Review Article

International Journal of Advanced Computer Research, Vol 9(45)
ISSN (Print): 2249-7277   ISSN (Online): 2277-7970
http://dx.doi.org/10.19101/IJACR.2019.940088

A survey of IoT security threats and defenses

Hassan I. Ahmed[1*], Abdurrahman A. Nasr[2], Salah Abdel-Mageid[3], and Heba K. Aslan[4]
Assistant Researcher, Department of Informatics, Electronics Research Institute, Cairo, Egypt[1]
Lecturer, Department of System and Computer Engineering, Al-Azhar University, Cairo, Egypt[2]
Professor, Department of Computer Engineering, Taibah Univeriisty, Saudi Arabia[3]
Professor, Department of Informatics, Electronics Research Institute, Cairo, Egypt[4]

Received: 13-July-2019; Revised: 11-October-2019; Accepted: 14-October-2019

Abstract

Internet of Things (IoT) plays a well-known role in the interconnection of the physical and virtual objects for the purpose of exchanging information. IoT environment can connect billions of devices or objects, each one has an ID for identification proof. The IoT system is considered one of the most important technologies in recent decades, and the focus of attention in many fields including healthcare, industry, agriculture, military applications, and space science. Thus, it is more attractive for cyber-attacks. The IoT requires multi-dimensional security solutions such as confidentiality, integrity, and authentication services. In this paper, we address different security challenges, threats, and defenses in the layers of IoT systems. It is known that the IoT system architecture consists of three layers: physical/sensor layer, network layer, and application layer. To be comprehensive and to facilitate comparative methods, the security problems of each layer separately and the suggested solutions have been analyzed. Moreover, the challenges of the IoT especially big data and also the evaluation strategies of the IoT system and their effects on the security operations have been evaluated.

Keywords

Internet of things (IoT), Radio frequency identification (RFID), Big data analytics, Distributed denial of services (DDoS).

1.Introduction

The IoT points to an ever-increasing network containing the things which are not only conventional computers or mobile objects, but also the physical things similar to temperature sensors, wearable devices, watches, and other smart objects. Academics, industries, and governments are interested in studying how to connect all things in the world to the internet, called Internet of Things. Its applications contain large numbers of devices (perceptions), which are difficult to implement security methods such as encryption because of the restrictions on time, memory, processing, and energy constraints [1]. Recently, the smart devices have increased with the increased availability of distributed networks. From *Figure 1*. We should know that the number of devices connected to it is increasing through a positive relationship with the time. Also, the market of IoT is increasing with time [2].

IoT is attracting for many organizations, one of them is Cisco internet business solutions group (IBSG), which reported that IoT is advantageous when the number of "objects/things" connected to the Internet is greater than the human's connection [3]. IoT enables several applications and objects for connecting with each other through the internet to a certain scale, facilitating communication and access to information, including business as-well-as technologies related challenges to realize business benefits. These applications and objects impose a strict challenge to the security of the IoT environment and systems. For example, privacy, confidentiality, integrity, authentication, and authorization of IoT system. Moreover, the IoT environment should provide solutions for other challenges such as reliability, performance, availability, mobility, management, interoperability, scalability, and big data. IoT security is a major area of concern, it is the most impacted challenges for IoT [4].

IoT architecture is divided into three layers: physical (aka perception/sensing) layer, network layer, and

*Author for correspondence

application layer. The security requirement of IoT must be provided for all layers, additionally, IoT security should also include the security of the overall system across the three layers which are known as cross-layer security. One of the most compelling security issues in IoT cross-layer security is intrusions detection and prevention. Intrusion is any malignant activities that could compromise the integrity, confidentiality, or availability of IoT resources. One of the worthy research challenges in IoT networks is securing them from malicious entities that perform vulnerable activities (threats or attacks). There are many attacks that threaten IoT resources, of which denial of service (DoS) is gaining more popularity with its variant distributed denial of service (DDoS). DDoS is an attack which attempts by a malicious node to disrupt resources or bandwidth of legitimate users when penetrated from a various compromised node. The DoS attack which includes flooding of a huge amount of traffic to occupy network resource, bandwidth, target CPU time. The most common DoS attacks are ICMP broadcast, SYN flood, Ping flood, DNS flood, UDP flood, etc. [5]. DDoS attacks can be involved in any layer of IoT three layers such as jamming attacks which is in sensor/physical layer, Flooding Attacks in the network layer and reprogramming and path-based DDoS Attacks are in the application layer. The security and privacy of IoT have many problems which need to pay more attention to the research issues of confidentiality, authenticity, and integrity of data in the IoT for the following reasons [6]: 1) IoT is covered many technologies such as traditional internet, mobile network, sensor network, computer network, and cloud and so on. 2) Every ‘thing’ will be connected to this ‘internet’, and these ‘things’ will communicate with each other.

The objective of this paper is highlighting the security problems with IoT and representing some directions to overcome the problems which face the researchers in this field. The outcome of the overgrowing of IoT is a motivation to save a platform to collect, store and analyze the big data generated from IoT devices. The data generated by IoT devices can be doubled through time that points to the “volume” of data, also the data generated has different formats which means the “variety” of data and the rate of data generation has a high score which donates the “velocity” characterizes of data. Volume, variety and velocity characteristics of data mean “Big Data” terminology [7].

This paper covers the big data challenges of IoT environment and the methods used to tackle these challenges. The rest of the paper is prepared such as follows: in section 2, we describe the literature review of IoT systems and security challenges moreover the security requirements for each layer. Then, the taxonomy of IoT security attacks per layer is discussed in section 3. Section 4, contains the taxonomy of security techniques used to address the IoT attacks in each layer. In section 5 the usage of IDS for addressing attacks on the IoT environment is discussed. Section 6, contains other security challenges of IoT like big data. Section 7, contains an evaluation of IoT with respect to the security. Section 8, contains a suggested solution for the increasing number of attacks on IoT environment along with the conclusion.

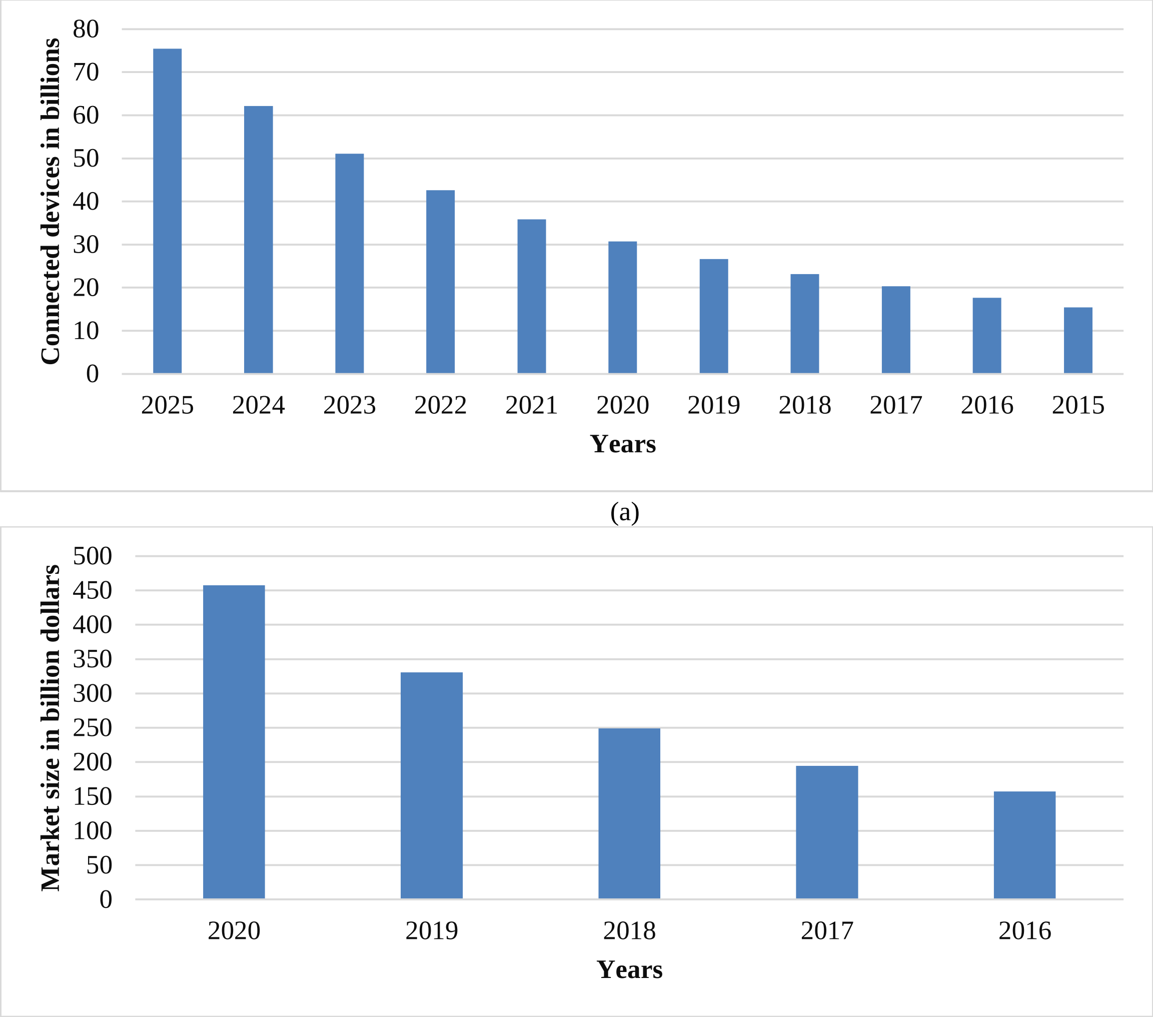
2.Literature review

The growth of IoT gives a lot of opportunities; combining mobile networks, the internet, social networks, and intelligent things to provide beneficial services or applications to users. Nevertheless, it is still not fully developed or protected. The significant challenge of IoT is guaranteeing data privacy and protection [8]. Radio frequency identification (RFID) technology, sensor technology, embedded system technology, and nanotechnology are the essential technologies of IoT. It is challenging to achieve a reliable connection between the individual nodes in IoT due to the node heterogeneity. RFID technology is used for automatic identification based on radio frequency electromagnetic fields. It identifies objects taking tags when communicating with the closest to a reader.

RFID was originally used throughout World War II due to recognizing airplanes identify friendly foe (IFF). RFID is now extensively used in almost all industrial areas (automotive, aerospace, logistics, health, transport, life, etc.). Data (the identification number for instance) carried in the electronic chip of the RFID tag which, can be handled by the reader [9]. The constrained resource such as RFIDs, sensor nodes, cell phones, etc. are elements used in IoT. The methods used for securing these things are managed by characteristics like the low energy consumption, tiny form factor, good performance, and robustness to attacks. Privacy, security, and trust will have to be adapted to prove these constraints; it makes the security process more challenge. Also, the IoT has a number of properties which create several concerns for security and raises further specifications for security. These properties are listed as follows [10]:

1. Mobility: The mobile manner of IoT devices which joined to the internet via a large set of providers.
2. Wireless: The connection of these devices to the internet via a broad range of wireless connections, Bluetooth, 802.11, Zigbee, WiMAX, and GSM/UMTS.
3. Device Use: The discovery of communication models is different to a specialized device because significant IoT devices have a particular use (e.g., blood pressure or heart monitors and household appliances).
4. Diversity: Computational abilities of these devices are varied from full-fledged PCs to low-end RFID tags.

IoT security categories are confidentiality, integrity, and authentication [11]. Confidentiality is the method that keeps information secret from the third parties. Integrity is the ability of the recipient in IoT verify that the received messages have not been modified during transmission or delivery. The importance of this security method because intruders cannot obtain the data. Authentication is the method of determining whether a message is, in fact, from where it claims it is, or what it is claimed to be. As mentioned above that IoT is constructed from three layers: physical/sensing layer, network layer, and application layer such as displayed in *Figure 2*.



