debnath[1], Saptarshi Debnath[1], Sreyashi Karmakar[2], MD Tausif Mallick[3] and Himadri Nath Saha[4,*]

[1]Department of Computer Science and Engineering, Institute of Engineering & Management, Kolkata, 700091, India

[2]Department of Information Technology, RCC Institute of Information Technology, Kolkata, 700015, India

[3]Department of AK Choudhury, School of Information Technology, University of Calcutta, Kolkata, 700098, India

[4]Department of Computer Science, Surendranath Evening College, University of Calcutta, Kolkata, 700009, India

*Corresponding Author: Himadri Nath Saha. Email: contactathimadri@gmail.com

Received: 26 January 2023 Accepted: 04 May 2023 Published: 22 September 2023

ABSTRACT

The Internet of Things (IoT) will significantly impact our social and economic lives in the near future. Many Internet of Things (IoT) applications aim to automate multiple tasks so inactive physical objects can behave independently of others. IoT devices, however, are also vulnerable, mostly because they lack the essential built-in security to thwart attackers. It is essential to perform the necessary adjustments in the structure of the IoT systems in order to create an end-to-end secure IoT environment. As a result, the IoT designs that are now in use do not completely support all of the advancements that have been made to include sophisticated features in IoT, such as Cloud computing, machine learning techniques, and lightweight encryption techniques. This paper presents a detailed analysis of the security requirements, attack surfaces, and security solutions available for IoT networks and suggests an innovative IoT architecture. The Seven-Layer Architecture in IoT provides decent attack detection accuracy. According to the level of risk they pose, the security threats in each of these layers have been properly categorized, and the essential evaluation criteria have been developed to evaluate the various threats. Also, Machine Learning algorithms like Random Forest and Support Vector Machines, etc., and Deep Learning algorithms like Artificial Neural Networks, Q Learning models, etc., are implemented to overcome the most damaging threats posing security breaches to the different IoT architecture layers.

KEYWORDS

Internet of Things (IoT); layered architecture; threat assessment; security; machine learning; attack detection; attack mitigation

1 Introduction

The Internet of Things (IoT) enables the installation of billions of linked devices virtually anywhere on Earth [1]. IoT applications are essential in the current environment as they reduce the need for human effort in many parts of life, promote effective resource utilization, ensure high-quality data, etc. [2]. IoT devices are capable of collecting huge volumes of temperature, pressure, and distance

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

proximity data using sensors from different Healthcare, Agricultural domains, etc. Therefore, IoT applications have been deployed in Smart Agriculture [3–6], Home Automation [7–10], Smart Cities [11–14], Smart Healthcare [15–17], and so on [18–20].

IoT devices have grown incredibly vulnerable to assaults and security breaches due to the widespread use of IoT applications [21–26]. From a security perspective, managing the IoT's enormous scale, which has grown at an exponential rate over time, has been a crucial problem. The current security mechanisms and technologies are not built to scale to billions of devices [27,28]. It is challenging to define uniform protection techniques and procedures for IoT devices since they frequently use various transmission technologies [29,30]. Threats to the IoT environment are primarily posed by the human element. Providing extensive information about ourselves, our company, and our residence could potentially be a weakness if any of this data is accessible to fraudulent users or other undesirable third parties [31,32]. In spite of this, the Application framework of IoT devices is entirely diverse and dynamic due to the unpredictable mobility of the devices, which causes unexpected changes to their communication capabilities and position over time [33].

Dealing with serious IoT security issues is now more important than ever because IoT will soon permeate every aspect of our lives and be accessed from anywhere [34–38]. In order to build such a society in an ever-increasing way, it is vital to have strong security, proper confidentiality, authenticity, and attack recovery. It is crucial to implement the essential changes in the architecture of the IoT applications to attain end-to-end secure IoT environments [39]. Undoubtedly, the impending IoT concerns will necessitate a new secure-by-design perspective, in which risks will be dealt with dynamically as IoT devices will learn to adapt to attacks in a number of different ways [40]. IoT technology has many advanced qualities such as safety, communication, intelligence, and scalability; though Machine Learning (ML) algorithms [41], and lightweight encryption techniques [42], the existing architectures in IoT [43,44] are not able to recognize all these types of features at a time. The above-mentioned factors have motivated us to write this article.

In this paper, the existing layer architectures are modified and a new Seven-Layered Architecture has been proposed which when implemented achieves a high attack detection accuracy. This work provides an array of contributions, including:

i) A new Seven Layer Secure-by-design Architecture has been proposed for the first time after extensive research work on the various existing layered architectures in IoT for security are studied.
ii) Assessment metrics of security threats are being performed to categorize the attacks according to the probability of their occurrence from high to low and the effects on the Internet of Things systems from high to low.
iii) The impact of IoT security in terms of confidentiality, availability, and integrity of any IoT system.
iv) The attacks occurring in these layers have been presented and categorized from the most dangerous to the least dangerous ones based on various parameters such as the probability of occurrence and the impression it has on the IoT applications.
v) Solutions with Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning algorithms (RL) have been thoroughly discussed with the capability of detecting and mitigating a range of attacks.
vi) Furthermore, we presented the feasibility of ML, DL, and RL algorithms in terms of time and space complexities and prediction accuracy.
vii) After extensive study of the literature, we have provided a direction for future research.

The following sections make up the remainder of this article: Section 2 depicts the Layered architectures in IoT and highlights the new proposed architecture. Section 3 portrays the proposed seven-layered IOT architecture. Section 4 depicts the assessment of various attacks from high to low. In Section 5, the attacks occurring in these layers according to their vulnerability are depicted. In Section 6, Machine Learning and Deep Learning techniques have been outlined to alleviate a range of assaults occurring in multiple attacks. Further, in Section 7, the ML and DL algorithms have been evaluated extensively based on their performance, the cost (time and space complexities), and the accuracy of prediction, to see if they are feasible to be implemented. Section 5 highlights what is to be deployed for IoT security.

The future works are discussed in Section 7 and the conclusion has been enlisted in Section 8.

2 Proposed Seven-Layer Architectures in IoT

There have been numerous layered architectures for the Internet of Things proposed, including three, four, five, and six-layered systems. The core concept of IoT is fulfilled by three-layer architecture [45,46], which has a very simple architecture. It was put forth while the Internet of Things was just being started, but it fell short of meeting all of its requirements. Cloud, data center, API, and Web Services were not prioritized in the previous architecture. As a result, the middleware layer, which consists of the API, Web services, data center, and cloud, was introduced and the four-layered architecture [31,45–47] was suggested. Five-layer design [32,39] was suggested because there were still some security and storage concerns. The business layer, which is the new layer, is in charge of managing business values, the entire IoT network, and data confidentiality. The five-layer architecture's inability to address every security risk prompted the development of a six-layer architecture [45], which included the Security Layer. Even when the Security Layer has been introduced, additional security checks are still necessary to boost the IoT network's security and make it more dependable and accessible. The future path of IOT security will be determined by the development of a high-quality architecture to enable dependable and cryptographically secure from the perception layer to the application layer [48]. The specifications and implementation of machine learning and lightweight encryption algorithms that meet the improvements in IOT applications make up the second factor. As a result, the existing IoT architectures do not support all the developments needed to add new sophisticated features to IoT, such as IoT data, Machine Learning techniques [49], and light encryption algorithms. The seven-layered IoT method can lead to high assault detection accuracy. As a result, we have suggested the seven-layer design, a revolutionary IoT ecosystem. The Perception Layer, Data Pre-processing Layer, Network Layer, Middleware Layer, Data Storage and Big Data Analysis Layer, Application Layer, and Business Layer make up the seven layers of the architecture.

IoT equipment produces massive amounts of data very quickly. This suggested architecture features a layer to manage massive volumes of data, which solves the problem of processing "Big Data". In order to store both non-structured and structured IoT data, this suggested architecture comprises a framework based on data storage. The Hadoop framework and a number of other databases are used in the innovative design to manage the data that the sensors and actuators collect in the Perception Layer. To stay up with current concerns and technology, this new design relies on big data and machine learning as its core components. Fig. 1 shows the layers that make up the seven-layer design. The new IoT seven-layer design is shown in Table 1 along with the main responsibilities of each layer.

