Design a secure IoT Architecture using Smart Wireless Networks

Nourah Almrezeq[1], Lama Almadhoor[1], Thowg Alrasheed[1], A. A. Abd El-Aziz[1,2] and Shadi Nashwan[1]

[1]College of Computer and Information Sciences , Jouf University, Al Jouf, KSA
[2]Faculty of Graduate Studies for Statistical Research, Cairo University, Cairo, Egypt

***Abstract*:** The Internet of Things (IOT) is a revolution in the technology world, and this field is continuously evolving. It has made life easier for people by providing consumers with more efficient and effective resources in faster and more convenient ways. The Internet of Things is one of the most exciting fields for the future by 2030. 90% of the planet will be connected and all devices in homes and businesses around us will be connected to the Internet making it more vulnerable to violations of privacy and protection. Due to the complexity of its environment, security and privacy are the most critical issues relevant to IoT. Without the reliable security of the devices, they will lose their importance and efficiency. Moreover, the security violation will outweigh any of its benefits. In this paper, an overview of various layered IoT architectures, a review of common security attacks from the perspective of the layer, and the best techniques against these attacks are provided. Moreover, an enhanced layered IoT architecture is proposed, which will be protected against several security attacks.

Keywords: Internet of Things (IoT), IoT Architecture, Secure architecture.

1. Introduction

When you submit your paper print it in two-column format Internet of Things (IoT), is the revolution that will make almost everything around us connected to the Internet, such as smartphones, washing machines, and smart healthcare systems [11]. The IoT makes people's lives simpler, easier, and more comfortable; where tasks could be accomplished without the need for human cooperation and where activities could be carried out without a human being's need for cooperation. What makes the IoT stand out is that it helps people to be free from the place. That means, a person can monitor the tools without having to deal with a particular device in a specific location. The explosive growth of the IoT and the increased number of devices has contributed to the processing of Big Data, which must be collected and analyzed effectively to make a decision or to improve a specific service to various smart devices.

Given advantages, such as cost reduction, performance improvement and increased efficiency are provided by the IoT [7]. On the other side, the IoT faces a wide range of challenges and problems, such as storage management, complexity, network structure, and energy efficiency. One of the major challenges at the moment is to achieve a safe and easy access control scheme for the information handled in these facilities [15]. The IoT is a mixture of technology, security, and privacy issues of these technologies. It must be safeguarded and dominated. Privacy infringement is also a nightmare on the IoT as the unauthorized use of data leads to a breach of users' privacy. IoT must ensure the security and the privacy of its users to gain the trust of the user. The problems of defending the IoT are discussed in many researches [6]. In this research, several improvements are proposed to the layered architecture of the IoT to keep pace with the rapid development of the IoT and to increase the volume of data that needs to be stored and processed. Furthermore, to comply with the safety and protection requirements. The existing research have an insufficient discussion of the security layer of IOT. This elaborates need to highlight and thoroughly review the largest number of IoT attacks in each layer and how to protect IoT from these attacks. The distance from the viewpoint of the layers is dropped in this research by defining and addressing security issues.

The rest of the paper is as the following structure: Section 2 provides a summary of the literature related to IoT architecture. Section 3 explains the proposed architecture and addresses in depth the major security problems and concerns on each layer as well. Section 4 deals with the practical implementation of some categories of attacks and checking their behavior. Section 5 describes and discusses the results of the implementation. The conclusion is presented in section 6.

2. Literature Review

The architecture of the IoT defines components, how they work, and how data is exchanged between them [14]. Security problems will be counterproductive and harmful to the services provided by the Internet of things. This great problem needs to be solved to take advantage of the services of the Internet of things to the fullest. Therefore, a secure infrastructure that identifies problems and explores the best protection methods is needed [5].

Given the various literature related to the Internet of Things architecture. It might be assumed that between all the researchers there is no set architecture and agreement. Various literature bodies have been proposed and many various IoT systems have been remodeled [17] by developing IoT and fulfilling the specification, security and privacy requirements. In the first stage of IoT's development, the three-layer architecture was introduced. This consists of three basic and simple layers called: perception layer, network layer, and application layer shown in Fig.1. Such layers have been explained in detail in [16] [17].

Because IOT is facing several security challenges, the three-layer architecture previously is enhanced to four-layer architecture. The four-layer architecture has been developed by adding only one layer called support layer to improve security and privacy levels [17]. Further through the defects encountered by the three basic layers, the support layer has been added. This support layer is an intermediary layer between the sensor layer and the network layer which helps verify that the data has only been sent by licensed entities and then transfers the information to the network layer

[17][20]. While some found promoting IoT frameworks as a friendly and an efficient forum. It has been categorized by researchers as a layer that provides sufficient cloud storage to avoid limitations on limited devices [11] shown in Figure 1.

