Journal of Theoretical and Applied Information Technology
15th July 2022. Vol.100. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CLASSIFICATION OF SECURITY ISSUES AND CYBER ATTACKS IN LAYERED INTERNET OF THINGS

DEEPTI RANI[1], NASIB SINGH GILL[2], PREETI GULIA[3]
Department of Computer Science & Applications, Maharshi Dayanand University, Rohtak, Haryana, India
[1]deepti.sindhu@gmail.com, [2]nasib.gill@mdurohtak.ac.in, [3]preeti@mdurohtak.ac.in

ABSTARCT

Internet of Things (IoT) has emerged as a very significant research area. In IoT, billions of 'things' are connected which communicate with one another over a network. While communicating among 'things', their users face several types of application and technical challenges. IoT system infrastructure comprises several layers. Different researches have been conducted so far to detect vulnerabilities, threats, and attacks arising in the IoT environment. Modern IoT architectures consist of physical and network components apart from different kinds of services and solutions. IoT systems face several services and security challenges. Privacy and security problems in IoT systems are quite unpredictable. The main objective of this paper is to identify and classify various security challenges faced by IoT users. Several types of security and privacy issues have been addressed in the present paper. This paper also presents a classification of security and privacy issues considered in different levels of IoT architecture.

Keywords: *Internet Of Things, Layers Of Iot Architecture, Classification Of Security Issues And Cyber-Attacks in IOT*

1. INTRODUCTION

Internet of Things (IoT) is rapidly revolutionizing almost all the application domains and developing as a most promising technology that has grabbed the attention of most Internet users. IoT has become very popular among people due to low production and installation costs and the advanced performance of wireless sensor networks (WSN) [1]. This technology has added great value to automation in various application areas such as home automation, energy automation, industry automation, health-care automation, vehicular automation, and many more. A Unique Identifier (UID) is assigned to each registered IoT component (device, service, etc.) and facilitates it to connect with the Internet. The number of IoT devices is increasing at a great rate. Many IoT industries are aiming to launch IoT and Artificial Intelligence enabled household devices at low prices. The growth rate of IoT devices is increasing with the demand for 5G networks. IoT technology has greatly improved the quality of people's lives. Statista Research Department predicted the count of IoT-enabled devices to become more than 75 billion by 2025 [2]. In recent years, the IoT industry and market have revolutionized much faster and it is on cloud nine. On the other hand, security issues of IoT systems are also increasing dramatically, which are difficult to be predicted, detected, and eliminated.

The dramatic expansion in IoT technology is changing business in industries across the world. More and more organizations integrate IoT technology into their infrastructures, but most of them have adopted this technology without considering security issues as primary concerns. Security is the most critical concern for every adopting environment and it is becoming extensive day by day. Along with growing functionality and productivity, network vulnerabilities arise too which invite various types of security issues. The increasing rate of integration of connected devices in the continent generates bulk of data. The absence of proper data security and management gives more opportunities to hackers to penetrate the user's systems for malicious activities that result in loss of data and economy and even threats to human lives. It is necessary for IoT practitioners and experts to understand the main forms of threats and their causes for the better development of IoT technology.

Cyber-attacks such as MITM attacks, DoS attacks, viruses, and so many variants of security breaches exploit various components of IoT systems. These attacks victimize devices, networks, communicating channels, data processing systems, services, and even applications of IoT systems. Smart homes, healthcare, and business are the most targeted areas of cyber-attacks. Authors in [3] discuss significant concerns of privacy and security issues occurring in IoT-based healthcare system. Major issues in IoT systems include malicious actions, system failure, network failure, data errors, and natural phenomena. These threats pose a serious impact not only on the information system but also on an individual's life too. Victimized IoT systems may cause serious consequences like disclosure of users' confidential data, loss of finance, and even potential risk of life [4]. The main contributions of the present paper are:

- To identify various security challenges present in IoT enabled smart environment.
- To present layer-wise classification of security vulnerabilities, threats, and attacks in IoT infrastructure.

In the present paper, section 2 highlights the basic concept of IoT system, its characteristics and security goals. Various components and functions of IoT systems also have been discussed to understand the security risks in various layers of IoT infrastructure. Section 3 presents a layer-wise classification of IoT security vulnerabilities, risks and attacks.

2. INTERNET OF THINGS (IOT)

The Internet of Things is a collection of objects and services that are embedded with different components such as sensor-enabled objects, communicating channels, network tools, routing protocols, software, service providers, etc. People are benefitted and are facilitated by IoT technology in different ways. Along with the potential software developers, there exist many types of malicious software developers too. Security is the primary concern for IoT systems. Modern potential software developers follow certain characteristics and security goals while designing an IoT environment.

2.1. IoT Characteristics and Security Goals

There are various security concerns for IoT-based smart environments, which can lead to serious issues. Certain security goals are required to be achieved to avoid these concerns which have been given below.

- **Access Control-** It allows only the users with privileges (Identity and rights) to access and control the data and services of IoT devices. Access control also denies accessing unauthorized users. Identification, Authentication, Authorization, and Accounting are the main components of Access Control which are abbreviated as IAAA.

- **Privacy-** Large numbers of objects communicate with each other in an IoT environment. Preventing access to unauthorized users or devices can ensure privacy. The utilization of up-to-date privacy-preserving techniques protects the privacy of huge heterogeneous IoT data.

- **Confidentiality-** It can be achieved by allowing only authorized users to access a system containing confidential information. Prevent unauthorized access to the communicating data between the nodes to protect it from altering [5].

- **Availability-** Availability is the fact in which data and the services must be available whenever it is required by only authorized users. Data packets communicating over the network might be intercepted, eavesdropped, or redirected by attackers using DDoS-like attacks [6]. Due to lack of availability any component could be made unavailable to the user.

- **Non-Repudiation-** Non-repudiation ensures that somebody can't deny the validity of the message requested by another node in the network. It includes techniques such as audit logs, digital signatures, and IAAA. Non-repudiation is an essential characteristic for trustworthy communication in any IoT environment [7].

- **Integrity-** Data integrity is the process of ensuring the precision, consistency, and dependability of information over its entire lifecycle [8]. An attacker might alter or manipulate the critical information within the packet and inject the invalid information; the receiver receives the manipulated packet. It might lead to major issues such as loss of data and hazards of life [9]. Data integrity ensures that data received by the receiver is not changed maliciously [10].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.2. IoT Components and Functions

Each layer of IoT architecture consists of certain components which help IoT systems in various layer-wise categorical functions starting from data collection, communication, processing, service providing, security, management, and finally distributing applications to end-users. This paper doesn't follow any specific IoT architecture. Based on various existing pieces of literature (related to IoT architectures), this paper considers six layers of IoT architecture. Table 1 presents various components and functions of IoT architecture considering six layers.

Table 1: Layer-wise IoT Components and Functions

IoT Layers	Components	Functions
Perception/ Sensing Layer	Sensor enabled (Physical) end-devices, controllers and applications	• Recognize the physical properties of IoT devices • Identify objects for information acquisition
Network/ Transport Layer	Network and Communication Technologies, Gateways and Communication Channels	• Connectivity, security. and communication • Connection of one smart object to another smart object, servers, and/or network components; • Data transmission and processing received from the perception layer
Processing Layer	Processors	• Data Accumulation and abstraction • Data extraction, aggregation, and analysis • Data processing • Deriving Information
Service layer	Edge nodes, Cloud data centre, IoT Fog and Cloud services, Service providers	• Supports services using APIs • Logging, filtering, and patching • Information aggregation and storage
Security Layer	Data security techniques, Antivirus, Firewalls	• Encryption • Authentication • Authorization • Access control • Identification • Integrity
Application Layer	Application Programmable Interface (API), Access Tools, Visualization Tools	• Distribution of application services to various domains • Data visualization, and application services
Management Layer	Management Tools and Techniques	• Things Management • Network Management • Process Management • Service Management • Security and Access Management • Application Management • Event management

2.3. Classifications of IoT Security Attacks

With the rise in demand for IoT systems, cyber-attacks are increasing exponentially. More and more devices are being connected to IoT networks. Heterogeneous IoT devices are connected over the Internet which makes the related IoT networks less secure. The enormous consumption of Internet and IoT technology has given rise to many security risks. The graph of cybercrimes in the IoT environment is increasing faster as compared to the increase in security measures. Cybercriminals perform digital theft on various digital platforms. Cyber-attacks might be classified in many forms. Many researchers have come up with different forms of classifications of IoT attacks.