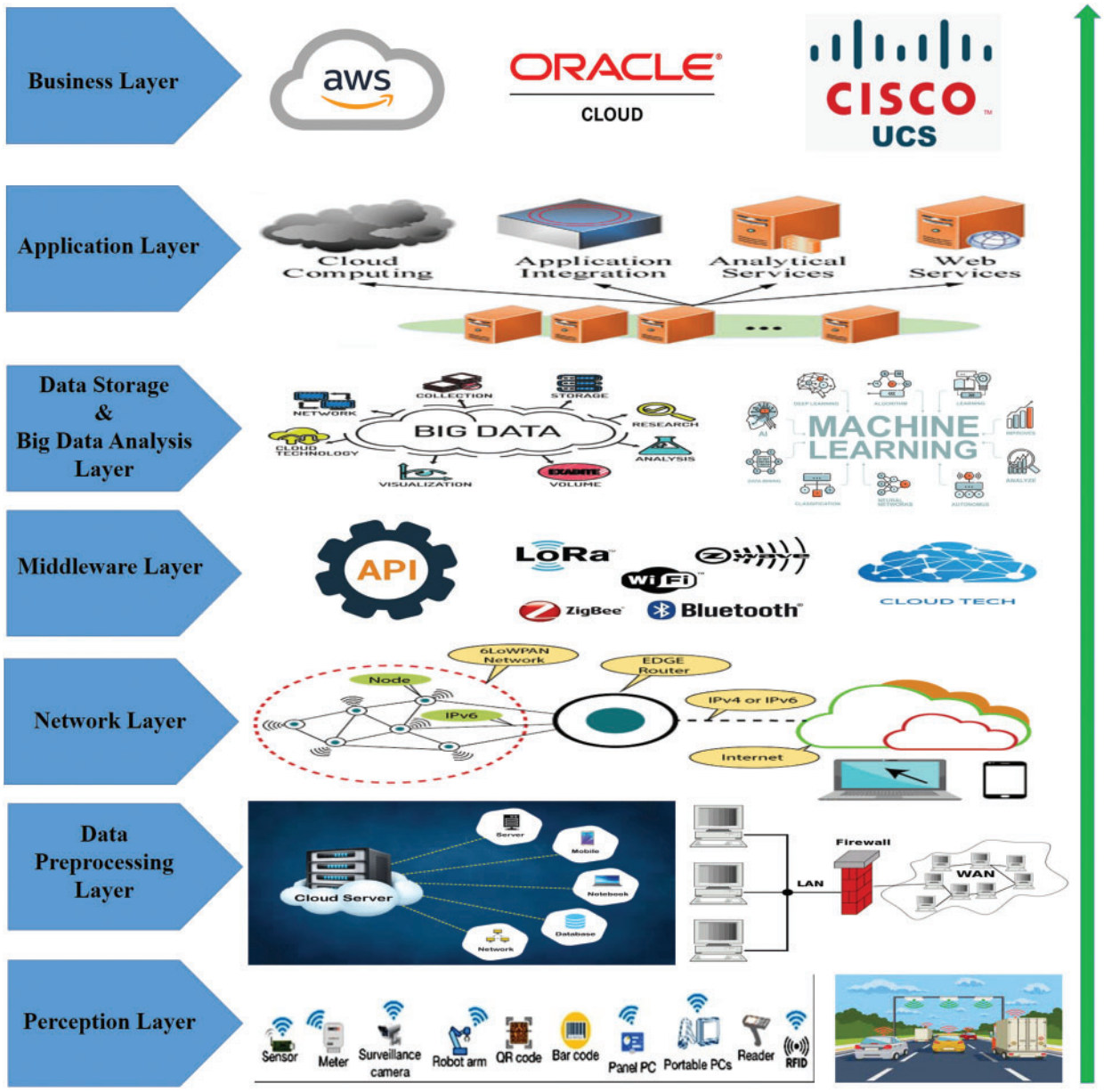

Figure 1: The proposed seven-layered IoT architecture

Table 1: Primary tasks and components of the seven-layered IoT architecture

Layers	Primary tasks
1. Perception layer	Sensing and data acquisition
2. Data Pre-processing layer	Sensor data protection, security based tasks
3. Network layer	Fog computing and edge computing based transmission of data
4. Middleware layer	Based on cloud computing, enables connectivity for IoT applications

(Continued)

Table 1 (continued)

Layers	Primary tasks
5. Data storage & big Data analysis	Data Profiling, Analysis using Machine Learning and Deep Learning Algorithms
6. Application layer	Caters to business values, delivery of applications to the end users
7. Business layer	Caters to Business values and user's privacy, management of the whole IoT system

3 Assessment of Various Attacks in IoT Architecture

In this part, we have suggested a classification system for the various attack types based on how frequently they occur in the IoT framework. The older work [47] has the following shortcomings:

- The number of criteria for an assessment was limited to only four.
- The range for evaluating the attacks does not fit within the level where 1 denotes low, 2 is medium and 3 is high.

To increase the accuracy of determining the likelihood of attacks, we have chosen eight separate criteria, where level 1 denotes low, level 2 is medium, and level 3 is high. In Table 2, the newly introduced criteria are listed and denoted with an asterisk (∗), and they are more focused on the security risks in the IOT network. The criteria used to categorize the most vulnerable assaults are based on the likelihood of their occurring which ranges from high to low depending on several circumstances.

Table 2: Probability of occurrence of attacks in different layers

Fields of assessments	Probability	
	Level	Score
∗Limited computational ability and hardware limitations (C1)	High	3
	Medium	2
	Low	1
Measuring different threats according to the layers (C2)	High	3
	Medium	2
	Low	1
∗Heterogeneous transmission technology (C3)	High	3
	Medium	2
	Low	1
Procedures for data security in layers (C4)	High	3
	Medium	2
	Low	1
∗Environment where IoT devices are deployed (C5)	High	3
	Medium	2
	Low	1

(Continued)

Table 2 (continued)

Fields of assessments	Probability	
	Level	Score
Human factors and third parties affecting the security of the layers (C6)	High	3
	Medium	2
	Low	1
∗Components of the device are vulnerable (C7)	High	3
	Medium	2
	Low	1
The scale of the attack surface and layer criticality (C8)	High	3
	Medium	2
	Low	1

All the various types of attacks are evaluated on the basis of the probability of occurrence and a range is created to identify the attack as High (3)/Medium (2)/Low (1) which is depicted in Table 3.

Table 3: Attack evaluating range

Range	Level
1–1.499 (as the value is closer to 1)	Low
1.5–2.499 (as the value is closer to 2)	Medium
2.5–3 (as the value is closer to 3)	High

We have set the range from 1–3 to determine the level of occurrence of an attack so it becomes easier to decide even if the number of criteria increases or decreases. When there is a combination of different levels of probability of attack (high/medium/low), it becomes a little confusing, so we set a range to determine at which level of occurrence the value can be. While calculating the level of probability of occurrence of an attack initially the total score (T_S) is calculated.

$$T_S = \sum_{i=1}^{n}; \text{ Where n (Number of Criteria)} = 8, 1 \leq C \leq 3, \text{where C is any integer} \quad (1)$$

$$\text{Average score } (S_A) = T_S/n; \quad (2)$$

Case I: If $1 \leq S_A \leq 1.499$ then the level of probability of occurrence of an attack is low.

Case II: If $1.5 \leq S_A \leq 2.499$ then the level of probability of occurrence of an attack is medium.

Case III: If $2.5 \leq S_A \leq 3$ then the level of probability of occurrence of an attack is high.

In Table 4, various impact levels of attacks are explained.

Let S_I is the Impact Score, $1 \leq S_I \leq 3$.

$$\text{Let threat assessment, } T_S = S_A * S_I \quad (3)$$

Table 4: Impact assessment

Level of impact	Range of values	Explanation
High	2.5–3 (as the value is closer to 3)	Significant damage that cannot be mitigated.
Medium	1.5–2.499 (as the value is closer to 2)	Significant damage relatively difficult to mitigate.
Low	1–1.499 (as the value is closer to 1)	Minor damage that can be mitigated easily.

If the range of T_A is $1 \leq T_A \leq 3$, the attack is the least dangerous.

If the range of T_A is $3 < T_A \leq 6$, the attack is more dangerous.

If the range of T_A is $6 < T_A \leq 9$, the attack is highly dangerous.

We have assumed that the least dangerous attacks are of lesser range as more and highly dangerous attacks are of more concern.

4 Security Threats in the Seven-Layered IoT Architecture

In the present era, security in IoT networks is a topic of the highest importance. To examine the security threats (attacks) that are likely to occur in the IoT architecture, the attacks occurring in layers 50 through 56 of the IoT network deserve the most attention. The attacks in this section have been listed from the most hazardous to the least dangerous so that attention can focus on solving the significant security problems provided by the IoT architecture. The criteria used to categorize the attacks that cause the most harm are based on the likelihood of occurrence (from high to low) and impact (from high to low) on the security of IoT applications.

Layer-wise classification has been made on these attacks which are as follows.

4.1 The Perception Layer

It also goes by the name of a sensing layer. It performs similar tasks to how human eyes, ears, and noses do. It is accountable for recognizing things and gathering information from them. To collect information there are numerous sorts of sensors attached to items such as RFID, 2-D barcode, and sensors. The applications' needs are taken into account when selecting the sensors. Several forms of information, including position, changes in the surroundings, motion, vibration, etc., can be gleaned from these sensors. But, attackers keep concentrating on them in an effort to utilize them to swap out the sensor with a different one. As an outcome, the bulk of hazards is associated with sensors, as seen in Table 5. After that, Table 6 contains an analysis of these attacks' vulnerability based on the likelihood of their occurrence (how easily they can be launched in the IoT network), the attacks that can be launched in response to such an attack, and the effect that such an attack has on the security of IoT applications [50].

