SECURITY CONCERNS IN 3-TIER ARCHITECTURAL FRAMEWORK OF INTERNET OF THINGS (IoT)

[1]Farheen Miraj Khan,[2]Syed Yasmeen Shahdad,[3]Syeda Meraj Bilfaqih, [4]Habeeba Sultana,[5]Mohammed Ashfaq Hussain

[1]Lecturer, [2]Lecturer, [3]Lecturer, [4]Lecturer,[5]Lecturer
[1]Department of Computer Science,
[1]King Khalid University, Abha, Saudi Arabia

ABSRACT

This paper performs a survey and analysis on the concerns of the Internet of things (IoT) security. The IoT architecture and framework aims to connect anyone with anything and anywhere. IoT connects large number of machines, IoT devices and sensors that use heterogeneous networks (wired and wireless). IoT characteristically have three layers as Perception, Network, and Application layer. This paper describes the security and privacy concerns of IoT at every layer of IoT architecture. Finally, the paper presents conclusion and future directions for securing the IoT at every level so as to maximize the efficiency of IoT systems.

***IndexTerms*— IoT, 3- tier Architecture, Security threats**

I. INTRODUCTION

Internet of things (IoT) is assemblage of the interconnected objects, devices, people, and different services which communicate, share the data and information to accomplish common goals in many different areas as well as applications. The implementation of IoT can be done in different domains which include transportation, healthcare, energy production and many different fields that need things so as to communicate across Internet in order to perform intelligent business tasks without requiring the human involvement.
The goal of IoT is to change the way that we live in today by allowing intelligent devices all around us to accomplish daily tasks with minimal human interference. Smart homes, smart cities, smart transportation etc. are some of the terms that are used in significance to IoT. The IoT concept can be seen in different sci-fi movies, cartoons, and shows, although it seems difficult to achieve, but the fact is that in near future many features of IoT would be realized. There are numerous application areas for IoT, extending from personal environments to the enterprise environments.Mainly due to the emerging technologies like Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN), IoT has seen a rapid growth in recent times. In RFID each single device is labelled or tagged, serving the primary identification process in IoT. Owing to WSN, each single “thing” (e.g., people, devices etc.) becomes an identifiable object (wireless) which can communicate amongst the physical, cyber, and the digital worlds[1].Apart from the benefits that IoT has come up with, there are numerous security concerns at different layers of IoT. This paper puts its focus on several security issues that can be found in all the three layers of IoT framework and architecture. The paper is planned as follows. Section 2 describes three layer IoT framework and architecture. Section 3, comprises of the security issues for each layer of IoT. Section 4 gives the relevant conclusion and talks about the future work that must be done, keeping in view the security concerns of IoT.

II. ARCHITECTURE OF IoT

In the architecture of IoT, each layer can be defined by the functions and devices, used in that particular layer. Different opinions can be found given about how many numbers of layers are in IoT. But many researchers believe that [2-4], the IoT mainly operates on the three layers that are as Perception, Network, and Application layer. Each IoT layer has intrinsic security problems linked with it. Fig. 1 shows the architectural framework of the IoT corresponding to different devices and the technologies that encompasses each layer.

2.1. PERCEPTIONLAYER

This layer is also known by the name “Sensors” layer in IoT. The main purpose of perception layer is acquiring the data from environment using help from sensors. The perception use sensors for detecting, collecting and processing information and then transmitting it to the network layer. In addition to this, perception layer can also perform IoT node collaboration for networks that are both local and in short range [3].

2.2. NETWORKLAYER

Network layer serves the purpose of data routing and data transmission to various hubs of IoT as well as devices that are spread over Internet. For providing the heterogeneous network services, devices such as internet gateways, routers, switches operates by using the latest technologies like 3G,Zigbee,4G,Bluetooth etc. network gateways work as mediator in-between different types of IoT nodes by performing data aggregation, filtration and transmission to and back from the different sensors[4].

2.3. APPLICATIONLAYER

This layer guarantees that the data is authentic, and confidential. The responsibility of this layer is to provide services and determine protocols for the process of message passing at this particular level in the application layer, the primary purpose of IoT that is the construction of the smart environments isaccomplished.

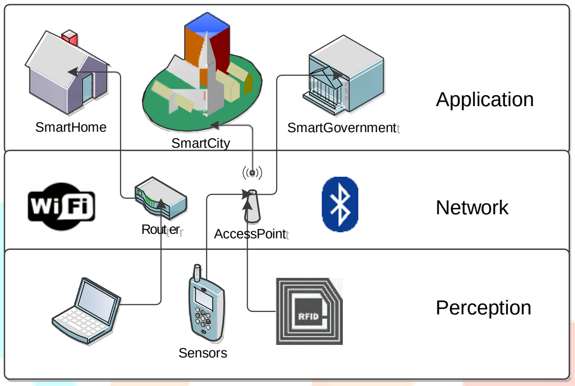

fig. 1. Three layer of IoT architecture

III. SECURITY ISSUESIN IoTLAYERS

Each layer of IoT is vulnerable to the security attacks. These attacks can range from being active types, or passive types, and can initiate the external sources or the internal network due to attack by an Insider [1]. Services are directly stopped by the active attack while as thepassive type monitors the network information of IoT without hampering its service. each layer of devices as well as services in IoT are prone to the Denial of Service attacks (DoS), that make device, resource or the network unavailable to the authorized users . Table 2 states the security concerns at each layer and following that is the detailed analysis of issues at each layer of IoT.