(a)

(b)

Figure 1 (a) Number of connected devices worldwide in 2015-2025 with IoT (b) IoT market size in billion dollars [2]

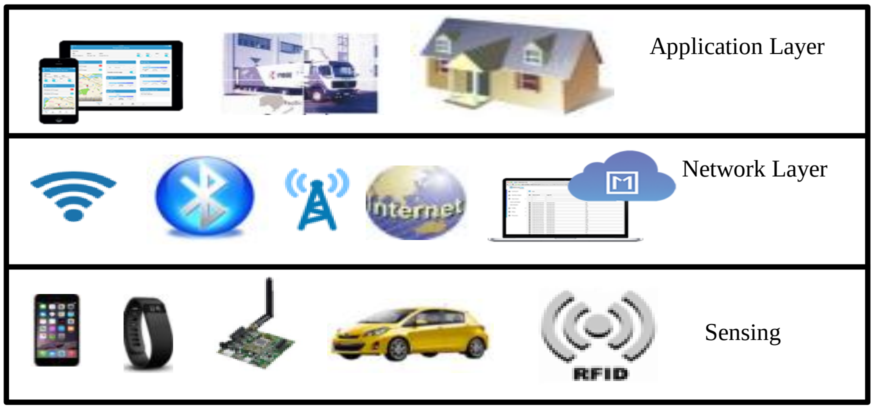


Figure 2 IoT Architecture

The Sensing layer is subjected to aggregating and sensing the information of IoT objects. The aggregation of information is done on this layer with the help of various devices such as sensor nodes, smart cards, and RFID tags. There are two main components or subpart of this layer: sensing node and sensing network. Sensing node such as controllers or sensors is used to make data acquisition and data control. While sensing network is used to send control signals to the controller or send the collected data to the gateway to be transmitted in the network layer [12].

The Network layer manages the wireless and wired networks. It transfers the gathered data through the sensors, and computers across the wired and wireless networks. It can also support connection-oriented service by maintaining the reliability of data delivery. Routing takes place at this layer where data is transmitted across different IoT devices over the internet. Routing, switching, gateway devices operate at this layer using a variety of technologies such as Zigbee, WiFi, 3G, Bluetooth, and LTE. The gateway acts as a medium between separate IoT devices by aggregating, filtering and moving data between different sensors [13].

Application layer provides an interface among the applications and the end users and the communication between them. It specifies the resource allocation and computation in producing, processing, screening and feature selection of data. It may have methods to recognize spam data, malicious data, and valid data through its filtering feature. It is known as “process layer”. It resolves the received information and makes control decisions to allow the achievement of intelligent processing by identification, connection, and control between devices and objects [14].

The security requirements in each layer are different due to its features. In overall, the IoT security considers the following requirements: sensing layer requirements, network layer requirements and application layer requirements and other requirements between layers and services operation like shown in *Figure 3*.

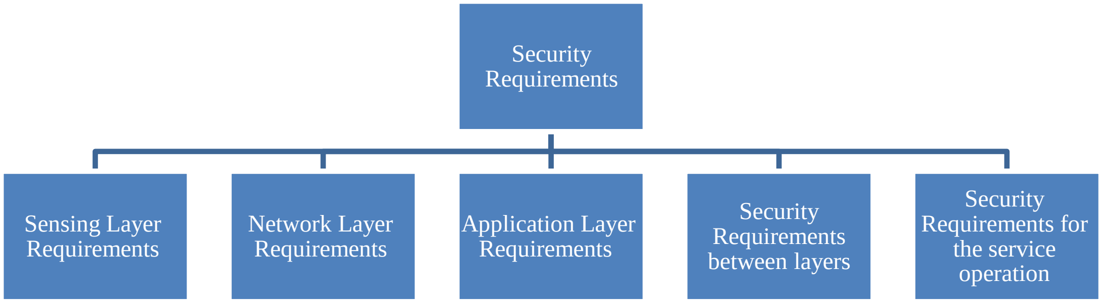

Security Requirements
Sensing Layer Requirements
Network Layer Requirements
Application Layer Requirements
Security Requirements between layers
Security Requirements for the service operation

Figure 3 IoT security requirements

a) Sensing layer security requirements: The authentication, confidentiality and data encryption are essential to prevent illegal node access [15].

There are more challenges in sensing layer are:

1. The things are constrained in the Cost, size and energy consumption.
2. The heterogeneity: A variation of things or various networks make the IoT so heterogeneous.
3. The communication: The IoT edges should be able to interact with each other.
4. The networks: The IoT includes hybrid networks, like WSNs, WMNs, and SCADA systems.

In this layer, the security requirements should be minimized because IoT devices have a limited energy to execute the heavy security instructions. However, most IoT devices are designed to be lightweight and small size. There is no more capacity for a massive battery. So, Conventional cryptography is difficult to run on IoT devices. There are methods of harvesting energy from physical resources (e.g., light, heat, vibration, and wind), but they require an upgrade to the hardware and significantly increase the monetary cost [16].

To overcame computing overload problem some research is done such as follows [17]:

1. Signal processing at the recipient side to prove sensing layer authentication. It specifies whether the transmission came from the expected transmitter in the expected location.
2. Encode information through using analog characteristics of a transmitter, which can serve as a unique key. This way of authentication has an advantage of radio signals, so little or no energy overhead because is needed.
3. A method provides a securely storing of encrypted IoT data on the cloud with utilizing lightweight cryptographic Elliptic Curve ElGamal and mutable order-preserving encoding algorithms [18]. Data encryption/decryption is done to the client-side.

b) Network-layer security requirements: The network layer implements a connection for all things in IoT which allows them to combine information from the surrounding environment. Also, it has a capability for aggregating data, then forwards to other layers, such as the sensing layer and application layer.

The security requirements in the network include confidentiality, integrity, privacy protection, authentication, key protection, availability, etc. The low-energy links in IoT networks often have very small maximum transmission units (MTUs). In contrast with today’s IP networks, which typically allow a minimum MTU of 1500 bytes or higher. The Internet throughout the 1990s (long before the perception of IoT), the IPv6 specification involves two design decisions that are problematic for small MTU links. First, IPv6 uses a 40-byte fixed length header with optional extension headers, which cause a big protocol overhead for small packets. Second, the IPv6 specification requires that all IPv6-capable networks sustain a minimum MTU size of 1280 bytes, which is unrealistic for the constrained links [19].

6LoWPAN is used to 802.15.4 networks to tackle the header compression and link layer fragmentation. Header compression allows removing unused fields (e.g., flow label and traffic class) and redundant information (e.g., the interface identifier in the IPv6 address. It also defines the compression scheme for extension headers and UDP header, which used frequently used in IoT. Link-layer fragmentation masks the actual MTU size of 802.15.4 and gives the network-layer the confusion that it is working over a standard acquiescent link capable of supporting 1280-byte MTU. However, few IoT applications are exacted to send packets that reach the MTU limit [20].

c) Application layer security requirements: The requirements in application interface layer strongly depend on the applications. Remote safe configuration, software downloading and updating, security patches, administrator authentication, unified security platform, etc. are requirements needed in application layer [21]. The known applications of IoT are smart home, medical and healthcare, smart city, military, energy management, environmental monitoring, industry, and connected vehicle. There are security risks in IoT devices as, some are even running complex software which resembling general-purpose computers. The requirements in application layer strongly depend on the applications. IoT applications show that low cost devices may be connected and accessible over the Internet. The environment of IoT is attractive for a new malware which can be used to create powerful botnets [22].

3.Discussion and analysis

IoT is known that the ability of computers to knew everything about “things” and using data that they collected without any guidance from a human then interconnected with each other through the internet.

The term, IoT was, presented by Kevin Ashton in 1998. IoT is a dynamic infrastructure network with self-configuring abilities based on standards and interoperability intercommunication protocols; physical and virtual ‘things’ in the IoT have uniqueness and attributes which are able of using sensible interfaces and being integrated as an information [23].

Billion number of sensor and devices will gain a connection with the internet via the year 2020 [24]. Many digital disruptions, or chaos might occur as a result of rising number of devices linked via the IoT. IoT is oversensitive to various security attacks by hackers or organized criminals where high volume of data is now being put online [25]. IoT data may be more sensitive data or may involve safety-critical operations (e.g., car and medical devices). Hence, security viewpoint is a part of the major concern in the development of IoT. There are several types of attacks in IoT such as Spoofing/Altering/Replay Routing attack, DoS attack, Sybil attack, and node capture attack on IoT. The layer-based attack and the attempt by an adversary to attack through a communication protocol stack is shown in *Table 1*.

Table 1 Layered taxonomy of IoT attacks

Layer	Attack	Description
Application	Virus, Worms, Trojan Horse, Spyware (Malicious Code Injection)	Software designed to infiltrate or damage IoT system without the owner’s informed consent
	Denial of Service	attempts to exhaust victim’s bandwidth or disrupt legitimate users’ access to services.
	Software Vulnerabilities	Nonstandard code used by hackers to cause vulnerabilities ion IoT network
	Privacy leak	IoT user data such as password, historical data, and social relations may be hacked through known vulnerabilities.
	Buffer overflow	common mistake made by software developers that can be used by attackers to gain access to a computer system.
	Cross-site scripting (XSS)	vulnerabilities in application which gives opportunity to use JavaScript for security compromises.
Network Layer	Traffic analysis attack	Uses Packet sniffers or port scanning application and then attacks on the targeted information
	spoofing	Spoofed routing loops or sources routes.
	Sinkhole Attack	Malicious path is announced through the IoT network
	HELLO flood	HELLO message used to deceive IoT nodes
	Blackhole attack	Dropping packets
	MITM attack	Intercept a communication between two nodes
Sensing Layer	Sybil attack	A malicious object uses different identities and ruined the routing protocol
	RF Interference	Noise signals over radio frequencies
	Jamming attack	Disturbs the wireless communication
	Tampering attack	Attacker has full control for node and extract the node’s information
	Object replication	Negatively effects on network performance
	Camouflage	Misroute packets.
	Tag cloning	capturing a tag’s identifying information
	Hardware Trojans	Exploits functionality of IoT object

Layer	Attack	Description
	Physical attacks	Direct harm of IoT objects

3.1Application layer attacks

Table 1 contains the classification of attacks based on IoT layers, in application layer virus, worms, trojan, spyware are a software which threatens the IoT security system: virus makes damage in IoT resources worms spread over the network using different system vulnerabilities, trojans masquerade as a legitimate applications and perform different malicious actions on victim's computer, spyware, that assemble different secret information about the victims machine like passwords, email accounts, credit card numbers, and contacts [26]. A series of methodologies were proposed to overcome this type of application layer attacks, IBM research group proposed n-grams method and this method was improved by using multiple machine learning algorithms [27]. Machine learning and data mining technique for malware detection is proposed. This model consists of the disassembly operation, the feature extraction operation, and feature selection operation. Three classification methods are applied on the dataset to produce and train the classifiers named as Ripper, C4.5, IBk [28].

DoS and DDoS attacks are intended to prevent the legal users from reaching a specific IoT resource or degrade normal services for legitimate users. It is Occurred by sending huge unwanted traffic to the sacrifice (machines or networks) to cause services exhaustion. Also, increase flow and connection capacity or the bandwidth [29, 30]. DoS/DDoS attacks cause that attackers can obtain complete access on the application layer and can be infertile, databases and private sensitive data. IoT network can be exaggerated by the execution of DoS or DDoS attacks by the attackers that influence the users on the network [31]. Bandwidth exhausting is a kind of DoS attack, a countermeasure of that attack is proposed by Bugenhagen and Wiley [32] which is based on counting data packets. By circumscribing the bandwidths, communications of data packets through the pinhole firewall may be altered to accommodate a high volume of data packet communications via the firewall.