Table 5: Attacks in the perception layer based on their vulnerability

Security threat	Description & reason behind its vulnerability
1. Node Capture Attack	An IoT system node is taken over by an attacker, who then replaces it with a malicious node that appears to be a part of the system but is actually under its control. This makes the entire IoT application less secure, making it the target of all assaults. Once the node has been taken over, the attacker can insert malicious code or false data into its memory, which may cause the entire Internet of Things application to malfunction. This can also result in a DDoS attack, a malicious code injection assault, or a false data injection attack.
2. Jamming Attack	This attack limits access to the transmission medium by producing intense interference that fills the channels and makes it impossible for conventional sensors to communicate. That results in a DoS assault. The IoT application is significantly damaged by jamming as well, but the harm is not as severe as that is caused by a node capture attack.
3. Eavesdropping and Interference Attack	Throughout several steps, such as data transmission or authentication, the attackers passively eavesdrop on the IoT network and capture data. Information theft results from this. Relay assaults are another method used by cybercriminals to eavesdrop on encrypted networks. It is less likely to happen than node capture and jamming, making the IoT framework more resistant to it. Relay and Snooping attacks may result.
4. Side-Channel Attack (SCA)	These kinds of side-channel attacks typically rely on the electromagnetic radiation, laser, timing, and power consumption of computer hardware. In a booting attack, for instance, node devices are targeted as they are restarted because edge devices are usually low-powered and may experience sleep-wake cycles. They are less vulnerable than the others because they do not impact the entire IoT network. This results in a timing assault, an Electromagnetic attack, and a booting attack.

Table 6: Analysis of perception layer attacks

Security threats	Probability of occurrence	Impact on the security of IoT applications
1. Node Capture Attack	High	High
2. Jamming Attack	High	Medium
3. Eavesdropping and Interference Attack	Medium	Medium
4. Side-Channel Attack (SCA)	Low	Low

4.2 The Data Pre-Processing Layer

The IoT architecture now has a new layer [44] that is dedicated to protecting sensor data with machine learning methods. It evaluates the data it receives from the Perception Layer to determine

whether it is secure from hackers and viruses. If so, the assault is discovered before being forwarded to the network layer. It verifies the items' authenticity [51] before passing them on to the network layer. Pre-processing data, which is done using databases, ML algorithms, and cloud computing approaches, is extremely important to create a secure IoT framework because it protects the network layer from heavy traffic and prevents storage devices from exceeding their capacity constraints. We have used the most recent encryption methods, such as AES and DES, to encrypt and decrypt the information for IoT data authentication. Based on their vulnerability, the attacks that are likely to occur are represented in Table 7, and further analysis of the assaults' vulnerabilities is presented in Table 8.

Table 7: Attacks in the data pre-processing layer based on their vulnerability

Security threat	Description & reason behind its vulnerability
1. Malware	It commonly causes the entire system to freeze or crash, disrupts operations, steals critical data, allows unwanted access to system resources, degrades computer or web browser speed, and disrupts network connections, making it the most vulnerable assault in this tier.
2. Exhaustion attack	The IoT network will experience an endless delay as a result of this assault's attempt to stop the IoT infrastructure's data processing, which will result in a DoS attack. Nonetheless, this is less expensive than malware.
3. Cryptanalysis attack	They are the least susceptible because they can not bring down the entire system and are challenging to launch. Although they may have been designed to render the network useless, such assaults do not entirely halt data transfer. This attack triggers a side-channel attack and a collision attack. They are therefore less susceptible than the aforementioned attacks.

Table 8: Analysis of data pre-processing layer attacks

Security threats	Probability of occurrence	Impact on the security of IoT applications
1. Malware	High	High
2. Exhaustion attack	High	Medium
3. Cryptanalysis attack	Medium	Medium

4.3 The Network Layer

Before any data is exchanged inside the IoT ecosystem, all connections are formed in this layer via Bluetooth, the Internet, and routing. The network layer is used to send the data obtained from the Data Pre-processing Layer to the online services, or cloud [52]. Innovative technologies like Edge Computing and Fog Computing have been introduced here for the first time in order to decrease the latency in the transport of IoT data. The key assaults to which this layer is vulnerable are forecast in Table 9, and their vulnerability analysis is shown in Table 10.

Table 9: Attacks in the network layer based on their vulnerability

Security threat	Description & reason behind its vulnerability
1. DDoS/DoS Attack (Denial of Service or Distributes DoS)	It is an ongoing attack and the one that is most susceptible to retaliation. In this attack, the attacker annihilates the target servers with a large number of unauthorized requests, leading to a denial-of-service problem and an endless delay that seriously affects the performance of the entire network. Traffic flooding, SYN flooding, and protocol attacks are all caused by this attack.
2. Routing Attacks	As opposed to DDoS assaults, active attacks by malicious nodes of an IoT application aim to alter the routing pathways while data is in transit. By intercepting and sending several copies of the same packet, replay attacks aim to cause obstruction and collisions in the network. Attacks like Sinkhole, Wormhole, and Replay result from this.
3. Sybill Attack	Their goal is to create fictitious Internet of Things (IoT) devices that send phony packets over the network. It is likewise an active attack and a host-addressing attack, although it is more challenging to start and therefore less dangerous than the attacks mentioned above. Host addressing and impersonation attacks can result from this approach.
4. Traffic Analysis Attack	Even though packet content is encrypted, an attacker may employ sniffer software to passively analyze the network traffic pattern and deduce packet content. Sensitive user data may be lost if insufficient security measures are taken to prevent it, but this risk is still lower than that posed by actual attacks.
5. Advanced Persistent Threat attack	An access attack involves the theft of important data or information. It is the least vulnerable because it does not harm the IoT network and has a minimal likelihood of happening.

Table 10: Analysis of network layer attacks

Security threats	Probability of occurrence	Impact on the security of IoT applications
1. DDoS/DoS Attack (Denial of Service or Distributes DoS)	High	High
2. Routing Attack	High	Medium
3. Sybill Attacks	Medium	Medium
4. Traffic Analysis Attacks	Low	Low
5. Advanced Persistent Threat attack	Low	Low

4.4 The Middleware Layer

The bulk of IoT network security solutions now includes cloud services to support current IoT devices. As a result, the Middleware Layer's backbone in the proposed architecture uses cloud infrastructure [53]. This layer acts as a bridge between the network and application layers, enabling

connectivity between various IoT components. The vulnerability analysis of the assaults is presented in Table 12. Table 11 presents the primary attacks that this layer is vulnerable to in the IoT ecosystem (ranked on their weakness).

Table 11: Attacks in the middleware layer based on their vulnerability

Security threat	Description & reason behind its vulnerability
1. Man-in-the-Middle (MITM) Attack	The attacker can take over the broker and function as a man-in-the-middle to intercept all communications without alerting the customers. As a result, of all the attacks in this stratum, this one is the weakest. As a result, of all the attacks in this stratum, this one is the weakest. ARP spoofing, SSL Stripping, DNS spoofing, HTTPS spoofing, Man-in-the-Browser, ARP spoofing, SSL Stripping, and Wi-Fi eavesdropping assaults are all a result of this attack.
2. Attacks on the Cloud	The attacker may take control, inject malicious code, or introduce a virtual machine into the cloud, all of which would result in a DoS problem. This assault results in cloud malware insertion and cloud flooding attacks. Because launching malware is less likely on the cloud than in MITM attacks, it is less risky.
3. SQL Injection Attack	Only when the attacker has taken control of the node are records in the database able to be changed, malicious SQL statements can be placed in programs, private information about any user can be accessed, and private data can also be obtained. This technique triggers a blind SQL injection as well as a UNION attack.
4. Signature Wrapping Attack	The web services of the middleware use XML signatures. In this attack, the attacker defeats the signature scheme and uses SOAP flaws to carry out actions or modify the eavesdropped communication (Simple Object Access Protocol). Yet, this attack is less likely to be discovered than the others because it is rarely launched.

Table 12: Vulnerability analysis of middleware layer attacks

Security threats	Probability of occurrence	Impact on the security of IoT applications
1. Man-in-the-Middle Attack	High	High
2. Attacks on the Cloud	High	Medium
3. SQL Injection Attack	Medium	Medium
4. Signature Wrapping Attack	Low	Low

4.5 The Data Storage and Big Data Analysis Layer

Big Data management, data storage, and data analysis are all handled by this layer. We suggested IoT architecture incorporates a framework based on data storage for the first time, allowing us to store both non-structured and structured IoT data. The Hadoop framework and a number of other

databases are used in the innovative design to manage the data that the sensors and actuators collect in the Perception Layer. Data profiling, data mining, and the application of machine learning are all topics covered by data analysis [54–61]. Before distributing information to customers, it is crucial for businesses to comprehend the issues and conduct relevant analyses of the data (Application layer). Data analysis can be used to predict cyberattacks, hence this layer is included to guarantee the security of IoT applications. Cybersecurity specialists can assess the data they have collected and then react in real-time thanks to big data analysis. In order to prevent cyberattacks, this layer thus casts a wider net. The vulnerability analysis of the attacks is shown in Table 14. Table 13 lists the primary attacks that this layer is susceptible to in the IoT ecosystem (ranked by their vulnerabilities).

Table 13: Attacks in the data storage and big data analysis layer based on their vulnerability

Security threat	Description & reason behind its vulnerability
1. DDoS/DoS Attack	It is an ongoing attack and the one that is most susceptible to retaliation. Attackers flood the target servers with a high number of unsolicited requests, creating a DoS circumstance and an indefinite delay that drastically impairs the operation of the entire network and causes famine throughout the entire IoT network. Traffic flooding, SYN flooding, and protocol attacks are all caused by this attack.
2. Malware	One of the most vulnerable attacks in this layer is malware, which has the potential to crash the entire IoT application, disrupt operations, steal sensitive data, permit unauthorized access to system resources, sluggish the speed of the computer or web browser, break network connections, and frequently freeze or crash the entire system.
3. Injection Attack	A cross-site scripting (XSS) attack introduces malicious programs into otherwise reliable and benign websites. Using a cross-site scripting vulnerability, attackers can get around access barriers like the same-origin policy. But, it does not happen as frequently, making the IoT system less vulnerable.
4. Phishing Attacks	There is a possibility of encountering phishing websites when surfing websites on the Internet. A user's whole IoT ecosystem is vulnerable to hacker attacks if their account and password are taken. But, it is quite uncommon, making it less of a threat to IoT security than the others.