Table 2. Security Concerns at Each IoT Layer

Layer	**Security Concerns and Threats**
Perception	Wireless signal strengths, physical attacks, dynamic IoT topology
Network	Traffic analysis, eavesdropping, passive monitoring, heterogeneity of network components and protocols
Application	Absence of global and standard trust policies, authentication mechanisms

3.1. PERCEPTION LAYER

This layer encountersthree security issues. Firstly the problem is in the wireless signals strength. Generally signals are transmitted among the IoT sensor nodes using the wireless technologies whose effectiveness could be compromised by the disturbing waves. Secondly, sensor node in the IoT devices could be intercepted by both the owner and attackers as the IoT nodes generally operates in the external and outdoor environments, which leads to the physical attacks on the IoT sensors and the devices by which attacker can be able to tamper hardware components of IoT device. Third concern is the network topology that is dynamic in nature as the nodes are usually moved around to different places. The perception layer mainly comprises of the sensors and RFIDs, by which there is limitation in their storage capacity, the power consumption, and the computation capability and that makes them vulnerable to different types of threats and attacks [1, 5].The privacy of the perception layer can be exploited easily by the Replay Attack that could be made by process of spoofing, altering or replaying the identity data of one of the IoT devices Or alternatively, attacker may get the encryption key by examining the time that is required to perform encryption and is known as the Timing Attack. One more privacy attack is when attacker takes over IoT node and captures every information that isFundamentally Node Capture attack. The Attacker can threaten the integrity of data in perception layer by adding additional node to network and sending the malicious data. This also leads to DoS attack, by the energy consumption of nodes in IoT system and thus depriving it from sleep mode which nodes usually use to save energy [6].

The security issues in perception layer listed above can be handled using the encryption process that may be point-to-point or end-to-end process of authentication (by which the identity of sender can be verified) and the access control system [5].

3.2 NETWORK LAYER

As already mentioned the IoT network layer is too vulnerable to the DoS Attacks. There can also be attack on confidentiality and the privacy at this layer due to traffic analysis, eavesdropping, and the passive monitoring [1]. These kinds of attacks have high probability of occurring because of remote access process and the data exchange of the devices. Also the security in the communication channel of this layer can be compromised if the devices keying material is eavesdropped. The mechanism of key exchange in IoT need to be very much secure in order to stop any intruder from committing the identitytheft by eavesdropping.The communication process in IoT is quite different from Internet as its not limited to machine and human interaction. Nevertheless, the machine- to-machine communication process that IoT has introduced has the compatibility issue. The heterogeneity of network components makes the usage of current network protocols difficult and it still produces the effective protection mechanisms. Attackers might as well takethe advantage by gaining more information about the users due to the fact that everything is connected and then can use this information for illicit activities [2]. Protection of network is very important in IoT, along with the protection of objects which is equally vital. The IoT Objects should have the required ability to know “state of network” and also to safeguard them from any threat or attacksagainst network. It can be achieved by development of software and protocols which enables the object to respond to any of the situations or behaviors which may be thought of as abnormal or might have their security being affected[7].

3.3. APPLICATION LAYER

Since there is absence of global policies and standards which administrate interaction and development of the applications, many security issues have come up. There are various authentication mechanisms for different software’s and applications that makes integration of them very much difficult in order to guarantee the data privacy and the identity authentication process. The big amount of the connected devices who share the data would cause the huge overhead on the applications which examine the data, and thus can have a huge effect on the service availability. Another issue which should be put in consideration, when designing applications in the IoT is that how various users would interact with them, volume of data that would be shown and who will have the responsibility for managing process of these applications. The must be some tools for the users so that they can have a control on what type of data they wish to reveal and also they need to be conscious about how this data would be used, when and by whom.

IV. CONCLUSION AND FUTURE WORK

The IoT architecture and framework has many existing concerns at each of the three layers and is also vulnerable to attacks at these layers. Therefore, there are many security challenges and requirements that need to be addressed which affect the IoT performance. These challenges and issues have to be solved in order to efficiently utilize this smart technology.in future we will focus on the security concerns at every layer of IoT and try to address it in order to maximize the IoT efficacy.

V. REFRENCES

[1]M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in Int'l Conference on Privacy and Security in Mobile Systems (PRISMS), 1-8,2014.

[2]K. Zhao and L. Ge, "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667, 2013.

[3]L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet theinternetofthings:Concept,architectureandnetwork characterization," Computer Networks, vol. 56, 3594-3608, 2012.

[4]M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC), 1-5, 2014.

[5]Q. Wen, X. Dong, and R. Zhang, "Application of dynamic variable cipher security certificate in internet of things," in Int'l Conference on Cloud Computing and Intelligent Systems (CCIS), 1062-1066, 2012.

[6]M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol. 111, 2015.

[7]R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," Computer, vol. 44, 51-58, 2011.