A software vulnerability can be seen as a flaw, defect or even an error in the system that can be utilized by an attacker in order to modify the common behaviour of the system. Because the number of software systems is increasing every day also the number of vulnerabilities is increasing. Software vulnerabilities, attacks cause IoT application loophole occur due to the non-standard code as it was written by programmers, as a result of buffer runoff. This technique or method is utilized by hackers to perform their aims. The solution for this type of attacks is achieved based on security expert's software. This process is depending on software metrics taken from source code and development history are discriminating and predictive of vulnerable code locations [33]. IoT software vulnerabilities may be seen in operating systems, application software, and control software like communication protocols and devices drives. Professional vulnerabilities regularly happen due to human weaknesses. Software vulnerabilities, attacks occurred as a result of unknowing the specifications or starting the design without a plan, weak communication between developers and users, a shortage of resources, experiences, and failing to manage and control the system [34].

In privacy leak attack the hackers have the ability to obtain the IoT device sensitive data from more sources or acquire illegal benefits by modifying this data. The trade-off among sensitive information utility and privacy is a great challenge for the academic community. Many studies are done recently with regard to the privacy protection of IoT data and anonymous protocols. The data encryption and masking similar to the homomorphic algorithm are tools that used by many solutions to protect sensitive information. However, these solutions may affect negatively on the availability of original data and increase the time delay. The original data must be retained with high availability with used privacy protection method which protects users' privacy and guarantees real-time at the same time this is a challenge. Another challenge is the current privacy protection method is a narrow application scope and in comprehensive protection [35, 36].

A buffer means a consecutive segment of memory that may hold various data types from a string of characters to array of integers. In a buffer overflow, additional data are earmarked to a fixed-length buffer than the buffer can include. The extra data overflow in a neighboring memory space, overwriting or damaging the data that previously exists beyond. A system crackup is a common result; however, a buffer overflows more presents possibilities for attackers to execute arbitrary code either to apply these coding errors to begin malicious actions [37]. *Table 2*, illustrates that buffer overflow faces weighted risk to IoT devices because of their limited memory, the languages they're programmed in, and the commonality of the programs [38].

Cross-site scripting is the vulnerabilities in website's usage of vibrant web design components may give someone the opportunity to use JavaScript for security compromising. It's called "cross-site" because it includes cooperation among a pair of separate websites to accomplish its goals. Usually, the achievement includes the usage of JavaScript, the website that's unsafe to cross-site scripting exploits does not own to use JavaScript itself at all. Particularly in the event of local cross-site scripting exploits makes the vulnerability have to exist in JavaScript transmitted to the browser through an authorized website. The Cookies are frequently used to give some sort of security against cross-site scripting [39].

Table 2 Risks of buffer overflow in IoT environment

Memory	The devices in the IoT environment regularly need to save the power, which drives to shortest amounts of energy efficient memory. The limited the buffer, the simpler it is to overflow, which causes the IoT the ideal platform for these types of attacks.
Language	Many IoT programs are coded in C or C++. Neither C nor C++ has a "waste collector" which raises the chance of buffer overflow. Furthermore, these languages employ pointers, which can be utilized via hackers to discover the location of significant code in memory.
Commonality	Ready-made, inexpensive, programs for IoT devices and when use the same code as everyone else. There is probability of execution the risk of having common vulnerabilities. Device can be infected along with thousands of others because of common code.

3.2Network layer attacks

Network layer makes IoT nodes collaborations within local and short-range networks. It can handle routing data and transmission to various IoT hubs and devices over the internet. Switches, routers, clouds, and gateways use wireless protocols in this layer [40]. In the architecture of IoT, the major task of the network layer (second layer) is to transfer the information across the network. Since IoT is realized in the basic communication framework, it is predisposed to different attacks like traffic analysis attack. In this attack type, the attacker continuously tries to conclude the traffic pattern based on the eavesdropped data. It intercepts and examines messages to gain network information. It analyses the packet traffic i.e. transmission of the packets from the node to another node and then starts with the active attacks on that situation [41].

Spoofing attacks are a type of attacks in the network layer in which attack can produce routing loops. Also, can extend or shorten the source routes through attracting either repelling network from choosing nodes. Also, there is another manner of spoofing attacks which is RFID spoofing in which the attacker targets the RFID signal to gain access the information imprinted on the RFID tag. Once the signal spoofed hacker uses it to transmit his own data using the original id. Now hacker obtained the full access to a system [42]. Sinkhole attack is another type of network layer attack in which a malicious node may announce the IoT nodes about a beneficial route or spurious path to attract so many nodes to redirect their packets through it. Regardless of not disrupting the network, it could be dangerous if it is joined with another attack [43]. Encryption and Authentication are some techniques used to secure the network against sinkhole attacks so, the attacker is not capable to connect the network. Also, the message digest algorithm which depends on security metrics is added to the packets of route request, after analyzing the received data the attacker can be dropped from the network [44]. Another method based on the detection metric method such as number of packets received and transmitted to validate the Intrusion Ratio (IR) by the IDS agent is used. This method identified whether the router node is a malicious node or not using the IR value [45].

IoT network layer may be infected by the Hello flooding attack in which the objects recently joining the network send broadcast packet known as a hello message. By this attack, an attacker can represent himself as a neighbor object to several objects. It does broadcast a hello message with a high-powered antenna to deceive other objects to send their packet through it. Hello flooding attack is so dangerous to the IoT system as it consumes up the resources such as the battery power of the nodes. Various protocols which based on HELLO packets assume that receiving this a packet is within radio range and is, therefore, a neighbor. The attacker may utilize a huge powered transmitter to deceive a wide area of nodes inside believing they are neighbors of that transmitting node. If the attacker wrongly broadcasts a preferred route to the base station, all of these nodes will try transmission to the attacking node, although various being out of radio range in reality [46]. The cryptographic is considered a solution for detection of HELLO flood attack, but it is less suitable in IoT environments with respect to storage space and battery power. It may be suitable for static networks, which have storage overheads, scalability concerns. The non-cryptographic method which suggests sending the packet for processing and detection of attacks is proper but, may produce communication overhead. The detection agent may be far from the network so, the packet should be sent for transmission for the processing operation. The energy needed for sending of the packet is larger than the energy needed for processing and calculation [47].

Black holes, attack means that some locations in the network wherever incoming or outgoing traffic is silently dropped, without notifying the source that the data did not reach the expected receiver. It is an attacking node that wrongly replies for any route to a particularized destination and drops all the gathered packets. If these malicious nodes work cooperatively as a group then the harm will be very serious. Malicious nodes spread about wrong routing information to the network and direct all data packets toward themselves, then crush all. [48]. *Figure 4* displays the operation of the black hole attack in the network, in which node M is the malicious node (Black Hole node). Node S is a source node launches route discovery by broadcast Route REQuest (RREQ) packet to all nearest neighbors. If the RREQ packet is reached to node M, it responds by faked Route REPly (RREP) packet through injecting a large sequence number in the attention of having a true or new route. The communication protocol is based on the sequence number to validate the freshness of the route. Then the source gets cheated by the faked RREP packet, and neglects all other responses of other nodes. The node S transmits data packets in such route. The M node, alternatively of forwarding data to the target it has clearly dropped it. In this way black hole attack decreases the packet delivery percentage of the network significantly [49, 50].

Man-in-the-middle (MITM) attacks were found in the past before the appearance of computers. A case of MITM attacks is the malicious postman which opens people's messages and reads or modifies their contents before delivering to its receiver. The MITM makes interception through the communication between a pair of nodes. Once the attacker interrupts the connection of his victims, he can take control the role of a proxy. In IoT environment, there are billions of vulnerable devices, and their number is growing rapidly a result, there are very different types of MITM attacks appeared. With the increasing need for IoT, MITM attacks will become an enormous challenge [51]. It is a pivotal and dangerous attack as it is one where the intruder acts as the real sender. As the intruder has the true communication, they can deceive the recipient into believing they are yet getting legitimate data as shown in *Figure 5*.

To protect IoT from MITM attacks may apply a robust encryption approach among the client and the server. The server validates a client's request by presenting then confirming a digital certificate and then the connection can be initiated. So, IoT corporations should produce the identification and authentication as a built-in ability when designing devices. Another approach to counter a MITM attack is by using an encrypted virtual private network (VPN). A VPN is a communication methodology among the devices [52].

Sybil attack is another type of network layer attack in which, a malicious object has the ability to use different identities in the same network. Sybil attacker shows incorrect ID or duplicate ID of any nodes so, it can deceive the other nodes in the IoT environment. Sybil attack creates redundancy problems in the routing protocol. The attacking node does not mimic any other node, but on the fly, it only appropriates the identity of other nodes. Sybil attack's impact on data integrity, nodes security, and the utilization of IoT resources [53]. Based on three dimensions, Sybil attack is classified into some types such as shown in *Figure 6*. The dimensions are the type of communication, the mode of acquiring Sybil identity (identification) and their participation in the network (participation) [54]:

1. Direct attack and indirect attack

With reference to the mode of communication between Sybil identities established by the attacker and real nodes, Sybil attacks are categorized into direct and Indirect. For the direct attack, the genuine nodes interact directly with Sybil nodes, but for the indirect attack, the communication is made via a malicious node.

2. Fabricated attack and stolen identity attack

Based on identification manner of Sybil attacks, they are divided into fabricated and stolen civil attack. A Sybil attacker can simply create an arbitrary number for the identification process. Such identities are termed as a fabricated random 32-bit integer.

Moreover, the identities may be assigned to Sybil nodes by spoofing the identity of one of its neighbors. This may have occurred when the network incorporates any mechanism to prevent fake identities from joining the network, this called stolen identities.

3. Simultaneous and non-simultaneous Sybil attack

Simultaneously, the malicious nodes can cooperate in an attack or the intruder can impersonate these Sybil identities one at a time. A particular identity may leave or join the network many times, i.e., one identity is used at any point in time. Multiple Sybil attackers can coordinate the swapping of Sybil identities periodically thereby making the detection process harder.

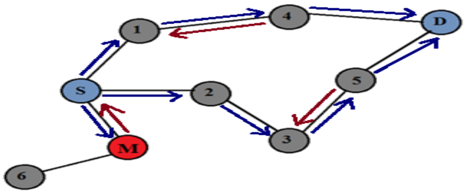


Figure 4 Black hole attack scenario

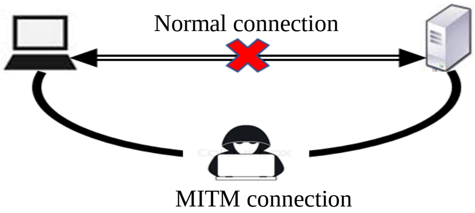


Figure 5 MITM attack scenario

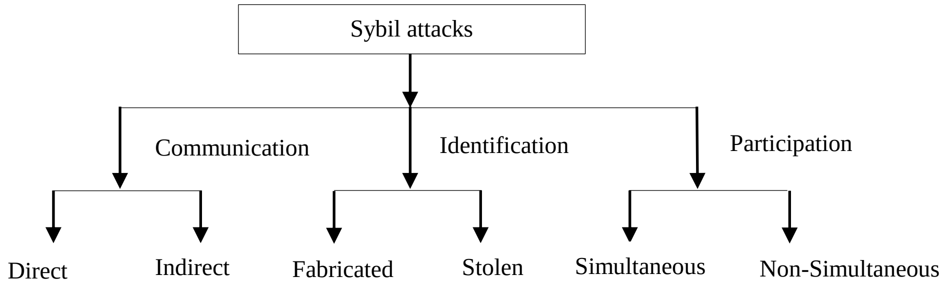


Figure 6 Sybil attacks classification

3.3 Sensing/physical layer attacks

Physical layer in IoT contains hardware components of IoT systems, such as controllers, RFID readers, sensors, and different types of RFID tags. Generally, each thing in IoT contains a digital identification hence, the sensing data easily have uniquely identified and IoT environment can be monitored and tracked for several targets and applications. The Universal Unique IDentifier (UUID) is the method of assigning a unique identifier to an object.

One of physical layer attacks is RF Interference attack in which a great number of noise signals are sent over radio frequencies in RFID communication as RFID systems work in a noisy and unstable environment the intrusion may use some of the material inhibiting RF tags or produce electromagnetic interference signals which have the same frequency with RFID communication system, preventing the normal communication between tags and readers [55]. In RF interference attack, the attacker makes denial of service attack by transmitting noise signals with radio frequency signals. So, it's recognized as a kind of denial of service attack.

