

21011101066-CIA-1-IOT

Renigale Rg

January 2023

1

## PAPER REVIEW

### IoT Elements, Layered Architectures and Security

AUTHORS: Muhammad Burhan, Rana Asif Rehman, Bilal Khan and Byung-Seo Kim.

#### INTRODUCTION

The Internet has become a basic need of millions of people who use it for many purposes according to their needs. People not only use the Internet for entertainment but also to fulfill their daily tasks and needs that cannot be done without it. It is estimated that about 48 percent of the world's population use the Internet due to its popularity and benefits that are provided to the people by the Internet. Another aspect of increasing the users of the Internet is that people can communicate and synchronize to other people all over the world via the Internet. Due to the benefits of the Internet, another field is growing, which allows objects and machines to connect and communicate to each other with the presence of the Internet, called the Internet of Things (IoT). There are several technologies and sensors used to implement the idea of IoT. There are a lot of applications in which IoT has been deployed, they have become smart and perform their work robotically by taking help from the Internet. This article deals with three such applications. The first one being health care where sensors are used to check human's body temperature, blood pressure and heart beat rate. The second application is smart home because humans use many electronic things like refrigerators, microwave ovens, fans, heaters and air conditioners at home. The sensors are installed to detect the problem and tell about the problem to the manufacturing company in order to solve it. The third application of IoT is animal tracking. The GPS sensors are installed in an animal's body to trace them easily. It is also used to monitor the animal's feed. According to this article, The number of IoT devices are increasing each and every day. The

reason for increasing the number of IoT devices is that they provide comfort in human life and perform work with better outcomes than humans. It has been reported that, in 2018, the number of IoT devices will have more than tripled since 2012 and there will be 50 billion devices that will work on the Internet . The article that I have read aims to

- Give a picture of all proposed layered architecture of IoT,
- Highlight the security attacks that can occur on each layer and affect the IoT applications,
- Present the communication technologies used by IoT applications along with characteristics and drawbacks as well, Sensors 2018, 18, 2796 4 of 37
  - Provide information about security mechanisms used to protect IoT.
- Suggest a new and generic six-layered secure architecture that can easily be extended with little impact to existing architectures to make secure IoT applications.

## IOT ELEMENTS

IoT provides many benefits and facilities to users. Thus, in order to use them properly, there is a need for some elements and these elements are called IOT elements.

### **i). Identification**

Identification offer explicit identity for each object within network. There are two processes in identification; naming and addressing. Naming refers as name of the object while addressing is the unique address of specific object. These both terms are very different from each other because two or more objects may have same name but always different and unique address.

### **ii). Sensing**

The process of collecting information from objects is known as sensing. The collected information is sent to the storage media. There are many sensing devices to collect the information from objects such as actuators, RFID tags, smart sensors, wearable sensing devices, etc.

### **iii). communication**

Communication is one of the main purposes of IoT in which different devices are connected to each other and communicate. In communication, devices may send and receive messages, files and other information. There are many technologies that provide facility of communication like Radio Frequency Identification (RFID), Near Field Communication (NFC), Bluetooth, Wi-Fi and Long Term Evolution (LTE).

### **iv). Computation**

Computation is performed on the collected information from the objects by using sensors. It is used to remove unnecessary information that is not needed. Many hardware and software platforms are developed to perform the processing

in applications of IoT.

**v). Services**

There are four types of services that are provided by the IoT applications. The first one is an identity-related service. It is used to get the identity of objects that have sent the request. The second one is Information aggregation is another service whose purpose is to collect all the information from objects. The third service is a collaborative service that makes decisions according to the collected information and sends appropriate responses to the devices. The last service is ubiquitous service, which is used to respond the devices immediately without rigidity about time and place.

**vi). Semantics**

It is the responsibility of IoT to facilitate users by performing their tasks. It is the most important element of IoT to fulfill its responsibilities. It acts like the brain of IoT. It gets all information and makes appropriate decisions to send responses to the devices.

## **IoT Layered Architectures with Security Attacks**

### **Three Layer Architecture**

It is a very basic architecture and fulfills the basic idea of IoT. It was proposed in the early stages of development of IoT.

