International Journal of Scientific Engineering and Science
Volume 5, Issue 2, pp. 29-34, 2021. ISSN (Online): 2456-7361

Internet of Things Security Issues and Countermeasures

Alaa A. Alsobhi, Sabah M. Alzahrani
College of Computers and Information Technology, Taif University, Saudi Arabia
Email address: alaaal.sobhe @ gmail.com, sa.sabah @ tu.edu.sa

Abstract— *Internet of Things is a new concept that protrudes recently. We can simply say the IoT is connecting the devices to each other and make it work together smoothly. As the current technology trend aims to include the IoT completely or even a small part of it with the existing technology. Of course, it is not an easy thing to implement it; this is due to the reason of the many issues and problems related to the architecture of IoT. Also, the current protection methods that do not provide us sufficient security make us afraid of using them and exposing ourselves to some danger. In our paper, we aim to know the reasons and challenges that stand against achieving the required security. We will review the difference between the IoT architects and offer review the difference of the IoT architecture design and offer some solutions that may help to increase the security.*

Keywords— *Internet of Things, Internet of Everything, IoT, IoE, IoT architecture, IoT security, IoT issues, and IoT countermeasures.*

I. INTRODUCTION

Many of us have dreamed of smart homes where devices and machines can respond to our orders automatically. For example, alarm bells and a coffee machine activate by the moment you open your eyes, lights illuminate as soon as you walk through the house or clapping by your hands, some hidden computers recognize your voice and responded to your commands to read your messages or check the weather for you and so on. Sure, you have read or witnessed such things in practical fiction stories for several decades, but now either they are already possible or close to becoming so. All of these new technologies are the basis of what we call the Internet of Things. IoT is the new trend of technology in this current era of course because the concept has attracted the attention of everyone, so many developers and companies are looking for a way to either develop or think about how to involve it in our daily life. But it is not that simple for many reasons related to the IoT structure, and we will talk about it in detail later. Also, because there are no basic security requirements for the IoT, Often they rely on the CIA Triad (confidentiality, integrity, and availability) they adding more security restrictions related to which domain that they apply the IoT application on it. So in simple words, we can say that IoT security it stands as an obstacle and a real issue against the developer's dreams. Imagine if someone access to our systems or devices without our knowledge and start controlling our house or start monitoring us by our security camera, It's a scary scenario to think about it. In this survey paper, the goal is to understand what is the IoT, what is the risks of using it, and why security is hard to implement. So the paper will contain 6 sections, the second section will talk about the IoT and its definition. After that, the architecture of the IoT is the third section Where the layers can be divided into three, four, and five. Section four will include the literature review after that we will analyze some security issues and countermeasures.

II. INTERNET OF THINGS

To understand anything we need to look at the history of it and when it began and how it developed. First of all, there is no constant and uniform definition of the IoT, this is due to the fact that the idea of the IoT does not belong to a specific company or specific person. we can say that it is an idea began with one person and developed by different companies depending on which area is used with and combined with what. In 1999 Kevin Ashton first proposed the term "Internet of Things" (He is an innovator and consumer sensor expert), who coined the term to describe the network connecting objects in the physical universe by the Internet. As we said before no owner owns the IoT so, there is no official definition of constant for it. But that is okay because, simply all the definitions fall into one concept which we will explain it as the following: Internet of Things (IoT) or Internet of Everything (IoE) is all hold the same meaning as a network of physical objects things that are embedded with (sensors or software, and other technologies) to give the ability connect and exchange or transfer data with other devices and systems through the internet without interference human. In other words, we can say that "Things" explain as: Everything, literally everything falls under the concept of the Internet of Things, clothing, furniture, household utensils, body parts, streets, and even animals. Anything that can stick to a processing unit and have an Internet link feature is considered a thing in the world of the Internet of Things. There are different application domains of IoT such as Home/Office, City, Healthcare, and so on. Figure 1 shows the top IoT applications in 2020 that were leaned on 1,414 projects where Manufacturing are most common (22%) after it was the Transportation (15%) and Energy IoT projects (14%)[1].