Another attack in IoT physical layer is a jamming attack in which the attacker does disturbance in the wireless communication medium. Essentially RF is an open medium, so, the jamming attack can cause a tremendous problem concerning wireless networks. The jamming attack, which is a kind of the denials of service attack which blocks the channel by introducing malicious traffic such as in *Figure 7*. In common, spread spectrum communication is a countermeasure toward physical-layer jamming in wireless networks [56]. It causes a denying for the service to allow users by jamming the 2.4 GHz frequency in a form that perturbs the signal into a level wherever the wireless network can no longer use [57].

Jamming attacks are categorized into the following [58, 59]:

1. Random jamming attack substitutes among continuous jamming period and inactivity. It does the jamming for T1 period time, it changes to sleep

mode and stays emitting radio signals. The jammer after sleeping for a period T2 being active and resumes jamming. The two periods T1 and T2 are either fixed or random. This type is suitable for jammers that do not have an inexhaustible power supply.

2. Constant jamming attack frequently transmits a radio signal based on a waveform generator which sends out random bits of the channel without following any rules of MAC-layer, which is letting authorized nodes to send out packets just if the channel stays idle. Therefore, a constant jammer can stop legal traffic sources from gaining hold of a channel and transmitting packets.
3. The reactive jamming attack is not waking up all time, but it is quiet until the medium is empty. When it senses that the channel is idle the jammer starts the injection of false data. This causes a denial of service which avoids the authorized user to transmit data. So, this type is difficult to be detected.
4. Deceptive jamming attack continuously sends regular packets on the channel without regarding the medium access protocol.

There are many anti-jamming methods such as frequency hopping spread spectrum (FHSS), power control, timing channel transmissions, and interference cancellation techniques [60]. To build a secure IoT system, we should save a detecting method for jamming attacks which infect the system through the physical layer. Detection jamming attacks are a challenging problem and are considered the first action toward developing a secure IoT environment. Carrier sensing time, signal strength, and packet delivery ration are static methods that can be utilized in the detection process. Object replication attack is a physical layer attack which has the ability to add physically a new object to the network. For example, by replicating the identification of an object a malicious object could be added. This attack could cause a huge drop in the network performance.

This attack type can extract the secret keys and also, can get access to sensitive data with the help of a then malicious object. In addition to that, the attacker causes performance degradation, corrupting or misdirecting the packets that arrive at the replicated node. The black nodes in *Figure 8* are the form of object replication attacks which are cloned and positioned in varied places in the network. This attack could be avoided by a central computing the data collection path through the base station and verifying the identities (authentication) of nodes by a trustworthy node [61]. Camouflage attack employees a forgery edge node to operate as a normal node to obtain, process, send or redirect packets also, such a node can function in a passive style in which it only conducts traffic analysis. This camouflaged node brings the packets from the other nodes and may misroute these packets where privacy analysis performs [62]. The RFID system contains three entities such as tags, reader and back-end servers such as in *Figure 9*. The RFID reader can be any device has the capability to query the object identity stored in RFID tag such as PDA or mobile phone. The tags are imbedded in its objects to identify the object as each tag has a unique identifier. Also, this tag may contain an information about the object such as address, service history and repairing history. RFID tags are classified into passive, active, semi-passive tag. The passive has no internal source power, but the other types have a source for power. There are a lot of attacks that threaten RFID system ranging from passive eavesdropping to active interference. Tag cloning attacks create a fake tag from the original tag by capturing the tag identification, they can reproduce original tags and utilize the cloned tag for a variety of malicious aims like DoS attacks [63]. The hardware Trojan attack is concerned with integrated circuits (ICs). Through hardware trojans, the IC is maliciously modified to enable the attacker to use the circuit or exploits its functionality to make data access or software running on the ICs. The intrusion can insert hardware trojans through altering the design before/during fabrication and specifies a triggering method that activates the trojan behaviors [64]. Physical damage attacks can physically attack IoT objects through physical access to the object's tag. The known physical attacks against IoT objects environment are direct harm, probe attacks, material removal, circuit manipulation, and clock glitching. Deploying IoT objects in unattended environments, they are significantly susceptible to physical attacks, the easiest one of which is a direct harm of its objects [65].

4. Classification of IoT security techniques to address the attacks in each layer

4.1Detection/countermeasure of application layer attacks

The application layer introduces some services such as access the IoT applications using PCs, mobile devices etc. It contains two kinds of applications, local and non-local. Local applications include local domains in the IoT systems like smart homes and health tracking. The non-local includes cloud computing, remote management, and web technologies. In the following sub-sections, detection and countermeasures methods for attacks are ordered.

4.1.1Detection/countermeasure of virus, worms, trojan horse, and spyware

Virus, Worms, Trojan Horse, and Spyware (Malicious Code Injection) are some skills of intrusion through application layer of IoT. They have programming and skills to access systems, steal important data, obstruct system operations or physically damage the object. The countermeasure and detection methods used against these types of attacks are as follows [66]:

1. Antivirus software, update patches for operating systems, security policy and Security updates.
2. Side-channel analysis.
3. Verify software integrity.
4. Control flow.
5. Protective Software.
6. Antivirus software, update patches for operating systems, security policy and Security updates.
7. Side-channel analysis.
8. Verify software integrity.
9. Control flow.
10. Protective Software.

4.1.2Detection/countermeasure of denial of service attacks

There is a shortage in the research on the detection of DDoS attack within the application layer. The methods of detection the DDoS attacks used in the network layer or sensing layer is inefficient to be used in the application layer. So, the conventional IDS (Intrusion Detection System) can't detect any abnormal behaviour against the application layer. The research proposed some methods toward detecting DDoS attacks in application layer such as follows in *Table 3*:

Table 3 Detection techniques against DoS attacks in IoT

Technique	**Method**	**Description**
Flow rate statistics	Page access behavior	Browsing order of pages and the performing correlation between browsing time and information size [67].
User browsing behaviors analysis	Abnormal behavior detection	Monitoring the user's movement through the website[68].
	Information theory-based metrics	Entropy of requests per session and the trust score for each user is calculated[69].
Cluster analysis	cluster users' sessions	Calculation the deviation between sessions and normal clusters[70].

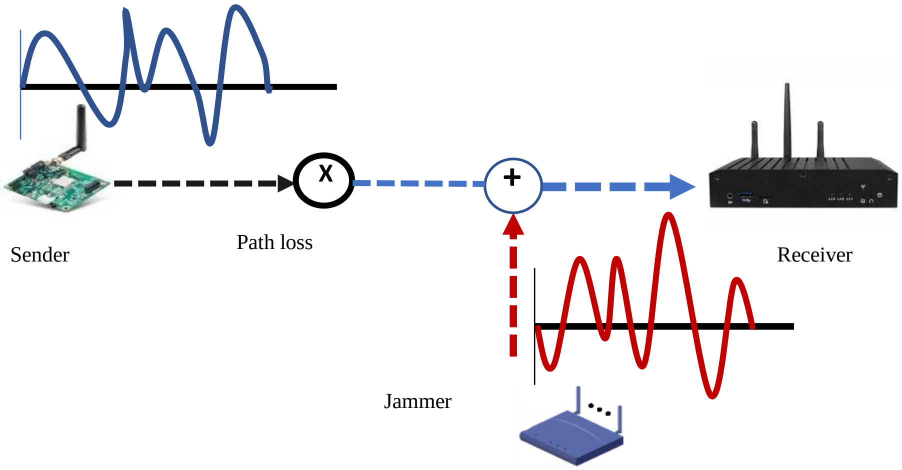


Figure 7 Jamming attack scenario

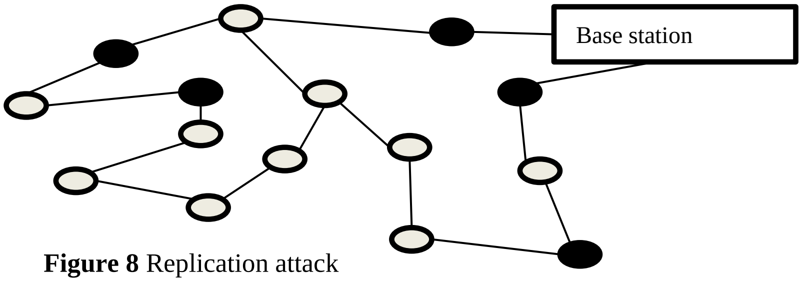


Figure 8 Replication attack

4.1.3Detection/countermeasure of software vulnerabilities attacks

A software vulnerability means an error or a weakness in the system that can be employed by the attacker to modify the common behaviors of the system. The intrusion tries to gain the system privileges to take useful information. Vulnerabilities may occur for the following reasons [71]:

1. Weak entropy: The attack accesses the system by guessing some random numbers generated by the system.
2. Weak cryptographic PING: Causes some cryptographic attacks.
3. Authentication schemes implemented improperly: Causes an authentication bypass by spoofing attacks.

The detection techniques of software vulnerability attacks are summarized in *Table 4* [72, 73].

Table 4 Detection techniques of software vulnerability attacks

Technique	Description
Fuzzing	Vulnerability in the software is identified by taking an invalid input or random input into the application and output behavior that is not expected and identify the error in the program and suspected vulnerability.
Scanners of Web Application	Examining web application by an automatic examiner to obtain vulnerabilities. It examines by surfing through the web pages and analysis the web application and come out with malicious input and further assesses it and sees its response.
Static Analysis Techniques	Directly applied to the source code to get specific information. there are different techniques such as pattern matching, lexical analysis, parsing, type qualifier, data flow analysis, taint analysis, and model checking.
Brick	Binary run-time integer-based vulnerability checker which detects integer-based vulnerability at run-time. It is a very effective approach as the result gives low false positive and negative.
CRED	C range error detector approach corrects the in-competencies and finds all buffer overruns attacks on programs with known vulnerabilities.

4.1.4Countermeasure of privacy leak attacks

Intrusions could obtain sensitive data from IoT devices or modifying these data. The privacy leak attack occurs or increases when collecting and transferring data from IoT devices. Suggested countermeasures to protect the IoT environment toward this type of attacks are [74]:

1. Ensuring that the IoT applications have strong passwords.
2. Ensuring access control for IoT applications when necessary.
3. Implementing two-factor authentications between IoT applications.
4. The Password recovery mechanisms should be secure.
5. The re-authentication mechanism is required for sensitive features of IoT application.
6. Ensuring options which are available for configuring password controls.

4.1.5Detection/countermeasure of buffer overflow attacks

In IoT, the detection and mitigation of buffer overflow attacks are a difficult problem. The intrusion gets administrative control of the root-privilege. There are some of detection methods for buffer overflow attacks such as in *Table 5* [75].

4.1.6Detection/countermeasure of cross-site scripting (XSS) attacks

Cross-site scripting attacks are recognized as XSS, attacks. The validation and verification mechanisms are some causes of XSS attacks in IoT applications. The XSS attack causes Cookie or other user's information stolen by a third party, forcing pages jumping, performing Trojans. The suggested detection methods of XSS attacks are summarized in *Table 6.*

Table 5 Buffer overflow attacks detection techniques

Technique	Description
Static analysis technique	The analysis is done actually without running the application. Object code or source code is inspected, and vulnerabilities flagged. This method doesn't cause runtime overhead.
Dynamic analysis	The analysis is done during system execution. Low false - positive and higher runtime cost.
Hybrid analysis	Static and dynamic procedures are applied. The static analysis is used beginning, to recognize potential vulnerabilities; then vulnerable stretches are instrumented also monitored at runtime via dynamic analysis.

Table 6 Techniques of XSS attacks detection

Technique	Description
Skip list	It is a multi-level sorted linked list which increases the searching efficiency of XSS attack detecting and reduces the wastage of system [76].
Hybrid Program Analysis	A hybrid method that merges static plus dynamic analysis procedures [77].
xHunter	A mechanism which takes the web trace as input and examines it for distinguishing XSS achievements [78].
Penetration Testing and Fault Injection	Combined with Web Services Security (WSS) also Security Tokens to identify XXS attacks [79].
Secure Web Application Proxy	SWAP can detect XSS attacks by comparing a reverse proxy which intercepts all HTML responses and a modified web browser [80].