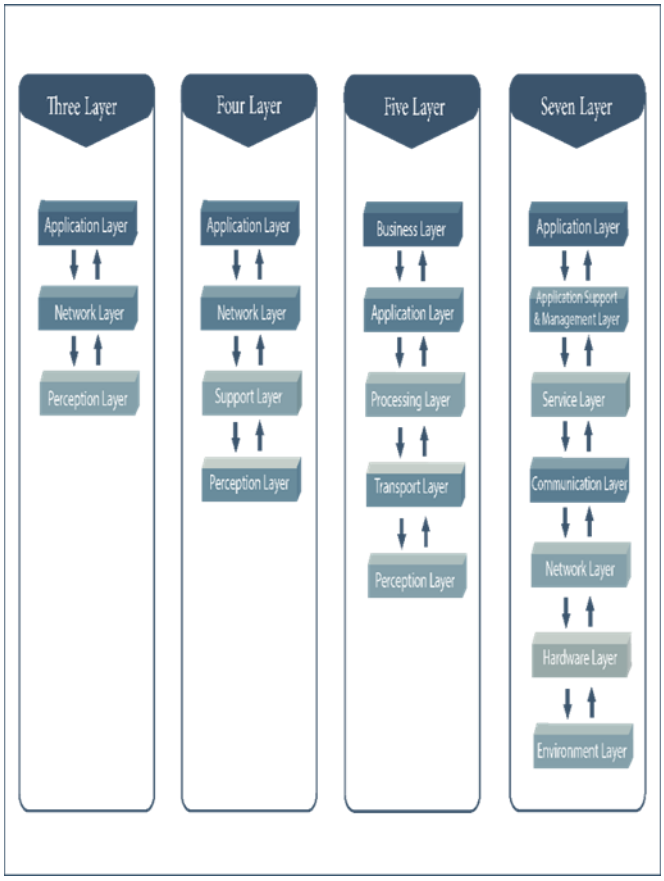

Figure1. The Layered Architectures of IoT

Although the researchers were persuaded that the layer of support was introduced to meet the requirements of protection and applications, another design was suggested which differs from the architecture of the four layers where the support layer was overlooked and two additional layers were added to the architecture of the three basic layers. These two layers called processing layer and business layer. The processing layer is responsible for data analysis, data mining and extraction of important data from big data and the business layer is responsible for the whole system and considered as the application manager [17] shown in Figure 1. They proposed in [6] according to the opinions of the latest researchers on IoT architecture. It includes seven layers of architecture, but this design is a kind of feature distribution on each layer and does not increase the level of protection, because there's no a layer from the seven layers addresses the limited storage problem nor a layer to analyze a large amount of data.

Security is one of the most difficult challenges facing the IOT. Hence, there is no single architecture. The proposed security solutions for a particular architecture may not be appropriate for another, due to the different types of attacks [18]. Layers play a big role in protecting the Internet of Things. Therefore, these layers must be protected and be safe to ensure the safety of these devices from loss and tampering with data [27].

Several researchers have reviewed security problems from the perspective of the four-layer architecture considering this is a wide and general architecture [5][8][11][18][20]. While, in [17] security problems are reviewed in three, four, and five-layer architecture. However, the description of security techniques has been shortened only to the traditional three-layer architecture.

The [26] presents the security features of each layer of the four-layer architecture with focusing on discussing the perception layer in detail. After the classification of the risks facing each layer, the author stated that the greatest risk facing the perception layer is the specific limitations of the technology used in this layer.

One of the most important features of the four-layer architecture is the presence of a layer of support for storage. It seems that only cloud technology can effectively meet the storage requirements. But [4] has been discussing some of the problems facing four-layer architecture. The most prominent of these problems is data management because of the huge volume of data. Many complex systems will lose this data and they need complex algorithms to solve this problem. With a huge in data volume, there is a requirement for new analytic techniques like artificial intelligence, machine learning, and other intelligent decision-making algorithms. So, five-layers may be the solution to this problem. The five-layer architecture is proposed to make the IOT safer. Data is processed separately in the processing layer through complex algorithms for data mining and classification. Besides, it enhances IoT services by making a decision based on correct and accurate data. Moreover, to increase the security level, business layer has been added to fully manage the system and enhance the security in the application layer.

This paper proposes an enhanced IoT architecture that gives more understanding and insights that required to meet the requirements of security and protection. Moreover, it discusses the best protection techniques against attacks in the layers.

3. Proposed Architecture

An architecture that consists of six layers and combines the advantages of four-layer and five-layer architecture to make the IoT environment safer is proposed. It is not fair to exclude the support layer from the structure of five layers because the market and storage layer does not have the same duties as the support layer. Big data cannot be stored in local storage, then cloud storage is required [11]. It also protects data from threats and ensures that information is provided only by an authorized user. The layer of the cloud is very powerful and valuable. With the development of IOT and the advent of big data, the cloud needs a large amount of data to be processed in infinite areas. In terms of security, the cloud is also relevant because it has strict policies to verify how important information can be accessed. It cannot also be dispensed with the proposed processing layer in the architecture of five layers, because when information is stored in the application layer, this data becomes more dynamic and vulnerable to intrusion due to big data, resulting in data loss. So, it can't be done without the big data storage layer. Big data obtained from the layer of perception must be processed separately in a layer to be more structured, which will also result in its protection [4]. Besides the business layer's importance in enhancing system security as a whole, see Figure 2. In general, it is responsible for managing and controlling applications.

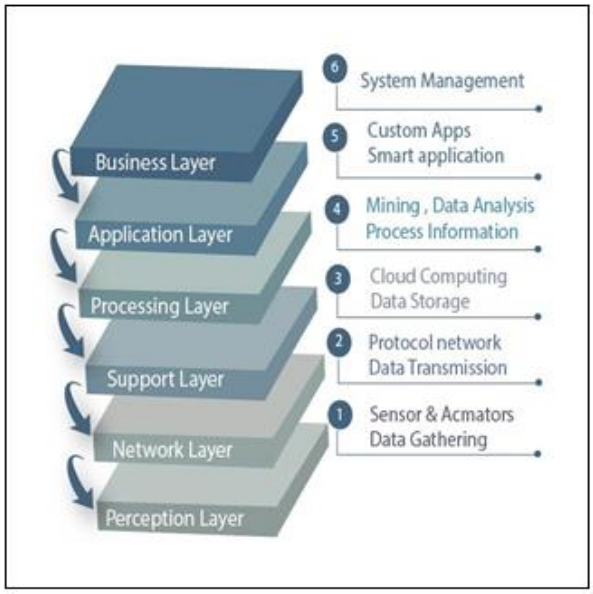

Figure 2. Improved Layer Architecture for IoT

3.1 Perception Layer

This layer is called a layer of sensors [17]. It's like the position of the human skin and face [19]. Many types of sensors are available, such as RFID, WSN, barcodes, or any other sensor network [20]. The basic purpose of this layer is to identify things and gather the data from them and then relate the things (i.e. devices) [22]. This layer is exposed to a range of threats such as: Node capture, Fake node, Side-Channel attack, Malicious code injection, Protecting sensor data, Mass node authentication, and Physical damage. A breakdown of them is at [11]. In eeither attack, it is difficult to identify the attacker, such as Eavesdropping, Replay attack, Timing attack, Information leakage, Label tracking, Copy attack, Forgery attack and Information tampering, there are details about them in [19]. Also, other types are displayed in [20] like Spoofing, WSN/ RF jamming and unauthorized access to the tags. The security mechanisms of the Perception Layer can be classified as the following:

