A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT

Abdul Wahab Ahmed
Departmen of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan

Mian Muhammad Ahmed
Departmen of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan

Omair Ahmad Khan
Departmen of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan

Munam Ali Shah
Departmen of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan

***Abstract*—Internet of Things referred as a pervasive network architecture which provides services to the physical world by processing and analyzing data. In this modern era Internet of Things has been shown much significance and rapidly developing by connecting heterogeneous devices with various technologies. By this way interconnectivity of large number of electronic devices connected with the IoT network leads the risk of security and confidentiality of data. This paper analyzes different security issues, their counter measures and discusses the future directions of security in IoT. Furthermore, this paper also discusses essential technologies of security like encryption in the scenario of IoT for the prevention of harmful threats in the light of latest research.**

***Keywords*—Internet of things; security threats; countermeasures; privacy**

I. Introduction

The term Internet of things (IoT) was firstly used by Kevin Ashton in 1999 [1] in the term of supply chain management but now it is used in a general perspective. We only do not get information from the internet but it follows the protocols the internet use to store information. It is estimates that in 2020 there will be 50 billion smart objects and devices as shown in Figure 2 so each person will have 6.6 physical devices which are very large in number [2]. Due to use of modern technology like RFID and Greenhouse monitoring etc a very rapid development arises in IOT but there is issue regarding privacy and security in different layers. Figure 1 gives an overview of IoT with its connectivity.

The enhancements of wireless sensor network are widely popular by some of its prospects and new discoveries. IOT refers to the communication between physical devices like smart phones and some other smart objects that exchange data and give useful services via internet [3]. Some applications (For Example: Greenhouse monitoring, Smart meter and grids) evolve much popularity through IoT. Mainly IoT is generated by some of its important components that contain sensing, varied access, processing of information (RFID, GPS etc) and some other components like its security.

The objective of IoT is to make interconnection between machines. Thus IoT surrounds and connects the real world through these physical devices which are embedded with different types of sensors [4]. The word "things" in IoT cover a wide range of physical objects and also includes several electronic devices including RFIDs, GPS and NFC etc.

The security of essential information on IoT should incorporate into different features such as identification, data privacy and confidentiality etc. So with the rapid development and a mixture of heterogeneous devices, it formulates very large scale of IoT infrastructure [5]. So it is predicted that IoT is feared to be under threats on its versatile technology and future capabilities [6]. The security threat to IoT such as Denial of Service, Brute Force, Man in the middle attacks and many other attacks are envisaged in the interconnected network. These attacks occurs because of weak password, no encryption, personal information leakage etc so storage of such confidential data on cloud in quite alarming.

If such security attacks are not solved to some safe level then this weak security services can be harmful for the market of IoT. It not only involves such security issues but also have some access control issues, authentication of various network and some information store problems [7]. This problem needs to have a well defined security infrastructure that can address these problems and reduce the security challenges [8].

A. Physical Layer

Physical layer deals with the physical environment and collects all the data obtained from real world with the help of sensor nodes and other physical devices. This layer is responsible for communication between various physical devices. The objective of this layer is to provide services to the network and authentication of devices. The main devices [9] in physical layer includes Arduino, ZigBee, Barcodes, RFID and all other type of sensors. Each device in IoT system must have a unique tag which allows strong connection to the network and mostly Universally Unique identifiers (UUID) are used in the whole network by various devices. Uniformly a device can

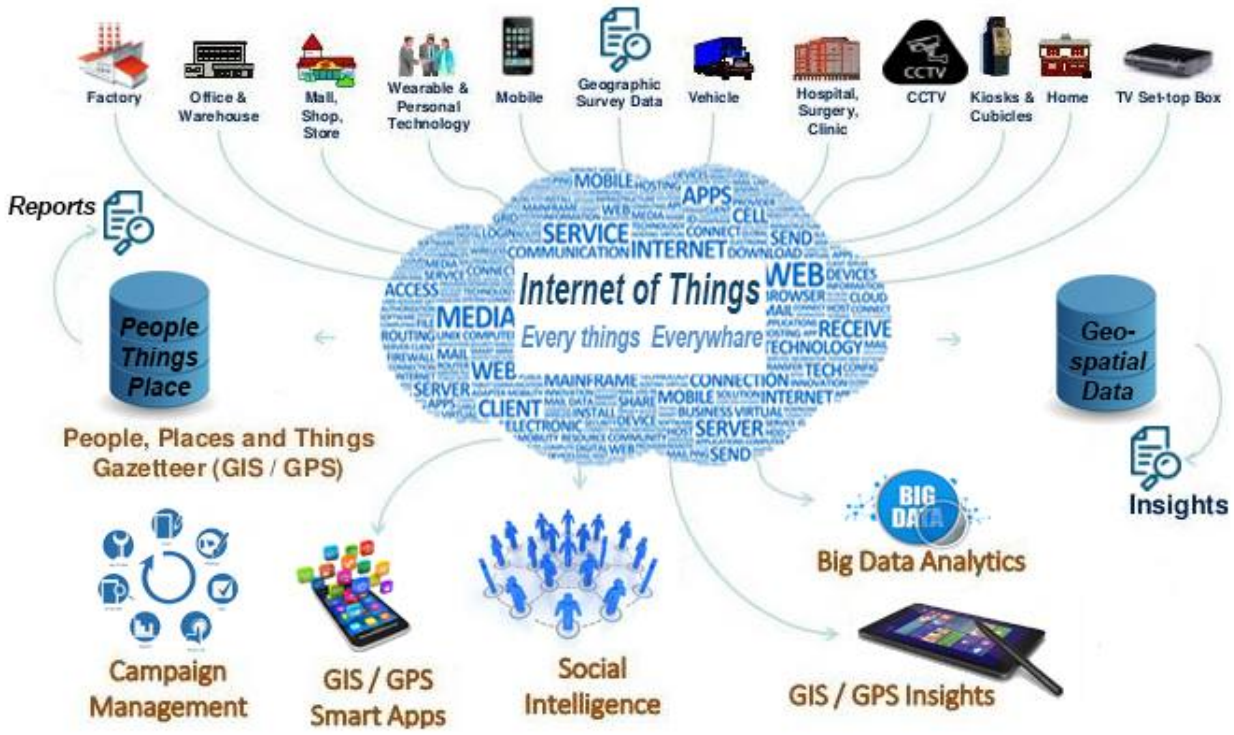

Fig. 1. IoT Diagram

be connected with many sensor nodes with unique ID because of uniquely identification of objects. Network layer carries the collection of transmitted information and transferred to central processing system.

