Turkish Journal of Computer and Mathematics Education Vol.12 No.13 (2021), 1761-1765

Research Article

ADAS Authentic Data Allowed Security In Internet Of Things

Raveena Yadav [a], Vinod Kumar[b]

[a] Research Scholar, Department of Computer Science Engineering, Delhi Technological University, Delhi, India
[b]Associate Professor, Department of Computer Science Engineering, Delhi Technological University, Delhi, India

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract: With the growing of population, things and networks, things connectivity is also taking a graph in exponential manner. This whole connectivity makes a whole network that is known as Internet of Things. But these devices are prone to cyber-attacks, so, security is one of the apex concerns and challenge for internet of things. Main motivation of writing this paper is that security is the main concern whether it is internet or internet of things. In this paper, we have proposed a model Authentic Data Allowed Security, in which only authentic packets are allowed to enter and usable by node and all other packets will be dropped by the router

Keywords: Internet of Things, Security, Authentic data

1. Introduction

Internet is one of the networks, in which our confidential data move from one device to another. So, there is a chance that intruder is waiting for accessing the data. That's why cyber-attack is increasing day by day, besides these new measures are also taken up for nurturing the privacy of data. In this high-tech world, devices are connected to internet and doing communication without the interference of human being and transferring the data from one node to another node and this is we can say Internet of Things (IoT). The idea of connecting devices to the internet, has come in the 90's and the term of IoT is coined by Kevin Ashton in 1999. There are many definitions given by different scientist and researchers. In [2], author described IoT as a revolutionary and global network, in which devices are getting smarter day by day and do the communication. In [5], IoT as the intelligent network in which smart devices can be tracked, monitored and managed remotely. IoT can be defined as the virtual connection between the two or more than two things and these connections are maintained by different networks such as WiFi, Bluetooth, Zig bee, RFID and many more networks are presents as shown in Figure 1.

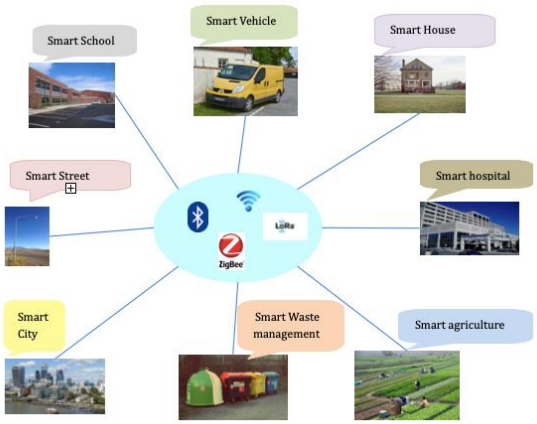

Figure 1: IoT in different sectors

There are several types of security issues happened and still happening in the IoT world such as intruder can access the information and misuse data, send the data continuously so that node or device would not able to use the resources, transfer the data to the wrong intruder and many other ways attacks can happen.

IoT can be understood with a contrast and comparative relation with the human body as shown in Figure 2. Human body has five sense organs; eyes, ear, nose, tongue and skin like this IoT has sensors that help in sensing the change in surrounding so that actuators can perform action. Nerves and neurons in the human body help in transmitting the messages, blood and oxygen, IoT has its different networks Bluetooth, Wi Fi, LoRa, Zig bee and many more through which communication happens in the IoT network.

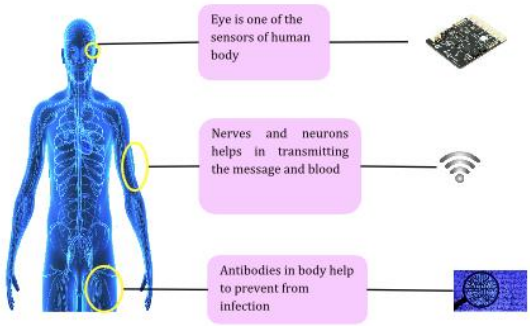

Figure 2 : IoT contrasting with Human body

This paper is divided into numerous sections, in the first section we already have discussed the Introduction of Internet of Things, in second section different layer of IoT, in section third various issues in IoT, in fourth section proposed model and in fifth section described the future scope of this research.

2. Layers in IoT

For better understanding of the complex network of IoT, researchers had divided the network into three layers, four layers and five layers. In this section, we discussed three layered model of architecture as shown in figure 3.

