Security Issues in Internet of Things - A Review

Jain Rishav Amit[1], Priyank Singhal[2]

[1]*Teerthanker Mahaveer University, Moradabad*

[2]*Teerthanker Mahaveer University, Moradabad*

[1]rishav.jain1611@gmail.com,

[2]priyanksinghal1@gmail.com

***Abstract*—**

IoT, Internet of Thing is a network of different physical devices connected to the internet. These devices includes various transducers such as sensors, actuators and many more such devices which enables the communication between these devices. Security at each level is a major concern in communication from transducers devices to applications. In this paper, I have reviewed various security challenges in IoT and also proposed their possible solutions.

***Keywords*— IoT, Security, Solutions**

I. INTRODUCTION

A. What is IoT?

When we look at the future where physical objects are connected to internet and makes themselves identifiable to other devices using actuators and sensing devices, then the concept that comes in our mind is Internet of Things [1]. In IoT network, we have a collection of RFID sensors, RFID readers, sensors, etc along with the wireless communication system. All these devices works together to carry out the process of sensing the working environment and taking the appropriate steps based on the data received. If we look at some of the examples of IoT then we talk about a system where the speed of the fan is maintained based on the number of peoples in the room, switching off the devices when everyone exists the room, automated fire detection system and so on [2].

Data can be transferred by the Internet of Things over the network without human interaction.

B. The concept of IoT and its basic characteristics:

Internet of things is a collection of physical objects which has ability to capture information for physical world. IoT is an intelligent system, which has computing and communicating ability. There are mainly three basic characteristics of Internet of Things [8]:

1) Comprehensive awareness:

Comprehensive awareness is due to the RFID, sensors and M2M terminal. These are used to get information of the object.

2) Reliable transmission:

The main aim of reliable transmission is transmission in real time with high accuracy.

3) Intelligent processing:

The main aim of intelligent processing is to analyse and collect the useful information to meet the user expectation.

C. Architecture of IoT

The IoT consists of different technological layers that all play a job within the route from merely connecting ‘things’ and IoT devices to building applications that serve a transparent goal, whether it’s for industry-grade IoT projects or consumer applications.[9]

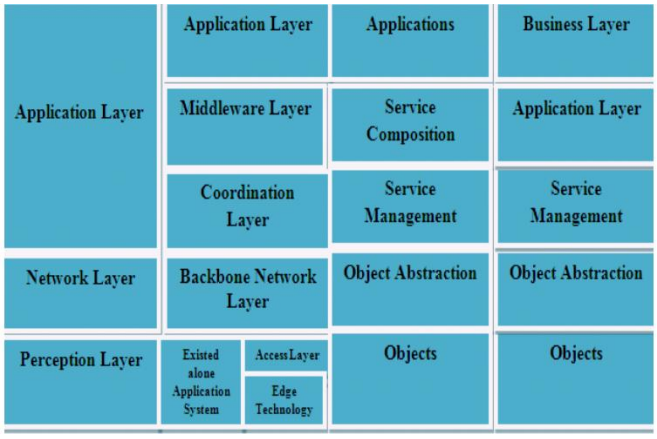

Fig. 1 The IoT Architecture (a) Three Layer (b) Middle-ware based Layer (c) SOA based Layer (d) Five-layer

The basic model behind IoT is a 3-layered architecture, which consists of the Application Layer, Network Layer, and Perception Layer. An abstraction is added to the IoT architecture in the recent literature. [3].

1) Objects Layer :

The first layer is objects or perception layer, it represents the sensors used in IoT that collect and process information. The perception layer includes actuators and sensors. The actuators and sensors perform different functionalities such as identifying motion, humidity, temperature, weight, location, vibration, acceleration etc. Digitization of the data and transferring the same to the Object Abstraction Layer is done at this layer. Transfer of data is carried out generally through secure channels. Initiation of big data is carried out at this level itself, as it starts reading the data from actuators and sensors. [3]

2) Object Abstraction Layer:

Data produced by perception layer is transferred to the Service Management layer by object abstraction layer through the secure channels. Data can be transferred through 3G, RFID, Wi-Fi, Bluetooth, ZigBee, GSM, etc. Data management processes and Cloud computing are done by this layer [3].

3) Service Management Layer:

After object abstraction layer, we have Service Management or Middleware layer. Service Management layer pairs a service with its requester based on addresses and names. This layer processes the received data and then makes decisions based on it and finally delivers the services required. Along with this, this layer also enables programmers of the IoT application to work with heterogeneous objects without any consideration to a specific hardware platform [3].