Table 14: Vulnerability analysis of data storage and big data analysis layer attacks

Security threats	Probability of occurrence	Impact on the security of IoT applications
1. DDoS/DoS Attack	High	High
2. Malware	High	Medium
3. Injection Attacks	Medium	Medium
4. Phishing Attacks	Low	Low

4.6 Gateways

There is no layer presented here. Encrypting and decrypting IoT data and converting communication protocols between layers are among this layer's primary responsibilities. The IoT nodes, firmware, and gateways [61] connect the IoT devices to the application layer. Table 15 shows the security flaws in the gateways, and Table 16 shows how vulnerable they are to assaults.

Table 15: Attacks in the gateways based on their vulnerability

Security threat	Description & reason behind its vulnerability
1. Man in the Middle attack	Without informing the customers, the attacker can take control of the broker, acting as a man-in-the-middle, and seize total control of all communication. It results in attacks such as IP spoofing, Email spoofing, HTTPS spoofing, Man-in-the-Browser, ARP spoofing, SSL Stripping, DNS spoofing, and Wi-Fi Eavesdropping. As a result, of all the attacks in this stratum, this one is the weakest.
2. Eavesdropping	The hacker's goal when eavesdropping is to obtain the encryption keys, particularly during the onboarding procedure. Relay and Snooping attacks result from it. Data theft and security breaches result from this.
3. Encryption attacks at gateways	A cryptographic system can become less secure if a bug in a code, cypher, cryptographic protocol, or key management system is discovered.

Table 16: Vulnerability analysis of attacks in gateway

Security threats	Probability of occurrence	Impact on the security of IoT applications
1. Man in the Middle attack	High	High
2. Eavesdropping	Medium	Medium
3. Encryption attacks at gateways:	Medium	Low

4.7 The Application Layer

This is the sixth and most challenging layer in the suggested IoT architecture. The application layer provides services to the applications and supports business values based on the data collected by sensors. Smart homes, smart cities, smart healthcare, animal tracking [62,63], and other topics are discussed in the applications of IoT [64,65]. The launch of botnets, buffer overflows, and reprogramming assaults like those in Table 17 that harm the IoT network are some of the most hazardous attacks that affect the application layer [59] and target the IoT network. Table 18 provides an analysis of these attackers' vulnerabilities.

Table 17: Attacks in the application layer based on their vulnerability

Security threat	Description & reason behind its vulnerability
1. Botnet Attack	Genuine users are prevented from accessing IoT applications by botnet attacks, which are destructive behaviors including credential theft, unauthorized access, data theft, and DDoS assaults that render the servers or network unnaturally congested and unable to respond. Session flooding and HTTP flooding are the results. Thus, they are all the most vulnerable.
2. Buffer Overflow	Attackers can manipulate the execution stack of a web application by using buffer overflows. An attacker can take control of a machine by forcing a web application to run arbitrary code by providing it with carefully crafted information. A trustworthy website is infiltrated with malicious code via XSS by attackers (cross-site scripting). An IoT account could be hijacked in the event of a successful XSS attack, and the IoT system could stop functioning. These attacks are extremely risky to IoT security since they can lead to object reference attacks, SQL injection attacks, false data injection attacks, and XSS scripting.
3. Reprogram Attacks	Attackers may try to remotely reprogram IoT devices if the programming process is not secured, however, such attempts are uncommon and relatively inexpensive.

Table 18: Vulnerability analysis of application layer attacks

Security threats	Probability of occurrence	Impact on the security of IoT applications
1. Botnets Attack	High	High
2. Buffer Overflow	High	Medium
3. Reprogram Attack	Medium	Low

4.8 The Business Layer

The entire Internet of Things system, including all apps, business and financial models, and user privacy, is managed by this business layer. The cloud-based IoT frameworks create a set of guidelines and regulations for managing data and messaging amongst the many participants in the IoT network, including users, devices, and the cloud system [66]. These frameworks make it possible to deploy high-level IoT applications quickly while hiding the complexity of the underlying protocols. This layer includes platforms like AWS IoT, Bosh IoT, Cisco IoT, Google IoT, and Oracle IoT. The primary attacks are identified in Table 19 and their analysis is provided in Table 20, even though the business layer is not particularly vulnerable to many of them.

Table 19: Attacks in the business layer based on their vulnerability

Security threat	Description & reason behind its vulnerability
1. Business Logic Attack	By manipulating the data transfer between an application's supporting database and a user, it takes advantage of the program's flaw. As a result, it is more exposed than a zero-day assault. There are a number of business layer flaws that can result in business logic attacks, including incorrect code, invalid password recovery, and encryption methods. It leads to privilege escalations and authentication flags, as well as to the identification of LDAP parameters and access to crucial infrastructure, developer's cookie tampering, business process/logic bypass, and critical parameter manipulation. Exploiting business constraints, obstructing business flows using client-side JavaScript, Flash, or Silverlight routines for personal gain, Extraction of an individual's identity or profile, unauthorized access to files or URLs and the extraction of business data, and DoS attacks using business logic.
2. Zero-Day Attack	In general, a "zero-day" refers to a newly discovered vulnerability or an exploit for a flaw that hackers can use to attack systems. An application's security vulnerability or problem that the vendor is unfamiliar with each significant assault has an effect. Without the user's knowledge or agreement, the attacker takes advantage of this security hole to take over the machine. Due to the fact that only the attacker is aware of these threats, they are extremely deadly.

Table 20: Vulnerability analysis of business layer attacks

Type of attack	Probability of occurrence	Impact on the security of IoT applications
Business Logic Attack	High	High
Zero-Day Attack	High	Low

5 ML and DL Algorithms in Detecting and Mitigating the Attacks in Seven-Layer Architecture

The identification of external dangers is the first stage in providing security. Without a reliable environment, the tremendous demand for these devices could disappear and their potential could be squandered. The Internet of Things will be the primary source of fresh information used to develop increasingly clever uses for smart sensors. All IoT networks, whether they are presently in use or will be in the future, urgently require security. Smart sensors are being used more and more frequently in our daily lives. Security issues are therefore in demand right now.

Because of their exceptional ability to anticipate assaults and mitigate them, machine learning and deep learning [67] techniques been widely employed in a number of real-world applications [68–76]. The current machine learning methods are low-cost and computationally cheap, and they support the growth of Big Data. However, not all algorithms can effectively identify all types of attacks, and only a select few algorithms are most effective for identifying and thwarting different attacks in the IoT architecture [77].

Several well-known Machine Learning [78] and Deep Learning algorithms, including SVM, Decision Trees and Random forests, Nave Bayes, Artificial Neural networks, and Deep Q learning algorithms, have been used in this section of the paper to detect attacks that have occurred at various layers of the IoT architecture. Because certain attacks target many layers, as we have shown, it is crucial to anticipate them in order to create a more secure IoT framework. According to our knowledge, we are the first to have worked with these conventional and a few untested algorithms that, on their own, are capable of foreseeing many of these significant threats and can be used to secure many layers at once. This ML and DL solutions are shown in Table 21 and are intended to forecast a variety of assaults that could harm more than one layer of the suggested design.

Table 21: Detection of the multilayer attacks and ML and DL solutions [18]

ML/DL solutions	Range of attacks it can mitigate	Layers primarily affected by these attacks	Aim of the algorithm
Artificial Neural Network algorithms Like: •CNN •RNN •Auto encoders •Multi-layer perceptron	i) Routing attacks: Sinkhole wormhole replay ii) malware iii) Authentication attacks and access attacks iv) DDoS attacks (by backpropagation and LVQ model of ANN)	Network layer, Data pre-processing, Big data analysis layer	Anomaly/intrusion detection, Malware analysis, Authentication
SVM (Support Vector Machines) Like: •Linear SVM •Kernelized SVM •2 class SVM SVR (Support Vector Regression)	i) DDoS attacks on the cloud: Cloud malware injection, Flooding attack ii) DDoS Attack iii) Malware iv) Malicious code Injection attacks v) SQL injection attack jamming vi) Sleep deprivation attacks vii) Side-channel attacks, Cryptanalysis attacks	All the seven layers	Attack detection, Mitigation

(Continued)

Table 21 (continued)

ML/DL solutions	Range of attacks it can mitigate	Layers primarily affected by these attacks	Aim of the algorithm
Random Forest and Decision Trees	i) Jamming ii) Exhaustion attacks iii) DDoS attacks iv) Malware (like ransomware) v) Buffer overflow attack vi) SQL injection attack vii) XSS scripting viii) Malicious code injection ix) Encryption attack (Crypto ransomware) x) Man in the Middle Attack	Perception Layer, Network Layer, Application Layer	Network Intrusion Detection, Intrusion Detection in Applications, User Authentication
Naïve Bayes algorithm	i) Encryption attacks (Crypto ransomware) ii) Malware Detection iii) DDoS attacks iv) Man-in-the-middle attacks	Perception Layer, Network Layer, Application Layer, Business Layer, Middleware Layer	Anomaly Detection, Intrusion Detection, Malware Detection
Deep Reinforcement Learning algorithms Like: • Q learning • Dyna Q • Deep Q network (DQN) (Performs best) • Double DQN Fuzzy Q learning	i) DDoS attacks ii) Access attacks iii) Privilege Escalation attacks iv) Jamming DoS attack v) Side channel attacks vi) Encryption attacks and Eavesdropping vii) Malware: cloud-based malware detection viii) Zero-day attacks	Network Layer, Perception Layer, Business Layer, Middleware Layer	Authentication, Access Control Anomaly Detection, Intrusion Detection, Malware Detection

It has been found that artificial neural networks algorithms like RNN (Recurrent neural networks), Auto encoders, CNN (convolutional neural networks), and Multilayer perceptron can be used to accurately detect DDoS attacks, malware, authentication attacks, access attacks, and routing attacks, which primarily target the Network Layer, data pre-processing, and Big Data analysis layers. To ensure a more secure IoT platform, artificial neural network algorithms seek to carry out intrusion detection, malware analysis, and authentication.