2.3.1. Types of attacks on IoT information security

Various types of vulnerabilities, security issues, and cyber-attacks are present in the IoT systems for breaching system security. There are two primary classes of threats and attacks which are carried out against IoT information security. Active and passive attacks potentially affect information security on various layers of IoT infrastructure.

- **Active attacks:** In the active types of attacks, an attacker intercepts the connection and system resources to affect the operations and to modify the information. Unauthorized access is performed by attackers with the aim of not only

information hacking but also harming and disturbing the opponent's communication. Active attacks cause harm to the system resources. Active attacks are more harmful than passive attacks as malicious acts are conducted against data confidentiality, integrity, and availability [11]. The impacts of active attacks are visible to the victim. So it is possible to detect such attacks.

- **Passive attacks:** In the passive types of attacks, an attacker intercepts the passing information with the intention of reading and exploring it. Here the aim of the attacker is to steal the information, without altering or modifying it. Hence, there is a threat to confidentiality. System resources are not influenced by passive attacks. Most of the time, victims remain unaware of the passive attacks which are not directly visible. So there is less possibility to detect such attacks.

3. GENERAL CLASSIFICATION OF IOT ATTACKS

In the present section, we focus on the classification of events using various machine learning algorithms via network traffic in the general IoT scenarios. IoT devices could be compromised in many ways. Several researchers presented a general classification of IoT security risks. Authors in [12] presented five general classes of attacks: software attacks, side-channel attacks, physical attacks, cryptanalysis attacks, and network attacks. Butun et al. [11] presented the concept of passive and active attacks and classified them into five (Physical, MAC, Network, Transport, and Application) layers. Security of IoT devices either may be compromised directly or indirectly through its different components like wireless sensor networks (WSNs), cloud, analytics, user interface, gateways, or end-user devices. Cyber-criminals use smart, brutal, intelligent, and stealthy methods of attacks which reduce the probability of being detected. IoT is an open platform for cyber threats. Attackers reduce the network performance, device performance, and throughput by attacking different layers of IoT. Till now, many types of attacks have been originated which degrade the performance of IoT. Many studies have been done to overcome the most significant problems in IoT. Due to the lack of advanced security mechanisms and anti-malware software, the transmitted and received signal of various IoT systems can be compromised easily that may cause serious hazards. No doubt IoT is expanding swiftly that is revolutionizing people's lives; still, there is no ending list of cyber threats on different levels of IoT infrastructures [13]. Viruses, Trojans, malware, ransomware, phishing like various types of cyber-attacks are commonly used by attackers everywhere in the cyber world.

3.1. Security risks on various layers of IoT architecture

The security of IoT infrastructure is a significant issue. More and more smart entities are being integrated with IoT systems. Physical and digital entities are highly influenced by IoT systems with introduction of new innovations and technologies in them. Despite the variety of qualities in IoT, it is affecting the cyber and physical world due to endless security vulnerabilities. Augmentation of vulnerabilities will pose terrible risks to the privacy and security of users' potential data, assets, and even human lives. Potential data, which is generally targeted, may include text, images, audio, video, etc.

Journal of Theoretical and Applied Information Technology
15th July 2022. Vol.100. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

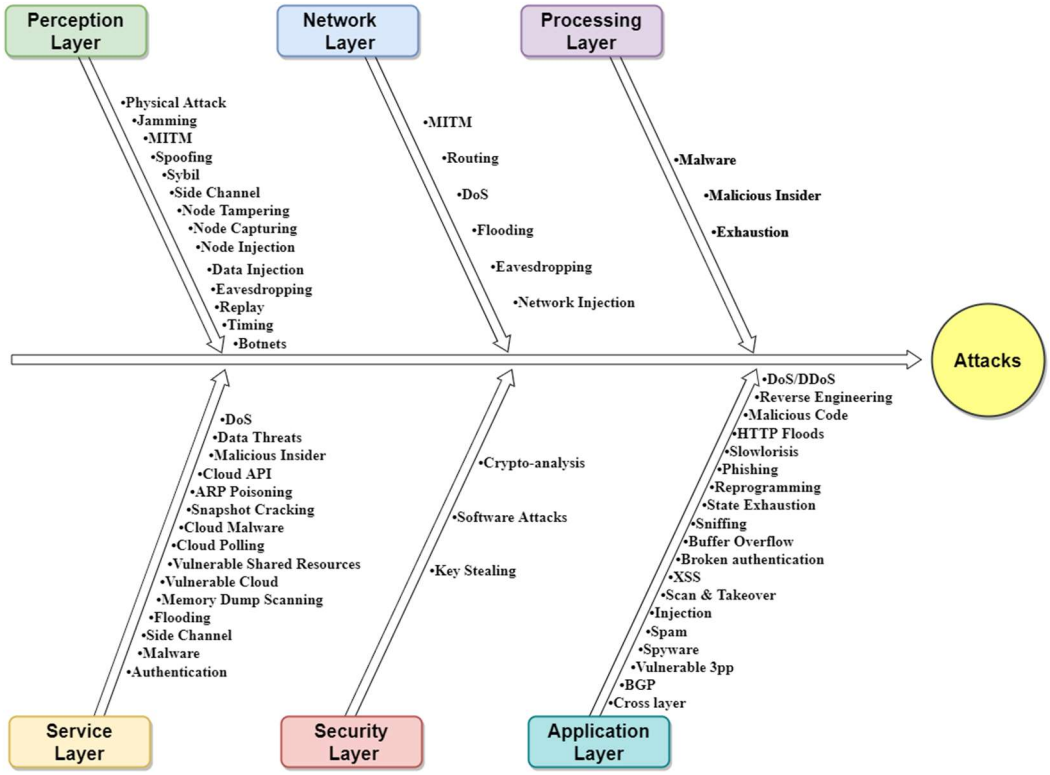

Figure 1: Layer-wise Security Attacks and Cyber-Threats in IoT Environment

Figure 1 presents various types of cyber-attacks and security issues on different layers of considered IoT architecture.

3.1.1. **Perception Layer** Attacks

Millions of smart devices are getting connected to IoT infrastructures day by day. The perception layer of IoT is responsible for the identification or detection of smart objects. This layer is also called the sensing layer or the physical layer [14]. This layer consists of several smart components like sensors, actuators, RFID tags, Wi-Fi, cameras, and microcontrollers using which things are monitored and controlled in physical and digital environments. Various components on the perception layer form wireless sensor networks (WSNs). These smart components enable things to interact with each other in the physical environment and to behave as smart objects [15]. These devices have high processing power and good capability to connect to the network of any environment. Devices are connected to the network with the help of general packet radio service (GPRS), Bluetooth, Wi-Fi, Zigbee, etc. [16]. Many types of sensors are used with IoT devices for sensing and collecting information from physical environments [17]. An enormous amount of data such as temperature, pressure, and quality of air, water, and soil, location, vibration, motion, weight, of various things in different environments are collected using sensors and monitoring devices. Collected data is actuated by actuators using actuation commands. The selection of sensors and other components depends on the application's requirements. Data is processed to get information that is transmitted to the network layer. Data is an expensive commodity of the current century. Several issues are revolving around the security of information systems which may hinder the appropriate deployment of IoT. So this is very important to identify various challenges which can affect the perception layer. Many security risks occur on each layer of an IoT network [15]. Security issues and cyber-attacks on the perception layer have been discussed below.

Physical Attacks: In the Physical attacks, the attacker may first attempt to gain physical access

to the targeted IoT device [18]. He might learn the attacking process by purchasing or accessing a copy of the device. Then using reverse engineering he can perform a "false attack test" to collect the types of outputs and other necessary information. After understanding the system he will prepare to perform a remote attack on an actual IoT device. Hardware-based right security measures are required to be implemented for encountering physical attacks. Accurate security measures might be carried out by understanding the attack surfaces and vulnerabilities faced by smart IoT devices. IoT devices comprise several components like sensors, actuators, micro-chips, and micro-controllers. Attackers can temper with victims' expensive objects with stealthy and harmful intentions. The physical layer of IoT system is vulnerable to various kinds of cyber-attacks.

Jamming: In a jamming attack, the IoT network is collapsed by the emission of radio-frequency signals on target wireless devices without adhering to a defined protocol. The radio interference disrupts the network operations that might cause message collisions and flooding of channels. Jamming severely affects the data communication that causes unpredictable responses of the system. Authors in [16] proposed an approach to detect jamming by consistency checking on signal strength to compute the ratio of successfully delivered packets. Young et al. [19] suggested an approach by measuring the signal strength to extract noise signals for comparing the values with a customized threshold.