B. Network Layer

Network layer is responsible for communication between different physical devices, management of network and also for maintenance of information through many communication protocols in an IoT system. There is not yet any fix protocol for IoT but most common protocol now a day used is MQTT 3.1 and CoAP (Constrained Application Protocol). With the help of Wireless Sensors, the main objective of the network layer is that it gathers information which is obtained from physical layer which is further transferred to information processing unit. Every device in the IoT network sends its private information with the help of wireless sensors [10]. The network layer carried transferring of information on the network of IoT. Hence reliable and secure transfer of data is done by this layer from physical layer to other layers.

C. Processing Layer

The working of processing layer is to combine the network and physical layer. Due to large amount of data it is very essential to store and process this data by associating with database for storage capabilities. Processing layer can automatically evaluate information and process data onto the basis of intelligent computing. Hence all the ubiquitous computing and intelligent processing function performed in this layer which is initial technology in this layer, so future technologies of this layer will more suitable for IoT. For this reason, the innovation of future technologies of this layer will be helpful for evolution of IoT system.

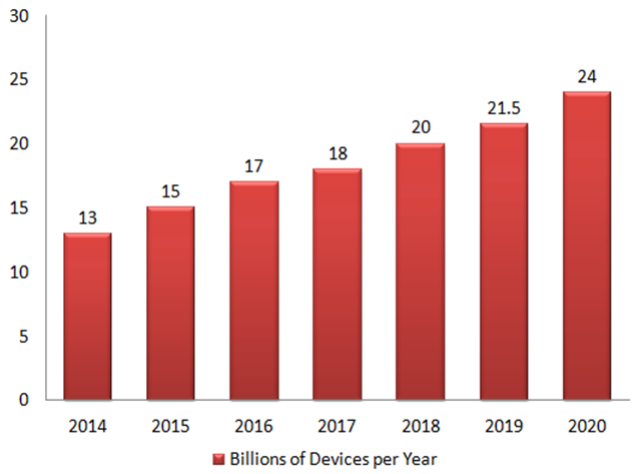

Fig. 2. Year Wise Growth in IoT Devices

D. Application Layer

The application layer is service oriented layer which provides context-aware services between connected devices in a pervasive way for end users. The processed information on

processing layer gives a platform to application of IoT which facilitates the user needs in various ways like transportation, communication and smart hospitals etc

This paper aims to discuss security of four layered architecture of IoT as shown in Figure 4. This paper also discusses different security features, security challenges of these layers and on the bases of former research different security aspects has discuss like cryptography, communication security, protecting sensor data and outline the challenges briefly. Rest of the paper is organized as follows. Section II provides a brief overview of the security threats to each layer and their countermeasure. Section III describes the countermeasures against each attack. Section IV provides the performance evaluation is done on the basis of the literature and in Section V gives the description work done in the paper is concluded.

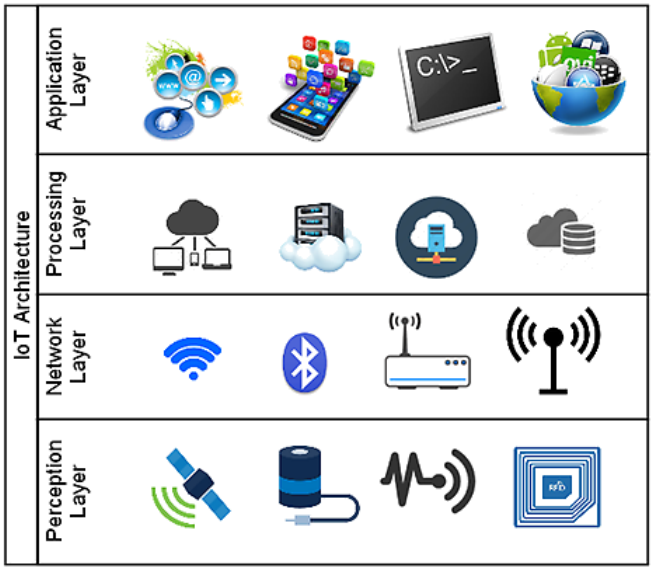

Fig. 3. IoT Layered Achitecture [86]

II. ATTACKS AT DIFFERENT LAYERS

In this section various security threats which threaten the confidentiality of data and their possible countermeasures on each layer which are suggested recently are briefly discussed as shown in figure 3.

A. Physical Layer

Physical layer composed of various enabling sensor technologies such as Bluetooth, GPS and Zigbee which are unprotected to different types of attacks. This type of attack is implemented [11] on the hardware parts of the IoT network and the adversary needs to be close to the IoT systems. Table 1 analyzes briefly on physical layer attacks.

1) Node Tempering: This type of attack may destroy the sensor node or cause damages by physically sending and receiving complete node or component of hardware or even electronically examine the nodes to get access and change sensitive information [12]. For Example:-shared cryptographic keys or influence the process of higher communication layer.

2) Jamming of node in Wireless Sensor Network: Node Jamming is much more popular in wireless sensor networks and is similar as in RF Interference attack explained above. This type of attacker gets involved in radio frequencies of wireless sensor nodes [13] and then afterwards it blocks the signals which stop the communication of nodes. When attacker successfully handles the blockage in key sensor nodes then it can stop service to IoT [14]. DoS attack can disturb RF signals by sending a large number of noisy signals which disrupt the network which in turn causes RF jamming.

3) RF interface on RFID: Dos attack can be impose on any tag of RFID. Denial of service attack implemented by sending noisy signal across radio frequency signal [15] when these noisy signals implemented on RFID then it stops communication.

4) Malicious Node Injection: This type of attack is also known as man in the middle attack. The attacker can actually set up a new malicious node between the sender and receiver node by this mechanism it controlled all the data [16] from one end to another in IoT system.

5) Physical Damage: The attacker can damage the network of IoT by attacking on the devices for its own purpose. This type of attack deals with the security that hosts by IoT system. This type of attack is different from Node Tempering attack [17] because in this attack attacker tries to directly damage the IoT services.

6) Social Engineering: In this type of attack the adversary can exploit the user of IoT system, to get useful and secret information and to achieve task by extracting that type of private information [18]. This type of attack is categorized into physical attack because the attacker physically communicates with the network of IoT to serve his task.