Encryption and hash technique: encryption helps in turning the message into an unknown ciphertext type. When a message is sent from a recipient, it transforms into a different form that nobody can understand the message except the authentic receiver because it owns the key [17].The famous algorithms cannot be used for encryption and decryption, due to their inherent implementation complexities and requirements for power. The lightweight encryption [22] is the one available. This method is designed to ensure information integrity and confidentiality [10]. But it faces two issues: first, information technology development makes it possible for attackers to change the contents of cipher-text, the intruder is trying to spoil the receiver's post. Therefore, using hashing algorithms would be the solution to this problem. It's used to know and restore the message information that the attacker has changed. It is used in combination with encryption, it provides digital signatures of the content of a message which ensures that an intruder, virus or other means have not altered a message [17]. Secondly, all encryption algorithms are very safe and effective, but they consume a great deal of battery power [11]. To solve this problem, a lightweight adaptive motion sensor can be built which extracts energy from the surrounding environment based on the principle of turboelectric nanogenerator [24] that can reduce power consumption [2].

Authentication technique: this approach prevents unauthorized users from accessing nodes and information from the perception layer [19]. For this layer, it is very important to ensure security and privacy [11]. This method allows a device to confirm someone connecting to a network resource's identity. So, it could be said that authorization precedes authentication [17].

A technique for intrusion detection: an active protection device type [19]. It provides solutions to many security threats by generating an alarm when any hazardous activity occurs by continuous monitoring and record-keeping of the intruder [20], and immediately enforces other measures to stop the illegal activity [17].

K-Anonymity technique: it means hide sensitive information [20] by constructing wearable device privacy block [9]. It is an effective method of protecting the user's data such as identity and location [2].

Risk assessment methodology: this method is intended to classify significant assets and to discover the new threats of all possible attacks and losses. In this process, after determining the risks, the most suitable solution will be taken to tackle the threats [13]. An example of the adaptive risk assessment approach for IOT is presented in [20].

PKI technique: a protocol-like public key infrastructure (PKI). It is a set of many mechanisms and techniques, such as encryption, authorization, authentication method and detection of intrusion (which have already been discussed in the section on techniques). It is applied in the IoT framework of awareness. To be sure, it is much better to use a set of mechanisms than just one [17].

Secure booting: can use the cryptographic hash algorithm to examine the integrity and the authenticity of the software on various devices of the IoT network. But in most conditions, most of the hash algorithms cannot be executed on the end devices of the network because possessing is very low computing power. So, the best solutions to this problem are WH and NH cryptographic algorithms because they need very low processing to implement [18].

The Security channel IPSec: It provides two types of security features which are encryption and authentication. To ensures data confidentiality, data is encoded and avoided Eavesdropping. By the receiver device, The sender of the data can be identified the IP is real or not [18].

Physical secure design: Designing the end devices physically secure can be solved most of the attacks of the perception layer. It involves chip selection, data acquisition unit design, radio frequency circuits, etc. These units must be of high quality and should not be easily changing. The design of an antenna for wireless communication has to be able to contact over the good range [18].

3.2 Network Layer

Many research called it the layer of transmission. It gathers from wired, wireless, and satellite networks [17]. It works in an internet standard like a network layer. This layer is essential for routing, data flow, transmitting data through a set of protocols, and moving data securely from the layer of perception to the layer of support. It's the IoT architecture's heart. This layer is exposed to a range of threats such as: Denial of Service (DoS) attack, Main-in-The-Middle (MiTM) attack, Storage attack, Exploit attack, Heterogeneity problem, Network congestion, RFIDs interference, Node jamming in WSN, Eavesdropping attack, RFID spoofing,

Routing attacks, and Sybil attack [11] is considered a good source to know more about them. Also, [20] presented other attacks such as Malicious code injection, Sinkhole attack, Sleep deprivation attack, Acknowledgment flooding, Hello-flood attack, and Wormhole. Also, [5] presented Traffic analysis attack, RFID cloning, RFID unauthorized access, and Selective forwarding.

The security mechanisms for the Network Layer can be classified as the following:

Honeypot: one of the biggest threats to information is the DoS attack. To deceive the unauthorized user to enter the main system, use honeypot as the main system. It was considered a trap and embarrassment for attackers. Honeypot is made up of two types: honeypot development and analysis. Honeypot research is more effective and provides the attacker with more information [3][21].

Risk-based adaptive: adaptive risk management observes, adapts, eliminates, detects and reacts in a critical time to new or unexpected threats, just as biological organisms adapt and respond to threats in their survival struggle. Based on the assessed threats, risk-based adaptation responsive access can be allowed. Potential risks used to improve IoT system security. Risk-based adaptation quantitatively incorporates adaptive risk-safety approaches, generates an appropriate level of risk, and ensures that data is used, obtained and transmitted at an acceptable level of risk [17].

Wireless security: authentication SSL / TLS protocols and key management developed to encrypt the network layer link. IP security protocol ensures that not only the network layer is secured for all layers, but also, for each device connected to the network, use PPSK (Private Pre-Shared Key) [8].

Wired security: the protected wired network has many strategies, such as firewalls and the IPS [8].

SDN with IoT: regarded a dynamic network but at a lower cost and efficient performance. This technology's structure is made up of three devices: IoT agent, IoT controller, and SDN controller. IoT agent is constantly monitoring the environment just like the sensor layer on the Internet of Things and when there is a different behavior that collects information from the alerts. Before sending and receiving data, both devices authenticate and stop the process of sending data to the network if they notice that there is manipulation. All devices are protected by the SDN controller [17].

Corroborative nodes communication protocol: all current nodes are strictly controlled by the responsible communication protocol. When a node is identified with suspicious behavior, the other nodes are monitored, through providing information about this node [17], and the trust director alerts all nodes.

Reputation system-based mechanism: the purpose of this protocol is to compare the value set in the reputation table when the node sends data to another node. This comparison is made through each node's watchdog function. If the quality of this packet is uncertain, all nodes will be notified [17].

Routing Security: routing protection ensures that it is distinct from the packet routing route which allows the system to detect any errors and prevents the packet from losing when the system fails [20].