Man in the Middle (MITM) Attack: This is one the most widely used way of attacks. Using the MITM attack, the attacker intercepts the original communication between two nodes (generally between client and server) and plays the role of a proxy user by establishing a new connection. In IoT environment, MITM attack takes place between an IoT device and the application of the user interface or a web server. Being sitting in the middle, the attacker disables all standard security implementations. Bluetooth connection is a very common medium of MITM attack as many IoT devices are operated using Bluetooth Low Energy (BLE) [20]. Figure 2 shows the most common network attack MITM.

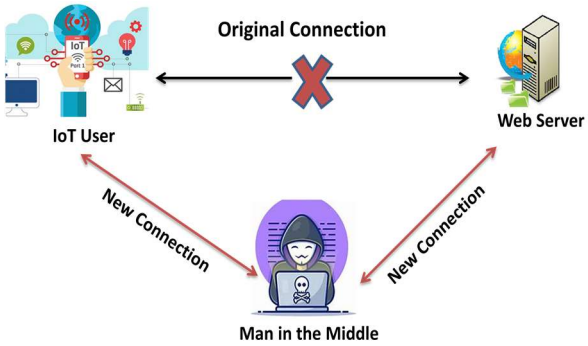

Figure 2: Man in the Middle Attack

Spoofing: This attack is also recognized as an identity spoofing attack. An ordinary IoT device relies on an openly accessible wireless communication medium for connection establishment without knowing the security measures. An attacker can impersonate a single legitimate user or multiple legitimate users by using a fake identity like IP (Internet protocol) or Media Access Control (MAC) to access the IoT network. After gaining unauthorized access to IoT network, an attacker can easily launch spoofing attacks like denial-of-service (DoS) and man-in-the-middle (MITM) attacks. An attacker may access the victim user's secret keys in advance. Some researchers have suggested the cryptographic authentication-based approach but it was not effective in the condition of physical attacks [21]. The Physical Layer Identification (PLI) mechanism can more effectively identify spoofing attacks by utilizing some properties of the physical layer such as channel frequency and impulse responses channel state information, received signal strength [22], and hypothesis tests [23]. But PLI is a slow mechanism because it can't detect many legitimate users simultaneously. Wang et al. [24] suggested a two-step virtual channel approach for attack detection in IoT networks. First, anomalies are detected by examining the virtual angles of arrival for attaining the path of connected IoT devices in the virtual channel space. This step is followed by a machine learning-based approach for actual attack detection. Madani et al. [25] proposed a signal-level device fingerprinting approach for wireless IoT networks. Abdulla et al. [26] proposed an ARP spoofing attack detection scheme with a neural network of artificial intelligence techniques. Einy et al. [27] provide a face spoofing detection mechanism using deep multicolor feature learning. Aldabbas and Authors in [28] suggested a software-defined

networking mechanism for detection and handling ARP spoofing.

Sybil Attack (SA): Malicious nodes make use of the modified fake identities to propagate spam and malware to generate Sybil nodes that can access the identity of an authorized node. Sybil nodes access routing information by interrupting the communication system. Like spoofing, a Sybil attacker too personifies the identity of a real network user through which they can disseminate spam, fishing, and malware to rob secret information of the user. Sybil attack aims to influence the privacy and confidentiality of a network user subject to access his personal information. This attack targets distribution storage, target routing, resource allocation, and data aggregation [29] which can cause network overhead [30]. Yu et al. [31] and Al-Qurishi et al. [32] proposed a social graph technique based Sybil-guard Sybil detection approach in which the social graph lies into honest regions. Authors in [33] presented a study of network features and a cryptography-based SA detection approach. Vaishnavi and Sethukarasi in [34] proposed a Sybil detection mechanism using blue tits algorithm.

Side Channel Attacks (SCA): Side-channel attacks (SCA) victimize the security of a system to access the secrets from its chips. Quickly growing connectivity leads to more and more development of embedded devices. Message encryption and security of such devices can be assured by applying computationally secure secret keys [35]. But implementation of these algorithms sometimes results in leakage of critical side-channel information in the form of electromagnetic radiation and high power consumption. According to an incident, the attackers attempted to falsify the e-cigarette batteries by stealing the secret encryption keys from authentic batteries. SCA are very crucial issues to resource-constrained edge devices that use the symmetric key.

Node Tampering: An attacker can replace the nodes by damaging the sensors. He can trigger an attack while developing the device by changing the procedure of manufacturing. He can access connected nodes to obtain sensitive and confidential information. The attacker can acquire the password of various smart devices such as Amazon Alexa/Echo, smart meters, IP cameras, medical diagnostic equipments, etc. So many vulnerabilities are associated with commercial and domestic smart devices. Many researchers have used swarm-based defense mechanisms for tampering detection [36].

Node Capturing: Nodes enabled with WSNs can be compromised by adversaries [36]. Node capture attack is the fusion of active, passive, and physical attacks [37]. Attackers can intelligently capture the sensor nodes to extract the confidential keys from their memory to disrupt the security, confidentiality, and reliability of the network and to establish a relationship with the user's node. Some authors used a matrix-based node capturing algorithm for detecting the captured node [6]. Agrawal et al. [38] presented an approach using a program integrity verification protocol equipped with a trusted platform module to verify the node capturing in sensor-enabled nodes.

Malicious Node Injection: The attacker can get complete access to the target network by injecting one or more malicious nodes into an authentic node. The objective of injecting is to manipulate the data of genuine nodes and to get unauthorized access to connected devices and networks. The best time to inject node is when the software is upgraded. Malicious nodes can intercept the delivery of a genuine message. Many pieces of research have been conducted for malicious node detection. Wang et al. [39] suggested a path-based node detection approach that was more efficient and simple than node-based methods. Some researchers focused to detect malicious nodes by getting incremental information. The incremental information can't directly help in finding the malicious nodes, but the accuracy of the detection process increases with an increase in the valuable information. Different machine learning (ML) based predictive analysis algorithms are also very efficient to identify malicious nodes. Machine learning is categorized into offline learning and online learning [40]. Sajid et al. in [41] proposed blockchain-based malicious node detection in intelligent sensor systems. The detection mechanism includes the combination of certain genetic algorithms and the Dijkstra algorithm. Nobahary et al. [42] approached a three-phase selfish (and malicious) node detection algorithm that was based on hierarchical game theory.

False Data Injection Attack: Once the attacker is able to access the victim's system, using any attack like MITM, he becomes able to access the sensors used by the user. He either attempts to

alter the data monitored by sensor nodes or adds some noise that is undetected by the user. Using this, the interceptor can twist the algorithm's prediction [43].

Eavesdropping: An eavesdropping attack takes place when an attacker intercepts, modifies, or deletes data traveling over electronic devices such as mobile devices, computers and IoT devices. It is the most common attack for wireless communication and is also recognized as snooping or sniffing attack. It anticipates unsecured (vulnerable) network traffic to access the data when it is transmitted between two nodes [6]. The major cause of unsecured network connections are not updating the applications of devices from time to time and not encrypting the data. Hackers could take over devices to spy on users' confidential and valuable information. Several pieces of research have been conducted to detect active and passive eavesdropping attacks. Eavesdropping is a dangerous threat and its detection is a crucial task. Some researchers have suggested protecting the system against eavesdropping by setting up a virtual private network (VPN) that encrypts the data traveling between two endpoints. Xu et al. [6] proposed an eavesdropping detection approach for MIMO-enabled IoT that is based on large dimensional random matrix theory.

Replay Attack: A replay attack is a kind of security risk for the data sent over the network (between sender and receiver devices). It takes place when an attacker acts as the original user and captures the network traffic with unauthorized access, manipulates the content, and sends it to the receiver. The receiver can't easily recognize whether the message has been sent from the original sender or an unauthorized user. This attack is a type of man-in-the-middle security breach in which original data is maliciously repeated or delayed by the hacker and is stored without permission. The main cause of this attack is weak cryptography system, stolen keys or passwords, limited security systems, and lack of software updating. Miao et al. [44] suggested a replay attack detection model containing three components. Rughoobur and Nagowah [13] proposed a lightweight detection framework for battery depletion replay attacks that was further made generic for other IoT systems. Authors in [45] proposed a deep learning-based replay detection approach for smart cities.

Timing Attack: A timing attack is a side-channel attack (SCA) that occurs in cryptographic systems. Information security of IoT users depends on the reliability of cryptographic libraries. Cryptographic systems are vulnerable to SCA due to the execution behavior [46]. An attacker attempts to capture sensitive data of a system by inspecting the execution time taken by cryptographic algorithms [47]. The execution time may vary for each operation and it relies on the input. Attackers can use timing attacks to extract various secrets such as login names, passwords, private keys, etc. which are maintained in a security system. The attackers can exploit login information to gain access to the system which can be leaked using brute force. Researchers in [35] suggested handling side-channel timing attacks by implementing the cryptographic ciphers during execution. They focused on RSA and AES cryptographic ciphers.