7) Sleep Deprivation Attack: Many sensor nodes are activated and perform its functions by replaceable batteries in IoT system and these sensor nodes are programmed to follow some functions such as sleep routines for the enhancement of their battery lifetime. This type of attack keeps the sensor nodes busy all the time [19] and will result in more battery consumption.

8) Malicious Code Injection: In this attack the adversary can physically insert a malicious program into a node and by implementing this attack into a node it would get access of the whole IoT system [20]. For Example: An attacker inserts any plug and play device into a node with harmful virus then it would gain full access of that node and control all the IoT system.

9) Unauthorized Access to the Tags: In this type of attack the adversary can get access to any of the tag without any authorization. This can be done due to the inadequacy of proper authentication procedure in RFID system [21]. The attacker cannot only access the data but can modify or even delete the complete information or data.

10) Tag Cloning: In IoT system, tags are deployed on various physical objects which are visible and thus data can be read and also modified [22] by some hacking techniques. So the crucial data can be easily accessed by any cybercriminal that can discover duplicate tag and hence the user cannot distinguish between duplicate and original data.

Fig. 4. Attacks and CounterMeasures on the Layers of IoT

11) Eavesdropping: In this type of attack the attacker can easily get confidential information such as password or some other data which are flowing from tag to user or user to tag [23]. This type of attack can happen because RFID has wireless characteristics.

12) Spoofing: In spoofing the adversary spreads false information on the RFID system and assumes this as original and makes that the data is appearing from original source [24]. Hence by this the attacker captures information and gets complete access to network.

13) Timing Attack: Another threatening attack of the confidentiality of the system is timing attack in which the attacker can get access of encryption key by analyzing the time which is required to do the [25] encryption task. Side Channel is also type of timing attack in which the adversary attacks on the encryption devices when there is leakage of information on the duration of device operation [26] like power consumption, processing or electromagnetic radiation etc.

14) Node Capture Attack: In node capture the attacker captures all private data and information by completely controls the node [27]. The adversary can add duplicate node to the network and by sending malicious data it threatens the confidentiality of the data.

15) Replay Attack: The privacy of the perception layer can be easily exploited by this type of attack. The adversary alters or replays the node by spoofs the information like identity and location etc of the node in the IoT system [28].

16) Routing Threats: The attacker can generate routing loops by altering and false routing information, [29] blocks the transmission of network and enlarge the network path by sending lot of error messages hence it increase point to point delay etc.

B. Network Layer Attacks

In the network attack the adversary needs to concentrate on the network of the IoT system and the attacker does not need to be close to the network of IoT. Table 2 analyzes briefly on the network layer attacks.

1) Traffic Analysis Attack: Traffic analysis attack is the main security attack on the network layer when using any web browser. The adversary can access secret information and other useful data which are from RFID technology because of its wireless attribute. Before applying this attack the attacker initially captures information and data about the connected network [30]. This work is accomplishing by using some sniffing operations such port scanning applications, packet sniffer applications etc.

2) RFID Cloning: In this type of attack the adversary can access of useful data by mimic RFID and copying data from valid RFID to another RFID tag [31]. This type of technique does not physically simulate an original RFID tag and differentiate between composed and original, dissimilar in the case of spoofing attack on RFID.

3) Malicious Code Injection: This type of attack causes severe effect to the network of IoT or even may block the complete network. In this attack, [30] the adversary injects a malicious code in to a system by comprising a node. So the attacker gains full control on IoT network.

4) Sleep Deprivation Attack: In Wireless sensor network the sensor nodes are charged with batteries which are not compatible because life time of such batteries is not so efficient so sleep routine procedure is used to the nodes to enhance the lifetime of battery [32]. In sleep deprivation attack the adversary keep battery awake which result in more battery consumption and at last it shut down the sensor nodes.

5) RFID Spoofing: In this attack the adversary captures the transmission of data by spoofing the signals of an RFID. Then making it to be authentic the attacker transmits his own data which have original ID [33] of RFID tag, hence by showing to be the actual source the attacker can access the IoT system.

6) RFID Unauthorized Access: In RFID systems, getting access of tags is very easy for anyone because mostly in the RFID system it lacks the established procedure or any system of authentication [34]. Thus it clearly means that attacker can change, read or delete the information of sensor nodes.

7) Sinkhole Attack: The attacker generates a sinkhole and tempts all traffic which is from the nodes of wireless sensor network. In the sinkhole attack it harms the confidentiality and privacy of data and by stopping the transmission of packets [35] rather than sending to its destination it denies the resource to the network.

8) Man In the Middle Attack: The adversary can have access to confidential data, breaching the privacy between nodes by controlling, monitoring [36] the network and cause interference in the communication between two sensor nodes. Dissimilar to the types of physical attack, the attacker not need to be physically close but in network layer it must concentrate on the communication of network protocol between one node to another in an IoT system.

9) Denial of Service: In denial of service attack the adversary can attack on the network of IoT by sending much traffic data. It controls all the data leads to well settle denial of attack. In this type of attack the user is unable to utilize its resource over the network [37].

10) Routing Information Attack: In this type of attack the attacker spoofs and changes the information about routing. Arise complexity of the network build a routing loops, sending false messages, sending errors, separate the network and drop traffic signals which result failure of sending data onto its destination [38]. Hello Attack is the example of such type of routing information attack.

11) Sybil Attack: It is a type of malicious attack in which a neighboring node in wireless sensor network accepts false information. This type of network layer [33] attack (Sybil Attack), it claims to hold the identification of large number of nodes. For Example: A Sybil node voted by many nodes rather than one node in the wireless sensor network.

12) Wormhole attack: Relocation of bits can be done from the original place of bits in network [39]. The mechanism of relocation is done from that channel of bits where there is link with low latency.

13) Hello flood attack: In hello flood attack the attacker sends useless messages from one node and causes a traffic jamming and block the channel in the network. Only a single malicious [40] node can do this and cause blockage of entire network by creating large number of traffic.