**i). Perception Layer**

It is also known as a sensor layer. It works like people's eyes, ears and nose. It has the responsibility to identify things and collect the information from them. There are many types of sensors attached to objects to collect information such as RFID, 2-D barcode and sensors. The sensors are chosen according to the requirement of applications. The information that is collected by these sensors can be about location, changes in the air, environment, motion, vibration, etc.

**ii). Network Layer**

Network layer is also known as transmission layer. It acts like a bridge between perception layer and application layer. It carries and transmits the information collected from the physical objects through sensors. The medium for the transmission can be wireless or wire based. It also takes the responsibility for connecting the smart things, network devices and networks to each other. Therefore, it is highly sensitive to attacks from the side of attackers. I

**iii). Application Layer**

Application layer defines all applications that use the IoT technology or in which IoT has deployed. The applications of IoT can be smart homes, smart cities, smart health, animal tracking, etc. It has the responsibility to provide the services to the applications. The services may be varying for each application because services depend on the information that is collected by sensors. There are many issues in the application layer in which security is the key issue. In particular, when IoT is used in order to make a smart home, it introduces many threats and vulnerabilities from the inside and outside.

## **FOUR LAYER ARCHITECTURE**

The three-layer architecture was most basic architecture. Due to continuous development in IoT, it could not fulfill all the requirements of IoT. Therefore, researchers proposed an architecture with four layers. In addition to the three layer architecture there is an additional layer in four layer architecture known as SUPPORT LAYER.

### **support layer**

Information is sent to a support layer that is obtained from a perception layer. The support layer has two responsibilities. It confirms that information is sent by the authentic users and protected from threats.

## **FIVE LAYER ARCHITECTURE**

The newly proposed five layer architecture has the ability to fulfill requirements of IoT. It also has the ability to make the applications of IoT secure. The workings of these layers and security attacks that can effect them are as follows:

### **i). Processing Layer**

The processing layer is also known as a middleware layer. It collects the information that is sent from a transport layer. It performs processing onto the collected information. It has the responsibility to eliminate extra information that has no meaning and extracts the useful information. However, it also removes the problem of big data in IoT. In big data, a large amount of information is received which can affect performance of IoT.

### **ii). Business Layer**

The business layer refers to an intended behavior of an application and acts like a manager of a whole system. It has responsibilities to manage and control applications, business and profits models of IoT. The user's privacy is also managed by this layer. It also has the ability to determine how information can be created, stored and changed. Vulnerability in this layer permits the attackers to misuse an application by avoiding the business logic.

## **SECURITY ISSUES IN COMMUNICATION TECHNOLOGIES OF IoT**

**ZigBee Technology**

ZigBee is a PAN (personal area network). It provides low-power consumption at a low cost to obtain the trust of maximum users. It provides wireless communication to transmit information within a short range. The layered architecture of ZigBee technology consisting of four layers by named application, network, Media Access Control (MAC) and physical layer.

**Bluetooth Technology**

Bluetooth is used for applications that want to communicate within a short distance. It provides many security mechanisms to make secure communication between sender and receiver. It provides a facility of encryption in which a message is converted into another form, called cipher text.

**Radio Frequency Identification**

RFID uses frequency waves for communication between two devices. It has three parts: tags, reader and a database. The tags are attached to the objects and read the state of the objects while a reader is used to read the information from tags. A database is considered as a third part and it is used to store information. It provides the facility of encryption to transmit the information. There are three types of encryption that can be used by it.

**Wireless Sensor Network**

WSNs have many nodes and each node has four parts: sensors, battery, micro-controller and memory. The functionality of WSN can easily be understood in this way in which sensors are used to collect the information and store it in its memory for reuse. It sends all information to the server. Batteries are also used that provide facilities to work continuously.

**CONCLUSION**

The emerging idea of Internet of Things (IoT) is quickly finding its path throughout our modern life, aiming to enhance the quality of life by connecting various smart devices, technologies and applications. Generally, the IoT would allow for the automation of everything around us. The paper has articulated different research about layered architectures of IoT and also described security attacks based on the layers that can affect the performance of IoT. The communication technologies have been presented with their features and limitations. The authors have surveyed the literature on the existing mechanisms to protect the IoT infrastructure and summarized the security methods on how they address the security issues in the IoT.