III. ARCHITECTURE OF IOT

There is no convention about the architecture of the IoT. And this is why there is different architecture according to the viewpoint of researchers. Some of them think about it as 3 layers while the other goes with the 4 layers because they

think that to improve the IoT, 3 layers can't achieve the renewable requirements. After that, they suggest an architecture that contains the 5 layers to face the security and privacy requirements [2]. Take a look at figure 2 that shows a summary of IoT layer architecture.

Figure 1: Examples of IoT application [1]

1. *Three Layer Architecture [2]*

It is the simplest shape where it holds the basal idea for the IoT. The 3 Layers are Know as perception, network, and the application layer.

1.1 Perception Layer: The other name for this layer is the sensor layer. If we compare it by the human will be as the senses where is responsible for gathering the information (as the location, the movement, the temperature, etc.) and characterize the things. A lot of sensors are linked by objects that help in the gathering step such as Radio-frequency Identification, Two-dimensional (2D) barcodes, and so on.

1.2 Network Layer: The other name for this layer is the transmission layer were it similar to the bridge that links between the perception and the application layer. It loads and transfers the information collected from the physical objects by the sensors. It takes the data where compiled from the sensors and then transfers it by a wireless or wired medium. Also, it is answerable for linking smart devices and networks together.

1.3 Application Layer: It is the layer that includes all applications (as smart homes, cities, and health care) connected to IoT. It is responsible to apply the services where it differs from application to others. And the reason is the different information that sensors gather. The main issue in this layer is security.

2. *Four Layer Architecture [2]*

As we say it before due to some requirements 3 Layers were not enough. It is containing the same three layers from the previous architecture plus the new layer known as a support layer. The layers arrangement will be as follows: Perception, support layer (the newest layer), Network, and Application. The perception, network, and application layers work similarly to the previous architecture.

2.1 Support Layer: This layer was created for the following reasons:

- To apply the security in the IoT architecture.
- The information was sent to the network layer immediately (on the 3 layers architecture), It raises the opportunity to get threats.
- The information now sends from the perception layer to the support layer.

This layer has two functions, The first one is to prove that the information was sent from the real users and protected this information from any threats. And the second function is to transmit the data from this layer (support) to the next layer (network) by using media transport such as wireless and wire.

3. *Five Layer Architecture [2]*

The previous architecture did not solve all the security problems and there is also a storage problem. And this was the reason to create the 5 layers architecture. It has the same 3 layers as the first architecture besides it has two new layers that they called as processing and business layer. The arrangement of layers will be perception, transport, processing (1st new layer), application, and business (2nd new layer).

3.1 Processing Layer or Middleware layer: It the layer that gathering the information from the transport layer, then it is processing this information, remove the additional information, and extract the valid information. This layer also solves the big data issue.

3.2 Business Layer: It is the purposed behavior of an application and acts as a system manager. It got the responsibility to monitor and manage this layer and applications layer. It also manages the privacy of the users and defines how should information store, modify, and create.

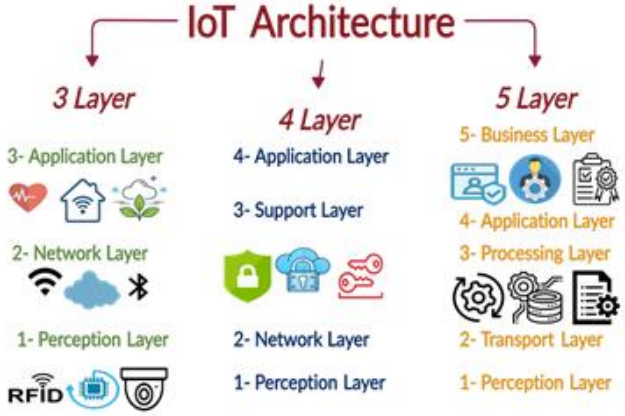

Figure 2: Different IoT architecture(3 layer, 4 layer and 5 layer) [2] .