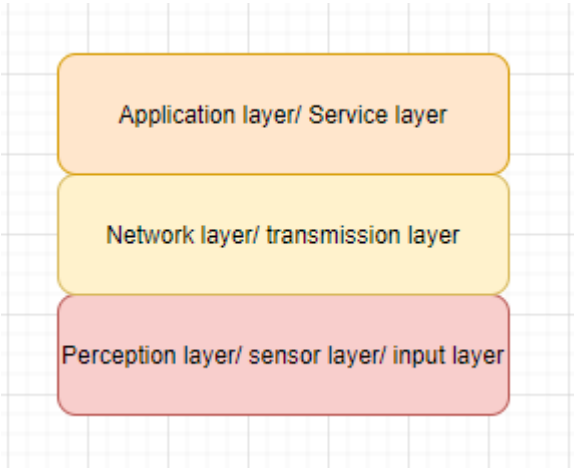

Figure 3: Three-Layered architecture of Internet of Things

Input layer: Perception layer of the IoT architecture takes the input from its surrounding. This layer can be called as sensor layer or input layer or perception layer. The main component of this layer is sensor, RFID and actuators, that helps in getting the information for further processing and identifying the objects uniquely. The range of sensor depends upon the power of sensor and area covered by that sensor.

2.1..Network layer

This layer helps in transmitting the message from one device to another device. In comparison to the human body like blood helps in transmitting the nutrients from one organ to another organ, network layer helps in sending the data. For transmitting the message network layer use WiFi, bluetooth, Zigbee, LoRa WAN and others technology.

2.2..Application Layer

Application layer on which IoT application are build and helps in managing the applications of IoT. This layer uses many protocols CoAP (Constrained Application Protocol), MQTT (Message Queue Telemetry Transport), XMPP (Extensible Messaging and Presence Protocol), AMQP (Advanced Message Queuing Protocol) to manage the application. These protocols are made for the constrained environment and act like Publish and Subscriber

3..Issues in IoT

The trending topic, IoT has given us a lot of advantages with this there are some issues also present, in this section we are going to discuss about some of the main issues.

3.1.Hardware issue

Hardware issue in IoT is basic concern, in which manufactures can left the loop hole unintentionally, this can leak our confidential data.

One more thing is related to hardware issue is that any customer buys an IoT device and try to find the flaws in device so that he can attack on other devices.

3.2.Security

Security is one of the major issues in IoT. IoT network contains a lot of data and that includes our personal and confidential information. It is one of thing that has not achieved 100 percent till date. There are some customers who have trust issue in using the devices that are connected to internet (IoT device).

a) This issue can be solved by using the encryption and decryption.

b) By using an authentication mechanism before accepting the data.

3.3.Energy management

In the perception layer, sensors take the information from surrounding. Sensors are low powered device if these will not use properly then probability of dying is very high. So, there should be a proper management of sensors. Researchers have given many algorithms for efficient management of wireless sensor network like LEACH, TEEN, PEGSIS and many others.

3.4.Data storage

As day by day, IoT network is growing with a very high pace. IoT things generate a huge amount of data in zettabyte. Maintaining and analyzing this heavy amount of data is one of the issues. This issue can be solved by two ways;

a) By removing the redundant data.

b) By storing only useful and informative data.

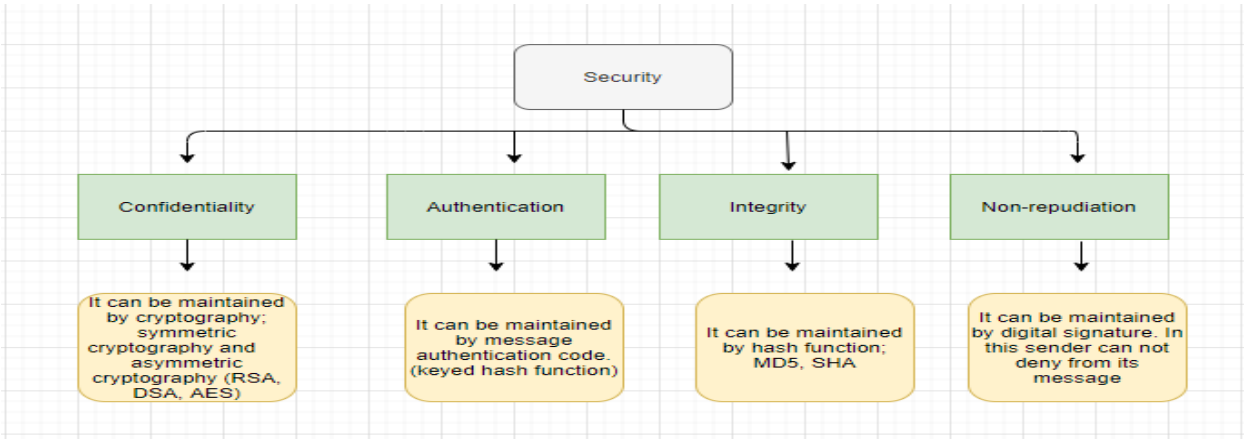

Figure 4: Types of security issues

4. Proposed Model

In proposed model, an authentic model for IoT device has introduced in which each IoT device has its own cloud storage in which all authentic IPs store. In this, a list of authentic IPs maintains and an intruder list in which all unauthentic IPs will store, it also updates data dynamically and set a threshold value.

When an IoT device receives a message from an authentic device, it will accept the packet and process it, if packet's IP neither belong to authentic IP nor intruder list then it will check its payload value, if its payload value is greater than threshold value then packet will be discarded and its IP address stores into intruder list else it will be accepted and added into authentic list if it receives from an unauthentic device then it will add it into the intruder list as shown in Figure 5.