Attack Name	References	Effects	Countermeasures	Countermeasure Reference	Countermeasure Description
Node Tempering	[10]	Alter sensitive information by damaging sensors	Physically secure Design	[76]	Physically Secure Designing of devices should not be changeable and not be of high quality.
Jamming node in WSN	[40]	Communication blockage between the nodes	IPSec Security channel	[77]	Node tempering and eavesdropping can be stopped by encryption and authentication which ensures confidentiality of data
RF interface on RFID	[12]	Stop communication by distortion in signals	Device Authentication	[41]	A new physical device before sending and receiving of data the device should authenticate itself
Malicious node injection	[13]	Create interruption in transmission process	Secure booting	[42]	Secure booting is done by cryptographic hash algorithm which checks the software on the devices by digital signature
Physical Damage	[14]	Attacking on devices and cause damage to the IoT network	Risk Assessment	[64]	provides confidentiality of data and avoiding security breaches in an IoT network
Social Engineering	[15]	Leakage of private information	Data privacy	[47]	when data is sending to the destination it avoids the attacker to access the essential data
Sleep Deprivation Attack	[16]	Shutdown of nodes	Device Authentication	[41]	Without any authentication the device cannot enters or connect with other node in the IoT system
Unauthorized Access to the Tags	[36]	Modify or delete the entire information	Device Authentication	[41]	With the help of Device Authentication, unknown device cannot communicate in the IoT network

Table 1. Physical Layer Analysis

14) Selective forwarding: In selective forwarding only compromised node can transmit data onto its destination. The attacker selects and restricts the nodes to achieve his malicious purpose and hence some nodes cannot forward the data packet [41].

C. Processing Layer Attacks

The processing layer consists of different type of technologies like data storage and data processing. Cloud attack is the most significant kind of attack in IoT system and the security threats in this layer which makes network vulnerable are analyzed in Table 3

1) Unauthorized Access: Processing layer provides data storage and various functionalities in applications processing task [42]. In this attack, the adversary can easily access services of the system in authorizing manner and deleting the crucial data which can cause lots of damage to the IoT network.

2) Malicious Insider: This is insider attack in which the attacker from inside the [43] organization attacks by altering the data because of his own purpose. In this attack the data can be easily modified and extracted from purpose of the inside user.

3) Application security: In context of application security, Software as a service (SAAS) provides available software and

Attack Name	References	Effects	Countermeasures	Countermeasure Reference	Countermeasure Description
Sinkhole Attack	[22]	Data leakage from the nodes	security aware ad hoc routing	[78]	Stops inside attacks from the network of IoT and the adversary is dropped from the network
Traffic Analysis Attack	[18]	Leakage of secret information about the network of IoT	Routing Security	[49]	Routing security is used for data confidentiality. In this technique transmitted data is stored in packets after the analysis of data it then sent to the processing
RFID Cloning	[19]	Access useful data by mimic RFID	Authentication	[48]	With the help of proper authentication mechanism. Cloning of RFID can be prevented
RFID Spoofing	[20]	Controls transmission process and data manipulation	GPS system technique	[79]	Encounter the spoofing attack
Wormhole Attack	[31]	Relocation of bits in the network	Routing protocol	[80]	Routing protocol is used to produce the multiple paths between the sender and receiver and checks the presence of route.
Hello flood Attack	[32]	traffic jamming and channel blockage	Hello flood Detection cum Prevention	[81]	a node sends hello message to check the strength of signal if strength is similar as in radio range then receiver accept the message
Routing Information Attack	[25]	Destruction of network by routing loops	Encrypting Routing Tables	[51]	OWAS identifies different security issues on web by encryption process in rout.

Table 2. Network Layer Analysis

data on cloud through internet. The adversary in IoT system can easily steal data [44] and can operate malicious activities by using internet. Their security problems are much different than normal network security problems. Open Web Application Security Project (OWASP) has identified many web services and security issues in SAAS.

4) Data security: To provide and ensure data security to the user is a major responsibility for SAAS provider. Many security problems occur to the backup of data onto the service provider [45] because data backup is performed by other party which can cause data theft.

5) Underlying infrastructure security: In Platform as a Service (PaaS), the developers cannot access the lower layer and the security of this layer is the responsibility for service providers [46]. The objective of developer is to maintain a secure application of IoT but security of the lower layer remains unprotected and cause vulnerability.

6) Third-party relationships: PaaS can also provide many third party components like mushups [47]. There is combination of many sources of mushups so it increases security issues of data and network.

7) Virtualization threats: Security of virtual machine is very important as other machines and the occurrence of any damage to machine affects the other. In this layer virtualization is very insecure about many kind of attacks [48].

8) Shared Resources: Same resource sharing and utilization in virtual machine can cause a various security threats in IoT network [49]. The adversary controls all the resources

Attack Name	References	Effects	Countermeasures	Countermeasure Reference	Countermeasure Description
Virtualization threats	[57]	Damaging the resource	Hyper Safe	[70]	Hyper Safe used for protection of the memory pages from being altered
Shared Resources	[58]	Unauthorized user can control the resources	Homomorphic encryption	[68]	cipher text is allowed to compute immediately without decryption
Application security	[51]	Data theft	Web Application Scanners	[50]	Discovery of various threats which is present on the front end of web
Data Security	[54]	Leakage of confidential data because data on Cloud	Fragmentation redundancy scattering	[67]	data on cloud is splits and allocates in to various fragments for storage in servers
Underlying infrastructure security	[55]	lower layer remains unprotected	Fragmentation redundancy scattering	[67]	Data divides and allocate to different fragments for storage
Third-party relationships	[56]	Data leakage	Encryption	[69]	In Encryption, Data is firstly encrypted and then sent to the cloud

Table 3. Processing Layer Analysis

which are shared between virtual machine by using covert channels. So sharing of data might threaten by data theft.

D. Software Layer Attacks

Software attacks are the major challenges arises in the IoT system. Software attacks are used to damage the system resources by using harmful viruses and attacks such as Trojan horse, worms, spyware etc that can breaches [50] the confidential data, altering data, damage the IoT devices and get access to useful information. Table 4 discussed its effects on IoT.

1) Phishing Attack: In this type of attack the adversary can capture useful information [51] and access of private data by spoofing authentication authorization of user. These attacks used to steal login credentials, information of credit card etc.

2) Virus, Worms, Trojan Horse and Spyware: The attacker affects the system of IoT by injecting malicious software in the system [52] which results in varying outcomes. These types of attacks harm the system by denying its services, altering data and get access to confidential data.

3) Malicious Scripts: In the IoT system usually devices are connected and communicating with each other via internet. The system occurs to a complete shutdown [53] when user monitors the gateway and runs the active-X script. This type of scripting occurs to web applications and is use to control the access and theft of data.

4) Denial of Service: The adversary can affect all users in a network of IoT system by injecting denial of service attack of the network of IoT by application layer hence unauthorized user can get access to systems information [50]. This type of attack also blocks the authorized users for communication with application layer. The attacker can get full access to the application layer.

5) Data Protection and Recovery: Privacy of user is involved in the communication with data. By improper procedure and algorithm of data processing the confidential data can be lost or may even cause a catastrophic damage [54].