Cluster-based intrusion detection system: this consists of two levels: intrusion detection at the cluster level (CLID) and intrusion detection at the network level (NLID). In CLID, the cluster is either malicious or not depending on the level of trust as a proxy to control the node [17].

Security aware ad hoc routing: type in anything that you want. Then click Quill It on the right to paraphrase your input [5].

Hello flood Detection cum Prevention: considered in IoT as a tool for refusing hello flood attack [5].

GPS location system: the best technique to avoid a spoofing attack was considered [5].

Point-to-Point encryption: is a technique used to secure devices by encrypting data from source until the data reaches decryption destination.

3.3 Support Layer

Because of a large amount of data, it is very important to preserve this information by integrating storage capabilities with the server. The support layer makes the application layer stable in the maintenance phase. On this level, all forms of computing and cloud computing will use the cloud offered as an Internet service to achieve reliability and economization of scale [12]. Support layer functionality includes data storage for database and service management from lower-level levels. This makes IoT software as a support system. Different IoT applications can be hosted on cloud computing which provides resource-constrained devices with storage [11].

With the rapid growth of IoT and the increase in devices and data volume over the internet [4], cloud provides the IoT systems and asset management with an effective solution. Cloud computing integrates with IoT to meet IoT design compliance requirements that meet all the necessary constraints [4].

IoT and cloud integration also makes security threats more dangerous altogether. Cloud maintains properly designed policies and licensed functions for access to sensitive information only by legitimate users. This layer is exposed to a range of threats such as: DoS attack, Malicious insider attack, Unauthorized access, Data security [17] and [5] are presented in detail. While [11] presents Interoperability and Portability, Business continuity and disaster recovery, Cloud audit, Tenants security, Virtualization security, Application security, Underlying infrastructure security, and Shared resources. The Security mechanisms for the Support layer can be classified as the following:

Authentication: in each layer, it's a similar authentication. This prevents an unauthorized user from accessing IDs integrated [20].

Intrusion Detection: detect when any suspicious activity happens in the process by continuous monitoring and recording of the behavior of the intruder that could help track the intruder [20].

Risk Assessment: assess the risk and provide the safety system with an appropriate solution [20].

Homomorphic encryption: ciphertext is allowed to compute immediately without decryption. It requires a high computation for data security [5].

Web application scanners: this uses various threats that occur at the front end of the internet to be identified. It secures fraud data [5].

Fragmentation redundancy scattering (FRS): the use of cloud-based secure data is separated into cloud data and distributed to specific server space fragments. The fragment has no useful data details. In this government, the theft of data is reduced [5].

Encryption: is explained in previous section.
Hyper Safe: protection memory pages from updated and also allows the pointing index to be restricted to change the information monitored on the pointer list. It is used to guard against risks to virtualization [5].

3.4 Application Layer

The network layer meets the needs of clients for certain internet services. Through the application layer interface, they can access these services. The application layer is the highest layer of IoT architecture responsible for the effici ent use of the collected data [1]. The application layer will describe many applications in which IoT technology is used, such as smart homes, smart cities, smart safety, animal tracking, and many other applications. Depending on the information collected by the sensors [17], services requests can vary from application to application. This layer is responsible for displaying and formatting information as well as providing a lot of applications to many users [17]. The device user interface is in the top layer [6]. This layer is exposed to a range of threats identified in [5][8][23] and [17] like Cross-Site scripting ,Malicious Scripts, The ability to deal with mass data, Data access and authentication, Phishing attacks, DDOS attack, Denial-of-Service (DoS) attack, Sniffing attack, Injection, Session hijacking, Social engineering, Viruses and Trojan house, Side Chanel attack, and Cryptanalysis attack. the security mechanisms for the Application layer can be classified as the following:
Access control: the access control system allows the authority to access set network sources and means or certain devices. This guarantees confidentiality and ensures that these reliable data are available.
In this layer, it accepts truthfulness, which means that it is licensed. It is really difficult to control access to the IoT. Traditional access systems do not get with the IoT scenario specifications showing a lack of mobility, scalability, and functionality with billions of devices around the world. These problems can be solved by a cooperative approach that allows "stuff" to make authoritative decisions without assigning this process to another entity [25][17]. It is a security strategy used to manage and control users and resources.
There are two types of access control: physical and logical. Regulation of physical access limits access to houses, stores, spaces, and campuses. However, logical access control restricts the connections between network, file, and data [17].
Data security: at this stage, authentication, and integrity are the most important method of protecting the information security and privacy of the entire IoT encryption framework. This prevents unauthorized access to data and tracks information that is compromised or stolen [5].
Intrusion Detection: the system provides security solutions to many threats by generating an alarm when any unexpected action is conducted due to the constant monitoring of the activity log of the intruder. Different methods of surveillance such as data mining anomalies can be used to detect intrusion [5].
Risk assessment: this provides effective security solutions and enhances existing security architectures [5].
Firewalls: if the encryption, authentication, and ACLs process failed to block the unauthorized user then the blocking process involves the firewall. When selecting a weak password, it may fail to encrypt and authenticate. Unwanted packets are therefore blocked by this process in the firewall [5].
Anti-virus, anti-spyware and anti-adware: a system that safeguards the confidentiality, stability, and reputation of the IoT network [5].
Virtual Identity (VID) Framework: it is used to address privacy issues to safeguard user data from unauthorized users [17].
Identity-Based Personal Location System: for the privacy of the user, the location information should not be transmitted in cleartext. It must be stored in an encrypted form to stop anyone from seeing the location [17].
Preference Based Privacy Protection: a service provider, a customer, and a third party communicate in a secure environment [17].
User Authentication: encryption and integrity mechanisms are essential for the security and safety of the system in addition to data theft [18][20].

3.5 Processing Layer

It is called the layer of middleware. This layer is responsible for excavating the enormous data sent from the network layer and deposited in the support layer. Moreover, it eliminates redundant and unimportant data that will affect the performance of the IoT [11]. The primary purpose of this layer is to make the data more structured and readable as well [4]. In this layer, data ingestion, analysis, cleaning, streaming, reporting, mining, learning machines are done. In this layer, Intellectual analysis of decision output is not appropriate for malicious data. Therefore, detecting malicious data is a big challenge. This layer is exposed to a range of threats such as: Exhaustion, Malware [17], and Tampering with Data [8]. The security mechanisms for the Processing layer can be represented through:
Intrusion Detect System: such methods have been used to detect any malicious activity by detecting and tracking the user [20].