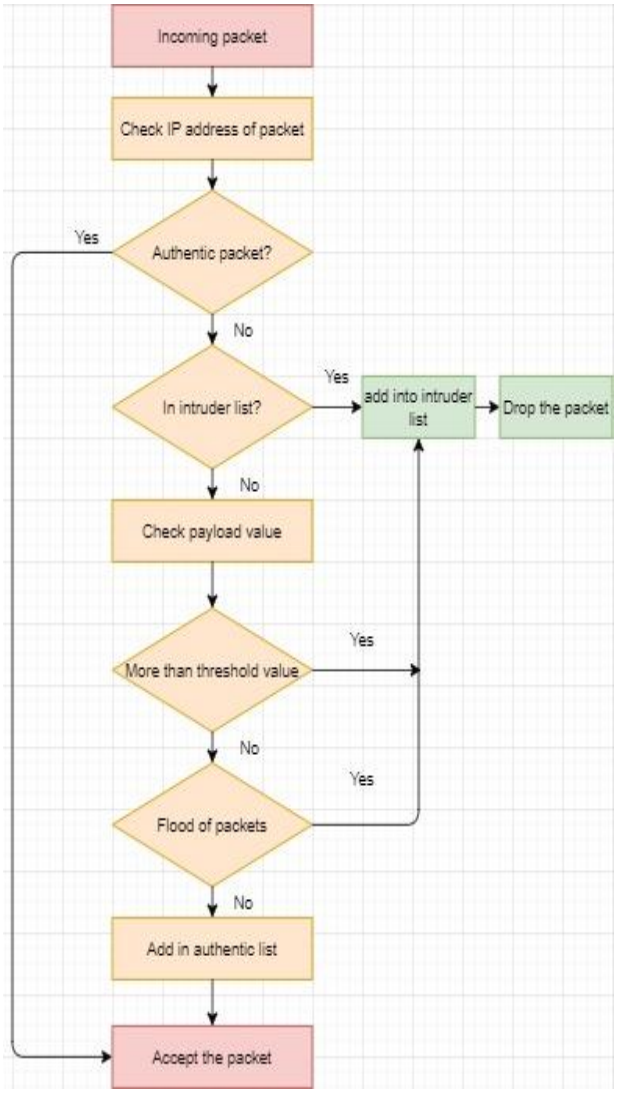

Figure 5 : Proposed framework

5. Future scope

Security is the major problem in internet world. One of the things of internet is internet of things that contains a huge amount of data, for securing this data, security is very important. In this we have a model for the security that basic function is accepting only authentic packet. The future scope of our research is implementation of our proposed model with the efficient energy management of sensor network. This combination will help in maintaining the perception layer of IoT.

6.Conclusion

With the increase of number of connected devices in IoT network, security issues and number of complaints regarding security will also increase. Both are these directly proportional to each other. In our research paper, we have mentioned about the basic information of Internet of things. There is no standardization of architecture for IoT, in this paper we have mentioned the three-layered architecture (Input layer, transmission layer and service layer) and some issues that can be happened in IoT. One security model related to authentication has been introduced in this paper. That allow only authentic packet to accept.

References

1. Ahmad W. Atamli and Andrew Martin,"Threat-based security analysis for the internet of things," in International Workshop on Secure Internet of Things. IEEE, 2014.
2. Michael Schiefer, "Smart home definition and security threats," in International Conference on IT Security Incident Management & IT Forensics. IEEE, 2015.
3. Talwana Jonathan and Huang Jian,"Smart world of internet of things and it's security concern," in IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and

Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2016.

4. Shao Xiwen, "Study on Security issue of internet of things based on RFID," in International Conference on Computational and Information Sciences. IEEE, 2012.
5. Alexandru Lavric andValentin Popa, "Internet of things and LoRa low power wide area networks challenges," in International Conference on Electronics, Computers and Artificial Intelligence (ECAI). IEEE, 2017.
6. Subha Koley and Prasun Ghosal, "Addressing hardware security challenges in internet of things: Recent trends and possible solutions," in International Conference on Ubiquitous Intelligence and Computing. IEEE, 2015.
7. Jean Pierre Nzabahimana, "Analysis of security and privacy challenges in internet of things," in International Conference on Dependable Systems, Services and Technologies (DESSERT). IEEE, 2018.
8. Anna Katrina Gomez and Simi Bajaj, "Challenges of testing complex internet of things devices and system" in International Conference on Knowledge and Systems Engineering (KSE). IEEE, 2019.
9. Xuemei Li and Li Da Xu, "A review of internet of things- resource allocation," in IEEE Internet of Things Journal. IEEE,2020.
10. Chang Le Zhong, Zhen Zhu and Ren Gen Huang, "Study on the IoT architecture and Access Technology," in International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES). IEEE, 2017