Botnets: Botnets are one of the most common risks that take advantage of IoT security vulnerabilities. These are networks composed of nodes that are infected by malware which converts them into bots. The bots attack a machine in response to the commands from the bot-master [48]. IoT is the favorite place of botnets because due to the lack of good security features the devices allow malware transmission [49]. Mirai botnet is the most notorious denial-of-service attack that was held in 2016. It is difficult to detect and combat botnet attacks.

3.1.2. Network Layer Atacks

The main objective of this layer is data transmission across the network that it accepts from its previous (perception/physical/sensing) layer. The network layer helps in connecting one smart object to another smart object(s), servers, and network devices. The features of the network layer are used to transmit and process sensed data [17]. There are enough possibilities of attacks on this layer because the layer accepts data from heterogeneous devices. Therefore, it is mandatory to make security levels high by deploying some authentication methods for data senders [12]. Another necessary security measure is point-to-point encryption to ensure rooting security and data privacy [50]. Most of the operations and security problems on this layer are similar to the network layer of the TCP/IP model [51]. Routing is the major task on this layer to prevent packet loss and deal with

malicious attackers and counterfeiters. Nodes with high traffic load and a number of hops are considered unreliable or malicious nodes [52]. Common and extensive security threats on the Network layer are:

Man-in-the-Middle (MITM) attack: This attack is also referred to as a manipulator-in-the-middle attack or MITM attack. MITM is one of the most prevalent attacks. Due to rapidly growing IoT technology numbers of devices, applications, and services are being developed for smart environments that raise security concerns in the network. IoT devices operate the amount of secret information such as MAC/IP addresses, passwords, and account details. The attacker can hack this information to identify the user's location [53]. MITM is an eavesdropping attack that occurs when the data flows between two endpoints and its confidentiality and integrity are compromised. It makes for users difficult to understand if he is connected to an actual secure connection or similar insecure false connection. In the IoT network, the nodes are directed toward gateway for communication. If a gateway is attacked all nodes sending and receiving data may become victims. MITM can be executed in active mode (alter information, inject malware in a session) and passive mode (spy on communication, steal passwords and sensitive data). Agyemang et al. [54] proposed a lightweight MITM detection and defense algorithm for Wi-Fi-enabled IoT gateways using packet analyzing. Researchers in [52] proposed MIMA detection by trust computation of each sensor node across different layers and aggregating the trust values to know whether the node is malicious or not. Choi et al. in [55] proposed a blockchain-based MITM detection approach. The main sources of MITM attacks are injection, replay, and resource Depletion attacks.

Routing attacks: Routing attacks can cause the messages or data to route elsewhere. It can result in crucial disruptions, information loss, and even threat of life. The attacker might attack the information communicating over the network to redirect, spoof, misdirect, alter, or destroy data packets flowing. Black-hole, wormhole, Gray-hole, Sybil and hello-flood attacks are common forms of routing attacks in IoT [28].

Denial of Service (DoS) Attack: Attack prevents authentic users to access devices and network assets. It is attained by flooding the network assets or targeting redundant requests to make them inaccessible for authentic users.

Flooding: In this attack, the attacker sends a large number of requests to the server to overload the network flooded with unnecessary traffic [56]. By this, the user faces problems in sending requests to the server and gets network overload messages.

Network Injection: In this attack, the hacker replaces the actual sender node with his malicious node (device) and that fake node acts as a part of the IoT network [57].

3.1.2.1. Radio Frequency Identification (RFID)

RFID is an important component of an IoT network. Radio Frequency Identification (RFID) is also used very commonly for identifying, recording, and controlling moving smart objects and people [58]. RFID Tags invite certain attacks most commonly such as Unauthorized Tag Cloning, Unauthorized Tag tracking, and Unauthorized Tag disabling.

3.1.2.2. Wireless Sensor Networks (WSN) Attacks

WSN is the most important component of IoT for sensing and aggregating data and providing it to personalized social applications [59]. At a time, a sensor in WSN can remain precisely in one of four states: healthy, compromised, responsive, and fail. A sensor transits among these states in its lifecycle [18].

Deployment of WSN in an unfriendly environment makes it vulnerable to various types of attacks. Threat or intrusion detection in wireless sensor networks is a significant area of research. It is important to ensure that the sensed data is communicated with proper security strategies (secure data routing protocols [60], secure network coding and delivered to secure end-user). Information security is a big concern of WSNs and these are always vulnerable because these are generally deployed in malicious environments. To improve the performance of hardware equipments, it is required to prevent and detect various types of attacks occurring in WSN. Unfortunately, it is extremely difficult to detect some attacks in WSN. Sometimes threat detection becomes a more critical problem than the threat itself. If a threat is not easily identifiable it may cause big harm. In WSN, maximum security can be

achieved by designing a productive threat detection model which can provide immediate alerts about attacks even stop the attacks and mitigate the harm.

Currently, several challenges are coming in the path of data/information security of wireless sensor networks including external attacks and internal attacks. It is more crucial to protect the system against internal attacks in contrast to external attacks because detection, revocation, prevention, and tolerance of compromised and replicated nodes are more challenging. External attacks can be prevented effectively with authentication and encryption strategies but these schemes are not usually applicable for internal attacks [18].

Internal attacks originate within the network itself. These are initiated by compromising and capturing nodes inside the network. Here, the major behaviors of internal attacks are tampering, replaying, forging, discarding, and misleading data packets. Malicious nodes acquire the data transmission schemes, network keys, and a lot of information that is sent across the network. Encryption and authentication mechanisms are also not effective in internal attacks. It results internal attacks to be more dangerous than external attacks. Network monitoring is also not helpful to detect internal attacks. Detection of internal attacks is a complicated procedure that can be executed in three steps: (1) analyzing the behaviors of attack, (2) detection of compromised nodes, (3) verification of replication [18].

Sleep Deprivation Attacks: Malicious nodes attack by making requests to victim sensor nodes only when it is essential to keep that awaken. These attacks enhance the power consumption of the target node to minimize the lifetime. Poor throughput maximizes the overhead in attack detection [61].

Barrage Attacks: The attacker performs bombardment of legitimate requests over victim nodes. But energy-intensive operations are not made performed by those nodes [61]. This type of attack causes the victim node to spend more energy in computation and communication. It is easily detectable.

Battery leakage attacks: Generally, it is impossible to replace or recharge the battery of sensory nodes. Low power sensor nodes remain the main targets that are immensely infected by attacks. These attacks may cause the reduction of energy level of sensory nodes, RAM destruction, and even death of nodes [62].

3.1.3. Processing Layer Attacks

The processing layer is a part of middleware layer that gathers the data transmitted by the transport layer and performs processing on it. It is also responsible to eliminate unusual and meaningless information. For solving big data problems, this layer only extracts the most useful information. A large amount of information can affect the performance of IoT system. There are many attacks that can affect this layer to degrade the performance of IoT.

Malware: This layer collects an enormous amount of data that it receives from its previous layers for processing and analysis [63]. There is enough possibility of Trojans and viruses to get into the system that facilitates attacker unauthorized access to data.

Malicious Insider (MI) Attack: MI attack arises inside the IoT environment that is initiated by an insider user to access the private information of another user. Lack of data encryption, password management, and the absence of appropriate passwords make the internal IoT environment vulnerable to attacks [64], [65].

Exhaustion: DoS attacks may cause several types of violations on the target system. This type of attack may target the battery of a device and can take over 100% of the system's processing power and memory. This attack disables the system to process further.

3.1.4. Service layer Attacks

Service layer in IoT architecture consists of cloud and fog services. Cloud services have highly improved the efficiency of IoT in terms of storage and speed. But cloud computing services are susceptible to inside and outside attacks. Cloud developers and service providers need to increase security measures to protect users' sensitive data from cyber threats [66]. Cloud services which are actively developed still have certain vulnerabilities that might be exploited by cyber-criminals. There are several security concerns that arise due to cloud vulnerabilities in cloud infrastructures [67]. Levels of cloud computing attacks are client-to-client and virtual machine to virtual machine.

DoS Attacks: Cloud computing environments are shared by a number of users that brings complexity to the environment. If any cloud platform is attacked, it is difficult to resolve such attacks and these attacks are much promising to create disaster on the infrastructure. Increasing cloud services and virtual data centers are opening new opportunities for cyber criminals [67]. The most modern attackers can spread attacks just using botnets, without attacking the entire infrastructure. The service layer is an attractive target for DDoS attackers because services provided by the service layer (SaaS) can be made unavailable using this attack [66].