3.6 Business Layer

The business layer refers to the planned behavior and activities of an application as a whole system administrator. It is responsible for IoT systems management and control, models of market and income. This layer covers the client's information as well. It can also know how information can be created, stored, and changed [17]. This layer manages the overall IoT system services and activities. Business Layer creates a business model, graphs, flowcharts, etc. based on the data received from the application layer. Moreover, the Business layer introduces, designs, tracks, analyzes, and develops elements relevant to IoT. This layer supports decision-making processes based on big data analysis. In addition, the four layers are supervised and managed by the business layer. In addition, it compares the output of each layer to the expected output to improve services. This layer is exposed to a range of threats such as: Business Logic Attack, Zero-Day Attack [17].
We summarize the threats for the six layers of the proposed IoT architecture and the best defense mechanisms against these threats in Appendix 1.

4. Implementation

Nowadays, huge systems have many heterogeneous devices that differ in type and nature. These devices need to be connected and networks should be integrated. But the

problem is that as the network grows, threats, and vulnerabilities grow so they will require more security management of these vulnerabilities by choosing appropriate security standards, such as protocols, encryption, and privacy. Hence, analysis and assessment have been done for network threats, vulnerabilities, and countermeasures have been built based on protocols for encryption, authentication, remediation of gaps, prevention of growth, and mitigation of damage. Focusing on the study of wireless networks as they are the most important and most vulnerable. So, the stages of implementation can be listed as the following: (1) determine the network models, routing model, and environment in which the system will operate; (2) identify the types of attacks wanted to be tested and to be evaluated; (3) use appropriate simulations to implement the network, implement challenges and gaps, and clarify the extent of the damage that will result from these attacks; (4) design security systems and safety valves to protect the network, address vulnerabilities and minimize attack damage; (5) monitoring the success of the specific defense systems, whether those which have been prevented and their impact has been reduced or those which were unable to deal with; and (6) clarify the research recommendations and clarify the required future studies that are hoped to be applied.

4.1 Network Model

Network model: the model that works on consists of a set of randomly distributed wireless devices and one sink node without mobility. All nodes have the same range and each has a unique ID through which it distinguishes between the units and the network works through that each unit is sending data to the sink node and for remote units using routing systems. The other units work to transfer information from the source to sink where the system works on multi-hop routing mode, a system that relies on the communication of the units directly with neighboring nodes that fall within the range of communication and then the rest of the nodes forward the packets until they reach their target.

This model has been identified because it contains a link between heterogeneous and unknown devices, which helps to show the impact of attacks and test threats fully and to clarify the success of the specific defense plan and the extent of its impact.

4.2 Routing Model

Routing model: The study is based on the **AODV** protocol that enables nodes to get routes to their destinations. There is a routing table that lists information about neighboring nodes and determines the number of hops to reach the target unit. When a unit wants to send a message, it first checks its routing table. If the route is not available, the process of discovering the route starts by broadcasting the **RREQ** packets, which is the request of the target node.

When the neighboring units receive this message, they review their routing table. If they know where the target unit sends the data to the source unit, they re-broadcast the message and continue this process until the target unit receives the message. Then they send a message **RREP** informing the source node path to the target unit and use a unique serial number of messages to prevent the entry of loops. This protocol is one of the best directive protocols and the fastest and least resource consumption. However, there is no security mechanism and it is vulnerable to a range of attacks that affect it significantly. Therefore, there is need to monitor the extent of damage and the success of the defense tools used.

4.3 Attacks Model

Attacks model: wireless networks face many attacks because of the dedicated wireless infrastructure and operating environment. Attacks can be categorized in different ways. At first, the attack can be classified as internal which the attacker knows full information about the units and can communicate with them. As well as an external attack in which the attacker lacks information about the network, units, and traffic. It is likely that his work is jamming and his impact is ineffective and hence the two main types of attackers namely passive and active attacks.

The passive attacks: it is an activity monitoring the flow of data and listen to it without causing any interruption or impact and the only harm is the loss of privacy and this type is divided into the following:

Eavesdropping: an attacker intercepts data sent between two nodes without knowing the nodes of the threat being affected by their communication and most likely this attack collects vital information for use in active attacks.

Traffic analysis: the attacker analyzes the data traffic and knows the source and interface. He/ She can distinguish unit sink or BS and determine where the critical points are located, and the extent of the system affected by. Moreover, he/ she can also analyze the types of defense tools used.

Camouflage: the attacker identifies the units and participates in the transfer of information. Moreover, he/ she will be a participant and useful until, gains confidence between units to transfer information, to assist an active attacker or transfer himself / herself from passive attack to active attack.

Active attack: is an effective behavior aimed to damage the unit or the network to influence the traffic of data. Also, the two main types of attackers namely can be identified into the following:

Flood attack: is the sending of a large number of messages to the victim unit which affects the receiver unit. The receiver unit will not be able to communicate with other nodes. This type includes many attacks, such as sending a number of welcome messages or fragmented messages that are transferred as a large number of messages causing overflow storage and thus prevent the reception of real requests. (http flood attack & SYN flood attack & UDP flood attack) will be applied.

Delay attacks: the attacker delays the messages that are transmitted at the beginning of the day to communicate with the units, to deceive, and to participate in the routing of these messages. Hence, he/ she delays either contact information or data itself, collects, and sends them together. This causes the loss of messages or work traffic congestion of data, reduces the effectiveness network and communication between the units, reduces the rate of productivity, and increases the delay as it consumes the resources of the victim unit. The species (ping Delay attack & UDP Delay attack & TCP Delay attack) will be applied.

Hole attacks: The attacker will not send messages contact information, nor data. There are many types of them, which prevents the arrival of any messages or information. Also, some of them send error information for misleading prevents communication with part of the network or report anon-existent number of units available. The types next (Blackhole & Grayhole & Sinkhole & Wormhole) will be applied.

