Internet of Things: Architecture, Existing Protocol and Security Challenges

Ansari Kashafurrehman, Raj Kumar
Department of Computer Science & Engineering,
Rattan Institute of Technology & Management
Palwal, Haryana India 121102.

Abstract

The Internet of Things (IoT) is part of every of human life, that deals from smart phones and environmental sensors to smart devices used in the industry. IoT is a large distributed network in which billions of devices are interconnected and capable of preprocessing raw data and taking decisions on their own .It is considered to be the largest wave of resolution as it does not require human to machine interaction. However, with rapid growth of IoT, challenges in terms of security have evolved as well. Since IoT consist of three layers perception layer, network layer and application layer.

This paper presents an effort to describe the IoT protocol stack and some of the most commonly used protocols and an analysis for various security problems at each layer including the cross-layer heterogeneous integration security issues.

Keywords: *IoT, protocols stack, security challenges.*

I. INTRODUCTION

The first-time the term "Internet of Things (IoT)" was used was by Kevin Ashton in 1999, the pioneer of British technology [11]-[16]. According to Kevin Ashton, Internet of Things defines the system of physical objects in the world that connect to the internet via a sensor. Ashton has also invented the term Radio-Frequency Identification (RFID) that tags the physical objects to the internet for the purpose of counting and tracking of goods without any human interference [12].

The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances and otheritems embedded with electronics, software, sens ors, actuators, and connectivity which enables these things to connect and exchange data[1-6]. Due to the expansion of internet in recent times and its being used in various devices and by humans, the scope of use of the internet of things in much broader than it could be imagined. The number of IoT devices increased 31% year-over-year to 8.4 billion in 2017 and it is estimated that there will be 30 billion devices by 2020. The global market value of IoT is projected to reach $7.1 trillion by 2020. It allows machine to machine (M2M) communication where big "things" will be able to communicate through the wired connections such as fiber optics and Ethernet. Furthermore, most of the connections are expected to take place via wireless networks with microchips embedded into the "things" using various standards such as ZigBee, Wi-Fi, Bluetooth, RFID, and NFC in order to achieve an effective communication. In common parlance, the Internet of Things refers to a new kind of world where almost all the devices and appliances that we use are connected to a network. We can use them collaboratively to achieve complex tasks that require a high degree of intelligence.For this intelligence and interconnection, IoT devices are equipped with embedded sensors, actuators, processors, and transceivers. IoT is not a single technology; rather it is an agglomeration of various technologies that work together in tandem.

Sensors and actuators are devices, which help in interacting with the physical environment. The data collected by the sensors has to be stored and processed intelligently in order to derive useful inferences from it. Note that we broadly define the term sensor; a mobile phone or even a microwave oven can count as a sensor as long as it provides inputs about its current state (internal state + environment). An actuator is a device that is used to effect a change in the environment such as the temperature controller of an air conditioner.

The storage and processing of data can be done on the edge of the network itself or in a remote server. If any preprocessing of data is possible, then it is typically done at either the sensor or some other proximate device. The processed data is then typically sent to a remote server. The storage and processing capabilities of an IoT object are also restricted by the resources available, which are often very constrained due to limitations of size, energy, power, and computational capability. As a result the main research challenge is to ensure that we get the right kind of data at the desired level of accuracy. Along with the challenges of data collection, and handling, there are challenges in communication as well. The communication between IoT devices is mainly wireless because they are generally installed at geographically dispersed locations. The wireless channels often have high rates of distortion and are unreliable. In this scenario reliably communicating data without too many retransmissions is an important problem and thus communication technologies are integral to the study of IoT devices. Now, after

processing the received data, some action needs to be taken on the basis of the derived inferences. The nature of actions can be diverse. We can directly modify the physical world through actuators or we may do something virtually. For example, we can send some information to other smart things. The process of effecting a change in the physical world is often dependent on its state at that point of time. This is called context awareness. Each action is taken keeping in consideration the context because an application can behave differently in different contexts. For example, a person may not like messages from his office to interrupt him when he is on vacation. Sensors, actuators, compute servers, and the communication network form the core infrastructure of an IoT framework. However, there are many software aspects that need to be considered. First, we need a middleware that can be used to connect and manage all of these heterogeneous components. We need a lot of standardization to connect many different devices. The Internet of Things finds various applications in health care, fitness, education, entertainment, social life, energy conservation, environment monitoring, home automation, and transport systems.