Data Threats: Generally, IoT users store several types of data on the cloud and that data may contain the amount of sensitive information related to user and business activities. Wi-Fi-enabled and Bluetooth-enabled devices transfer data to an online platform or cloud server [68]. This data is adaptable to breaches, damage, or loss due to certain vulnerabilities, human actions, and unforeseen circumstances. To prevent such emergencies cloud developers must use highly efficient modern encryption algorithms to confirm the data integrity while transitioning from user to cloud.

Malicious Insider attacks: Authorized cloud users may act maliciously and they can schedule attacks to reveal data on cloud surface.

Cloud API Vulnerabilities: Some application programmable interfaces (APIs) let users interact with cloud-based services. APIs may contain several vulnerabilities that may crucially impact the management, coherence, monitoring, and provision of the cloud. This occurs due to weak controls over APIs.

ARP Poisoning: In Address Resolution Protocol (ARP) poisoning attack, the attackers take advantage of the weakness of ARP protocol to depict a network IP address to a malicious MAC followed by updating the ARP cache with Malicious MAC [69]. For small networks like personal clouds, this attack can be minimized using static ARP. For large-scale clouds, the attack can be prevented by locking a single port to a specific IP address.

Snapshot Cracking: There are numerous cloud agents with distinct business models like Google cloud, Microsoft Azure, Amazon EC2, and etc. But all cloud agents not encrypt their virtual memory storage [67]. Encrypted virtual memory has certain drawbacks like sharing resources with other users, data mount, etc. A VM administrator can easily attack on VM himself using snapshots [68].

Cloud Malware Injection: A malicious service implementation module (SaaS, Paas, or IaaS), an application, or a virtual machine is injected into the cloud platform [68]. For launching this attack, the malicious user has to create a malicious application, service, or VM instance and then he can insert it into the cloud system. All the requests automatically redirect toward a new instance where the malicious code is executed. It occurs due to a lack of an integrity check of service instances [70].

Cloud Polling (CP): CP attack is a type of MITM attack. In the active mode, a smart home device constantly communicates with the cloud seeking the firmware updates. Interceptors can redirect the network traffic using Address Resolution Protocol (ARP) poisoning or by modifying the settings of Domain Naming System (DNS) [69]. He also can intercept the HTTPS traffic using self-signed certificates, or using an SSL strip like tool. Most IoT devices do not check the authenticity of the level of certificates. So attackers can effectively use the self-signed certificate method that allows them to attack the IoT devices [71].

Vulnerable Shared Resources: Cloud computing provides sharing facility. Multiple users can share various technologies like virtualization and cloud harmony on a single cloud platform. There are critical technological vulnerabilities in a cloud environment, utilizing which an attacker can make significant damages to the cloud users. Vulnerable cloud administrators or shared resources can allow attackers to compromise virtual machines or even the host sometimes.

Vulnerable Cloud Services: Cloud computing is designed to distributed cloud services but these services are not much secure against each other. An attacker can exploit the vulnerable cloud services to obtain illegitimate access to the data of legitimate users [72].

Memory Dump Scanning: An attacker may dump memory containing text including login, password, secret key information, emails, SSH, etc. The attacker can obtain personal information from a dump memory. Attacker retrieves a bulk amount of data from VM and it is very difficult

to scan critical information out of this data without keywords. In order to speed up data scanning, attackers can use social engineering techniques utilizing the dump information. A malicious user can utilize this information to guess login passwords and secret keys [68].

Flooding Attacks: Despite secure data transmission between the client and the server, that attacker can attack data on the cloud. The client sends requests to the cloud server to access data and on the other hand, the malicious user also sends nonsense frequent requests to access data to the cloud system. It may result in a bulk of requests from different clients due to which cloud server feels request overload. Due to request overload, the service instances running on the cloud platform become unable to respond to normal users. This is a serious vulnerability of flooding attacks that causes DoS attacks. Once a service instance running on the cloud is attacked by DoS, the malicious user can access miscellaneous information and computational resources [70].

Side Channel Attack: In this attack, a malicious virtual machine (VM) instance is positioned close to a cloud server that is used to launch an attack on the cloud server [35].

Malware Injection Attack: In this attack, the malicious user aims to inject malicious code or services to forge existing services. While running the services on the cloud, a user can't differentiate between valid and invalid services. Through this attack, the attacker can achieve data modification, change functionalities, and create deadlock [73]. The attacker implements a malicious service targeting IaaS and SaaS to run on cloud servers. This attack is also called meta-data spoofing [74].

Authentication Attacks: Authentication is a very sensitive property in virtual as well as hosted services. There are so many authentication-related vulnerabilities that can be exploited to access system services illegally [74].

3.1.5. Security layer Attacks

The security layer has been harmonized with IoT architecture to make the architecture secure. Many types of attacks are performed by cybercriminals on IoT devices, networks, and applications to access users' information. This layer attempts to protect every layer of IoT architecture from outside and inside attackers. It also manages to make the incoming and outgoing network traffic secure. Although the security layer manages the security on the entire IoT infrastructure still there exist some challenges that may impact the security of IoT resources (data, devices, communication, and so on). So it is required to dive deeply to consider various factors on which IoT security is dependent. IoT devices depend on other devices (phone, laptop, etc.) for connection and communication [75]. Security layer puts high efforts to encrypt and secure communication data still malicious users can access IoT devices and critical information. Software errors in the software utilized for IoT also may cause security issues. It may happen due to a programmer's mistake or it can be created intentionally by any insider. The main attacks that can affect the user's information system are denial of service (DOS) and man-in-the-middle (MITM) attacks. These attacks can be utilized in many forms to impact the elements on different layers of IoT systems.

Crypto-analysis Attack: This type of attack targets the ciphertext to crack the encryption to get the plaintext. The attacker might steal the secret key used for information encryption. Different ways of crypto-analysis attacks include plain-text attacks, man-in-the-middle attacks, cipher-text attacks, etc. [14].

Software Attacks: Attackers exploit software vulnerabilities to attack the system. Cryptography algorithms may also be vulnerable that could allow attackers to break the system's security. An intruder may affect the cryptographic algorithm at its various phases from designing to implementation. There are many possibilities to make the security algorithm vulnerable. A software (algorithm) designer might be bribed, threatened, or cheated to create adversaries in the security system of specific IoT assets. Lack of proper coding, inefficient or outdated software tools, weak encryption, and guessable passwords may also be responsible for software weakness and attacks [76]. It is suggested to empower the security system by utilizing the latest security mechanisms like multiple security systems, access control, and utilizing various securities attributes such as integrity, confidentiality, and authentication [77].

3.1.6. Application Layer Attacks

This layer is liable for providing application-specific services to the end-user. Applications that use IoT technology or where

IoT is deployed are included under the application layer. Information collected/ processed/ analyzed on previous layers is presented to the user through this layer [78]. This layer performs convergence between social IoT needs and industrial technologies. Some applications of IoT may be a smart home, smart grid, smart, smart education, smart industry, smart city, smart transportation, smart health, smart agriculture, and smart wearable. When IoT technology is applied to any application domain, it introduces many kinds of vulnerabilities and threats in applications and hardware outside and inside. Causes may vary depending on the application [11]. An unsecured IoT network gives hackers easy access to devices and allows them to put devices together on the surface of IoT botnets. Such botnets are exploited in sneaking ways that are used for brute force attacks. The DDoS attack is one of the most massive large-scale attacks for which botnets are used. According to IoT business news, billion of IoT devices around the world are being hijacked due to vulnerable security and inefficient detection techniques. Organizations need to improve security controls that can efficiently detect and block malicious threats, in order to protect their applications, websites, and services.

Application layer protocols contribute significantly to the complex IoT environment. These protocols manage the communications among applications and services running on various IoT devices and cloud/edge structures. MQTT, CoAP, DDS, AMQP, and XMPP are standard messaging protocols whereas 'mDNS' and 'SSDP' are service discovery protocols [75]. But services and components provided by these protocols are not sufficient to protect devices enabled with IoT. Many security threats may originate from misconfiguration of components and potentially vulnerabilities software. The lack of proper security services and the open nature of application layer protocols can permit attackers to compromise the IoT environment.

Denial-of-service (DoS) Attack: The malicious user pretends to be an authenticated user and logs into the system by stealing the credentials. He interrupts the normal jobs of the system (network and applications).

Malicious Code Injection: An unauthorized user injects certain malicious codes into the user's system from an unknown remote location and attempts to rob or alter the data of the authorized user.