IV. Literature Reviews

PAPER 1: Hyungsik Shin and others [3];

Their paper was support by NRF of Korea and KEPCO. They mentioned that the security in IoT considered a big obstacle for a lot of reasons:

1. IoT has different platforms and the number of devices that are shared is big (This is the most common reason).
2. Devices on the network have different architecture and it uses various protocols (no one type of security can be used).
3. Increasing the devices that are linked to the network, causing a difficult way of managing it.
4. Size of IoT network is really huge, synchronously controller it causes a lot of issues.

And they classified the layers of IoT architecture into 3 layers (Perception, Network, and Application). The IoT has been developed by a different group and it has various forms and implementations accordingly. There still is no unanimity about the precise definition of IoT. Therefore, there were no predefined security standards among the different groups at the initial phase of IoT development, as we know IoT was developed by different people and has a different application, there is no main define for it, there are no security goals. so it is important to implement and apply the confidentiality, integrity, availability (CIA triad), Energy Efficiency, and Heterogeneity. There was 2 light weight block cipher proposed in 2013. The SIMON and SPECK are suggested by the NSA (national security agency). Unfortunately, the two were refusal in 2015 by ISO standardization.

PAPER 2: Rao, K.S.N.and D.S.S. [4];

In their paper, they define the IoT as a technology that supports the integration between the materials and digital infrastructure to produce new applications. The IoT infrastructure can be divided into three or five layers. If it three layers it will have first the perception then the network and finally the application. And if it five layers it will have the business, application, service management, object abstraction, and perception. As we know IoT includes linked devices, so we need to use authentication for the device. but it is one of the challenges that make applications susceptible to attacks. access control needs to have a tough technique for making sure that only authorized users can be accessed. Trust is a complex concept, so it is hard to make decisions to rely on it. The phone security also considers a challenge. Problems of using RFID and so on. And finally, the suggested some solutions.

PAPER 3: Ghadeer, H [5];

On their paper talked about that security is the main problem in the IoT, that need to be fixed. And it is arduous to implement security because they focusing on making it easy to use. After that, they mentioned the CIA triad and they defined the three components according to the ISO/IEC/ IEEE 24765 (Confidentiality, Integrity, and Availability). Then they divided the IoT security attacks into three types: Physical attacks, Software attacks, and Network attacks. Lock at Table 1 that summarizes each type.

The IoT architecture consists of five layers: the perception layer, network layer, middleware layer, application layer, and business layer. They mentioned in their paper the security issues and suggested solutions. Also, each layer of the architecture has different challenges.

PAPER 4: Jihad DAZINE, A.M.a.L.H. [6];

In this paper, their goal was to analyze the security of the IoT, and the problems related to the IoT architecture. And they cited an example of an effect of bad security, the "Stuxnet" virus that damaged the Iranian military equipment in 2010. They relied on his paper 4 layers of IoT architecture, the perception layer or recognition layer then the Network layer, Middleware layer or computation layer, finally the Application layer. And for the requirements of the IoT security were the same as the security goals "CIA" and extra important requirements were added as authentication, non-repudiation, anonymity, authenticity, and privacy. Then they discussed IoT security threats according to each layer. And as they mentioned the IoT security threats according to each layer, the IoT security countermeasures were also different from each layer. See Table 2 which contains all the IoT issues and countermeasures.

Table 1: Summary of the three attack types from paper 3.

Type of Attack	Explained of the Attack	Example
1- **Physical Attacks**	The **hardest** to implement on the hardware, the tools cost a lot. This attack may happen on several physical components.	1- **Physical Objects** 2- **Sensors** (Wireless Sensor Networks (WSN), RFID tags).
2- **Software Attacks**	It is the **main source** of the security attack on the IoT. The **software malicious** that cause an attack.	Virus, Trojan Horse, Logic Bombs, Worms, and DOS.
3- **Network Attacks**	It is a type of attack that **targeting IoT communication channels** while it happens by an **active attack** where the providing services shut down. OR a **passive attack** where it can dominate the service without turning off the service.	**1-Active Attack**: DoS attack, The Node (Subversion, Malfunction, and so on), False Node, Message Corruption, and MITM attack. **2-Passive Attack**: It is targeting privacy as Traffic Analysis, Eavesdropping, and Monitor.