Attack model design that is shown in Figure 3 is used to

design an attacker model. Normal modules are used, but they are modified on the network layer and their routing elements. A set of commands is put that execute the attack whether by sending messages, delaying, or listening, and then linking these units to a central unit that manages.

The hacking process is called the controller, which is responsible for sending a message to the modified unit to start the attack and also alerting them to stop it. This unit can manage a group of attacks where the attack can be complex or depends on a negative attack at first to identify the elements and data network.

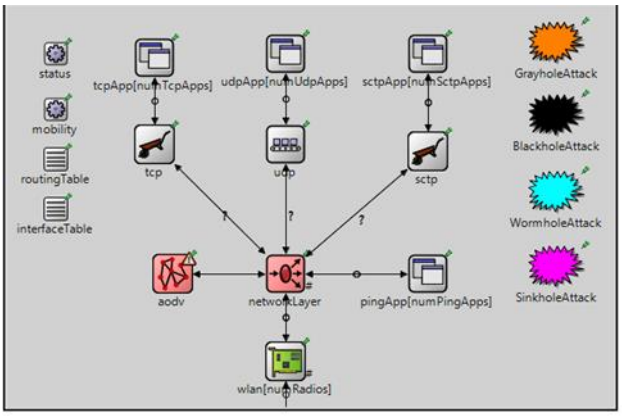

Figure 3. Attack Model Design

4.4 Simulation Model

Simulation model: to implement the network and specific modules, the network simulation program omnet ++ will be used. It provides all the elements of the network and modules and it uses the library inet which contains tools for the design of wireless modules and design of all layers of the unit. In addition, it provides tools to produce the units of attack and defense elements used. Moreover, the network according to specifications will be implemented as shown in Table 1. Three scenarios for the network will be implemented as shown in Figure 4:

Table 1. Simulation Parameter

Parameter	value
Simulation area	50*50
No. of Nodes	100
Channel Type	Wireless channel
Simulation time	100 seconds
Initial energy of node	1J
Nodes distribution	Uniformly distributed
Energy model	Battery
Communication channel	Bi-directional
Antenna Model	Omnidirectional antenna
Radio Propagation Model	Two-way ground

First scenario: is the normal application of the network without any control or with the presence of an attacker. Then use it to monitor the natural analysis of performance, to measure, and to compare the results of damage to attackers.

Second scenario: is the implementation of the network with the addition of several attackers of the types that have been already shown in the attack model.

Third scenario: is the application of the network with a group of harmful elements that will attack. But different defense units will be added and the defense operation will be monitored and to how extent it succeeded in preventing or minimized its damage.

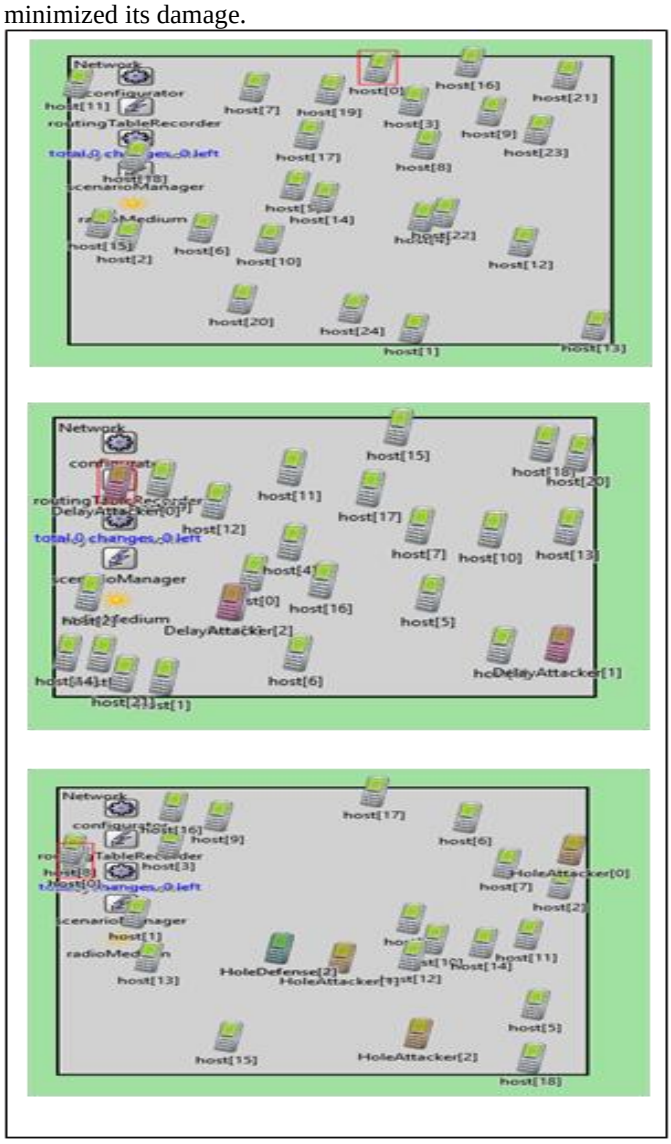

Figure 4. The Three Implementation Scenarios

5. Results and Discussion

Analyzing and understand the impact of network and pelvic attacks, relying on performance measures, is measured by the simulation software in case of attack. It is considered that packets are dropped as they are sent from source to sink. Figure 5 presents the results for a set of scenarios represented by Delay attack, Hole attack and Dropping attack, in order to reveal the effect of these attacks on the nodes that were sent and the nodes that deleted as of a result of the delay and the nodes that was successfully received. The number of attacks for each type in the scenario has been increased to see how many nodes are affected by these different attacks.

Defense Model: After explaining how performance is affected, and problems result from the attack of malicious nodes on the network from the loss of messages and reduce productivity and delays. Now a protection model with a set of tools and methods of defense are proposed. System consists of two levels of defense. The first level is the traditional defense tools that have been dealt in many

techniques, such as encryption of data, contact information, the use of multiple paths and not rely on a single path or reliance on one information as well as marking messages to distinguish them, and ensure the validity of the message using a time system and validity of access time. Despite all these solutions the system still faces problems. It is unable to deal with all kinds of attacks and also the high cost that the system spends to reach this level of security. Therefore, the second level has been designed.