4.2Detection/countermeasure of network layer attacks

The network layer is liable for the system management and maintenance of information through communication protocols. In IoT, the common protocol used is MQTT3.1 and constraint application protocol (CoAP). So, the network layer must save security needs for data, this can be done through some detection techniques for attacks which threatening its data such as in the next sub-sections.

4.2.1Detection/countermeasure of traffic analysis attack

In this attack, the intrusion can access the secret data which from RFID technology as it can arrest the private information using port scanning applications. Also, it can have some information by observing the frequency and timing of packets. The researchers in this field proposed some methods for detection and mitigation this type of attack as shown in *Table 7* [81].

Table 7 Techniques of traffic analysis attack detection

Technique	Description
Adaptive Link Padding	It is a dummy traffic sending mechanism for observing the delay between packets to determine if the gaps were natural or deliberately injected.
Dependent Link Padding	It is similar to an adaptive link padding scheme, except the generated dummy traffic is depends on incoming traffic rate.
Honeypots	This aids in tracing the effects of the intrusion.
Honeytokens	It adds information to check the intercepting or stolen and abused by an intrusion. Each use of certain honeytokens simply indicates illegal access.
Decoy Documents	Detects misbehaving as it contained embedded guides which are accomplished meanwhile the document is opened.
Decoy WiFi traffic	In this mechanism, camouflage packets contain webmail service cookies, FTP and HTTP protocol messages. Then, spread them via unencrypted WiFi network, then check the legal.

4.2.2Detection/countermeasure spoofing attack

The usual approaches are used in the authentication application to tackle the problem of a spoofing attack. Nevertheless, these approaches may be unsuitable in IoT environment because they need additional infrastructure and computational power. The researcher proposed methods to detect spoofing attacks like in *Table 8* [82].

4.2.3Detection/countermeasure sinkhole attack

It is one of the routing attacks which cause high threat for IoT networks. The goal is attracting a great amount of traffic in the known area for harming the reception of data on a collection point. So, it harms the reliability and integrity of data sent by IoT nodes. With respect to, detection of this kind of attack in IoT environment, researchers proposed some methods which summarized in *Table 9*.

4.2.4Detection/countermeasure HELLO flood attack

It is a network layer attack in which the intrusion can flood many requests to any legitimate node causing power consumption and security falling out. The researcher tried to propose a method for detection and mitigating HELLO flood attacks, these are summarized in *Table 10*.

4.2.5Detection/countermeasure Blackhole attack

The techniques which were proposed to detect Blackhole attacks are summarized in *Table 11*.

Table 8 Techniques of spoofing attack detection

Technique	Description
Received signal strength (RSS) mechanism and IDOL model	This proposal is based on measuring the strength of the signal between network nodes to detect spoofing attacks and localized them
K-means cluster algorithm	This proposal is an approach for detecting wireless spoofing attacks, define the number of attacks and localize them.
Receiver tracking states breaker and consistency between the carrier phase and the code phase breaker.	Detects the intermediate spoofing attacks by analyzing abnormal variations in the receiver signal
Adaptive Intrusion Detection System	This technique is based on the mathematical analyzing for network bandwidth using game theory

Table 9 Detection techniques of sinkhole attack

Technique	Description
INTI [83]	It is IDS for identifying sinkhole attacks and analyzing the behaviours of each node.
SVELTE [84]	It is IDS with an interspersed mini-firewall to the IP-connected IoT which utilizes RPL as a routing protocol within 6LoWPAN systems.
VeRA [85]	Detects any misbehaviour node based on the version number and the rank values. It was proposed for RPL based networks.
Semi-auto building a specification-based IDS model [86]	It is a model for RPL-based networks. It based on state transitions and relevant statistics of the trace file to detect sinkhole attacks and others.

Table 10 Detection techniques HELLO flood attack

Technique	Description
A signal strength and time threshold based AODV-HFDP [87]	Is the Ad-hoc On-demand Distance Routing beside Hello flood Detection with Prevention which is proposed for detection of the node that generates a hello flood intrusion.
Neighborhood based IDS [88]	The detection of the malicious node is done based on a principle that the sensor nodes which are neighboring to each other spatially are tended to have similar behavior. If a node proves a vital variation in its behavior in contrast with other nodes in the region, it is considered as a malicious node.
GIDS and NIDS [89]	It is a proposed for detection Hello flooding and Sybil attacks. GIDS is a centralized module on 6BR (IPv6 border router) and NIDS is a distributed module on sensor nodes which cooperates with each other to detect the attack.

Table 11 Detection techniques of blackhole attacks

Technique	Description
DPRAODV [90]	The Detection, Prevention, and Reactive AODV model. If the

Technique	Description
	RREP_seq_no value is higher than the threshold value of normal AODV, the node is considered a malicious node and added into the blacklist.
Neighborhood-based and routing recovery [91]	Detects the blackhole attack through neighbor set information.
CUSUM [92]	A dynamic threshold cumulative sum to check the abnormal changes in objects behavior based on the sequence numbers (SQNs) that occur due to the presence of black hole nodes in the network.
Hint based probabilistic approach [93]	Identifies black hole attacks using probabilistic routing strategy.

4.2.6Detection/countermeasure of MITM attack

Man, in the middle attack is a description of the attack which occurs during communication between user and IoT network. The danger of this type of attack is its ability to perform packet sniffing. The MITM attack through the rogue access point (AP) is a type of MITM attacking the proposed detection techniques for this type are summarized in *Table 12* [94].

4.2.7Detection/countermeasure of Sybil attack

There are three categories of Sybil attacks such as SA-1, SA-2, and SA-3. The goal of the SA-1 attack is to manipulate all options and manage the whole system. While the purpose of SA-2 and SA-3 is to distribute spam, advertisements, and malware to improve resource utilization; take and disrupt the user's privacy, and maliciously manipulate the estimation system but SA-3 is achieved via the mobile domain [95]. The detection approaches for Sybil attacks are summed in *Table 13* [96].

4.3Detection/countermeasure of sensing layer attacks

Sensing layer in IoT has a large interest in the research community with respect to detection and mitigation the sensing layer attacks. The countermeasures and detection technique for each attack in the sensing layer is pointed in the following subsections.

4.3.1Detection/countermeasure of RF interference and jamming attacks

RF interference and jamming attacks are two types of DoS, which have an ability to easily block the transmission and reception of packets and exhaust the node power. The proposed approaches for distinguishing the interference and jamming attacks are summarized in *Table 14* [97].

4.3.2Detection/countermeasure of tampering attacks

This kind of attack can do data modification, data injection and data replying. Regarding the data modification attack can break the security scheme to alter the packet contents. In data injection, the attacker tries to inject malicious packets into the data stream. In data replaying, the attacker tries to resend older packets to the receiver. The detection techniques are summarized in *Table 15*.

Table 12 Techniques of detection rouge AP MITM attacks

Technique	Description
Client-side bottleneck bandwidth analysis	This technique depends on the client bottleneck bandwidth value.
A passive approach	This suggestion depends on the use of RTT to identify rogue AP also authorized AP.
Radius authentication server	It contains 4 parts: security management interface, database, the radius authentication server, and rogue AP. This method needs ISP.

Table 13 Detection techniques of Sybil attack

Technique	Description
Detection based on network features	This technique depends on the network characteristics, it applies both network and nodes attributes to discover the SA. The use of network features is proper for networks constrained resource like IoT.
Detection Based on Cryptography	IT is based on cryptography of asymmetric and symmetric keys. Cryptography requires a high cost for generating secure keys and needs to keep updated identity lists furthermore not suitable for IoT.
Detection Based on the Relationship Between Neighbors	A number of packets are exchanged through neighbors of a

Technique	Description
	node to know information about its behavior.

Table 14 Techniques of RF interference and jamming attacks detection and mitigation

Detection techniques	Description
Signal strength	The jamming attacks effect on the signal strength so it is a parameter help in detection of jamming and the interference attacks in sensing layer.
Carrier Sensing Time	It is a measure for detecting the constant jamming attacks. It detects whether the channel is busy or idle by examining the noise level by a fixed threshold.
Packet Delivery Ratio	The packets delivered successfully toward the destination regarding the combined number of packets forwarded by the source is called PDR. Thus, PDR value is an indicator for jamming.
Mitigation technique	**Description**
Adaptive CCA [98]	Use a back-off strategy when the collision occurs with traffic generated by non-IEEE 802.15.4 devices decreases network throughput.
DynCCA [99]	This method dynamically adapts the threshold of clear channel assessment of 802.15.4 communications to decrease the impression of malicious nods.

Table 15 Detection techniques of tampering attack

Technique	Description
TD [100]	It is a tamper detection (TD) tool for networks of IoT concerning healthcare applications.
PMU and PDC based random time hopping [101]	This approach applies a random time hopping sequence for detecting data tampering.

4.3.3Detection/countermeasure of object/node replication attack

Object replication attack can discover the secret keys, data and code stored in a sensor node also, can replicate it through a huge number of clones then install them in the network. This attack may be a base for launching a various attacks like DoS attacks and Sybil attacks.[102]. The researchers have proposed some methods for detection and mitigation such as in *Table 16* [103].

4.3.4Detection/countermeasure of camouflage attack

Camouflage attack is one of the significant threats in the computer security field. OCSVM [104] is a proposed algorithm to accomplish single value classification and sequence data for detecting camouflage attack. This research proposal is based on new string kernel function and SVM. LEAPS [105] (Learning Enhanced with Analysis of Program Support) is a camouflage attack detection system based on supervised statistical learning to classify benign and malicious system events.

4.3.5Detection/countermeasure of clone tag attack

Their two major approaches in handling tag cloning; prevention and detection. The prevention, provides security against clone tags attack using encryption and cryptography of tags. But this approach can't be implemented in low cost, power and storage tags. A detection approaches are relevant for cloning attacks. The detection tactics are summarized in *Table 17*.

4.3.6Detection/countermeasure of Hardware Trojans

Hardware Trojans (HTs) can steal the internal sensitive data also, can modify the original functionality of the chip. System shutdown and leaking important information are two of the activities of this attack type. The detection techniques of hardware trojans attacks are summarized in *Table 16*.

5. IDS for IoT attacks detection

It's very hard to design a specific security mechanism for IoT as this environment is heterogeneous, fragmented and not supportive of interoperability. Some solutions for enhancement IoT security have been developed. These methods applied for performing data confidentiality and authentication, access control toward IoT, also saving privacy among users and things. However, even with those mechanisms, IoT networks still saver from attacks. IDS could be used in IoT to ensure the security facing a variety of attacks. With regard to, the maturity of IDS technology for traditional networks, current solutions are ineffectual for IoT as they not flexible enough against the complex and heterogeneous IoT ecosystem.

Characteristics such as constrained-resources devices, network architecture, specific protocol stacks, and standards, explain the need for the development of IDS for IoT. Some of the recommended IDS methods are summarized in *Table 19*. *Table 18* is showing Detection techniques of trojans attacks.

Table 16 Detection techniques of object/node replication attack

Technique	Description
Centralized Techniques.	The node IDs and location information are checked in a base station (centralized node). If it finds two different locations with the same ID, it occurs a node replication alarm.
Distributed Techniques	The detection is made through locally distributed node named "claimer-reporter-witness", via transferring the location claim to randomly selected node named witness node.

Table 17 Detection techniques of clone attacks

Techniques	Description
DCTD [106]	The cloned tag detection protocol to anonymous RFID based on the improved tree-based anti-collision algorithm.
BASE, DeClone and DeClone + [107]	BASE ID-independent protocol. This protocol is based on the cardinality contradiction caused by clone tags. This protocol preferred for the small system. DeClone is accelerated clone detection for a big anonymous RFID system. DeClone+ is improved version of DeClone method.
GREAT [108]	This technique tackles the cloning attack detection toward anonymous RFID networks without needing tag IDS.
DTD [109]	Double-Track Detection (DTD) for RFID system security.