Table 2: IoT security threats and security countermeasures.

Layer	Attacks Type	Countermeasures
Perception	This includes 6 attacks type: Unauthorized Access & tag cloning, Eavesdropping, Spoofing, Jamming, Sleep deprivation attack, and Physical attacks.	Authentication, Encryption (such as RSA, DSA, BLOWFISH, and DES), Anonymity (is acquired by the K-Anonymity approach), Intrusion detection, Risk assessment, and Physical security.
Network	This layer is targeted by 8 types of attacks: Sybil Attack, Buffer reservation attack, Malicious code injection, Sinkhole Attack, DoS attack, RPL routing attack, Replay attack, and MITM attack	End to end encryption, Routing security, and Data privacy
Middleware	Dos attack, Unauthorized Access, and Malicious Insider.	Authentication, Data Security, Software updates, Intrusion detection, Security applications, Risk Assessment, and Non-technical measures
Application	DoS Attack, Spear Phishing Attack, Insecure software, CoAP security with the internet, and Sniffing Attack.	
Other	The cross-layer threats: the trust guarantee, secure sharing of the data, and user privacy IoT maintenance that may cause some threats: fail of administration system, gateway, misconfiguration, and so on.	

PAPER 5: Burhan and others [2];

On their paper talked about that security is the main problem in the IoT, that need to be fixed. And it is arduous to implement the security because they are focusing on making it easy to use. After that, they mentioned the CIA triad and they defined the three components according to the ISO/IEC/ IEEE

24765(Confidentiality, Integrity, and Availability). Then they divided the IoT security attacks into three types: Physical attacks, Software attacks, and Network attacks. Look at figure 3 that summarizes each type. Since each layer on the architecture have a different challenge so they mentioned some security issues and suggested solutions. Also, they suggested new architecture that holds a 6-layer perception Layer, observer Layer, processing Layer, security Layer, network Layer, and application Layer. Look at figure 4 that shows Suggested layers. Observer Layer: This layer makes sure if the information is protected from hackers and viruses then send it to the next layer otherwise will not send the information.

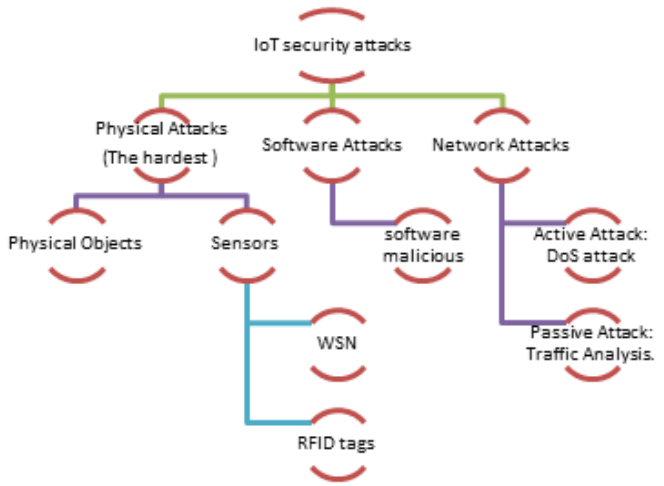

Figure 3: IoT security attacks type

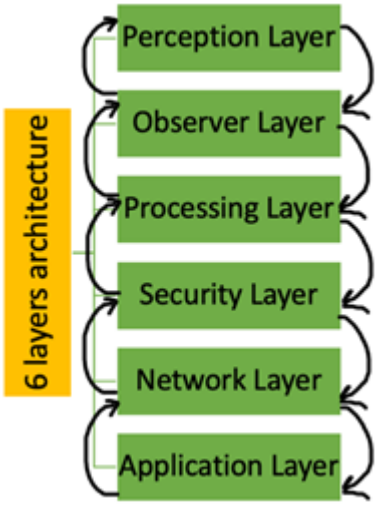

Figure 4: IoT 6 layer architecture [2].