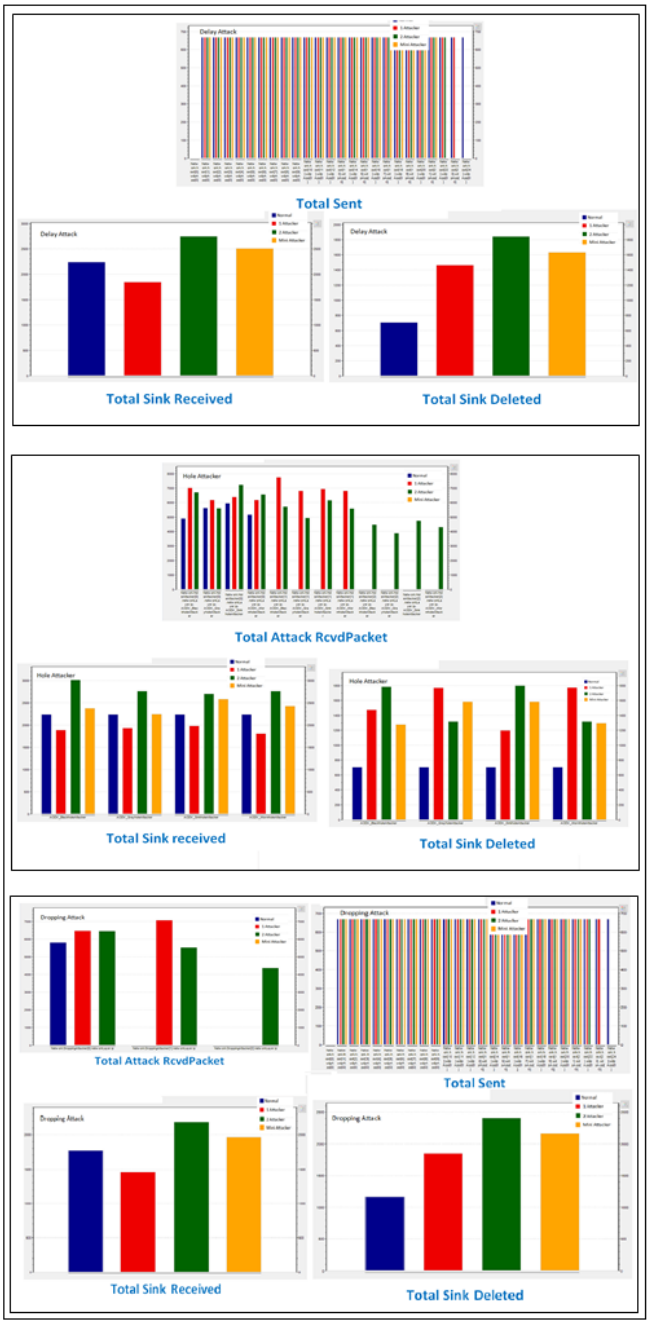

Figure 5. Analysis of the Attack Impacts

The second level used to monitor and analyze the performance of a group of units and to identify any malicious node that could pose a threat. This technology cannot be distributed to all units because their cost is high and also affect the speed and productivity of unit detection controller. Hence, when a unit detects and identifies any attack, all units are analyzed and monitored. Then, this unit communicates with the adapter, which is managing the second level of defense.

The adapter receives information from the unit and then connects it to the notification controller unit which is responsible for the announcement of malicious node data for all nodes in the network where it can communicate with it. So, it defenses all network elements and informing them of the identity of the attacker. Hence the best way is gotten to defend and also not to use all the tools of defense for lack of influence on the efficiency of work in the network. A comparison between the two scenarios of the network under attack is offered, but one important operation of the defense system and the results presented show how successful the system to respond to attacks. After adding the defense levels to the previous scenario, the results depicted in Figure 6 prove that there is a control over the node whatever how many attack numbers increase for each type of attack. In addition, the number of nodes that fallen and deleted due to the attack effect after adding defense levels is less than the number of nodes that fallen and deleted due to the attack effect before adding defense levels.

Figure 6. Defense Model

6. Conclusion

In this paper, we proposed a secure IoT architecture consists of six layers. The proposed IoT architecture combines the advantages of four-layer and five-layer architecture which enhances the security of the IoT environment. The most common threats for each layer and the best technique to secure it are reviewed and summarized in Appendix 1. In the proposed IoT architecture, a group of attacks and their defense behaviors against these attacks have been implemented by focusing on the study of wireless networks as they are the most important and most vulnerable. Moreover, the performance of the AODV protocol was measured in the presence of some malignant nodes. In addition, three scenarios were applied to illustrate the impact of these attacks on network performance.