4) Application Layer:

This layer provides the services requested by customers. For example, it provides the air humidity measurements and temperature to customer. To meet customer needs, smart and high quality services are provided at application layer.[3].

In the large scale development of the Internet of Thing network, this layer is very helpful. Application related to IoT could be smart transportation, smart planet, smart school, smart home and so on [4]. Application layer is a top most layer consisting of formulas, business logic and UI to user end. [6].

5) Business Layer:

Management of overall IoT system activities and services is done at this layer. Based on data received from Application Layer, this layer build business model, flowcharts, graphs, etc.[4]

Implementation, designing, monitoring, analysing and developing the elements which are related to IoT is carried out at this level. In addition to this, all other underlying layers are monitored and managed at this layer. Output generated at each layer are examined and compared to enhance services and find out the errors if any at this layer[3]. Decision making processes based on Big Data analysis is also supported in this layer.

D. SECURITY ISSUES IN IoT:

The key infrastructure of IoT is the Internet, which opens the door for some prominent security issues. As many physical objects are connected in a network in IoT via Internet, various security issues are inevitable. Let us look at some of the security issues categorised based on the various layers of IoT.

1) Security issues at perception layer of Iot:

Being the bottom most layer in the IoT, this layer is the only source of information as this

layer comprises of all sensor devices, RFID readers and actuators. Internet of Things cannot provide a security protection system and it is vulnerable to the attack due to diversity, energy limited, simple and weak protective capability of sensing node which affects the security of WSN, RFID and M2M terminal. Security problems such as information replay attacks, leakage, tampering, information tracking, cloning attacks and man-in-the-middle attacks are included in RFID. The security problems faced in perception layer includes physical capture, congestion attack, capture gateway node, DoS attacks, unfair attacks, forward attack and node replication attack[8].

1.1) Security issues included in the wireless sensor networks (WSNs):

Wireless sensor network is a collection of nodes that sense the environment and control the same. Interaction between computers or peoples and the surrounding environment is enabled by WSN. WSN comprises of actuator nodes, sensor nodes and so on. Following are the security issues that may occur in WSN[5]:

i. Attacks on secrecy and authentication
ii. Silent attacks on service integrity
iii. Attacks on network availability

1.2) Security issues in RFID technology:

RFID technology is especially used as RFID tags for machine-driven automatic exchange of information with no manual involvement. Due to the incorrect security status of the RFID technology, these RFID tags are very much vulnerable to different attacks from outside. [5]. Following are the four different types of attack to which RFID technology is vulnerable to:

i. Unauthorized tag disabling: This is a type of DoS attack where RFID tags are made incapable or inefficient permanently or some times temporarily. These attack makes the RFID tags to work inaccurately and this leads RFID tags to misbehave and malfunction when scanned through RFID reader. These attacks can easily be done from far distance which allows attackers to attack from other far places without coming near to the tags.

ii. Unauthorized tag cloning: In this attack, identification information of the RFID tags is captured by manipulating the tags through dishonest RFID tags reader. As and when the identification information of the RFID tags are compromised, it is easy to replicate the tags and bypass the security measures of the system. [5].

iii. Unauthorized tag tracking: In this attack, dishonest RFID tag readers trace the RFID tags and this leads to sharing of sensitive information such as location history to the attackers. So, If look from the customer viewpoint, then buying a product which have RFID tags does not guarantee them with the confidentiality concerning their purchase and also invites risk to their privacy.

iv. Replay attacks: In this type of attack, one side of communication is recorded i.e. spied and the information received from the eavesdropping is used at later time for various purpose such as replying to any query or bypass the authentication.

2) Security issues at physical layer in IoT:

Functionalities such as receipt and transmission of data, selection of carrier frequency along with its generation, encryption and decryption of data, modulation and demodulation of data, etc are done at the physical layer in IoT [5]. Following are the ways by which this layer is generally attacked:

i. Jamming: This is kind of DoS attack where the communication channel between the various nodes is occupied which leads to the prevention of the communication between the nodes with one another. The transmission of radio signals are exploited to interfere with the radio frequency which are being used by the network of sensors and actuators.This attack can be done on continuous basis or can also be done in isolated way, both damaging the network [7].

ii. Node tampering: Node tampering is nothing but the extraction of sensitive information from the communication channel.