E. Encryption Attacks

In IoT system these types of attacks is entirely using for breaking the procedure of encryption techniques.

1) Cryptanalysis Attack: The purpose of this type of attack is to retrieve the encryption key which is being used for breaking the mechanism of encryption in IoT system [55]. Cryptanalysis Attacks let the possession of plaintext. Chosen-plaintext attack, Known-plaintext attack, Ciphertext-only attack and Chosen Ciphertext attack are some examples of cryptanalysis attack.

2) Side channel Attack: In this type of attack, the attacker can find the encryption key which is used for the purpose of decrypting and encrypting data [56]. By this way the adversary can get access to hacked data by using some particular techniques such as Electromagnetic analysis and power..

3) Man In the Middle Attack: During a mechanism of challenge-response when two authorized users in an IoT network establishing a secure communication [57], then this time an attacker position himself and intercepting the signals. The adversary can also interfere in the communication between the users by exchanging the keys and then the attacker will able to perform encryption or decryption.

III. COUNTERMEASURESAT DIFFERENT LAYERS

In this section countermeasure of the above mention attacks are discussed.

A. Physical Layer Security

Physical Layer is the bottom most layer of IoT network which provides different features of security to the hardware. Security at physical layer is discussed in four various types as discussed below:

1) Secure Physical Design: In Physical Layer most of the threats are resolved by designing the devices which are physically secure. Designing of such component [58] like acquisition unit, radio frequency circuits etc should not be changeable and not be of high quality. In WSN the design of antenna is physically secure and has ability to communicate over long distance.

2) Device authentication: When a new physical device enters in to the IoT network, then before sending and receiving of data the device should authenticate itself [59]. When the device has accurately identified then the system always keeps the malicious devices out of the network.

3) Secure Booting: Authenticity and originality of the software can be checked by applying cryptographic hash algorithm. This algorithm verifies the software on the devices by digital signature [60]. Many cryptographic hash algorithms cannot be implemented because of low processing capability on many devices. Some cryptographic hash algorithm such as NH and WH cryptographic algorithm are suitable for some devices which has low utilization of power.

4) Data Confidentiality: In data confidentiality all tags and data of each physical device should be encrypted before sending the data to provide confidentiality [61]. Strong technique of cryptographic encryption such as AES cannot be applied because power consumption is low. So Blowfish or RSA can be applied on these devices because these techniques have low processing power.

5) Data integrity: To avoid the tempering of sensitive data, the technique of error detection [62] is provided at each physical device. Better error detection techniques can be applied such as WH cryptographic hash method but it refers to that type of mechanism which have ability to utilize low power such as Cyclic Redundancy Checks (CRC) and parity bit.

6) Data Privacy: Symmetric and asymmetric encryption function like DSA, RSA, BLOWFISH and DES etc guaranteed data privacy by preventing the attacker to unauthorized access of essential data when data is sending to the destination. These encryption algorithms can be easily applied because of their less consumption of power.

7) Risk Assessment: Dynamical Risk Assessment technique provides confidentiality of data and avoiding security breaches in an IoT network [63]. It is essential for security perspective of IoT by discovering different types of threats to the network. When an error is discovered with such security strategies than RFID runs an automatic kill command of tags of RFID which stops unauthorized access to data.

8) Privacy of sensitive information: Privacy of sensitive information is the most crucial concept for providing security to the data onto the system. With the help K-anonymity [64] technique it provides mechanism to hide the sensitive information on the system hence anonymity of identity is achieved by providing protection for the information such as location and identity etc.

9) Anonymity: Identification of nodes and hiding of private information like data address and location are very important for confidentiality. Zero-Knowledge technique [65] would be the best solution for anonymity but it has a drawback that having a large processing power because of strong algorithm it cannot be implemented on the devices which have less consumption power. So K-anonymity is a best approach for less power physical devices in IoT network [66].

10)IPSec Security channel: IPSec Security channel has two types of secure functionalities, encryption and authentication which provides security [67]. Node tempering and eavesdropping can be stopped by encryption which ensures confidentiality of data. The receiver can identify that the sender of the data onto IP is fake or real.

B. Network Layer Security

The network layer is threatening by many types of attacks. Due to the observance of the many wireless channels, attacker can easily control the communication between devices. The security of network layer is splits in four types which are described below.

1) Data privacy: The safety control procedure control the network of any type of error occurs and hence integrity of data has applied to justified that data received to the user is similar to the original [68] like encryption of point to point. Authentication mechanism is used to avoid illegal access to data onto sensor node.

2) Security aware ad hoc routing: Security aware ad hoc routing (SAR) protocol prevents from inside attacks of the network [69] of IoT. Some security measurements are added to the packets and the adversary is dropped from the network after the analysis of received data.

3) Authentication: Illegal access of the nodes can be avoided with the help of proper authentication technique and encryption process [70]. In network layer the most common type of attack is DoS attack which can affect the network by spreading useless information.

4) Routing security: In many applications secure routing is essential for the sensor network. Due to the insecure routing protocols, different routing algorithms are applied to secure the confidentiality of data transferring towards various sensor nodes in IoT system [71]. However, multiple paths provide secure routing which fixed errors in the network and increase

Attack Name	References	Effects	Countermeasures	Countermeasure Reference	Countermeasure Description
Virtualization threats	[57]	Damaging the resource	Hyper Safe	[70]	Hyper Safe used for protection of the memory pages from being altered
Shared Resources	[58]	Unauthorized user can control the resources	Homomorphic encryption	[68]	cipher text is allowed to compute immediately without decryption
Application security	[51]	Data theft	Web Application Scanners	[50]	Discovery of various threats which is present on the front end of web
Data Security	[54]	Leakage of confidential data because data on Cloud	Fragmentation redundancy scattering	[67]	data on cloud is splits and allocates in to various fragments for storage in servers
Underlying infrastructure security	[55]	lower layer remains unprotected	Fragmentation redundancy scattering	[67]	Data divides and allocate to different fragments for storage
Third-party relationships	[56]	Data leakage	Encryption	[69]	In Encryption, Data is firstly encrypted and then sent to the cloud

Table 4. Application Layer Analysis

performance of the system. For routing purpose source routing is a technique in which transmitted data is stored in packets after the analysis of data it then sent to the processing.

5) GPS location system: GPS system encountered the spoofing attack from network layer of the IoT system [72]. S. Daneshmand et al. describe and implemented the GPS location technique which is the best solution proposed yet.