References

[1] International Journal of Advanced Research in Computer Science, Vol. 8, No. 1, 2017.
[2] A. Čolaković, M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," Computer Networks, Vol. 144, pp. 17-39, 2018.
[3] A. M, A. Thileeban S, D. Jeswin Nallathambi, "Use of honeypots for mitigating DoS attacks targeted on IoT Networks," IEEE International Conference on Computer, Communication, and Signal Processing, Chennai, India, pp. 1-4, 2017.
[4] A. Tewari, B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," Future Generation Computer Systems, Vol. 108, pp. 909-920, 2018.
[5] A. Wahab, O. Ahmad, M. Muhammad, M. Ali, "A Comprehensive analysis on the security threats and their countermeasures of IoT," International Journal of Advanced Computer Science and Applications, Vol. 8, No. 7, pp. 489-499, 2017.
[6] D. Gamal Darwish, "Improved layered architecture for Internet of Things," International Journal of Computing Academic Research (IJCAR), Vol. 4, No. 4, pp. 214-223, 2015.
[7] E. Ahmed et al., "The Role of big data analytics in Internet of Things," Computer Networks, Vol. 129, pp. 459-471, 2017.
[8] E. Leloglu, "A Review of security concerns in Internet of Things," Journal of Computer and Communications, Vol. 5, No. 1, pp. 121-136, 2017.
[9] F. Liu, T. Li, "A Clustering K-anonymity privacy-preserving method for wearable IoT devices," Security and Communication Networks, Vol. 2018, pp. 1-8, 2018.
[10] H. Khattak, M. Shah, S. Khan, I. Ali, M. Imran, "Perception layer security in Internet of Things," Future Generation Computer Systems, Vol. 100, No. 28, pp. 144-164, 2019.
[11] I. Ali, S. Sabir, Z. Ullah, "Internet of Things security, device authentication and access control: A Review," International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 8, pp. 1-11, 2016.
[12] J. kaur, A. Bhandari Gandhi, "Security And DDos mechanisms In Internet Of Things," International Journal of Advanced Research in Computer Science, Vol. 8, No. 9, 2017.
[13] J. R.C. Nurse, S. Creese, D. De Rour, "Security risk assessment in Internet of Things systems," IT Professional, Vol. 19, No. 5, pp. 20-26, 2017.
[14] K. Middha, "Internet Of Things (Iot) Architecture, challenges, applications: A Review," International Journal of Advanced Research in Computer Science, Vol. 9, No. 1, pp. 389-393, 2018.
[15] L. Cruz-Piris, D. Rivera, I. Marsa-Maestre, E. e la Hoz, a. R. Velasco, "Access control mechanism for IoT environments based on modelling communication procedures as resources," Sensors, Vol. 18, No. 3, pp. 917-938, 2018.
[16] M. Bilal, "A Review of Internet of Things architecture, technologies and analysis smartphone-based attacks against 3D printers," 2017
[17] M. Burhan, R. Rehman, B. Khan and B. Kim, "IoT elements, layered architectures and security issues: A Comprehensive Survey", Sensors, vol. 18, no. 9, p. 2796, 2018. Available: 10.3390/s18092796.
[18] M. Muhammad Ahemd, M. Ali Shah and A. Wahid, "IoT Security: A layered approach for attacks & defenses", in International Conference on Communication Technologies (ComTech), 2017.
[19] M. Shideng, H. Huang Hai, "The perceptual environment security mechanism research for Internet of Things," 2015 International Conference on Intelligent Systems Research and Mechatronics Engineering, Zhengzhou, China, 2015.
[20] M. U. Farooq, M. Waseem, A. Khairi, S. Mazhar, "A Critical analysis on the security concerns of Internet of Things (IoT)," International Journal of Computer Applications, Vol. 111, No. 7, pp. 1-6, 2015.
[21] S. C, V. C.P, "Internet of Things and security issues," International Journal of Computer Science and Mobile Computing, Vol. 5, No. 1, pp. 133-139, 2016.
[22] S. Roy, U. Rawat, J. Karjee, "A Lightweight cellular automata based encryption technique for IoT applications," IEEE Access, Vol. 7, pp. 39782-39793, 2019.
[23] W. Zhang, B. Qu, "Security Architecture of the Internet of Things oriented to perceptual layer," International Journal on Computer, Consumer and Control (IJ3C), Vol. 2, No. 2, 2013.
[24] X. Zhao et al., "Ultralight, self-powered and self-adaptive motion sensor based on triboelectric nanogenerator for perceptual layer application in Internet of things," Nano Energy, Vol. 48, pp. 312-319, 2018.
[25] Y. Andaloussi, M. El Ouadghiri, Y. Maurel, J. Bonnin, H. Chaoui, "Access control in IoT environments: Feasible scenarios," Procedia Computer Science, Vol. 130, pp. 1031-1036, 2018.
[26] I. Cvitić, M. Vujić and S. Husnjak, "Classification of Security Risks in The Iot Environment," 26th DAAAM International Symposium, Vienna, Austria, pp. 0731-0740, 2016.
[27] S. A. Kumar, T. Vealey, H. Srivastava, "Security in Internet of Things: challenges, solutions and future directions," 49th Hawaii International Conference on System Sciences, Koloa, HI, pp. 5772-5781 2016.

Appendix 1

Layer Name	Threat Name	Defense Mechanism
	Eavesdropping, Spoofing attack [10][17][20].	Authentication [10].
	Node capture [11][17].	PKI technique [10].
	Fake node [11][17][18].	Secure Booting [18].
	Malicious code injection [11].	Intrusion detection [18].
	Physical damage [11][19].	Secure Physical Design, risk assessment [18][5].
	Information tampering, RF/WSN jamming attack [20][18][10][19].	IPSec Security channel[18]
	Fake node injection [18].	K-anonymity technique [18].
Network Layer	DOS, DDOS [3][21].	Honeypot, access control [3][21].
	Masquerading , unauthorized access [28]	Risk-Based adaptive [17].
	RFID cloning, RFID unauthorized access [18][5].	Wireless security (TLS/IPSec, PPSK)[8].
	Malicious Scripts [18].	Wired security (Firewall, intrusion prevent system) [8].
	Node attack, Man in the Middle attack [18].	Corroborative nodes communication protocol [17].
	Node attack [18].	Reputation system-based mechanism [17].
	Traffic analysis attack [5][18].	Routing security [20][5][18].
	Man in the Middle attack [18].	Point-to-Point encryption [18].
	Sinkhole attack [5][18].	Security aware ad hoc routing [5][18].
	Hello flood attack [5].	Hello flood detection cum prevention [5].
	RFID Spoofing attack [5][18].	GPS location system [5][18].
Support Layer	Unauthorized access [20][5].	Authentication [20].
	Malware, DDOS attack [17].	Intrusion Detection [20].
	Unauthorized access [20].	Risk Assessment [20].
	Application security [5][18].	Web application scanners [5][18].
	Data security, underlying infrastructure security [5][18].	Fragmentation redundancy scattering (FRS)[5][18].
	Third-party relationships [5][18].	Encryption [5][18].
	Shared resource, Data security [5][18].	Homomorphic encryption [5].
Processing Layer	Malware [17]	Intrusion Detect System [20]
Application Layer	Denial of Service (DoS) [18].	Access control [18].
	DDOS attack [21].	Intrusion detection [21].
	Malicious Scripts [18].	Firewalls [18].
	Virus, Worms, Trojan Horse, Spyware [18].	Protective Software [18].
	Data Protection and Recovery [18].	Cryptographic Hash Functions [18].
	Software Vulnerabilities [18].	Awareness of security [18].
Business Layer	Business Logic Attack, Zero-Day Attack [17].	Encryption [17].