3) Security issues at network layer in IoT:

Risks such as confidentiality, integrity, illegal access, DoS attacks, data eavesdropping, man-in-the-middle attack, destruction,virus attack, etc are faced by Internet of Thing in the network.In IoT, large number of physical devices are sensed producing a data in different formats along with huge volume from multi-sources with heterogeneous characteristics. This invites a need of transfer of huge amount of data on network which have its own security issues such as network congestion, resulting in DoS attacks [8]. Routing is the main function at this layer[5]. Following are the various DoS attacks which may occur in network layer:

i. Hello flood attack: In this type of attack, the channel of communication is congested with high numbers of unnecessary messages causing high traffics in channels. An useless message is send through a malicious node and then the attacker replays that message creating a high traffic on channel.

ii. Homing: In homing attack, traffic for key managers and cluster heads are searched within the traffic. Entire network of IoT can be shut down by using both of this.

iii. Selective forwarding: In this type of attack, an attacker compromises a node, selected based on his requirements of malicious objective. As and when an attacker compromises the node, then he only allows a selected data to be sent from that node to achieve his objectives.

iv. Sybil: In this attack, a single node is replicated by an attacker and presented as multiple nodes with different identify to other nodes.

v. Wormhole: In the Wormhole attack, relocation of bits of data is done from their original position. This relocation of bits of data packet is achieved by passing the useless bits of data over a link with low latency.

vi. Acknowledgement flooding: Acknowledgements becomes essentials while routing algorithms are employed in the IoT network. In this type of attack, an attacker compromises a node and then sends false acknowledgement to the senders and this leads to wrong flow of data and creating a disturbance in the network.

4) Security issues at application layer in IoT:

Computer technology, communication technology and industry professional are closely integrated which results in the application of IoT leading to find the applications in various aspects. Tampering and eavesdropping are the major security challenges in application layer [8]. Responsibility of traffic management is carried out at this layer. Softwares for various applications are provided so that this can help collection of information by sending queries and also help to carry out data in comprehensive way. [5]. By stimulating the sensor nodes, huge traffic is created towards the base station creating a path-based DoS attack in the application layer.

II. *COMMUNICATIONS AND SECURITY ON THE IOT*

Communication protocols are illustrated in the figure 2. Following are the different protocols that supports the internet communication in IoT, enabling communication in sensing devices. [9].

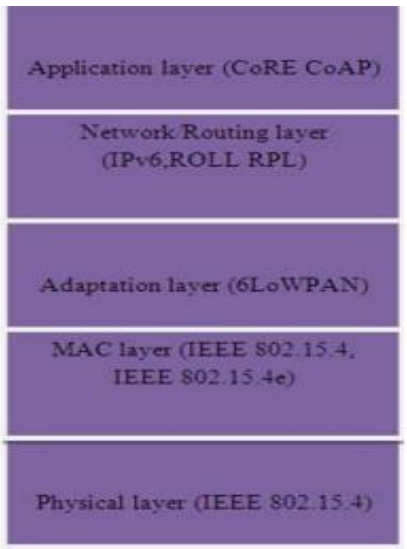

Figure 2: Communication protocols in the IoT

A. ***Protocol Stack for the IoT***

The most of the communications and security solutions are made by the constraints of sensing platforms and scale factors. New security protocols and communications are being designed by Institute of Electrical and Electronics Engineers (IEEE) and The Internet Engineering Task Force (IETF) which are playing a major role in the security of the applications of IoT. Characteristics and constraints of low energy sensing devices and low rate wireless communication are taken into account while developing these security protocols. It is also guaranteed that the new standardized solutions are being designed in such a way that they will be supporting the old standards to keep up with the existing internet standards. Along with this, it is also guaranteed that sensing devices should be able to communicate with other Internet entities in the context of future IoT distributed applications.

Let us have look at the various protocols with their characteristics following bottom up approach:

1) At the physical layer, IEEE 802.15.4 supports Medium access control layers and communications with low-energy. IEEE 802.15.4. So, this standard provides a base to the higher layers for the communication in the IoT network and also sets various rules for the communication at the lower layers.

2) Low-energy communication environments using IEEE 802.15.4 at most 102 bytes for the transmission of data at higher layers of the stack. A value that is much less than the maximum transmission unit (MTU) of 1280 bytes is required for IPv6. This aspect is addressed by adaptation layer (6LoWPAN) by enabling the transmission of IPv6 packets over IEEE 802.15.4. 6loWPAN and also implement mechanisms for packet fragmentation and reassembly, among other functionalities.