6) Routing protocol: Ad hoc On demand Multipath Distance Vector (AOMDV) is a routing protocol which encountered the wormhole attack [73]. Amish et al. propose this technique by producing multiple paths between the sender and receiver in every discovery of rout. In this technique route table is checked by the sender that for two nodes communication, route is available or not. If the rout is available then it provides information about routing rather it transmits the packet.

7) Hello flood Detection cum Prevention: Virendra et al. propose a technique to prevent hello flood attack in IoT. In this technique a node sends hello message to check the strength of signal if strength is similar as in radio range then receiver accepts the message and information about routing is sent to the rout [74].

8) Data Integrity: A cryptographic hash mechanism is used to for the integrity of data [75]. This function is used to check the transmission of data onto the other node. When tempering of data is proved error correction process can also be used.

C. Processing Layer Security

There are some concepts of security measures in processing layer which is discussed below:

1) Web application scanners: This application is using for identification of different threats [76] which is present in the front end of web. Other web firewall applications are also detecting the attacks of potential attacker.

2) Fragmentation redundancy scattering (FRS): In FRS the essential data onto cloud [77] is splits and allocates in to various fragments of storage in servers. The fragment has not any useful information about the data so risk of data theft is minimized in this scenario.

3) Homomorphic encryption: This technique is based on entire mechanism of homomorphic encryption. In this technique [78] cipher text is allowed to compute immediately without decryption. High computation requires for data security in this method.

4) Encryption: Encryption technique is used to ensure the data confidentiality in IoT. Data is firstly encrypted and then sent to the cloud. Encryption helps to overcome against side channel attacks [79]. There are various kinds of encryption such as Advanced Encryption Standard etc.

5) Hyper Safe: Hyper safe provides protection for the memory pages from being altered and also allows restriction of pointing index that changes monitored data onto the pointer indexes [80].

D. Application Layer Security

The categorization of security mechanism in application layer is discussed below:

1) Data security: For securing the confidentiality of data and privacy of entire IoT system Encryption, Authentication and Integrity are the most essential procedure at this level. It avoids any unauthorized access to the data and protecting data to be hacked or theft.

2) Access Control Lists (ACLs): Setting up the rules and allows request for the access and monitoring of the network is the important part which ensures the confidentiality of the system and data privacy [81]. ACL can manage by stopping or allowing incoming or outgoing traffic and monitors access requests from many users in the IoT system.

3) Intrusion Detection: Intrusion Detection process [82] provides security solutions to many threats by producing an alarm when any uncertain action is performed in the system because of continuous controlling a log of intruder's activity. Intrusion detection can be done by various detection techniques such as anomaly detection in data mining [83].

4) Risk Assessment: The risk assessment produces effective security approaches and gives enhancement of [84] already existing architectures and planning of security.

5) Firewalls: When encryption, authentication and ACLs process failed to block the unauthorized user then firewall comes in process [85] for the blockage. When weak password was chosen then encryption and authentication process can be failed. In firewall, filtration of packets is done hence unwanted packets are blocked by this process.

6) Anti-virus, Anti-spyware and Anti-adware: Software which provides security such as anti-virus, anti-spyware and anti-adware is essential for the confidentiality, reliability and integrity of the IoT network. IV. PERFORMANCE EVALUATION Evaluation of security threats on the network of IoT are done in this section and discuss their countermeasures. Furthermore, this paper mentions the effects of these attacks on IoT network and also presents separate countermeasures for which it reduces the damage of the IoT and prevention of vulnerability. Detail of our performance analysis is discussed in table.1 in which detailed analysis has been done on the basis of each attack.

IV. PERFORMANCE EVALUATION

Evaluation of security threats and their countermeasures to the network of IoT is discussed in this section. Furthermore, this paper mentions the effects of these attacks of IoT network and also presents separate countermeasures for which it reduces the damage to the IoT and prevention of vulnerability. Detail of our performance analysis is discussed in table.1 in which detailed analysis has been done on the basis of each attack.

V. CONCLUSION

IoT has been considered as an important research topic for the last few years where physical objects would communicate by using various network technologies. The vast advancement of the services of IoT requires the authentic and factual security mechanism. This paper gives a broad overview of IoT by describing the working of layers and then discusses different security loopholes on different layers of IoT (Physical Layer, Network Layer, Processing Layer and Application Layer). Furthermore it presents the countermeasures against security threats from the prevention of any damage to IoT network.As IoT is going to be an essential part of our life, steps should be taken to ensure security and privacy of the user.

REFERENCES

[1] Daniele Miorandi, Sabrina Sicarib, Francesco De Pellegrini, "Internet of things: Vision, applications and research challenges" survey paper September 2012, pp 1497–1516.

[2] Misra, Gourav, et al. "Internet of things (iot)–a technological analysis and survey on vision, concepts, challenges, innovation directions, technologies, and applications (an upcoming or future generation computer communication system technology)." American Journal of Electrical and Electronic Engineering 4.1 (2016): 23-32.

[3] Torğul, Belkız, Lütfü Şağbanşua, and Figen Balo. "Internet of Things: A Survey." (2016): 104-110.

[4] Kraijak, Surapon, and Panwit Tuwanut. "A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends." Communication Technology (ICCT), 2015 IEEE 16th International Conference on. IEEE, 2015.

[5] Sicari, Sabrina, et al. "Security, privacy and trust in Internet of Things: The road ahead." Computer Networks 76 (2015): 146-164.

[6] Alaba, Fadele Ayotunde, et al. "Internet of things Security: A Survey." Journal of Network and Computer Applications (2017).

[7] Geng Yang, Jian Xu, etc.: Security Characteristic and Technology in the Internet of Things. J. Journal of Nanjing University of Posts and Telecommunications (Natural Science). 30(4) (2010) (in Chinese)

[8] Andrea, Ioannis, Chrysostomos Chrysostomou, and George Hadjichristofi. "Internet of Things: Security vulnerabilities and challenges." Computers and Communication (ISCC), 2015 IEEE Symposium on. IEEE, 2015.

[9] A. Mukherjee, "Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints," Proc. IEEE, vol. 103, no. 10, pp. 1747–1761, 2015.

[10] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012, vol. 3, pp. 648–651, 2012.

[11] Pan, Yao, et al. "Taxonomies for Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems." International Journal of Interactive Multimedia & Artificial Intelligence 4.3 (2017).