II. IOT ARCHITECTURE

There is no single consensus on architecture for IoT, which is agreed universally. Different architectures have been proposed by different researchers. The IoT layers differ from each other by the role they and the devices operating at them.

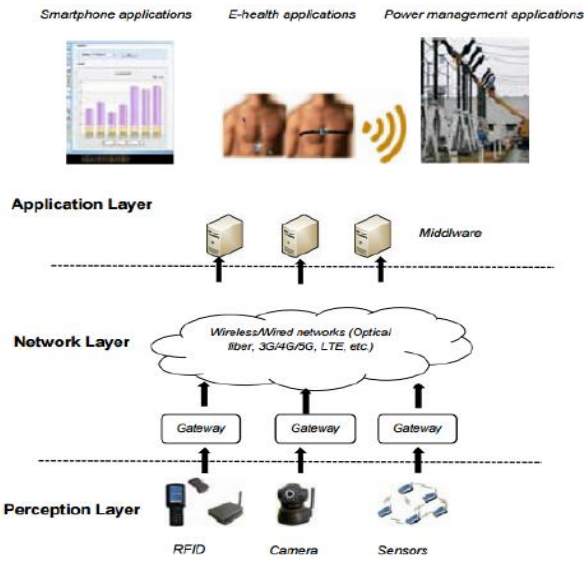

Figure 1.IoT Architecture

A. Perception layer is concerned with collecting and sensing the information of IoT objects. The collection of valuable information is done by this layer with the help of various devices such as sensor nodes, camera and RFID tags. Perception node such as controllers or sensors is used for data control and data acquisition. While perception network is used to send control signals to the controller or send the collected data to the gateway to be transmitted in the Network Layer.

B. Network layer has the function of managing wireless and wired connections. It transfers the gathered data through the sensors, and computers across the wired and wireless networks .It can also support connection oriented service through maintaining reliability of data delivery. Routing takes place at this layer where data is transmitted across different IoT devices and hubs over the internet. Routing, switching, gateway devices operates at this layer using variety of technologies such as Zigbee, WiFi, 3G, Bluetooth and LTE. The gateway acts as a medium between separate IoT devices by aggregating, filtering and moving data between different sensors.

C. Application layer is the interface between the applications and the end users. It provides the means for the communication between them. It can support various services required by business. In addition, it recognizes the resource allocation and computation in producing, processing, screening and selection of data. It has the ability of recognizing spam data, malicious data and valid data through its filtering feature. It resolves the received information and make control decisions to allow the achievement of intelligent processing by identification, connection, and control between devices and objects. It is also known as Process layer.

III. PROTOCOL STACK FOR IOT

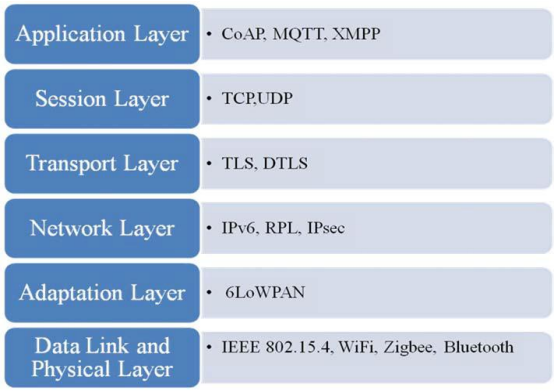

Figure 2.IoT Protocol Stack

The IoT protocol stack is shown in Fig.2. The protocols used at each layer are different than the protocols used in the traditional networking [17]. From the bottom to top approach the protocol stack can be described from the physical layer to application layer as follows.

A. Physical and Data Link Layer

This is first layer of the protocol stack. IoT sensors work at these layers as physical devices. The

other communication protocols like Bluetooth, ZigBee etc.