Reverse Engineering Attack (REA): In this type of attack, an attacker analyzes the software to access the user's fragile information and credentials [78]. In order to get access to IoT objects and software, an attacker can use software vulnerabilities and programming errors with the help of reverse engineering.

DDOS Attack: Distributed Denial of Service (DDoS) is one of the most notorious and widely used security attacks which are triggered through open ports [79]. DDoS attack aims to block and interrupt the authorized user's requests by flooding the host server with a large number of requests. This attack prevents legal users from accessing the network resources by disrupting the network communication. In a DDoS attack, a network of devices is compromised by malicious users to form a botnet. The botnets send a heavy stream of traffic to the target server which causes a denial of service by exhausting communication and computation services. The attacker can use an internal network or remote network to commit an attack. The system can be accessed either physically or through wireless communication. An instance of this phenomenon is to produce high-energy radio signals to distort the wireless communication surrounding using jammers [48]. 'Mirai' is a well-known and largest DDoS attack that happened in October 2016. In this massive attack, attackers used robust malware which infected millions of connected devices throughout the world. The systems can be protected against DDoS by detecting and preventing attacks in the IoT devices and mitigating the consequences of attacks on end routers.

HTTP Floods: This attack is a volumetric DDoS attack designed to overload a targeted server with HTTP requests. The attacker sends apparently legitimate requests in large quantities from different locations to crash the targeted web application. They repeatedly send requests to saturate the target to make it unable to respond to normal traffic that causes denial of service for additional requests from genuine users. All browser-based Internet requests are done through HTTP. It is commonly used to load web pages and upload form like content over the Internet. It is very difficult to differentiate malicious traffic from normal traffic. Malicious users employ botnets to maximize the attack consequences.

HTTP GET and HTTP POST are two types of HTTP flood attacks. HTTP flood attack is based on GET and POST requests done by the client. Using GET method receives data from the server means it is used to retrieve data (e.g. images, files). POST method sends data to the server. It usually triggers complex processing on the server (e.g. database access).

Slowlorisis: It is a type of DDoS attack that uses partial HTTP requests to open the connections between a machine and a target web server. The aim of this attack is to keep the connections open for a long time and using this attacker can overload and slow down the target. This type of DDoS attack can be launched using very low bandwidth and it only affects the target by influencing other services and ports.

Phishing Attack: A malicious user sends data to the user's system pretending as a high-ranking authority to attack the system. The attacker gains the credentials to victimize the genuine user and damage data [80].

Reprogramming attack: Using network programming, an attacker reprograms the software used for an IoT object from a remote location to manipulate its normal behavior (functionality) and control the application partially or completely. An attacker can attack integrity, privacy, confidentiality, and other features.

State Exhaustion DDoS Attack: Such attacks usually aim at firewalls, edge load balancers, and active traffic monitoring services by emphasizing the scale of the TCP state of these devices. These attacks can be operated at small traffic volumes, still can overburden even extensive enterprise services. Such attacks hardly have signatures that prevent these from filtering. Modern attackers can access millions of vulnerable IoT devices can initiate complicated DDoS attacks at a large scale.

Sniffing Attack (SA): The attacker establishes a sniffer application into the system to obtain its confidential information (username/passwords, network usage, identity theft, etc.). In SA, attackers can monitor the traffic or route the traffic to a malicious destination in order to monitor, capture, and analyze [81].

Buffer Overflow Attacks: An attacker can initiate a buffer overflow attack by overwriting the application's memory that alters the program's execution path. When any response is triggered it destructs the system's files and exposes private information. The attacker sends some extra codes having new instructions to gain access to the system. If the attacker is aware of memory layout, he can feed input that can't be stored by the buffer, overwrite the areas containing execution code, and replace it with new code to gain control over the system programs.

Broken Authentication and Session Management: Attackers can obtain credentials to access user accounts. By exploiting authentication vulnerabilities the whole system can be compromised. An attacker may attempt to access the login using a list of known username/password combinations that might be obtained via certain data breaches. After that, he can use a script to test all the combinations on the login systems and repetitive login sessions.

Cross site scripting (XSS): The malicious programmers insert custom codes into a URL path or a website through web applications [78]. The attacker can inject malicious JavaScript code into the victim's browser. XSS attack happens when this code is viewed by victim users.

Scan and Takeover: In the absence of strong authentication and authorization of an IoT system application such as poor encryption and password protection, and limited hardware resources the attacker can accommodate the system, control it and take over the system.

Spam Attack: In the absence of proper security mechanisms, the malicious user can establish a connection with the target system using an IP address and send malware to the IoT application.

Injection Attacks: Like other web applications, the IoT web applications are vulnerable to such attacks. In order to compromise the IoT system, an attacker adds an additional request to the existing one. XML and SQL are widely used for this type of attack [82].

Spyware: Due to the absence of enough resources in IoT applications, it is difficult to enable encrypted communication over the network layer using TLS. Attackers can compromise the system using spyware that enables attackers to read the data sent over the network and manipulate it.

Vulnerable 3pp libraries: Without proper monitoring, 3pps or third-party publishers could be hacked before entering into applications via

system updates. It can utterly compromise and accommodate the system.

BGP Hijacking: Border Gateway Protocol (BGP) hijacking is also referred to as IP hijacking, route hijacking, or prefix hijacking. The attackers can take over a group of IP addresses stored in the Internet routing table by corrupting it and maintaining using BGP. Internet being a global network can enable any connected host to talk to others anywhere in the world. IP hijacking can be conducted intentionally or accidentally in many ways. Like session hijacking, intrusions are implied into in-process BGP session and it needs some information to reset the attack and successfully masquerade as one of the peers. This attack can be utilized to change the routes of the peer. It facilitates traffic analysis, black-holing, and eavesdropping.

Cross layer Attack: Many researchers addressed a new class of attack called the cross-layer attack. The attack mainly targets the network layer of the IoT protocol stack. It is eminent due to the lack of communication between MAC, routing, and upper layers. Asati et al proposed a strategy of such attack that was termed as Rank Manipulation and Drop Delay cross-layer attack. The investigators found how an attack with very small intensity on Routing protocol for low power-lossy networks (RPL) degrades the all-inclusive application throughput. The proposed attack reduces the network performance. Connectivity, latency, and throughput of the network are reduced to a significant extent. It is very difficult to detect this attack due to the very small deviation of the protocol parameter.

Zero-day Attack: It is a security issue in the application area of a system. This attack is unfamiliar to a user and is exploited without the user's knowledge and consent [83].

4. CONCLUSION

This paper presents different layers of IoT architecture along with their components and services. The paper also analyzes the IoT architecture to identify various types of attacks on different layers of IoT infrastructure. Cyber-attacks on each layer of IoT infrastructure have been identified and classified for better understanding. This paper also presents a wide exploration of vulnerabilities and causes of various types of cyber-attacks arising in IoT environment. The present paper also explains different ways of attacks followed by attackers in IoT environment. There is wide scope of the present paper to help design security diagnostics and solutions against various threats and attacks on different layers of IoT architecture. Layer-wise classification provides a distributed platform to find problems and it becomes easier to solve them as compared to a single complex problem. Causes and vulnerabilities explained in the present paper will be further helpful to design advanced and secure IoT devices and to develop healthy IoT environment in future.

REFERENCES:

[1] F. Li and P. Xiong, "Practical secure communication for integrating wireless sensor networks into the internet of things," *in IEEE Sensors Journal*, Vol.13, no. 10, pp. 3677–3684, Oct. 2013.

[2] Arne von See, "Internet of Things (IoT) - statistics & facts," Statista, https://www.statista.com/topics/2637/internet-of-things.

[3] I. Sadek, S. U. Rehman, J. Codjo, B. Abdulrazak, "Privacy and Security of IoT Based Healthcare Systems: Concerns, Solutions, and Recommendations," In: Pagán J., Mokhtari M., Aloulou H., Abdulrazak B., Cabrera M. (eds) How AI Impacts Urban Living and Public Health. ICOST 2019. Lecture Notes in Computer Science, Vol. 11862. Springer, Cham, 2019.

[4] Al-ur-Rehman, S. Ur Rehman, I. U. Khan, M. Moiz and S. Hasan, "Security and Privacy Issues in IoT," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 8, pp. 147-157, November 2016.

[5] Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.K.R. Choo, A. Y. Zomaya, "Blockchain for smart communities: Applications, challenges and opportunities," *J. Netw. Comput. Appl.,* Vol. 144, pp. 13–48, 2019.

[6] L. Xu, J. Chen, M. Liu, X. Wang, "Active Eavesdropping Detection Based on Large-Dimensional Random Matrix Theory for Massive MIMO-Enabled IoT," Electronics, Vol. 8, no. 2, 146, pp. 1-16, 2019.