[12] Kaushal, Kanchan, and Varsha Sahni. "DoS Attacks on different Layers of WSN: A Review." International Journal of Computer Applications 130.17 (2015).

[13] Wahid, Abdul, et al. "A Survey on Attacks, Challenges and Security Mechanisms in Wireless Sensor Network." International Journal For Innovative Research in Science & Technology 1 (2015).

[14] Sonar, Krushang, and Hardik Upadhyay. "A Survey: DDOS Attack on Internet of Things." International Journal of Engineering Research and Development 10.11 (2014): 58-63.

[15] Peris-Lopez, Pedro, et al. "attacking RFID systems." Security in RFID and Sensor Networks (2016): 29.

[16] Illiano, Vittorio P., and Emil C. Lupu. "Detecting malicious data injections in wireless sensor networks: A survey." ACM Computing Surveys (CSUR) 48.2 (2015): 24.

[17] Jacobson, Michael. "Vulnerable Progress: The Internet of Things, the Department of Defense and the Dangers of Networked Warfare." (2015).

[18] Ghafir, Ibrahim, et al. "Social engineering attack strategies and defence approaches." Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on. IEEE, 2016.

[19] Kumar, Sathish Alampalayam, Tyler Vealey, and Harshit Srivastava. "Security in internet of things: Challenges, solutions and future directions." System Sciences (HICSS), 2016 49th Hawaii International Conference on. IEEE, 2016.

[20] Farooq, M. U., et al. "A critical analysis on the security concerns of internet of things (IoT)." International Journal of Computer Applications 111.7 (2015).

[21] Da Xu, Li, Wu He, and Shancang Li. "Internet of things in industries: A survey." IEEE Transactions on industrial informatics 10.4 (2014): 2233-2243.

[22] Doinea, Mihai, et al. "Internet of Things Based Systems for Food Safety Management." Informatica Economica 19.1 (2015): 87.

[23] Rahman, Abdul Fuad Abdul, Maslina Daud, and Madihah Zulfa Mohamad. "Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework." Proceedings of the International Conference on Internet of things and Cloud Computing. ACM, 2016.

[24] Jeyanthi, N., Shreyansh Banthia, and Akhil Sharma. "Security in IoT Devices." Security Breaches and Threat Prevention in the Internet of Things. IGI Global, 2017. 96-116.

[25] Sadeghi, Ahmad-Reza, Christian Wachsmann, and Michael Waidner. "Security and privacy challenges in industrial internet of things." Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015.

[26] Babar, Sachin, et al. "Proposed embedded security framework for internet of things (iot)." Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on. IEEE, 2011.

[27] Roman, Rodrigo, Jianying Zhou, and Javier Lopez. "On the features and challenges of security and privacy in distributed internet of things." Computer Networks 57.10 (2013): 2266-2279.

[28] Jan, Mian Ahmad, and Muhammad Khan. "Denial of Service Attacks and Their Countermeasures in WSN." IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC) 3 (2013).

[29] Puthal, Deepak, et al. "Threats to Networking Cloud and Edge Datacenters in the Internet of Things." IEEE Cloud Computing 3.3 (2016): 64-71.

[30] Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. "Towards an analysis of security issues, challenges, and open problems in the internet of things." Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015.

[31] Sari, Arif. "Security issues in RFID Middleware Systems: Proposed EPC implementation for network layer attacks." Transactions on Networks and Communications 2.5 (2014): 01-06.

[32] Nia, Arsalan Mohsen, and Niraj K. Jha. "A comprehensive study of security of internet-of-things." IEEE Transactions on Emerging Topics in Computing (2016).

[33] Borgohain, Tuhin, Uday Kumar, and Sugata Sanyal. "Survey of security and privacy issues of Internet of Things." arXiv preprint arXiv:1501.02211 (2015).

[34] Cvitić, Ivan, Miroslav Vujić, and Siniša Husnjak. "Classification of security risks in the IoT environment." 26th International DAAAM Symposium on Intelligent Manufacturing and Automation. 2016.

[35] Jing, Qi, et al. "Security of the Internet of Things: perspectives and challenges." Wireless Networks 20.8 (2014): 2481-2501.

[36] Conti, Mauro, Nicola Dragoni, and Viktor Lesyk. "A Survey of Man In The Middle Attacks." IEEE Communications Surveys & Tutorials 18.3 (2016): 2027-2051.

[37] Zhang, Congyingzi, and Robert Green. "Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network." Proceedings of the 18th Symposium on Communications & Networking. Society for Computer Simulation International, 2015.

[38] Jing, Qi, et al. "Security of the Internet of Things: perspectives and challenges." Wireless Networks 20.8 (2014): 2481-2501.

[39] Pongle, Pavan, and Gurunath Chavan. "Real time intrusion and wormhole attack detection in internet of things." International Journal of Computer Applications 121.9 (2015).

[40] Yassen, Muneer Bani, Shadi Aljawaerneh, and Reema Abdulraziq. "Secure low energy adaptive clustering hierarchal based on internet of things for wireless sensor network (WSN): Survey." Engineering & MIS (ICEMIS), International Conference on. IEEE, 2016.

[41] Airehrour, David, Jairo Gutierrez, and Sayan Kumar Ray. "A trust-aware RPL routing protocol to detect blackhole and selective forwarding attacks." Australian Journal of Telecommunications and the Digital Economy 5.1 (2017): 50.

[42] Ye, Ning, et al. "An efficient authentication and access control scheme for perception layer of internet of things." (2014).

[43] Chen, Long. Security Management for The Internet of Things. Diss. University of Windsor (Canada), 2017.

[44] A. Razzaq, K. Latif, H. F. Ahmad, A. Hur, Z. Anwar, and P. C. Bloodsworth, "Semantic security against web application attacks," Inf. Sci. (Ny)., vol. 254, pp. 19–38, 2014.

[45] D. H. Patil, "Data Security over Cloud," Int. J. Comput. Appl., pp. 11–14, 2012.

[46] B. R. Chandramouli and P. Mell, "State of Security Readiness," Crossroads, vol. 16, no. 3, pp. 23–25, 2010.

[47] K. Hashizume, D. G. Rosado, E. Fernández-medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," pp. 1–13, 2013.

[48] N. Kilari and C. Applications, "A Survey on Security Threats for Cloud Computing," Int. J. Eng. Res. Technol., vol. 1, no. 7, pp. 1–10, 2012.

[49] K. Dahbur, "A Survey of Risks , Threats and Vulnerabilities in Cloud Computing," in International Conference on Intelligent Semantic Web-Services and Applications, 2011.