B. Adaptation Layer

A new layer is introduced between the Data Link and Network called Adaptation Layer. This layer enables the packets of IPv6 to get transferred over the 802.15.4 network by making the suitable adaptations. The protocols works on this layer is 6LoWPAN which stands for IPv6 over Low Power Wireless Personal Area Network. This protocol is specially designed for IoT devices working at low power.

C. Network Layer

The protocol which is primarily used at this layer is IPv6. As in case of IoT the router and its connecting devices are mainlyconstraint have categorized as low power lossy network(LLN). Hence IPv6 Routing Protocol for Low-Power and
Lossy Networks (RPL) is used at this layer which providesfacility for devices to perform point to point or multipoint communication.

IV. SECURITY CHALLENGES IN IOT

The key challenges facing the realization of the Internet of Things is the security challenges, especially in the area of privacy and confidentiality among heterogeneous management and network capacity constraints.

The devices of Internet of Things use many technologies,including communications, sensors, big data, etc., therefore, they have different security issues and because of the features of devices of Internet of Things such as low power consumption,
light calculations, etc other issues emerge as well. In this section, we summarize the security needs of internet devices:

1. Lightweight Protocol and Encryption

We have to select lightweight protocol and encryptionin accordance to the device and the importance of the data, processing capabilities and power consumption of the device.

2. Communications Security

The devices of internet of things can use communications such as short distance (Bluetooth), wireless, and wired. Therefore, security issues are required to support availability, confidentiality, authentication, and so on.

3. Data Protection

The data on devices of internet of things can include user information, including physical information, locus of induction, user behavior, etc. Therefore, data must remain confidential until being sent to other devices or storage locations using appropriate encryption

.

4. Physical protection

Due to the ease of access to internet devices, we have to find a way in order to control physical access.

5. Identification and Allowing Access to Devices of Internet of Things

We can add or reduce several devices of Internet of Things in the network and each device has different licenses and domains. Therefore, it is necessary to identify and authenticate internet devices and permit the use of ID / password / MAC / certificate.

6. Monitoring and Controlling internet Devices

Malware can damage, infect, or violated internet devices. Therefore, we need to control the activities of internet device in order to identify malicious behaviors

D. Perception Layer - The IoT perception layer is facing three security issues. First, IoT nodes operate in outdoor environment, leading to physical attack where the hardware components can be tampered by the attacker. Second, the heterogonous nature of the dynamic network allows mobility of IoT devices. However, due to the computation capability, power consumption, and storage capacity limitation, it makes them susceptible to many kinds of threats and attacks. Third, since IoT uses wireless technologies for transmission of information, other existing waves can cause reduction in the strength of the wireless signals

Security threats	Description
Unauthorized access	Due to physically capture or logic attacked, the sensitive information at the end-nodes is captured by the attacker;
Availability	The end-node stops to work since physically captured or attacked logically;
Spoofing attack	With malware node, the attacker successfully masquerades as IoT end-device, end-node, or end-gateway by falsifying data
Selfish threat	Some IoT end-nodes stop working to save resources or bandwidth to cause the failure of network
Malicious code	Virus, Trojan, and junk message that can cause software failure
Denial of Services (DoS)	An attempt to make a IoT end-node resource unavailable to its users
Transmission threats	Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc.
Routing attack	Attacks on a routing path

Figure 3. Security Concerns at Perception layer

E. Network Layer- As mentioned before, the transmission medium□s broadcast nature and the sensor nodes computation and power limitation makes network layer more prone to DOS attacks. Aside from the DoS attacks, the privacy and confidentiality of the network layer can be compromised by passive monitoring, traffic analysis and eavesdropping attacks. These attacks occur due to the data exchange between the devices and remote

access mechanisms which are the main functions provided by this layer.

Although IoT provides the ability of automatic data transfer across the network without requiring human to computer or human to human interaction by introducing machine-to-machine communication, attackers can make use of all devices and objects which are connected to perform information theft and criminal activities. Therefore, protecting the objects is equally important to protecting the network. Objects should have a mechanism for sensing network threats and providing the necessary protection against various network attacks. This can be accomplished by designing software and protocols which can allow device instant reaction against unexpected situation which can have a negative impact on the security.