[7] E. Oriwoh, H. M. Al-Khateeb, M. Conrad, "Responsibility and Non-repudiation in resource-constrained Internet of Things scenarios, "Conference: *International Conference on Computing and Technology*

Innovation (CTI 2015), IEEE, at: United Kingdom, 2015.

[8] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A Survey of Internet of Things (IoT) Authentication Schemes," Sensors, Vol. 19, no. 5: 1141, pp. 1-43, March 2019.

[9] M. Abomhara and G. M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks, Journal of Cyber Security and Mobility," Vol.4, issue 1, Article no. 4, pp. 65-88, May 2015.

[10] Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," in *Proceedings of the IEEE*, Vol. 104, no. 9, pp. 1727-1765, Sept. 2016.

[11] I. Butun, "Industrial IoT: Challenges, Design Principles, Applications, and Security," Springer Nature Switzerland AG, Springer, Cham, 2020.

[12] C. Ramakrishna, G. K. Kumar, A. M. Reddy, P. Ravi, "A Survey on various IoT Attacks and its Countermeasures," International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), Vol 5, Issue 4, pp. 143-150, Apr. 2018.

[13] P. Rughoobur, L. Nagowah, "A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare," Conference: 2017 *International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS*). pp. 811-817, 2017.

[14] O. E. Mouaatamid, M. Lahmer, and M. Belkasmi, "Internet of Things Security: Layered classification of attacks and possible Countermeasures," Electronic journal of information technology. E-T1-no. 9, pp. 24-37, Jan. 2016.

[15] M. Burhan, R. A. Rehman, B. Khan and B-S Kim, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey," Sensors (Basel), vol. 18, no. 9: 2796; pp. 1-37, 2018.

[16] S. Rizvi, A. Kurtz, J. Pfeffer and M. Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT," *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 163-168.

[17] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," Hindawi Journal of Electrical and Computer Engineering, vol. 2017, Article ID 9324035, pp. 1-25, Jan 2017.

[18] M. Yu, J. Zhuge, M. Cao, Z. Shi, L. Jiang, "A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices," Future Internet, Vol. 12, no. 27, pp. 1-23, 2020.

[19] M. Young and R. Boutaba, "Overcoming Adversaries in Sensor Networks: A Survey of Theoretical Models and Algorithmic Approaches for Tolerating Malicious Interference," in *IEEE Communications Surveys & Tutorials*, Vol. 13, no. 4, pp. 617-641, Fourth Quarter 2011.

[20] T. Melamed, "An Active Man-In-The-Middle Attack On Bluetooth Smart Devices," Int. J. of Safety and Security Eng., Vol. 8, No. 2, pp. 200–211, 2018.

[21] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," in *IEEE Wireless Communications*, Vol.17, no. 5, pp. 55-62, 2010.

[22] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Transactions on Parallel and Distributed systems*, Vol. 24, no. 1, pp. 44–58, Jan. 2013.

[23] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "Phy-layer spoofing detection with reinforcement learning in wireless networks," IEEE Transactions on Vehicular Technology, Vol. 65, no. 12, pp. 10037–10047, Dec. 2016.

[24] Q. Wang, X. Zhu, Y. Ni, L. Gu, H. Zhu, Blockchain for the IoT and industrial IoT: A review, Internet of Things, Vol. 10, 100081, 2020.

[25] P. Madani, N. Vlajic, and S. Sadeghpour, "MAC-Layer Spoofing Detection and Prevention in IoT Systems: Randomized Moving Target Approach," CPSIOTSEC'20: Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy, Nov. 2020, pp. 71–80.

[26] H. Abdulla, H. Al-Raweshidy, and W. S. Awad, "ARP Spoofing Detection for IoT

Networks using Neural Networks," *Proceedings of the Industrial Revolution & Business Management: 11th Annual PwR Doctoral Symposium (PWRDS) 2020*, pp. 1-9, 2020.

[27] S. Einy, C. Oz, and Y. D. Navaei, "IoT Cloud-Based Framework for Face Spoofing Detection with Deep Multicolor Feature Learning Model," Hindawi Journal of Sensors Vol. 2021, Article ID 5047808, pp. 1-18, Aug. 2021. https://doi.org/10.1155/2021/5047808

[28] A. Alharbi, M. Zohdy, D. Debnath, R. Olawoyin and G. Corser, "Sybil Attacks and Defenses in Internet of Things and Mobile Social Networks," IJCSI International Journal of Computer Science Issues, Vol. 15, Issue 6, pp. 36-41, Nov. 2018.

[29] H. Aldabbas, R. Amin, "A novel mechanism to handle address spoofing attacks in SDN based IoT," Cluster Computing, Vol. 24, pp. 3011-3026, 2021.

[30] K. Zhang, X. Liang, R. Lu and X. Shen, "Sybil Attacks and Their Defenses in the Internet of Things," in *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372-383, Oct. 2014.

[31] H. Yu, M. Kaminsky, P. Gibbons, and A. D. Flaxman, "SybilGuard: Defending against Sybil attacks via social networks," *IEEE ACM Trans. Netw.*, Vol. 16, no. 3, pp. 576–589, Jun. 2008.

[32] M. Al-Qurishi, M. Al-Rakhami, A. Alamri, M. Alrubaian, S. M. M. Rahman and M. S. Hossain, "Sybil Defense Techniques in Online Social Networks: A Survey," in *IEEE Access*, Vol. 5, pp. 1200-1219, 2017.

[33] D. Evangelista, F. Mezghani, M. Nogueira and A. Santos, "Evaluation of Sybil attack detection approaches in the Internet of Things content dissemination," *2016 Wireless Days (WD)*, 2016, pp. 1-6.

[34] S. Vaishnavi and T. Sethukarasi, "SybilWatch: a novel approach to detect Sybil attack in IoT based smart health care," *J Ambient Intell Human Comput.,* Vol. 12, pp. 6199–6213, 2021.

[35] M. Mushtaq and M. K. Bhatti, "SCADD: Side Channel Attacks, Detection Defenses," Special Track along with the 5th International Conference on Cyber-Technologies and Cyber-Systems (CYBER) 2020, Nice-France.

[36] E. Sasikala E. and Dr. N. Rengarajan, Analysis of swarm intelligent based defense algorithm for detecting jamming attack in wireless sensor networks (WSNs)" The Free Library, Advances in Natural and Applied Sciences, Feb. 2016.

[37] B. Butani, P. K. Shukla, and S. Silakari, "An Exhaustive Survey on Physical Node Capture Attack in WSN," International Journal of Computer Applications, Vol. 95, No. 3, pp. 32-39, June 2014.

[38] S. Agrawal, M. L. Das and J. Lopez, "Detection of Node Capture Attack in Wireless Sensor Networks," in *IEEE Systems Journal*, Vol. 13, no. 1, pp. 238-247, March 2019.

[39] C. Wang, T. Feng, J. Kim, G. Wang, W. Zhang, "Catching packet droppers and modifiers in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 23, no. 5, pp. 1–9, 2009.

[40] B. Li, R. Ye, G. Gu, R. Liang, W. Liu, K. Cai, "A detection mechanism on malicious nodes in IoT," Computer Communications, Vol. 151, pp. 51-59, 2020.

[41] M. B. E. Sajid, S. Ullah, N. Javaid, I. Ullah, A. M. Qamar, F. Zaman, "Exploiting Machine Learning to Detect Malicious Nodes in Intelligent Sensor-Based Systems Using Blockchain", *Wireless Communications and Mobile Computing*, Vol.2022, Article ID 7386049, pp. 1-16, 2022.

[42] S. Nobahary, H. G. Garakani, A. Khademzadeh, A. M. Rahmani, "Selfish node detection based on hierarchical game theory in IoT," EURASIP Journal on Wireless Communications and Networking, Vol. 219:255, pp. 1-19, 2019.

[43] G. R. Mode, P. Calyam, K. A. Hoque, "False data injection attacks in Internet of Things and deep learning enabled predictive analytics," in the IEEE NOMS 2020 conference, 2020.

[44] F. Miao, M. Pajic and G. J. Pappas, "Stochastic game approach for replay attack detection", *52nd IEEE Conference on Decision and Control*, 2013, pp. 1854-1859.

[45] A. A. Elsaeidy, N. Jagannath, A. G. Sanchis, A. Jamalipour and K. S. Munasinghe, "Replay Attack Detection in Smart Cities Using Deep Learning," in *IEEE Access*, Vol. 8, pp. 137825-137837, 2020

[46] S. Takarabt, A. Schaub, A. Facon, S. Guilley, L. Sauvage, Y. Souissi, Y. Mathieu, "Cache-Timing Attacks Still Threaten IoT Devices," In book: Codes, Cryptology and Information Security, pp.13-30. Mar. 2019.