Linear SVM, Kernelized SVM, and Support Vector Regressors are examples of Support Vector Machines that may identify DDoS assaults that target the middleware layer of the cloud as well as other DDoS attacks that target all other levels of the IoT architecture. Together with a variety of cryptanalysis and jammer assaults aimed at the perception layer, it may also foresee the presence of malware in the Data Preprocessing and Big Data analysis layer.

Random forests and decision trees, on the other hand, are incredibly flexible because they can reliably identify attacks like jamming, exhaustion, DDoS, malware (like ransomware), buffer overflows leading to object referencing attacks, SQL injection attacks, XSS scripting, malicious code injection, encryption attacks (like Crypto ransom wares), and Man in the Middle Attacks. The Perception layer, Network layer, and Application layers—all of which are vulnerable to significant attacks—are the most crucial levels that make up the IoT architecture. Algorithms for Random Forests and Decision Trees can be employed exclusively to serve a variety of security-related functions in IoT applications, including intrusion detection [79] in smart networks and smart apps as well as to verify the authenticity of IoT devices.

In order to create Machine Learning models that are capable of making speedy predictions, we have also worked with the Naive Bayes method, one of the most straightforward and efficient categorization techniques. It is a probabilistic classifier that performs exceptionally well at identifying malware, TCP, UDP, and HTTP flooding DoS assaults, Man in Middle attacks, and attacks on the application, business, middleware, and network layers.

The area of Deep Reinforcement learning algorithms has not before been extensively examined, as it is in this study. They may offer a way to detect the security threats that are present throughout the IoT infrastructure, as we have shown. It is possible to accurately predict the presence of DDoS attacks, access attacks, privilege escalation attacks, jamming attacks, snooping attacks that may launch MITM and Relay attacks, encryption attacks, and malware with the help of algorithms like Q learning, Dyna Q, Deep Q Network (DQN), Double DQN, and Fuzzy Q learning. If these attacks are effectively identified, the network layer, middleware layer, and perception layer can all be made secure. On the other hand, a range of heterogeneous Internet of Things (IoT) protocols have led to an exponential rise in the number of zero-day attacks and business logic attacks. Several centralized-based strategies have been presented [78–80] to detect harmful activity in IoT systems. To meet IoT needs, many techniques have suffered from a high delay. These business layer assaults are also detectable by Deep Q Network techniques.

6 Performance Analysis of ML and DL Algorithms for Detecting and Mitigating the IoT Attacks for Seven Layer Architecture

The numerous Machine Learning [80–88] and Deep Learning Algorithms that can be developed in order to detect and mitigate attacks in the seven-layer architecture of IoT [54–61,67] have been mentioned in the preceding section. This section's thorough analysis of these algorithms aims to considerably comprehend the computation and cost (time and space complexities) of these methods. Although Deep Learning is a subsection of Machine Learning the prediction accuracy and the self-learning properties of these algorithms are particularly useful to stay up with the current breakthroughs in IoT. The algorithms suggested here are thoroughly analyzed in Tables 22 to 29 to provide a comprehensive understanding of the jobs they accomplish, their time and space complexity, the training time needed, the computational difficulties [89,90], advantages, and disadvantages as well as classification accuracy.

Understanding which machine learning or deep learning algorithm is best for a certain attack requires knowledge of the aforementioned algorithms (Table 30 and Fig. 2 present the classification accuracy of the IoT attacks for seven-layered architecture). The few characteristics that make up an algorithm's work, cost relative to time, cost relative to space, training time, and computational complexity serve as the foundation for analysis.

6.1 Deep Learning Algorithms

Table 22: Computational analysis of artificial neural networks algorithms

Advantage	Disadvantage	Time complexity	Space complexity	Classification accuracy
• Non-Linearity • Robustness • Self-Learning algorithm • Mimics Artificial Intelligence	• Longer Training Time which depends on the number of layers added to the neural network, the dataset, and the number of classes it has to classify • Computationally expensive	**Prediction Time** For the feed forwarded neural network of 3 Layers: O(n2) **Training Time** $O(n_1 * n_2 * n_3)$ n_1, n_2 and n_3 are the number of layers	Depends on the number of layers and the size of the dataset	Maximum Once it is trained, it can even outperform humans in a few tasks

6.2 Support Vector Machines and Support Vector Regressors

Table 23: Computational analysis of SVM and SVRs

Advantages	Disadvantages	Time complexity	Space complexity	Classification accuracy
i) Flexible algorithm ii) Good for unbalanced semi-structured and unstructured data iii) Good for generalization iv) SVM can handle non-linear and high dimensional data v) It uses a convex optimization problem so there is no problem with local minima	i) Choosing /estimating the kernel functions and the hyper-parameters is difficult ii) Time required is more than other supervised algorithms depending on the kernel iii) Kernelized SVMs are very difficult to interpret in real-life applications.	**Prediction Time** $O(n_{sv}p)$, where n_{sv} = number of support vectors and p = number of features **Training Time** $O(n^2p+n^3)$ n the number of the training sample, p the number of features	O(m * n) for m features and n training samples	Very High

6.3 Random Forest and Decision Trees

Table 24: Computational analysis of random forest and decision trees algorithm

Advantage	Disadvantages	Time complexity	Space complexity	Classification accuracy
i) Good with large datasets ii) Robustness iii) Ensemble learning method iv) Generates forests for further use and better performance Easy to understand and interpret	Overfitting for some datasets with noisy classification and regression tasks Leads to huge overfitting and depends on the data that it is trained on.	**Prediction Time** O(nmlogn) for n instances and m attributes and O(M(nmlogn)) M is the number of trees **Training Time** $O(n^2p)$; n the number of the training sample, p, the number of features	O(nmlog(n) for n instances and m attributes and O(M(nmlog(n))	High

6.4 Naïve Bayes Algorithm

Table 25: Computational analysis of the Naïve Bayes algorithms

Advantage	Disadvantages	Time complexity	Space complexity	Classification accuracy
i) Fast ii) Highly scalable iii) Ability to scale linearly with the number of rows and predictors	i) Strong feature-independent assumptions may lead to weak predictions	**Prediction Time** O(p); p the number of features **Training Time** O(np); n the number of the training sample, p the number of features	O(np) For n features and p no. of label classes	Higher than Logistic Regression (because less amount of training data is needed here)

6.5 K-Nearest Neighbour

Table 26: Computational analysis of the K-Nearest neighbour

Advantage	Disadvantages	Time complexity	Space complexity	Classification accuracy
KNN is an extremely quick algorithm that does not need any training time (unlike SVM, Linear Regression, etc.). Only when making real-time predictions does it draw on the training dataset it has stored	While dealing with large dimensional data, KNN struggles. This is due to the fact that a large number of dimensions comes at a significant computational cost when calculating the distance in each dimension.	O(np)	O(nd)	High

6.6 Neural Network (NN)

Table 27: Computational analysis of the neural network

Advantage	Disadvantages	Time complexity	Space complex ity	Classification accuracy
• NNs can implicitly identify complex nonlinear interactions between dependent and independent variables and needs minimal statistical learning. Hence, all potential interactions between predictor variables may be found using these techniques. • NNs have the capacity to function in the presence of imperfect knowledge, and output is still produced after training.	The "black box" aspect, significant computational overhead, and propensity for overfitting of NNs are problems.	Given that p is the number of features, nl_i is the number of neurons at layer I in a neural network, and n is the number of training samples: $O((pnl_{l1}) + (nl_1)\ (nl_2) + \ldots\ldots)$	O(n)	High

6.7 Principal Component Analysis (PCA)

Table 28: Computational analysis of the principal component analysis (PCA)

Advantage	Disadvantages	Time complexity	Space complexity	Classification accuracy
1. In circumstances where there are plenty of features and it is challenging to see how they relate to one another and determine their association, PCA is a great option. Also, it is exceedingly challenging to narrow down the vast amount of features to only those that are useful. 2. The ML algorithm can be accelerated using PCA by eliminating the correlated variables (which do not affect decision-making), and the learning time of the approach is significantly reduced with fewer features. 3. PCA transforms high-dimensional data into lesser information that helps in solving the over-fitting issue (2 dimensions).	• Major elements are interpreted incorrectly. Major components, however more challenging to comprehend, are linear combinations of the characteristics of the original data. After computing principal components, it can be difficult, for instance, to identify the dataset's most important characteristics. • Finding a balance between information loss and dimensionality reduction. Notwithstanding its benefits, dimension reduction comes at a cost. Loss of information is an essential PCA component. However, we have to decide between dimensionality reduction and information loss when using PCA, and this trade-off needs to be managed.	$O(n^2\mathrm{p} + n^3)$	O(nd + d2) = O(d2)	Very High