V. IOT SECURITY ISSUES AND COUNTERMEASURES

This section will contain two parts. The first one will discuss the challenges and problems facing the IoT from different perspectives, such as the communication technologies issues, and according to the IoT architecture layers. Then the second part will offer some suggested solutions that can be followed to reduce issues on IoT security.

❖ *Communication Technologies [2]:*

1. *ZigBee Technology:* It is a personal area network (PAN).
2. *Bluetooth Technology*: It uses for short area communications.
3. *Radio Frequency Identification (RFID):* It uses communication frequency waves and it includes 3 parts (the tag, the reader, and the database).
4. *Wireless Sensor Networks (WSNs):* It holds many nodes, and each one contains 4 parts (memory, battery, microcontroller, and sensors)
5. *Wireless Fidelity (Wi-Fi):* It is a wireless network transfer communication on the shape of a signals radio. No encrypt technique.
6. *The 5G Network:* It is the 5th generation of cellular technology, that provides more speed, covering, and realization of the wireless.

Look at Table 3 that analyzes each type of communication technology.

TABLE 3: Summary of communication technologies [2].

Communication Technologies	Mechanism	Security Technique	Advantages / Disadvantages
Zigbee	Wireless	Encryption and Integrity	Low-power consumption at a low cost. Fixed key (never be changed)
Bluetooth	Wireless	Encryption, Authentication	Cable replacement, Low cost Blue-jacking, bluesnarfing
RFID	Frequency waves	Data encryption standard, advance encryption standard	No duplication on the data No mechanism to verify authentication
WSN	Wireless	Key, Encryption, Authentication	Low Cost, Power, and Resilience Service attacks, DOS, DDOS, authentication problem
Wi-Fi	Wireless on a shape of signals radio.	Authentication, Authorization	Fast, Secure, Convenient Eavesdropping, No encryption mechanism
5G Network	Wireless	Authentication, Authorization	Fast, Secure, Convenient DDoS

❖ *The security issues according to each layer:*

1- *Perception layer [3], [5] :*

- Physical attack.
- It is hard to implement some protection on the sensors.
- illegal user.
- Sensor nodes may be compromised
- The nature of the sensor nodes where nodes require to be variable places.
- The material node attack and spoofing
- Denial of Service attack

- Timing attack and Replay attack

2- *Network layer [5] :*

- Because of the big number of network components, it is difficult to use TCP/IP communication protocol to deal with the IoT infrastructure.
- The devices are linked to low network bandwidth with less pressing power.
- The design of the IoT network is used to all different types of devices and adding more devices will lead to losing control of these devices.
- Data are prone to sniffing attacks.
- IP address spoofing attack and MITM attack.

3- *Middleware Layer [5]:*

- The attacker's main target is cloud availability.
- DoS against the Cloud of IoT.

4- *Application layer [5]:*

- That attack on the software by using some lacuna on the application.
- The CIA Triad are the main problems on this layer.
- Brute-force attack