Table 18 Detection techniques of trojans attacks

Technique	Description
Power consumption information [110]	This approach depends on measuring the deviation of power consumption. If there is deviation means that attack occurred.
Many-core based on machine learning technique [111]	It is a run-time detection architecture based on support vector machine (SVM)
Random Forest Classifier hardware trojan detection [112]	In this technique 11 from 51 features of hardware trojan attacks are used as input of RFC to detect the attack.

Table 19 IDSs used for IoT attacks detection

IDS Objectives	Methodology
Dos attack detection	Network-based IDS captures and analyses the network packet based on DoS detection architecture [113]
Detection of IPv6-enabled wireless sensor networks attacks.	Used NIDS, HIDS and EMS (Event Management System) in the proposed architecture[114].
Identify wormhole attack	IDS which used the position information for the node plus neighbours to discover the wormhole attack. Also, used received signal strength to identify attack nodes [115].
Detects malicious attacker in order to defend networks from selective forwarding attacks in IoT.	IDS which depends on the game-theory model to analyse the malicious behaviour of attackers in the IoT systems [116].

6. Research challenges in IoT security

The challenges which face the IoT are the security challenges in the heterogenous networks and capacity constraints. The security agents must prove the reliability, economy, efficiency and effectiveness of the security. IoT must guarantee the privacy and confidentiality of the user. The security challenges of IoT can be categorized as following [117]:

Implementation challenges

The basis for development of the services in IoT domain its necessary to introduce standard for design, operating system and communication. The challenges which concerned with implementing the IoT are:

1. The architecture of IoT security.
2. Detection of IoT attacks
3. Tools for managing the identification of users and objects.

4. User information control
5. Confidentiality Methods for exchanging sensitive information.
6. The standardization of heterogeneous technologies, devices, applications, connections and communications, represent a major challenge.
7. network infrastructure should provide security of communication and data transmission

Privacy challenges

The privacy means identifying information which its leakage causing the knowing of personal data and accessing the data sources. In the ear of IoT cyber-attacks of sensing layer can know the identity of users without needing to know the physical address. They can gain this through eavesdropping the data packet along with the existing remote information. The challenges of privacy are data collection policies and data anonymity.

Network infrastructure challenges

The infrastructure of IoT causes more demand for coordination and upgrading. It should ensure that the safely delivery of data. The categories of infrastructure challenges are:

1. Hardware

The IoT may contain multiprotocol hardware, multi-standard, sensors, controllers, relays and so forth, they cause more challenge in IoT network.

2. Network connection

The connection of network sensors which can collect, monitor and analyze data may cause challenge.

3. Architecture

The extended architecture of IoT which gives the ability to connect new users and sensors cause challenge in IoT security. As it changed from Single-domain systems will become multi-domain.

4. Software and algorithms

The software and super-algorithms needed for IoT cause challenge with respect to the security point of view.

5. Cloud computing

The infrastructure of IoT may be extended to use the cloud for storing and processing data collected. The user access to cloud and gaining specific interesting data needs some privilege which causes challenges for IoT security.

QoS challenges

With respect to quality of service, IoT network should guarantee many factors to provide QoS specifications. These factors such as security of individual object and user, the performance of the system, usability which is the goal of the system, reliability, which proves the activity of the system with respect to the time, stability, which is the ability of the system to save its performance all time interoperability, which gives the ability for communication and exchange information between objects and the scalability which gives the system's ability to be expanded without affecting its performance. All these factors must effect on the IoT security so, the QoS has more challenges on IoT security.

Big data challenges

The concept Big data is associated with the computer science when the volume of data generated become difficult to be handled by traditional techniques. In IoT environment the volume of data produced by its contents like sensors, social media, devices, temperature sensors, health care applications, and many other software applications and digital things that usually create massive amounts of structured, unstructured, or semi-structured data is greatly increased. So, it is an inefficient way to use conventional database systems for processing, storing, or analyzing big data [118]. The big data technology is known as a new generation of technologies and architectures which target to carry out the value from a large volume of data with different formats by allowing capturing, discovery, and analyze data with high-velocity. As a result of the increasing number of connected devices such as mentioned above in *Figure 1* it has been observed five main Big data challenges (the five Vs.): increasing data volume, increasing velocity of data as in/out and change of data, increasing variety of data types and structures, increasing data veracity and increasing value of data which is the contribution of data with ability for making decisions[119]. Big data analytics is a process used for analyzing a large data sets that contain a mixture of data types to obtain useful information.The foremost goal of big data analytics is to support business associations to get clarified understanding of the data, then make efficient decisions. Big data analytics allow data laborers and specialists to analyze a large amount of data which difficult to use traditional tools. *Figure 10* shows the relationship between IoT and big data analytics is that it is used to enhance decision making. The numerous obvious features of IoT is its analysis of data collected from connecting objects. Big data analytics in IoT needs processing a massive amount of data on the fly and saving it through different storage methods.

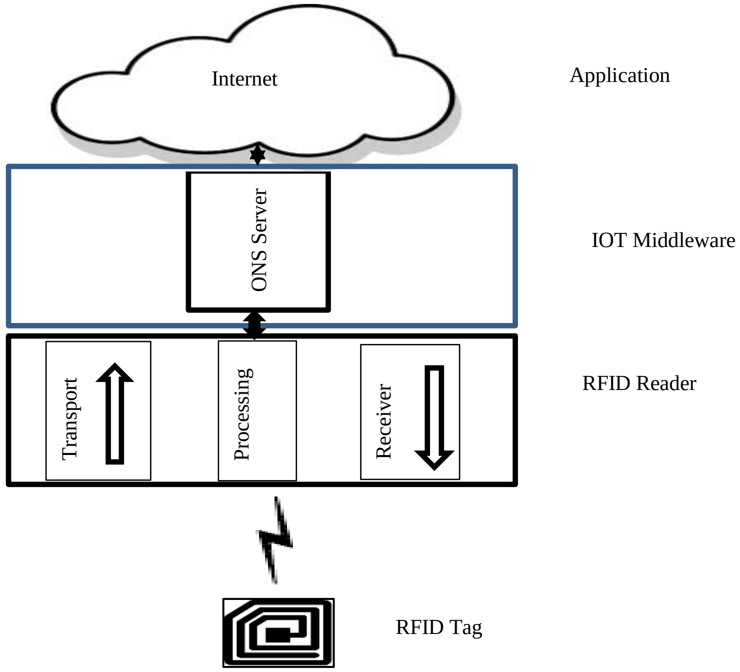


Figure 9 RFID system

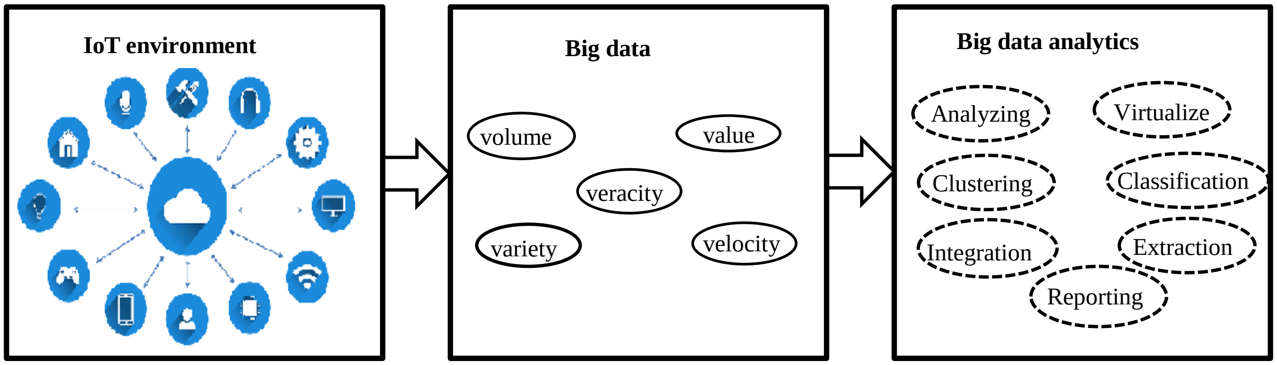


Figure 10 Relationship between IoT and Big data analytics

7.Evaluation of IoT with respect to the security

It is important for the security of IoT to choose the appropriate evaluation strategies for its infrastructure. The evaluation operation includes a comprehensive range of tools, processes, and methodologies. *Table 20* summarizes the evaluation strategies that can be used during IoT infrastructure's design, deployment, development, and operations [120, 121].

8. Conclusion and future work

By the last few years, the IoT has been recognized as a major research domain as the physical objects would interact through different network technologies. The broad progression of the services of IoT needs authentic and genuine security tool. This paper presents a comprehensive overview of IoT by illustrating the working of layers, the security requirement of each layer, and then addresses different security attacks on different layers of IoT (Sensing Layer, Network Layer, and Application Layer). Too, it gives the detection methods and countermeasures toward security attacks in IoT. As IoT is considered a vital part of our life, it faces many challenges like big data, this paper provides these challenges and their effects on IoT security. It also gives the evaluation strategies of IoT with respect to the security. The future work which is suggested from this research is how to design a comprehensive security system for IoT because the attacks can threaten IoT from any layer. The design of this system may be a cross- layer security which guarantees the security of all layers in IoT architecture. There are many harmful attacks in IoT attacks such as DoS attacks which can infect IoT architecture through all three layers. Consequently, the cross-layer approach is considered more suitable for sufficient security solution. The cross-layer solution need interaction between all components in all layers plus the huge number of objects connected to IoT cause big data challenge. So, cross layer with big data analytics technique can improve security agent in IoT environment. The scenario of operation of cross-layer, big data cluster and decision making can be outlined as shown in *Figure 11*.

Figure11, ADD is an application layer attack detector, which can detect attacks in application layer through aggregating data from application-based attack detectors ADD1-n and transferring data to big data analytics to store, and processes in a big data cluster to extract useful information to detect attacks. NAD is, network layer attacks detector can transfer network layer data to big data analytics. Also, SAD is a sensor layer attack detector can transfer physical layer data to big data analytics. ADD1-n, SAD1-n can detect short term data between applications and sensors respectively. After the data is processed through big data analytics cluster the output is transferred to decision making module to specify the type of traffic.