[47] D. Brumley and D. Boneh, "Remote timing attacks are practical," USENIX Security Symposium, August 2003.

[48] Dr. S. Rethinavalli and Dr. R. Gopinath, "Botnet Attack Detection in Internet of Things Using Optimization Techniques," International Journal of Electrical Engineering and Technology (IJEET), Vol. 11, no. 10, pp. 412-420, Dec. 2020.

[49] K. Angrishi, "Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT Botnets," Cryptography and Security, arXiv 2017, pp. 1–17, 2017.

[50] Interlink Networks, "Link Layer and Network Layer Security for Wireless Networks," White paper, Interlink Networks LLC, pp. 1-8, 2006.

[51] C. Walls, "Point-to-Point Protocol," Embedded Software (Second Ed.), ScienceDirect 2012.

[52] A. Kore, S. Patil, "IC-MADS: IoT Enabled Cross Layer Man-in-Middle Attack Detection System for Smart Healthcare Application," Wireless Personal Communication, Vol. 113, pp. 727–746, 2020.

[53] J. J. Kang, K. Fahd, S. Venkatraman, R. Trujillo-Rasua and P. Haskell-Dowland, "Hybrid Routing for Man-in-the-Middle (MITM) Attack Detection in IoT Networks," *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, 2019, pp. 1-6

[54] Justice O. Agyemang, J. J. Jerry Kponyo, I. Acquah, "Lightweight Man-In-The-Middle (MITM) Detection and Defense Algorithm for WiFi-Enabled Internet of Things (IoT) Gateways," Enhancing Security in Internet of Things Devices, pp. 1-6, Jan. 2019.

[55] J. Choi, B. Ahn, G. Bere, S. Ahmad, H. A. Mantooth and T. Kim, "Blockchain-Based Man-in-the-Middle (MITM) Attack Detection for Photovoltaic Systems," *2021 IEEE Design Methodologies Conference (DMC)*, 2021, pp. 1-6.

[56] L. Rajesh and P. Satyanarayana, "Detecting Flooding Attacks in Communication Protocol of Industrial Control Systems," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 1, pp. 396-401, 2020.

[57] T. Shah, S. Venkatesan, "Authentication of IoT Device and IoT Server Using Secure Vaults", 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference On Big Data Science and Engineering, 2018, pp 819-824.

[58] X. Zhu, S. K. Mukhopadhyay, and H. Kurata, "A review of RFID technology and its managerial applications in different industries," Journal of Engineering and Technology Management, vol. 29, no. 1, pp. 152–167, 2012.

[59] Prof. Jing Tao Han, Prof. Zheng Yi Jiang and Prof. Xiang Hua Liu, "Node Capture Attack Detection in Dynamic WSNs Based on New Node Tracking," Advanced Materials Research, Vol. (945-949), pp. 2372-2379, 2014.

[60] U. Palani, G. Amuthavalli, V. Alamelumangai, "Secure and load-balanced routing protocol inwireless sensor network or disastermanagement," IET Information Security, Vol. 14, Issue 5, pp. 513-520, 2020.

[61] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense," international Journal of Distributed Sensor Networks, pp. 1-8, July 2006.

[62] C. Padmini, B. A. Kumar, V. P. Kumar, "Leakage Power Attack Resiliency in Novel-7T SRAM," International Research Journal of Engineering and Technology (IRJET), Vol. 07, Issue 05, pp. 5914-5919, May 2020.

[63] J. Jeon, J. H. Park, and Y-S Jeong, "Dynamic Analysis for IoT Malware Detection With Convolution Neural Network Model," Special Section On Emerging Approaches To Cyber Security, Vol. 8, pp. 96899-96911, 2020.

[64] A. Sanzgiri, D. Dasgupta, "Classification of insider threat detection techniques," *CISRC '16: Proceedings of the 11th Annual Cyber and Information Security Research Conference, Oak Ridge, TN, USA.* 5-7 Apr. 2016; ACM 2016, p. 25.

[65] J. R. Nurse, A. Erola, I. Agrafiotis, M. Goldsmith, S. Creese, "Smart insiders: Exploring the threat from insiders using the

Internet-of-things," Proceedings of the 2015 International Workshop on Secure Internet of Things (SIoT), Vienna, Austria. 21–25 September 2015, pp. 5–14.

[66] S. Iqbal, M. L. M. Kiah, B. Dhaghighi, M. Hussain, S. Khan, M. Khan, K-K. R. Choo, "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," Journal of Network and Computer Applications, Vol. 74, pp. 98-120, Oct. 2016.

[67] M. Bamiah, S. Brohi, S. Chuprat, and M. N. Brohi, "Cloud implementation security challenges," in Proc. *2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)*, 2012, pp. 174-178.

[68] M-D. Nguyen, N-T. Chau, S. Jung, and S. Jung, "A Demonstration of Malicious Insider Attacks inside Cloud IaaS Vendor," International Journal of Information and Education Technology, Vol.4, No. 6, pp. 483-486, Dec. 2014.

[69] S. Hijazi and M. S. Obaidat, "Address resolution protocol spoofing attacks and security approaches: A survey," Security and privacy, Vol. 2, Issue 1/e49, Dec. 2018.

[70] R. K. Singh, A. Bhattacharjya, "Security and Privacy Concerns in Cloud Computing," International Journal of Engineering and Innovative Technology (IJEIT), Vol. 1, Issue 6, pp. 20-27, June 2012.

[71] Z. P. Cekerevac, Z. Dvorak, L. Prigoda, and P. Cekerevac, "Internet of Things And The Man-InThe-Middle Attacks – Security And Economic Risks," MEST Journal, Vol. 5, no. 2, 2017, pp. 15-25.

[72] G. K. Shyam and M. A. S. Ansari, "Security concerns in cloud computing. International Journal of Trend in Scientific Research and Development (IJTSRD), Vol. 2, Issue 5, pp. 2296-2301, 2018.

[73] R. Canzanese, M. Kam, S. Mancoridis, "Toward an automatic, online behavioral malware classification system," Proc. *IEEE 7th International Conference on Self-Adaptive and Self-Organizing Systems (SASO*), *Philadelphia, PA, USA.* Sept. 2013, pp. 111–120.

[74] I. Leguías, M. Vega and M. Vargas-Lombardo, "Emerging Threats, Risk and Attacks in Distributed Systems: Cloud Computing," Innovations and Advances in Computer, Information, Systems Sciences, and Engineering, Lecture Notes in Electrical Engineering, Vol. 152, pp. 37-51, 2013.

[75] C. Bormann, A. P. Castellani and Z. Shelby, "CoAP: An Application Protocol for Billions of Tiny Internet Nodes," in *IEEE Internet Computing*, Vol. 16, no. 2, pp. 62-67, March-April 2012.

[76] C. Konstantinou and M. Maniatakos, "Impact of firmware modification attacks on power systems field devices," *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2015, pp. 283-288.

[77] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, W-C. Hong, "Internet of Things: Evolution, Concerns and Security Challenges," Sensors 2021, Vol. 21, no. 5, 1809, pp. 1-33, Mar. 2021.

[78] H. Sajjad and M. J. Arshad, "Evaluating Security Threats for each Layers of IoT System," Computer Networks, Vol. 10, pp. 20-28, Oct. 2019.

[79] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," IEEE Transactions on Parallel and Distributed systems, Vol.24, no. 1, pp. 44–58, 2013.

[80] S. Madakam, R. Ramaswamy, S. Tripathi, "Internet of Things (IoT): A Literature Review", Journal of Computer and Communications, Vol. 2015, no. 3, pp. 164-173, May 2015.

[81] B. Ahlawat, A. Sangwan, V. Sindhu, "IOT System Model,Challenges and Threats," International Journal Of Scientific & Technology Research, Vol. 9, Issue 03, pp. 6771-6776, Mar. 2020.

[82] S. Kumar K, S. Sahoo, A. Mahapatra, "Security Enhancements to System on Chip Devices for IoT Perception Layer", *IEEE International Symposium on Nanoelectronic and Information Systems,* 2017, pp 151-156.

[83] L. Bilge, T. Dumitras, "Before we knew it: An empirical study of zero-day attacks in the real world," In Proceedings of the *2012 ACM Conference on Computer and Communications Security, Raleigh, NC, USA*, 16–18 October 2012; ACM: New York, NY, USA, 2012; pp. 833–844.