❖ *Some suggest countermeasures according to each layer [5]:*

1. *Perception layer:*
   - Filter the traffic of signals between the devices of the IoT
   - Turn off the RFID tags that you don't need it
   - Implement some authentication methods on the nodes of the sensor.
   - Improved the authentication either by giving access to just the legal user or establishing a secure key.
   - Using some lightweight Authentication techniques.
   - Implement some control mechanisms on the access and on the authentication.
2. *Network layer*:
   - Make communication protocol should be standardizing.
   - Apply an Intrusion Detection System (IDS). And there are two kinds of IDS: HIDS (Host based Intrusion Detection Systems) and NIDS (Network based Intrusion Detection Systems)
   - Establishing communication protocol that backing the M2M communication. and the examples are: foundation a protocol that deals with M2M communication an example of it: AMQP, MQTT, and CoAP.
   - Setting up an encryption process for IoT data to avert data sniffing
   - Design a suitable communication protocol based on the CIA triad.
   - Reduce the use of the Internet Protocol Version 4 and use the Internet Protocol Version 6.
3. *Middleware Layer:*
   - Fix the availability problems by applying some methods to control the access of illegal users.
   - Provide E2E (End to End) data life cycle protection
   - Establishing a platform of IoT protocol to ensure security.
   - Provide SLA (Service Level Agreement).
4. *Application layer:*
   - We can apply the security by implementing the idea of the CIA Triad.
   - Use security tools as: firewalls and proxy servers
   - The availability can accomplish by using: Virtual Machine Monitor, Intrusion Detection System, and Service Level Agreement
   - We can use the idea of the iPhone when you try many PIN the iPhones lock (we can avert the brute-force attack).
   - The IoT software should be always update to the last version.

❖ *Other Countermeasures :*

1- Develop the lightweight block cipher algorithms [3].
2- Biometric Security [4]: It holds two type
   - Physiological traits such as: finger-print (it is the most common use), iris eye, DNA, and veins.
   - Behavioral traits: It uses for the authentication such as the person walk pattern, the sound, and signature
3- CoAP with Security Features [4]: CoAP stands for Constrained Application Protocol. If we use it with IPSec or TLS it will provide secure communications.
4- Embedded Security Solutions [4]: IoT contain a big number of tiny devices embedded systems are the most use. It uses encryption algorithms like AES, ECC, and RSA.
5- RFID Authentication Schemes [4]: They use it to identify a unique entity or for authentication.
6- Trust Management Scheme [4]: The privacy of a node is taken as a dead earnest part of the trust management. Also, Digital signatures are used to achieve trust.

VI. CONCLUSION

By the end of our survey paper; we have concluded that the field of the IoT is still lacking in many things in many aspects where This greatly affected IoT security. One of the most important things that there is no unified architecture of the IoT, as the presence of many architectures (3- layer,4-layer,5-layer) has made it difficult to implement one security mechanism on them all. Also, since there are no unified security standards, and they often rely on the CIA triangle and add some necessary standards according to the application. So it would be beneficial if there was an official body or a union of companies operating in IoT, that sets laws and rules of the IoT and specifies safety standards that must be followed and adhered to, and determine the methods of communicating between the layers. Where we believe that if the concept and architecture are consolidated, researchers and developers will have a unified vision that enables them to unite their efforts in research and development. This will make a big difference in the advancement and development of security and the production of innovations.

REFERENCES

[1] Scully, P. *Top 10 IoT applications in 2020*. July 8,2020 [cited 2020 29 november]; Available from: https://iot-analytics.com/top-10-iot-applications-in-2020/.

[2] Burhan, M., Rehman, R. A., Khan, B. and Kim, B. S., *IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey*. Sensors (Basel), 2018. **18**(9).
[3] Hyungsik Shin, H.K.L., Ho-Young Cha, Seo Weon Heo, and Hyungtak Kim, *IoT Security Issues and Light Weight Block Cipher*, in *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. 2019, IEEE: Okinawa, Japan, Japan. p. 381.
[4] Rao, K.S.N.a.D.S.S., *Security Challenges and Counter Measures in Internet of Things*, in *2020 International Conference on Computer Communication and Informatics (ICCCI -2020)*. 2020, IEEE: Coimbatore, INDIA.
[5] Ghadeer, H., *Cybersecurity Issues in Internet of Things and Countermeasures*, in *2018 IEEE International Conference on Industrial Internet (ICII)*. 2018. p. 195-201.
[6] Jihad DAZINE, A.M.a.L.H., *Internet of things security*, in *2018 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD)*. 2018, IEEE: Marrakech, Morocco, Morocco. p. 137.