6.8 Deep Reinforcement Learning Algorithms

Table 29: Computational analysis of deep reinforcement learning algorithms

Advantage	Disadvantages	Time complexity	Space complexity	Classification accuracy
• Can achieve long-term results • Absence of Training dataset, therefore it learns from experience • Maintains a balance between exploration and exploitation	Not generalizable Training time is slow Not preferable for small problems Computationally expensive	**Prediction Time** Exponential time complexity: O(en) As the Q value grows, time complexity increases **Training Time** $O(n^2)$; n is the number of the training sample.	Depending on how big the state space variables are. In direct proportion to the state space variables, Q value increases Exponential complexity: O(en)	Not generalizable Training time is slow Not preferable for small problems Computationally expensive

Table 30: Classification probabilities of all applied DL and ML algorithms

Performance of models	Classification probability	Classification accuracy (range)
Deep Learning approaches (ANN, Q Learning model)	Maximum. If trained, it can even execute some tasks better than humans	(99–95)%
Deep Reinforcement Learning	Depending on how many state space variables there are	(99–95)%
Support Vector Machines	Very High	(95–85)%
Support Vector Regressor	Very High	(95–85)%
Random Forest	High	(85–80)%
Decision Trees	High	(85–80)%
Naïve Bayes Algorithm	Higher than Logistic Regression	(82–80)%
K-Nearest Neighbour	High	(85–80)%
Neural Network	High	(85–80)%
Principal Component Analysis (PCA)	Very High	(95–85)%

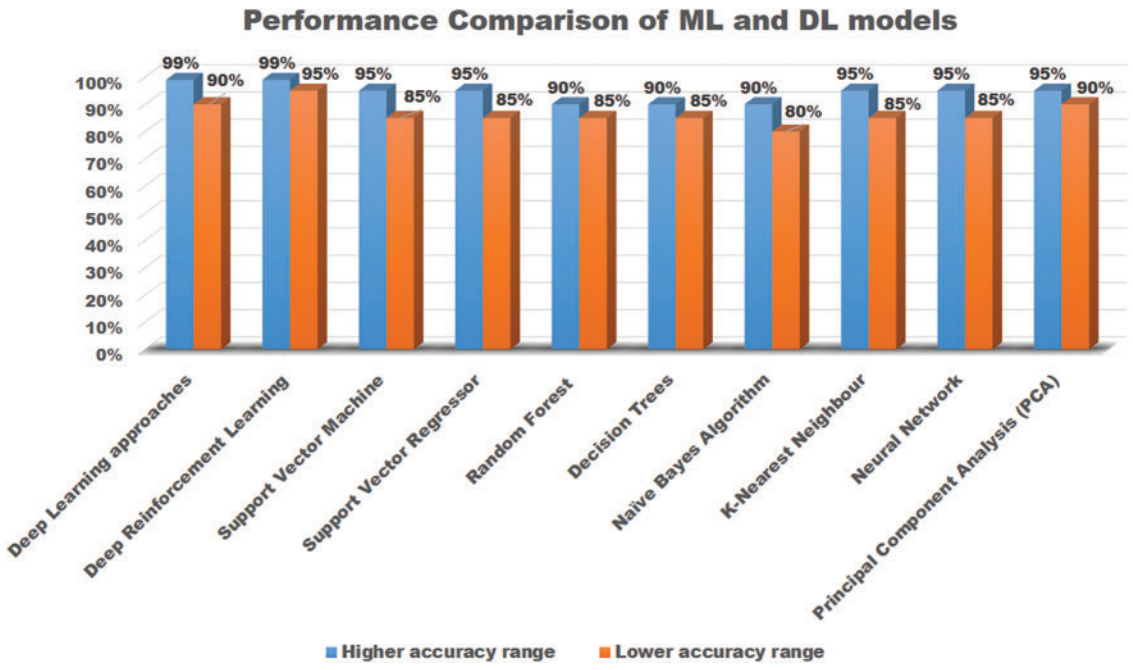

Figure 2: The graphical representation of the DL and ML models' performance on IoT attacks

7 Future Research Directions

The IoT environment faces a variety of difficulties that, with more work, can be successfully handled. It is essential to understand the industry and its requirements, risks, prices, and privacy concerns in order to deliver an end-to-end secure IoT platform for human consumption. In this section of the report, the significant difficulties as well as potential future research directions are discussed. These are what they are:

Data analysis using ML and AI algorithms while safeguarding the fog layer.

A variety of ML and AI approaches can be applied to increase the intelligence of the fog layer. The fog layer must be able to decide how long the data should be kept there too and when it should be erased or transferred to the cloud for extended storage. The efficient implementation of IoT systems depends on data analysis occurring nearby the IoT node and in real-time. Instead of having to send the data elsewhere for analysis, a number of ML and DL-based algorithms can be developed to analyze the data in the node itself. By limiting data flow, the security of the application can be further improved.

7.1 Design of a Service-Oriented Language (SOL)

Secure data transfer, data processing, and management of the entire Internet of Things ecosystem are now burdensome due to the cost of maintaining a high level of user service in this period of quick technological breakthroughs. The Internet of Things is a platform for diverse networks that makes it more difficult for different devices and communication technologies to function together, which makes the network more susceptible to hacking and slowdowns. A widely accepted language that is service-oriented should be created taking into account network services for the industry's benefit. With the aid of such a language, the creation of services, their implementation, and the integration of resources will be simpler, minimizing overall market losses and ensuring service-oriented secure communication.

7.2 A Consolidated Information Framework (CIF) Needs to be Created

There are currently an enormous number of IoT-connected gadgets that are collecting real-time data. This data require the control of a high-frequency, high-bandwidth route. A CIF must be developed to fulfill the requirements of Big Data. The database management systems that are currently in use are unable to handle the amounts of real-time data obtained by all of these IoT devices. In order to solve the existing issue, additional work might be done to increase the effectiveness of large data storage. By analyzing various threat detections and mitigations utilizing ML and DL techniques.

7.3 Data Mining and Secure Routing Protocols Should Be Obtained

The real-time sensors and actuators do not filter the raw data they collect. It takes effective decision-making and data mining to sort through the vast amounts of recorded data. Here, a big data strategy should be used. In order to support the present IoT ecosystem, secure routing protocols need also be developed that can manipulate the web services that may be implemented in addition to the inclusion of cutting-edge software.

7.4 Efficient Block Chain Mining Algorithms for IoT Security

The Block Chain is a scalable, decentralized platform that can securely record confirmed transactions. Blockchain has been used by several researchers to secure IoT applications. But, the existing blockchain mining algorithms incur a substantial computational overhead which in turn makes the entire system costlier and raises the average energy depletion and computational interruption. End-to-end encryption must therefore be incorporated into the design of effective blockchain mining algorithms in order to guarantee a quick, low-cost, low-energy manner of securely storing transactions.

7.5 Security, Communication, and Identification Normalization in IoT

A significant barrier to making IoT services safer is the interoperability problem. Another approach that needs to be used to develop a safe IoT ecosystem is normalization or standardization. In order for diverse IoT applications to compete more effectively with the created apps in the Application Layer of IoT design, it is necessary to lower initial barriers for service providers. As IoT technologies proliferate, security, connectivity, and identity standards must be standardized in a way that enables an effective deployment of IoT applications.

7.6 Implementation of Fog Computing in Designing a Strong Security Mechanism for IoT

Although ML, DL, and RL have been used in this study to present the existing solutions for the network security of IoT applications, additional work is still required to guarantee an end-to-end protected IoT network. In this regard, deploying fog computing can assist in lowering network traffic and latency. Using fog computing, a robust security system must be created so that assaults may be stopped before they reach the cloud. The IoT application will be more dependable and secure as a result of the decreased network traffic and attacks.

7.7 Developing Simple Cryptographic Protocols Shield Internet of Things Devices from Potential Threats

IoT devices are limited by their battery life. It is possible to create a small cryptographic protocol for secure and energy-efficient communication.

7.8 Powerful Battery Backed Up Smart Edge Devices for IoT Security

Edge computing has been applied in a number of industries, such as sustainable farming, green cities, and smart healthcare. However, under the IoT design, edge devices are very vulnerable to attacks. If the edge layer is not secure, the entire IoT ecosystem is going to be in danger. They mostly rely on battery backups because they are resource-limited. The entire Internet of Things (IoT) ecosystem becomes vulnerable to attacks if the edge device's battery is somehow drained, such as by forcing it to run in an endless loop by a hacker. So, in order to avoid battery drain and guarantee the safety of the overall IoT ecosystem, it is essential to create smart edge devices with a substantial battery backup.

7.9 Developing an Application-Specific Data Protection Technique Is Very Necessary

The healthcare system will need appropriate access control systems to secure sensitive health records while maintaining data integrity and confidentiality is of the utmost importance in the case of VANET.

7.10 Developing Protective Measures against Traffic Analysis Attacks

Preventing traffic analysis, which keeps data communication in IoT networks private, is another key research field. However, it is accepted that more research may be done in this area to offer a more reliable and safe framework for IoT programs to work in, even if potential solutions for IoT security have been revealed. To revolutionize the way people perceive IoT technology and to make it accessible to students around the world, future work can be pursued to make the IoT system more capable of being implemented in the academic field. This will enhance a brighter future for readers in particular and the globe in general.