[50] Zhang, Zhi-Kai, et al. "IoT security: ongoing challenges and research opportunities." Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on. IEEE, 2014.

[51] Thakur, Himani, and Supreet Kaur. "A Survey Paper On Phishing Detection." International Journal of Advanced Research in Computer Science 7.4 (2016).

[52] Akbari Roumani, M., et al. "Value analysis of cyber security based on attack types." ITMSOC: Transactions on Innovation and Business Engineering 1 (2016): 34-39.

[53] Dorsemaine, Bruno, et al. "A new approach to investigate IoT threats based on a four layer model." New Technologies for Distributed Systems (NOTERE), 2016 13th International Conference on. IEEE, 2016.

[54] A. Viejo, "Systems and methods for reducing unauthorized data recovery from solid-state storage devices," Merry, Jr. al, vol. 2, no. 12, p. Merry, Jr. et al, 2011.

[55] Ndibanje, Bruce, Hoon-Jae Lee, and Sang-Gon Lee. "Security analysis and improvements of authentication and access control in the internet of things." Sensors 14.8 (2014): 14786-14805.

[56] Choi, Jaehak, and Youngseop Kim. "An improved LEA block encryption algorithm to prevent side-channel attack in the IoT system." Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2016 Asia-Pacific. IEEE, 2016.

[57] Conti, Mauro, Nicola Dragoni, and Viktor Lesyk. "A Survey of Man In The Middle Attacks." IEEE Communications Surveys & Tutorials 18.3 (2016): 2027-2051.

[58] B. Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber – Physical Security of a Smart Grid Infrastructure," Proc. IEEE, vol. 100, no. 1, pp. 195–209, 2012.

[59] Trappe, Wade. "The challenges facing physical layer security." IEEE Communications Magazine 53.6 (2015): 16-20.

[60] Lake, David, et al. "Internet of things: Architectural framework for ehealth security." Journal of ICT Standardization, River Publishing 1 (2014).

[61] J. P. Kaps, "Cryptography for ultra-low power devices." PhD diss., WORCESTER POLYTECHNIC INSTITUTE, 2006.

[62] Rault, Tifenn, Abdelmadjid Bouabdallah, and Yacine Challal. "Energy efficiency in wireless sensor networks: A top-down survey." Computer Networks 67 (2014): 104-122.

[63] C. Liu, Y. Zhang, J. Zeng, L. Peng, R. Chen, Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology, in Eighth International Conference on Natural Computation (ICNC), 2012

[64] K.E. Emam, F.K. Dankar, Protecting Privacy Using kAnonymity, in Journal of the American Medical Informatics Association, Volume 15, Number 5, 2008

[65] Flood, Padraig, and Michael Schukat. "Peer to peer authentication for small embedded systems: A zero-knowledge-based approach to security for the Internet of Things." Digital Technologies (DT), 2014 10th International Conference on. IEEE, 2014.

[66] Sun, Gang, et al. "Efficient location privacy algorithm for Internet of Things (IoT) services and applications." Journal of Network and Computer Applications (2016).

[67] D. Migault, D. Palomares, E. Herbert, W. You, G. Ganne, G. Arfaoui, and M. Laurent, "E2E : An Optimized IPsec Architecture for Secure And Fast Offload," in Seventh International Conference on Availability, Reliability and Security E2E:, 2012.

[68] Abomhara, Mohamed, and Geir M. Køien. "Security and privacy in the Internet of Things: Current status and open issues." Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on. IEEE, 2014.

[69] S. Sharmila, "Detection of sinkhole Attack in Wireless Sensor Networks using Message Digest Algorithms," IEEE, pp. 0–5, 2011.

[70] Zhao, Kai, and Lina Ge. "A survey on the internet of things security." Computational Intelligence and Security (CIS), 2013 9th International Conference on. IEEE, 2013.

[71] Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security for the internet of things: a survey of existing protocols and open research issues." IEEE Communications Surveys & Tutorials 17.3 (2015): 1294-1312.

[72] S. Daneshmand, A. Jafarnia-jahromi, A. Broumandan, and G. Lachapelle, "A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array," ION GNSS12 Conf., pp. 1–11, 2012.

[73] Amish, Parmar, and V. B. Vaghela. "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol." Procedia computer science 79 (2016): 700-707.

[74] Singh, Virendra Pal, Aishwarya S. Anand Ukey, and Sweta Jain. "Signal strength based hello flood attack detection and prevention in wireless sensor networks." International Journal of Computer Applications 62.15 (2013).

[75] Singla, Aashima, and Ratika Sachdeva. "Review on security issues and attacks in wireless sensor networks." International Journal of Advanced Research in Computer Science and Software Engineering 3.4 (2013).

[76] B. L. Suto, "Analyzing the Accuracy and Time Costs of Web Application Security Scanners," San Fr., no. October 2007, 2010.

[77] Y. Singh, F. Kandah, and W. Zhang, "A Secured Cost-effective Multi-Cloud Storage in Cloud Computing," IEEE INFOCOM, pp. 619–624, 2011.

[78] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," SIAM J. Comput., vol. 43.2, pp. 831–871, 2014.

[79] D. Koo, J. Hur, and H. Yoon, "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage q," Comput. Electr. Eng., vol. 39, no. 1, pp. 34–46, 2013.

[80] S. Kumar, S. Pal, A. Kumar, and J. Ali, "Virtualization , The Great Thing and Issues in Cloud Computing," Int. J. Curr. Eng. Technol., pp. 338–341, 2013.

[81] M. Ongtang, S. Mclaughlin, W. Enck, and P. Mcdaniel, "Semantically rich application-centric security in Android," Secur. Commun. Networks, no. August 2011, pp. 658–673, 2012.

[82] Animesh Patcha, Jung-Min Park, An overview of anomaly detection techniques: Existing solutions and latest technological trends, in Computer Networks, Volume 51, Issue 2, 2007

[83] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic and Marimuthu Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions."

[84] C. Liu and Y. Zhang, "Research on Dynamical Security Risk Assessment for the Internet of Things Inspired by Immunology," in 8th International Conference on Natural Computation, 2012, no. Icnc, pp. 874–878.

[85] S. L. Wiley, O. Park, and U. S. C, "Pin-hole firewall for communicating data packets on a packet network," 2011.

[86] M. M. Ahmed, M. A. Shah and A. Wahid, "IoT Security: A Layered Approach for Attacks & Defenses," in International conference on communication technologies, 2017,