Security threats	Description
Data breach	Information release of secure information to an untrusted environment
Transmission threats	The integrity and confidentiality of signaling
Denial of Services (DoS)	An attempt to make a IoT end-node resource unavailable to its users
Public key and private key	The comprise of keys in networks
Malicious code	Virus, Trojan, and junk message that can cause software failure
Transmission threats	Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc.
Routing attack	Attacks on a routing path

Figure 4. Security Concerns at Network layer

F. Application Layer - The application layer has many security related issues as IoT lacks standards and global polices that controls the development and the interaction between different applications.

The big amount of data that is shared by the connected devices can result into a large overhead on the applications that analyze the data leading to a great impact on the services availability. There are several things to keep in mind when designing an applications in IoT, the amount of data that will be shared, the interaction nature between various users and different applications, and the application management. Some tools must be designed to allow the users to have control upon data disclosure and authenticate the other communication parties.

Security threats	Description
Remote configuration	Fail to configure at interfaces
Misconfiguration	Mis-configuration at remote IoT end-node, end-device, or end-gateway
Security management	Log and Keys leakage
Management system	Failure of management system

Figure 5. Security Concerns at Application layer

V. CONCLUSIONS

The security issues at IoT architecture was the focal point ofthis paper. Services provided by each layer have been highlighted as well as the security issues were introduced. In addition, the security challenges across the layers have been analyzed .It was observed that each layer from the IoT framework is exposed to different types of attacks. For this reason, many security challenges need to be solved. IoT is an innovative technology but still in its early development stage. There are some further studies which research can focus on such as developing lightweight cryptographic algorithms, and developing a secured architecture for IoT system.

REFERENCES

[1] "Internet of Things A to Z: Technologies and Applications". Wiley.com. 2018-06-13. Retrieved 2018-06-05.

[2] Brown, Eric (13 September 2016). "Who Needs the Internet of Things?". Linux.com. Retrieved 23 October 2016.

[3] Brown, Eric (20 September 2016). "21 Open Source Projects for IoT". Linux.com. Retrieved 23 October 2016.

[4] "Internet of Things Global Standards Initiative". ITU.Retrieved 26 June 2015.

[5] "Internet of Things: Science Fiction or Business Fact?" (PDF). Harvard Business Review. November 2014. Retrieved 23 October 2016.

[6] Hendricks, Drew. "The Trouble with the Internet of Things". London Datastore.Greater London Authority.Retrieved 10 August 2015.

[7] Vermesan, Ovidiu; Friess, Peter (2013). Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems (PDF). Aalborg, Denmark: River Publishers. ISBN 978-87-92982-96-4.

[8] Santucci, Gérald. "The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects" (PDF). European Commission Community Research and Development Information Service.Retrieved 23 October 2016.

[9] Mattern, Friedemann; Floerkemeier, Christian. "From the Internet of Computers to the Internet of Things" (PDF). ETH Zurich.Retrieved 23 October 2016.

[10] Lindner, Tim (13 July 2015). "The Supply Chain: Changing at the Speed of Technology". Connected World.Retrieved 18 September 2015.

[11] W. Mingjun, Y. Zhen, Z. Wei, D. Xishang, Y. Xiaofei, S. Chenggang, et al., "A research on experimental system for Internet of Things major and application project," in System Science, Engineering Design and Manufacturing Informatization (ICSEM), 2012 3rd International Conference on, 2012, pp. 261-263.

[12] K. Rose, S. Eldridge, and L. Chapin, "The Internet of Things (IoT): An Overview– Understanding the Issues and Challenges of a More Connected World," Internet Society, 2015.

[13] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future generation computer systems, vol. 29, pp. 1645-1660, 2013.

[14] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of internet of things (IoT)," International Journal of Computer Applications, vol. 111, 2015.

[15] T. V. N. Rao, S. K. Saheb, and A. J. R. Reddy, "Design of Architecture for Efficient Integration of Internet of Things and Cloud Computing," International Journal, vol. 8, 2017.

[16] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," Wireless Personal Communications, vol. 58, pp. 49- 69, 2011.

[17] Maria Rita Palattella et al. , "Standardized Protocol Stack for the Internetof (Important) Things", IEEE COMMUNICATIONS SURVEYSTUTORIALS, 2012.