3) Routing Protocol for Lossy Networks (RPL) and Low-power supports Routing over 6LoWPAN environments. Rather than being a routing protocol, RPL provides a framework which is adaptable to the requirements of particular IoT application domains. Routing requirements and optimization goals are identified by defining Application-specific profiles.

4) Communications at the application layer are supported by Constrained Application Protocol (CoAP). IETF has designed this protocol to provide interoperability in conformance with the representational state transfer architecture of the web.

III. RELATED WORK

Table 1: Security issues and their current proposed solutions in IoT

	ISSUES	**TECHNOLOGY**	**SOLUTION**	**LIMITATIONS**
WSN	Limited storage capacity, power and computing ability. Attacks to routing protocol	Secure routing protocol in WSN.	Secure routing protocols should be used which are designed especially for WSN.	Network is influenced to partitioning under attack when an alternate path is not available.
RFID Tags	Multiple tag in one	Conflict collision prevention in	Anti-Collision algorithm	It requires additional central

	reader's working scope	RFID		control area to calculate working scope which increases complexity and cost.
Network Layer	DDos/ Dos attack	Access control and network encryption technologies.	Access Control	Access control refers that only authorized users can access the WiFi network.
Adaptation Layer	DDos Attack	Supervision capability: enhance management	Information disclosure protection disaster control and recovery, supervision	Not distributed
Application Layer	DDOS attack	Intrusion detection system	GuardDog, other vendors	Heavy processing overhead.

Various security issues to which IoT is vulnerable along with their possible solutions are illustrated in table 1. When we talk about WSN, then we may face issues such as limitation of storage capacity, power and computing ability. As we have multiple nodes in WSN, it is also vulnerable to the various attacks at the routing protocol. Secure routing protocols which are specially designed for WSN is one of the possible solution to these problems. In RFID tags, major security issue evolve the possibilities of multiple tags being in range of RFID tags reader. Using Anti-collision algorithm is possible solution to this issue. In network layer, DoS attack is a main issue and the possible solution to this is access control. At adaption layer, again DoS attack is a severe security issue. Possible solution at this layer for DoS attack are disaster control, recovery and information disclosure. The DoS attack is one of the issues in application layer and solution for this is GuardDog.

IV. CONCLUSION AND FUTURE WORK

In this paper, current state of the IoT has been discussed. This was followed by a brief discussion on various levels of IoT architecture and communication protocol stack employed. While discussing the current state of Internet of Things, various security issues involved at various layers of architecture have also been discussed and there probable solutions have also been proposed.

In future, a framework to detect various attacks in IoT is planned to be proposed and its effectiveness will be measured.

REFERENCES

[1] Jun Wei Chuah ―The Internet of Things: An Overview and New Perspectives in Systems Design‖ 2014 International Symposium on Integrated Circuits 978-1-4799-4833-8/14.

[2] Sarita Agrawal, Manik Lal Das ―Internet of Things – A Paradigm Shift of Future Internet Applications‖ Institute of technology, nirma university, ahmedabad – 382 481, 08-10 december, 2011.

[3] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash ―Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications‖ ieee communication surveys & tutorials, vol. 17, no. 4, fourth quarter 2015.

[4] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi and Talha Kamal ―A Review on Internet of Things (IoT)‖ International Journal of Computer Applications (0975 8887) Volume 113 - No. 1, March 2015.

[5] Tuhin Borgohain, Uday Kumar and Sugata Sanyal ―Survey of Security and Privacy Issues of Internet of Things‖

[6] Krushang Sonar, Hardik Upadhyay ―A Survey: DDOS Attack on Internet of Things‖ International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X Volume 10, Issue 11 (November 2014), PP.58-63.

[7] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A. Spirito and Mark Vinkovits ―Denial-of-Service detection in 6LoWPAN based Internet of Things‖ 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).

[8] QuandengGOU, Lianshan YAN, Yihe LIU and Yao LI ―Construction and Strategies in IoT Security System‖ 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing.

[9] Qi Jing • Athanasios V. Vasilakos • Jiafu Wan • Jingwei Lu • Dechao Qiu ―Security of the Internet of Things: perspectives and challenges‖ Wireless Netw DOI 10.1007/s11276-014-0761-7.

[10] A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks‖ [Deng+].