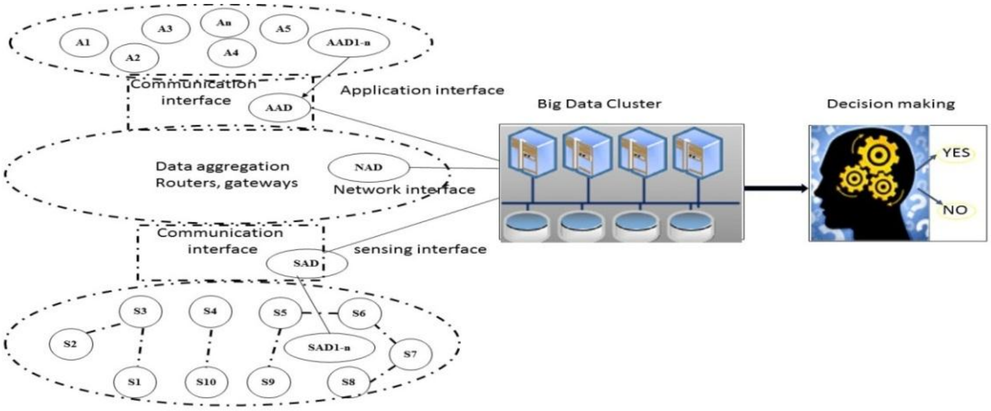


Figure 11 Cross-layer detection powered with big data analytics

Table 20 Evaluation strategies of IoT

<table>
<tr><th>Strategy</th><th>Description</th></tr>
<tr><td>Threat detection model</td><td>Analysis of IoT infrastructure to accomplish method to discover and detect threats. An example of evaluation the detection system like IDS is performance metrics. These metrics are computed from confusion matrix which is represent classification results of the IDS based on true and false classification measurements, confusion matrix is defined in <i>Table 20.</i>
<table>
<tr><td>Actual</td><td>Predicted</td><td>Predicted</td></tr>
<tr><td></td><td>Attack</td><td>Normal</td></tr>
<tr><td>Attack</td><td>TP</td><td>FN</td></tr>
<tr><td>Normal</td><td>FP</td><td>TN</td></tr>
</table>
Table 20 Confusion Matrix.
From confusion matrix, some numeric values can be produced like:
1- Classification rate (CR)= $\frac{TP+TN}{TP+TN+FP+FN}$ (1)
2- Detection rate (DR)= $\frac{TP}{TP+FN}$ (2)
3- False positive rate (FPR)= $\frac{FP}{FP+TN}$ (3)
4- Precision (PR)= $\frac{TP}{TP+FP}$ (4)
5- Recall is equivalent to the DR
6- F-measure (FM)= $\frac{2}{\frac{1}{PR}+\frac{1}{Recall}}$ (5)</td></tr>
</table>

Strategy	Description
Authentication and access control evaluation	It includes end-to-end analysis for authentication and access control methods which are used in an IoT environment.
Device risk analysis	The analysis of device hardware and software causes a better understanding of the attack surface and threats associated with the device.
Privacy evaluation	It includes an end-to-end evaluation of an IoT infrastructure design also, evaluate the individual and organization privacy.
Encryption evaluation	Evaluation encryption algorithms used by both the devices and the cloud; this allows a better understanding of the attack surface.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Tsai CW, Lai CF, Vasilakos AV. Future internet of things: open issues and challenges. Wireless Networks. 2014; 20(8):2201-17.

[2] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide. Accessed 27 December 2018

[3] http://www.cisco.com/web/about/ac79/index.html. Accessed 13 March 2018.

[4] Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D. Security of the internet of things: perspectives and challenges. Wireless Networks. 2014; 20(8):2481-501.

[5] Sonar K, Upadhyay H. A survey: DDOS attack on internet of things. International Journal of Engineering Research and Development. 2014; 10(11):58-63.

[6] Suo H, Wan J, Zou C, Liu J. Security in the internet of things: a review. In international conference on computer science and electronics engineering 2012 (pp. 648-51). IEEE.

[7] Alansari Z, Anuar NB, Kamsin A, Soomro S, Belgaum MR, Miraz MH, et al. Challenges of internet of things and big data integration. In international conference for emerging technologies in computing 2018 (pp. 47-55). Springer, Cham.

[8] Weber RH. Internet of things–new security and privacy challenges. Computer Law & Security Review. 2010; 26(1):23-30.

[9] http://www.centrenational-rfid.com/introduction-to-the-rfid-article-15-gb-ruid-202.html. Accessed 17 April 2018.

[10] Liu Y, Zhou G. Key technologies and applications of internet of things. In fifth international conference on intelligent computation technology and automation 2012 (pp. 197-200). IEEE.

[11] Oracevic A, Dilek S, Ozdemir S. Security in internet of things: a survey. In international symposium on networks, computers and communications (ISNCC) 2017 (pp. 1-6). IEEE.

[12] Li S, Tryfonas T and Li H. The internet of things: a security point of view. Internet Research. 2016; 26(2):337-59.

[13] Yousuf T, Mahmoud R, Aloul F, Zualkernan I. Internet of things (IoT) security: current status, challenges and countermeasures. International Journal for Information Security Research. 2015; 5(4):608-16.

[14] Cai H, Da Xu L, Xu B, Xie C, Qin S, Jiang L. IoT-based configurable information service platform for product lifecycle management. IEEE Transactions on Industrial Informatics. 2014; 10(2):1558-67.

[15] Atzori L, Iera A, Morabito G. The internet of things: a survey. Computer Networks. 2010; 54(15):2787-805.

[16] Trappe W, Howard R, Moore RS. Low-energy security: limits and opportunities in the internet of things. IEEE Security & Privacy. 2015; 13(1):14-21.

[17] Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W. A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal. 2017; 4(5):1125-42.

[18] Shafagh H, Hithnawi A, Droescher A, Duquennoy S, Hu W. Talos: encrypted query processing for the internet of things. In proceedings of the ACM conference on embedded networked sensor systems 2015 (pp. 197-210). ACM.

[19] Stephen E. Internet protocol, version 6 (IPv6) specification. RFC2460. 1998.

[20] Kushalnagar N, Montenegro G, Schumacher C. IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals. 2007.

[21] Ning H, Liu H, Yang LT. Cyberentity security in the internet of things. Computer. 2013; 46(4):46-53.

[22] Yang Y, Wu L, Yin G, Li L, Zhao H. A survey on security and privacy issues in Internet-of-Things. IEEE Internet of Things Journal. 2017; 4(5):1250-8.

[23] http://www.internet-of-things-research.eu/. Accessed 17 April 2018.

[24] Singh S, Singh N. Internet of things (IoT): security challenges, business opportunities & reference architecture for e-commerce. In international conference on green computing and internet of things (ICGCIoT) 2015 (pp. 1577-81). IEEE.

[25] Borgohain T, Kumar U, Sanyal S. Survey of security and privacy issues of internet of things. 2015.

[26] Gavrilut D, Cimpoesu M, Anton D, Ciortuz L. Malware detection using perceptrons and support vector machines. In computation world: future computing, service computation, cognitive, adaptive, content, patterns 2009 (pp. 283-8). IEEE.

[27] Kolter JZ, Maloof MA. Learning to detect and classify malicious executables in the wild. Journal of Machine Learning Research. 2006:2721-44.

[28] More SS, Gaikwad PP. Trust-based voting method for efficient malware detection. Procedia Computer Science. 2016; 79:657-67.

[29] Loukas G, Öke G. Protection against denial of service attacks: a survey. The Computer Journal. 2010; 53(7):1020-37.

[30] Chandola V, Banerjee A, Kumar V. Anomaly detection: a survey. ACM Computing Surveys. 2009; 41(3).

[31] Medaglia CM, Serbanati A. An overview of privacy and security issues in the internet of things. In the internet of things 2010 (pp. 389-95). Springer, New York, NY.

[32] Bugenhagen MK, Wiley WL. Pin-hole firewall for communicating data packets on a packet network. United States Patent US 8,015,294. 2011.

[33] Shin Y, Meneely A, Williams L, Osborne JA. Evaluating complexity, code churn, and developer activity metrics as indicators of software vulnerabilities. IEEE Transactions on Software Engineering. 2010; 37(6):772-87.

[34] Abomhara M. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility. 2015; 4(1):65-88.

[35] Zhou W, Jia Y, Peng A, Zhang Y, Liu P. The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE Internet of Things Journal. 2018; 6(2):1606-16.

[36] Guo L, Dong M, Ota K, Li Q, Ye T, Wu J, et al. A secure mechanism for big data collection in large scale internet of vehicle. IEEE Internet of Things Journal. 2017; 4(2):601-10.

[37] https://www.veracode.com/security/buffer-overflow. Accessed 26 May 2018.

[38] https://resources.altium.com/pcb-design-blog/internet-of-things-security-vulnerabilities-all-about-buffer-overflow. Accessed 26 May 2018

[39] https://www.techrepublic.com/blog/it-security/what-is-cross-site-scripting. Accessed 29 May 2018.

[40] Millar S. Network security issues in the Internet of Things (IoT). Queen's University Belfast. 2016.

[41] Uke SN, Mahajan AR, Thool RC. UML modeling of physical and data link layer security attacks in WSN. International Journal of Computer Applications. 2013; 70(11).

[42] Ahemd MM, Shah MA, Wahid A. IoT security: a layered approach for attacks & defenses. In international conference on communication technologies 2017 (pp. 104-10). IEEE.

[43] Pongle P, Chavan G. A survey: attacks on RPL and 6LoWPAN in IoT. In international conference on pervasive computing 2015 (pp. 1-6). IEEE.

[44] Sharmila S, Umamaheswari G. Detection of sinkhole attack in wireless sensor networks using message digest algorithms. In international conference on process automation, control and computing 2011 (pp. 1-6). IEEE.

[45] Stephen R, Arockiam L. Intrusion detection system to detect sinkhole attack on RPL protocol in internet of things. International Journal of Electrical Electronics and Computer Science. 2017; 4(4):16-20.

[46] Kaur P, Gurm JS. Detect and prevent HELLO FLOOD attack using centralized technique in WSN. International Journal of Computer Science & Engineering Technology. 2016; 7(8):379-81.

[47] Magotra S, Kumar K. Detection of HELLO flood attack on LEACH protocol. In international advance computing conference 2014 (pp. 193-8). IEEE.

[48] Aljumah A, Ahanger TA. Futuristic method to detect and prevent blackhole attack in wireless sensor networks. International Journal of Computer Science and Network Security. 2017; 17(2):194-201.

[49] Zandiyan S, Fotohi R, Koravand M. P-method: improving AODV routing protocol for against network layer attacks in mobile ad-hoc networks. International Journal of Computer Science and Information Security. 2016; 14(6):95-103.

[50] Nisha SK, Arora SK. Analysis of black hole effect and prevention through IDs in manet. American Journal of Engineering Research. 2013; 2(10):214-20.

[51] Cekerevac Z, Dvorak Z, Prigoda L, Cekerevac P. Internet of things and the man-in-the-middle attacks–security and economic risks. MEST Journal. 2017; 5(2):15-25.

[52] https://www.globalsign.com/en/blog/man-in-the-middle-attacks-iot/. Accessed 04 July 2018.

[53] Balachandran N, Sanyal S. A review of techniques to mitigate sybil attacks. IJANA. 2012.

[54] Dhamodharan US, Vayanaperumal R. Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method. The Scientific World Journal. 2015.

[55] Li H, Chen Y, He Z. The survey of RFID attacks and defenses. In international conference on wireless communications, networking and mobile computing 2012 (pp. 1-4). IEEE.

[56] Raymond DR, Midkiff SF. Denial-of-service in wireless sensor networks: attacks and defenses. IEEE Pervasive Computing. 2008; 7(1):74-81.

[57] https://www.spamlaws.com/jamming-attacks.html. Accessed 17 July 2018.

[58] Panyim K, Hayajneh T, Krishnamurthy P, Tipper D. On limited-range strategic/random jamming attacks in wireless ad hoc networks. In conference on local computer networks 2009 (pp. 922-9). IEEE.

[59] Xu W, Ma K, Trappe W, Zhang Y. Jamming sensor networks: attack and defense strategies. IEEE Network. 2006; 20(3):41-7.

[60] Tang X, Ren P, Han Z. Jamming mitigation via hierarchical security game for IoT communications. IEEE Access. 2018; 6:5766-79.

[61] Millar S. Network security issues in the Internet of Things (IoT). Queen's University Belfast. 2016.

[62] Sunitha K, Chandrakanth H. A survey on security attacks in wireless sensor network. International

Journal of Engineering Research and Applications. 2012; 2(4):1684-91.

[63] Liu AX, Bailey LA. PAP: a privacy and authentication protocol for passive RFID tags. Computer Communications. 2009; 32(7-10):1194-9.

[64] Tehranipoor M, Koushanfar F. A survey of hardware trojan taxonomy and detection. IEEE Design & Test of Computers. 2010; 27(1):10-25.

[65] Deogirikar J, Vidhate A. Security attacks in IoT: a survey. In international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) 2017 (pp. 32-7). IEEE.

[66] https://www.guru99.com/learn-everything-about-trojans-viruses-and-worms.html. Accessed 13 August 2018.

[67] Yatagai T, Isohara T, Sasase I. Detection of HTTP-GET flood attack based on analysis of page access behavior. In pacific RIM conference on communications, computers and signal processing 2007 (pp. 232-5). IEEE.

[68] Xie Y, Yu SZ. A large-scale hidden semi-Markov model for anomaly detection on user browsing behaviors. IEEE/ACM Transactions on Networking. 2008; 17(1):54-65.