8 Conclusion

IoT security has become more complex day by day. Additionally, it is crucial to safeguard the entire IOT environment due to technological improvements and new threats to the IoT ecosystem that have been noticed. Advanced Machine Learning, Deep Learning, and Reinforcement learning have enhanced IOT security. In this paper, the multilayer security threats occurred based on their vulnerabilities to the service-oriented IoT network, and their applications are solved by a novel and modern technological architecture to increase the security of the IoT ecosystem. Evaluation parameters like the ease of launching the attack, the probability of occurrence of the attacks, etc., have been analyzed by the ML and DL techniques to predict a range of attacks so that to mitigate several attacks at a time.

The feasibility of the algorithms presented in this paper is explored to make it more transparent which algorithm should be used and why. Each method has been compared in subsections of the paper to demonstrate their aim, advantages, disadvantages, and real-world application areas. In order to improve IoT security, the time and spatial complexity of each of these methods has been presented along with their computing costs and prediction accuracy. This paper aims to encourage research enthusiasts to make advancements in the IoT ecosystem for secure, reliable, and available networks and pave their way to design a more intelligent end-to-end secured IoT ecosystem.

Acknowledgement: All the above authors prepared this manuscript themselves.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: All the authors have equal contribution to prepare the manuscript.

Availability of Data and Materials: We have not used any type dataset or materials from the external source.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. N. Saha, A. Mandal and A. Sinha, "Recent trends in the Internet of Things," in *IEEE 7th Annual Computing and Communication Workshop and Conf. (CCWC)*, Las Vegas, NV, pp. 1–4, 2017.

[2] H. N. Saha, N. Saha, R. Ghosh and S. Roychoudhury, "Recent trends in implementation of Internet of Things–A review," in *IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conf. (IEMCON)*, Vancouver, BC, pp. 1–6, 2016.

[3] J. Muangprathub, N. Boonnam, S. Kajornkasirat, N. Lekbangpong, A. Wanichsombat *et al.,* "IoT and agriculture data analysis for smart farm," *Computers and Electronics in Agriculture*, vol. 156, pp. 467–474, 2019.

[4] G. Lavanya, C. Rani and P. Ganeshkumar, "An automated low cost IoT based fertilizer intimation system for smart agriculture," *Sustainable Computing: Informatics and Systems*, vol. 28, pp. 100300, 2020.

[5] F. Bu and X. Wang, "A smart agriculture IoT system based on deep reinforcement learning," *Future Generation Computer Systems*, vol. 99, pp. 500–507, 2019.

[6] K. Lakhwani, H. Gianey, N. Agarwal, S. Gupta, V. Rathore *et al.,* "Development of IoT for smart agriculture a review," in *Emerging Trends in Expert Applications and Security*. Singapore: Springer, pp. 425–432, 2019.

[7] B. R. Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *Journal of Cleaner Production*, vol. 140, no. 3, pp. 1454–1464, 2017.

[8] T. K. L. Hui, R. S. Sherratt and D. Díaz Sánchez, "Major requirements for building smart homes in smart cities based on Internet of Things technologies," *Future Generation Computer Systems*, vol. 76, pp. 358–369, 2017.

[9] M. Alaa, A. A. Zaidan, B. B. Zaidan, M. Talal and M. L. M. Kiah, "A review of smart home applications based on Internet of Things," *Journal of Network and Computer Applications*, vol. 97, pp. 48–65, 2017.

[10] S. R. Paveethra, B. Barathi, M. Geethapriya, M. Arthi and V. Ahasthiya, "Theoretical modelling and implementation of home energy management system using IoT based automation system," *Materials Today: Proceedings*, vol. 45, pp. 1790–1793, 2020.

[11] T. Kim, C. Ramos and S. Mohammed, "Smart city and IoT," *Future Generation Computer Systems*, vol. 76, pp. 159–162, 2017.

[12] Y. Qian, D. Wu, W. Bao and P. Lorenz, "The Internet of Things for smart cities: Technologies and applications," *IEEE Network*, vol. 33, no. 2, pp. 4–5, 2019.

[13] V. A. Memos, K. E. Psannis, Y. Ishibashi, B. Kim and B. B. Gupta, "An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework," *Future Generation Computer Systems*, vol. 83, pp. 619–628, 2018.

[14] H. N. Saha, S. Gon, A. Nayak and S. Moitra, "IoT based garbage monitoring and clearance alert system," in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conf. (IEMCON)*, Vancouver, Canada, pp. 204–208, 2018.

[15] L. Greco, G. Percannella, P. Ritrovato, F. Tortorella and M. Vento, "Trends in IoT based solutions for health care: Moving AI to the edge," *Pattern Recognition Letters*, vol. 135, pp. 346–353, 2020.

[16] S. Selvaraj and S. Sundaravaradhan, "Challenges and opportunities in IoT healthcare systems: A systematic review," *SN Applied Sciences*, vol. 2, pp. 641, 2020. https://doi.org/10.1007/s42452-019-1925-y

[17] H. A. El Zouka and M. Hosni, "Secure IoT communications for smart healthcare monitoring system," *Internet of Things*, vol. 13, pp. 100036, 2019.
[18] M. Tavana, V. Hajipour and S. Oveisi, "IoT-based enterprise resource planning: Challenges, open issues, applications, architecture, and future research directions," *Internet of Things*, vol. 11, pp. 100262, 2020.
[19] H. N. Saha, S. Gon, A. Nayak, S. kundu and S. Moitra, "IoT based garbage monitoring and clearance alert system," in *IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conf. (IEMCON)*, Vancouver, BC, Canada, pp. 204–208, 2018.
[20] Y. Jung and R. Agulto, "A public platform for virtual IoT-based monitoring and tracking of COVID-19," *MDPI Electronics*, vol. 10, no. 1, pp. 12, 2021.
[21] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, 2017.
[22] Y. Yang, 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*, vol. 4, no. 5, pp. 1250–1258, 2017.
[23] M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2017.
[24] F. A. Alaba, M. Othman, I. A. T. Hashem and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.
[25] A. R. Sfar, E. Natalizio, Y. Challal and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, 2018.
[26] M. Noor and H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Computer Networks*, vol. 148, pp. 283–294, 2019.
[27] B. Liao, Y. Ali, S. Nazir, L. He and H. U. Khan, "Security analysis of IoT devices by using mobile computing: A systematic literature review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020.
[28] M. M. Ogonji, G. Okeyo and J. M. Wafula, "A survey on privacy and security of Internet of Things," *Computer Science Review*, vol. 38, pp. 100312, 2020.
[29] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, 2019.
[30] M. Ammar, G. Russello and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018.
[31] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal *et al.,* "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721– 82743, 2019.
[32] L. Antão, R. Pinto, J. Reis and G. Gonçalves, "Requirements for testing and validating the industrial Internet of Things," in *IEEE Int. Conf. on Software Testing, Verification and Validation Workshops (ICSTW)*, Vasteras, pp. 110–115, 2018.
[33] X. Luo, L. Yin, C. Li, C. Wang, F. Fang *et al.,* "A lightweight privacy-preserving communication protocol for heterogeneous IoT environment," *IEEE Access*, vol. 8, pp. 67192–67204, 2020.
[34] H. Mrabet, S. Belguith, A. Alhomoud and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors Journal*, vol. 20, no. 13, pp. 3625, 2020.
[35] M. A. M. Sadeeq, S. R. M. Zeebaree, R. Qashi, S. H. Ahmed and K. Jacksi, "Internet of Things security: A survey," in *2018 Int. Conf. on Advanced Science and Engineering (ICOASE)*, Duhok, Iraq, pp. 162–166, 2018.
[36] S. Tweneboah-Koduah, K. E. Skouby and R. Tadayoni, "Cyber security threats to IoT applications and service domains," *Wireless Personal Communication*, vol. 95, pp. 169–185, 2017.
[37] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng *et al.,* "Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice," *Journal of Hardware System Security*, vol. 2, pp. 97–110, 2018.
[38] Q. Gou, L. Yan, Y. Liu and Y. Li, "Construction and strategies in IoT security system," in *2013 IEEE Int. Conf. on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, Beijing, China, pp. 1129–1132, 2013.