[69] Devi SR, Yogesh P. Detection of application layer DDoS attacks using information theory based metrics. CS & IT-CSCP. 2012; 10:217-23.

[70] Ye C, Zheng K, She C. Application layer DDoS detection using clustering analysis. In proceedings of international conference on computer science and network technology 2012 (pp. 1038-41). IEEE.

[71] Li P, Cui B. A comparative study on software vulnerability static analysis techniques and tools. In international conference on information theory and information security 2010 (pp. 521-4). IEEE.

[72] Amankwah R, Kudjo PK, Antwi SY. Evaluation of software vulnerability detection methods and tools: a review. International Journal of Computer Applications. 2017; 169(8):22-7.

[73] Freitez WR, Mammar A, Cavalli AR. Software vulnerabilities, prevention and detection methods: a review. SEC-MDA 2009 (pp. 1-11).

[74] https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures/. Accessed 16 September 2018.

[75] Teixeira FA, Pereira FM, Wong HC, Nogueira JM, Oliveira LB. SIoT: securing internet of things through distributed systems analysis. Future Generation Computer Systems. 2019; 92:1172-86.

[76] Chun S, Jing C, ChangZhen H, JingFeng X, Hao W, Raphael M. A XSS attack detection method based on skip list. International Journal of Security and its Applications. 2008; 10(5):95-106.

[77] Khin SL. Mitigating SQL injection and cross site scripting vulnerabilities using program analysis and data mining techniques (Doctoral Dissertation). 2013.

[78] Athanasopoulos E, Krithinakis A, Markatos EP. Hunting cross-site scripting attacks in the network. In proceedings of the workshop on web 2010 (pp. 1-8).

[79] Caselli M, Kargl F. A security assessment methodology for critical infrastructures. In international conference on critical information infrastructures security 2014 (pp. 332-43). Springer, Cham.

[80] Wurzinger P, Platzer C, Ludl C, Kirda E, Kruegel C. SWAP: mitigating XSS attacks using a reverse proxy. In proceedings of the ICSE workshop on software engineering for secure systems 2009 (pp. 33-9). IEEE Computer Society.

[81] Chakravarty S. Traffic analysis attacks and defenses in low latency anonymous communication (Doctoral Dissertation, Columbia University). 2014.

[82] Devi PK, Manavalan R. Spoofing attack detection and localization in wireless sensor network: a review. International Journal of Computer Science & Engineering Technology. 2014; 5(9): 877–86, 2014.

[83] Cervantes C, Poplade D, Nogueira M, Santos A. Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for internet of things. In international symposium on integrated network management 2015 (pp. 606-11). IEEE.

[84] Raza S, Wallgren L, Voigt T. SVELTE: real-time intrusion detection in the internet of things. Ad HOC Networks. 2013; 11(8):2661-74.

[85] Dvir A, Buttyan L. VeRA-version number and rank authentication in RPL. In international conference on mobile Ad-Hoc and sensor systems 2011 (pp. 709-14). IEEE.

[86] Le A, Loo J, Chai K, Aiash M. A specification-based IDS for detecting attacks on RPL-based network topology. Information. 2016; 7(2):1-19.

[87] Singh VP, Ukey AS, Jain S. Signal strength based hello flood attack detection and prevention in wireless sensor networks. International Journal of Computer Applications. 2013; 62(15):1-6.

[88] Khosravi H, Azmi R, Sharghi M. Adaptive detection of hello flood attack in wireless sensor networks. International Journal of Future Computer and Communication. 2016; 5(2):99-103.

[89] Sherasiya T, Upadhyay H. Intrusion detection system for internet of things. International Journal of Advance Research and Innovative Ideas in Education. 2016; 2(3):2244-9.

[90] Raj PN, Swadas PB. Dpraodv: a dyanamic learning system against blackhole attack in AODV based MANET. International Journal of Computer Science. 2009; 2:54-9.

[91] Baghel L, Mishra P, Samvatsar M, Singh U. Detection of black hole attack in mobile ad hoc network using adaptive approach. In international conference of electronics, communication and aerospace technology 2017 (pp. 626-30). IEEE.

[92] Panos C, Ntantogian C, Malliaros S, Xenakis C. Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks. Computer Networks. 2017; 113:94-110.

[93] Chauhan RK. An assessment based approach to detect black hole attack in MANET. In international

conference on computing, communication & automation 2015 (pp. 552-7). IEEE.

[94] Lee J, Tu C, Jung S. Man-in-the-middle attacks detection scheme on smartphone using 3G network. In the fourth international conference on evolving internet 2012 (pp. 65-70).

[95] Zhang K, Liang X, Lu R, Shen X. Sybil attacks and their defenses in the internet of things. IEEE Internet of Things Journal. 2014; 1(5):372-83.

[96] Evangelista D, Mezghani F, Nogueira M, Santos A. Evaluation of sybil attack detection approaches in the internet of things content dissemination. In wireless days 2016 (pp. 1-6). IEEE.

[97] Shaikh M, Syed AH. A survey on jamming attacks, detection and defending strategies in wireless sensor networks. International Journal of Research in Engineering and Technology. 2014; 3(3): 558-61.

[98] King A, Brown J, Roedig U. DCCA: differentiating clear channel assessment for improved 802.11/802.15. 4 coexistence. In international conference on wireless and mobile computing, networking and communications 2014 (pp. 45-50). IEEE.

[99] Sparber T, Boano CA, Kanhere SS, Römer K. Mitigating radio interference in large IoT networks through dynamic CCA adjustment. Open Journal of Internet of Things. 2017; 3(1):103-13.

[100]Elngar AA. IoT-based efficient tamper detection mechanism for healthcare application. IJ Network Security. 2018; 20(3):489-95.

[101]Aman MN, Javed K, Sikdar B, Chua KC. Detecting data tampering attacks in synchrophasor networks using time hopping. In PES innovative smart grid technologies conference Europe (ISGT-Europe) 2016 (pp. 1-6). IEEE.

[102]Sei Y, Honiden S. Distributed detection of node replication attacks resilient to many compromised nodes in wireless sensor networks. In proceedings of the international conference on wireless internet 2008.

[103]Khan WZ, Aalsalem MY, Saad MN, Xiang Y. Detection and mitigation of node replication attacks in wireless sensor networks: a survey. International Journal of Distributed Sensor Networks. 2013; 9(5):1-22.

[104]Ku Z, Hu Z. Camouflage attack detection based on KMOD kernel function. In international conference on computer science and software engineering 2008 (pp. 1031-4). IEEE.

[105]Gu Z, Pei K, Wang Q, Si L, Zhang X, Xu D. Leaps: detecting camouflaged attacks with statistical learning guided by program analysis. In international conference on dependable systems and networks 2015 (pp. 57-68). IEEE.

[106]Yimin G, Shundong L, Jiawei D, Sufang Z. Deterministic cloned tag detection protocol for anonymous radio-frequency identification systems. IET Information Security. 2016; 10(1):28-32.

[107]Bu K, Xu M, Liu X, Luo J, Zhang S, Weng M. Deterministic detection of cloning attacks for anonymous RFID systems. IEEE Transactions on Industrial Informatics. 2015; 11(6):1255-66.

[108]Bu K, Liu X, Luo J, Xiao B, Wei G. Unreconciled collisions uncover cloning attacks in anonymous RFID systems. IEEE Transactions on Information Forensics and Security. 2013; 8(3):429-39.

[109]Huang J, Li X, Xing CC, Wang W, Hua K, Guo S. DTD: a novel double-track approach to clone detection for RFID-enabled supply chains. IEEE Transactions on Emerging Topics in Computing. 2015; 5(1):134-40.

[110]Sui Q, Wu Z, Li J, Li S. A detection method of hardware Trojan based on two-dimension calibration. In international conference on computer and communications 2016 (pp. 2795-9). IEEE.

[111]Kulkarni A, Pino Y, Mohsenin T. SVM-based real-time hardware Trojan detection for many-core platform. In international symposium on quality electronic design 2016 (pp. 362-7). IEEE.

[112]Hasegawa K, Yanagisawa M, Togawa N. Trojan-feature extraction at gate-level netlists and its application to hardware-Trojan detection using random forest classifier. In international symposium on circuits and systems 2017 (pp. 1-4). IEEE.

[113]Kasinathan P, Pastrone C, Spirito MA, Vinkovits M. Denial-of-service detection in 6LoWPAN based Internet of Things. In international conference on wireless and mobile computing, networking and communications 2013 (pp. 600-7). IEEE.

[114]Amaral JP, Oliveira LM, Rodrigues JJ, Han G, Shu L. Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks. In international conference on communications 2014 (pp. 1796-801). IEEE.

[115]Pongle P, Chavan G. Real time intrusion and wormhole attack detection in internet of things. International Journal of Computer Applications. 2015; 121(9):1-9.

[116]Brown J, Du X. Detection of selective forwarding attacks in heterogeneous sensor networks. In international conference on communications 2008 (pp. 1583-7). IEEE.

[117]Ghorbani HR, Ahmadzadegan MH. Security challenges in internet of things: survey. In conference on wireless sensors 2017 (pp. 1-6). IEEE.

[118]Marjani M, Nasaruddin F, Gani A, Karim A, Hashem IA, Siddiqa A, et al. Big IoT data analytics: architecture, opportunities, and open research challenges. IEEE Access. 2017; 5:5247-61.

[119]Kumar MP, Santhoshkumar SP, Gowdhaman T, Shajahaan SS. A survey on IoT performances in big data. International Journal of Computer Science and Mobile Computing. 2017; 6(10):26-34.

[120]https://azure.microsoft.com/en-us/overview/iot/?site=mscom_iot. Accessed 13 June 2018.

[121]Kumar G. Evaluation metrics for intrusion detection systems-a study. Evaluation. 2014; 2(11):11-7.

Hassan I. Ahmed received the B.Sc. (Hons.), M.Sc. degrees in Computer Science and Engineering from Tanta University and Menoufia University, Egypt, in 2005, and 2010, respectively. He is currently a Ph.D. student and Assistant researcher at Department of Informatics, Electronics Research Institute, Cairo, Egypt. His current research interests include Neural Networks, Intrusion Detection Systems, Network Security, Big Data Analytics and IoT.
Email: Hassanibrsayed@gmail.com

Abdurrahman A. Nasr is a Lecturer of software engineering, Computer and System Engineering Department, Faculty of Engineering, Al-Azhar University at Cairo. He received his M.Sc. and Ph.D. degrees in Electrical Engineering from Al-Azhar University in 2012, and 2014 respectively. His fields of interest include Artificial Intelligence, Stochastic Process, Machine Learning, Data Mining, Mathematics, Operating Systems and IoT.
Email: anasr@azhar.edu.eg

Salah M. Abdel Mageid received his M.S. and Ph.D. in Systems and Computers Engineering from Al-Azhar University in 2002 and 2005, respectively. He is currently a Professor in Computer Engineering Department, College of Computer Science and Engineering, Taibah University, Saudi Arabia. He performed his post-doctoral research in 2007 and 2008 in the Computer Science and Engineering Department, School of Engineering, the Southern Methodist University at Dallas, TX, USA. He was a member of TEMPO (Tool for Extensive Management and Performance Optimization) project in Cairo University and Vodafone Egypt as an industrial partner in 2014 and 2015. His research interests include Mobile Computing, Cellular Networks, Sensor Networks, Cognitive Radio Networks, Vehicular Ad-hoc Networks, Big Data and Data Analysis, Internet Services and Applications.
Email: sabdelmageid@taibahu.edu.sa

Heba K. Aslan is a Professor at Electronics Research Institute, Cairo-Egypt. She received her B.Sc. degree, M.Sc. degree and Ph.D. degree in Electronics and Communications Engineering from the Faculty of Engineering, Cairo University, Egypt in 1990, 1994 and 1998 respectively. Aslan has supervised several masters and Ph.D. students in the field of computer networks security. Her research interests include: Key Distribution Protocols, Authentication Protocols, Logical Analysis of Protocols and Intrusion Detection Systems.
Email: hebaaslan@yahoo.com