[39] P. Hao, X. Wang and W. Shen, "A collaborative PHY-aided technique for end-to-end IoT device authentication," *IEEE Access*, vol. 6, pp. 42279–42293, 2018.
[40] D. Chasaki and C. Mansour, "Security challenges in the Internet of Things," *International Journal of Space-Based and Situated Computing*, vol. 5, no. 3, pp. 141–149, 2015.
[41] M. P. Nath, S. B. B. Priyadarshini, D. Mishra and S. Borah, "A comprehensive study of contemporary IoT technologies and varied machine learning (ML) schemes," in *Soft Computing Techniques and Applications, Advances in Intelligent Systems and Computing*, vol. 1248. Singapore: Springer, pp. 623–634, 2021.
[42] A. Shah and M. Engineer, "A survey of lightweight cryptographic algorithms for IoT-based applications," in *Smart Innovations in Communication and Computational Sciences*, vol. 851. Singapore: Springer, pp. 283–293, 2019.
[43] F. Alshohoumi, M. Sarrab, A. AlHamadani and D. Al-Abri, "Systematic review of existing IoT architectures security and privacy issues and concerns," *International Journal of Advanced Computer Science and Applications*, 2019. https://doi.org/10.14569/ijacsa.2019.0100733
[44] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, protocols, and applications," *Journal of Electrical and Computer Engineering*, vol. 2017, pp. 25, 2017.
[45] M. Burhan, R. A. Rehman, B. Khan and B. S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," *Sensors*, vol. 18, no. 9, pp. 2796, 2018. https://doi.org/10.3390/s18092796
[46] I. U. Din, M. Guizani, S. Hassan, B. S. Kim, M. K. Khan *et al.,* "The Internet of Things: A review of enabled technologies and future challenges," *IEEE Access*, vol. 7, pp. 7606–7640, 2018.
[47] M. Aydos, Y. Vural and A. Tekerek, "Assessing risks and threats with layered approach to Internet of Things security," *Measurement and Control Journal*, vol. 52, no. 5–6, pp. 338–353, 2019.
[48] K. Xing, S. S. Srinivasan, M. J. Rivera, J. Li and X. Cheng, "Attacks and countermeasures in sensor networks: A survey," in *Business Media*. New York, NY: Springer Science, Springer, pp. 25, 2010.
[49] H. Khattak, M. Ali Shah, S. Khan, I. Ali and M. Imran, "Perception layer security in Internet of Things," *Future Generation Computer Systems*, vol. 100, pp. 144–164, 2019.
[50] S. Rathore and J. Park, "Semi-supervised learning based distributed attack detection framework for IoT," *Applied Soft Computing*, vol. 72, pp. 79–89, 2018.
[51] R. Sharma, N. Pandey and S. K. Khatri, "Analysis of IoT security at network layer," in *6th Int. Conf. on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, pp. 585–590, 2017.
[52] M. A. A. Da Cruz, J. J. P. C. Rodrigues, J. Al-Muhtadi, V. Korotaev and V. H. C. Albuquerque, "A reference model for Internet of Things middleware," *IEEE Internet Things Journal*, vol. 5, pp. 871–883, 2018.
[53] J. Sengupta, S. Ruj and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, pp. 102481, 2020.
[54] P. P. Ray, "A survey on Internet of Things architectures," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 291–319, 2018.
[55] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.
[56] M. M. Ahemd, M. A. Shah and A. Wahid, "IoT security: A layered approach for attacks & defenses," in *2017 Int. Conf. on Communication Technologies (Com Tech)*, Rawalpindi, pp. 104–110, 2017.
[57] S. Shachar, V. Sachidananda, Y. Meidan, M. Bohadana, Y. Mathov *et al.,* "Security testbed for internet-of-things devices," *IEEE Transactions on Reliability*, vol. 68, no. 1, pp. 23–44, 2019.
[58] C. Prakash and R. K. Saini, "A model on IoT security method and protocols for IoT security layers," in *Mobile Radio Communications and 5G Networks. Lecture Notes in Networks and Systems*, vol. 140. Singapore: Springer, pp. 771–780, 2021.
[59] M. I. I. Zarif, M. Hasan, M. M. Islam and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things*, vol. 7, pp. 100059, 2019.
[60] A. Q. Gill, G. Beydoun, M. Niazi and H. U. Khan, "Adaptive architecture and principles for securing the IoT systems," in *Innovative Mobile and Internet Services in Ubiquitous Computing*, vol. 1195. Cham: Springer, pp. 173–182, 2021.

[61] N. M. Kumar and P. K. Mallick, "The Internet of Things: Insights into the building blocks, component interactions, and architecture layers," *Procardia Computer Science*, vol. 132, no. 15, pp. 109–117, 2018.
[62] R. Addo-Tenkorang, N. Gwangwava, E. N. Ogunmuyiwa and A. U. Ude, "Advanced animal track-&-trace supply-chain conceptual framework: An Internet of Things approach," *Procedia Manufacturing*, vol. 30, pp. 56–63, 2019.
[63] A. A. Hammam, M. M. Soliman and A. E. Hassanein, "DeepPet: A pet animal tracking system in Internet of Things using deep neural networks," in *13th Int. Conf. on Computer Engineering and Systems (ICCES)*, Cairo, Egypt, pp. 38–43, 2018.
[64] S. N. Swamy, D. Jadhav and N. Kulkarni, "Security threats in the application layer in IOT applications," in *Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, Palladam, pp. 477–480, 2017.
[65] L. Nastase, "Security in the Internet of Things: A survey on 66 protocols," in *21st Int. Conf. on Control Systems and Computer Science (CSCS)*, Bucharest, pp. 659–666, 2017.
[66] T. J. Saleem and M. A. Chishti, "Deep learning for Internet of Things data analytics," *Procedia Computer Science*, vol. 163, pp. 381–390, 2019.
[67] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Generation Computer Systems*, vol. 82, pp. 761–768, 2018.
[68] L. Cui, S. Yang, F. Chen, Z. Ming, N. Lu *et al.,* "A survey on application of machine learning for Internet of Things," *2018 International Journal of Machine Learning and Cybernetics*, vol. 9, pp. 1399–1417, 2018.
[69] F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020.
[70] H. Tyagi and R. Kumar, "Attack and anomaly detection in IoT networks using supervised machine learning approaches," *Revue d'Intelligence Artificielle*, vol. 35, no. 1, pp. 11–21, 2021.
[71] M. Shafiq, Z. Tian, Y. Sun, X. Du and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for Internet of Things in smart city," *Future Generation Computer Systems*, vol. 107, pp. 433–442, 2020.
[72] M. Moh and R. Raju, "Machine learning techniques for security of Internet of Things (IoT) and fog computing systems," in *Int. Conf. on High Performance Computing & Simulation (HPCS)*, Orleans, pp. 709–715, 2018.
[73] A. E. Attaoui, S. Largo, S. Kaissari, A. Benba, A. Jilbab *et al.,* "Machine learning-based edge-computing on a multi-level architecture of WSN and IoT for real-time fall detection," *IET Wireless Sensor Systems*, vol. 10, no. 6, pp. 320–332, 2020.
[74] B. A. Homssi, A. Al-Hourani, Z. Krusevac and W. S. T. Rowe, "Machine learning framework for sensing and modeling interference in IoT frequency bands," *IEEE Internet of Things Journal*, vol. 8, pp. 4461–4471, 2020. https://doi.org/10.1109/JIOT.2020.3026819
[75] A. Kanawaday and A. Sane, "Machine learning for predictive maintenance of industrial machines using IoT sensor data," in *8th IEEE Int. Conf. on Software Engineering and Service Science (ICSESS)*, Beijing, pp. 87–90, 2017.
[76] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy *et al.,* "AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning," in *IEEE 9th Annual Computing and Communication Workshop and Conf. (CCWC)*, Las Vegas, NV, USA, pp. 0305–0310, 2019.
[77] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Generation Computer Systems*, vol. 108, pp. 909–920, 2020.
[78] P. Sun, J. Li, M. Z. A. Bhuiyan, L. Wang and B. Li, "Modeling and clustering attacker activities in IoT through machine learning techniques," *Information Sciences*, vol. 479, pp. 456–471, 2019.
[79] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman and A. Alazab, "Novel ensemble of hybrid intrusion detection system for detecting Internet of Things attacks," *MDPI Electronics*, vol. 8, no. 11, pp. 1210, 2019.
[80] L. Xiao, X. Wan, X. Lu, Y. Zhang and D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41–49, 2018.

[81] J. Cañedo and A. Skjellum, "Using machine learning to secure IoT systems," in *14th Annual Conf. on Privacy, Security and Trust (PST)*, Auckland, pp. 219–222, 2016.
[82] P. Punithavathi, S. Geetha, M. Karuppiah, S. K. H. Islam, M. M. Hassan *et al.,* "A lightweight machine learning-based authentication framework for smart IoT devices," *Information Sciences*, vol. 484, pp. 255–268, 2019.
[83] G. Abbas, A. Mehmood, M. Carsten, G. Epiphaniou and J. Lloret, "Safety, security and privacy in machine learning based Internet of Things," *Journal of Sensor and Actuator Networks*, vol. 11, no. 3, pp. 38, 2022.
[84] S. M. Tahsien, H. Karimipour and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *Journal of Network and Computer Applications*, vol. 161, pp. 102630, 2020.
[85] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang *et al.,* "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.
[86] L. Chen, S. Thombre, K. Järvinen, E. S. Lohan, A. Alén-Savikko *et al.,* "Robustness, security and privacy in location-based services for future IoT: A survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.
[87] I. U. Din, M. Guizani, B. S. Kim, S. Hassan and M. K. Khan, "Trust management techniques for the Internet of Things: A survey," *IEEE Access*, vol. 7, pp. 29763–29787, 2019.
[88] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi *et al.,* "Machine learning for Internet of Things data analysis: A survey," *Digital Communications and Networks*, vol. 4, no. 3, pp. 161–175, 2018.
[89] A. Singh, N. Thakur and A. Sharma, "A review of supervised machine learning algorithms," in *3rd Int. Conf. on Computing for Sustainable Global Development (INDIA Com)*, New Delhi, pp. 1310–1315, 2016.
[90] A. Anika, M. H. Rahman, S. Islam, A. S. M. M. Jameel and C. R. Rahman, "A comprehensive comparison of machine learning based methods used in bengali question classification," in *IEEE Int. Conf. on Signal Processing, Information, Communication & Systems (SPICSCON)*, Dhaka, Bangladesh, pp. 82–85, 2019.