Survey on Internet of Things (IoT): Security issues and countermeasures

Jisha C.T[1], Mamatha Balachandra1[2], Derroll David[3]

[1]Assistant Professor, Computer Science and Eng., Vimal Jyothi Eng. College, Kannur
[2]Associate Professor, Computer Science and Eng, M.I.T
[3]Assistant Professor, Computer Science and Eng., Vimal Jyothi Eng. College, Kannur

Abstract:- *In the recent years, people need to use Internet at anytime and anywhere. Internet of Things (IOT) allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service. IOT can be distinguished by various technologies, which provide the creative services in different application domains. This implies that there are various challenges present while deploying IOT. The traditional security services are not directly applied on IOT due to different communication stacks and various standards. So flexible security mechanisms are need to be invented, which deal with the security threats in such dynamic environment of IOT. In this survey we present the various security issues with their respective countermeasures.*

Keywords — *Actuators, Internet-of-Things, Sensor Network, Smart objects, Sensors, Security, Ubiquitous*

I. Introduction

(The term Internet of Things (IOT), also known as Internet of Objects refers to the networked interconnection of everyday objects, which is generally viewed as a self-configuring wireless network of sensors whose purpose would be to interconnect all things [1]. Today the world is totally dependent on the information provided on internet, which is captured by taking images or through text. This clearly specifies the major involvement of a human being for collection of the information. But the problem with human involvement is that, people have limited time and less accuracy, which leads to inappropriate and inconsistent data. Hence, such a system is needed which can automatically capture the data and transfer it to the internet without any human to machine interaction. Internet of things is a scenario in which all the things are connected to the internet through the information sensing devices for the purpose of intelligent identification and management [2]. These things are provided with the unique identifiers which can be read using RFID tags with the help of sensors (information sensing devices).

The thing in the internet of thing can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built in sensors to alert the driver when the pressure is low or any other manmade object that has a unique IP address with the ability to be connected to the network for the transfer of the data [3]. There is a major participation of wireless technology, Micro-electromechanical Systems (MEMS) and the internet in the making of IOT [2]. One of the basic things needed to sense the object in the environment is RFID. Sensing can be possible by assigning each object a unique identifier and then connected to the internet, for smart processing by the transfer of information. IPv6 is playing a very important role in the development of IOT, by using its huge address space one can easily assign an IP address to every thing on this planet and could transfer the data over network.

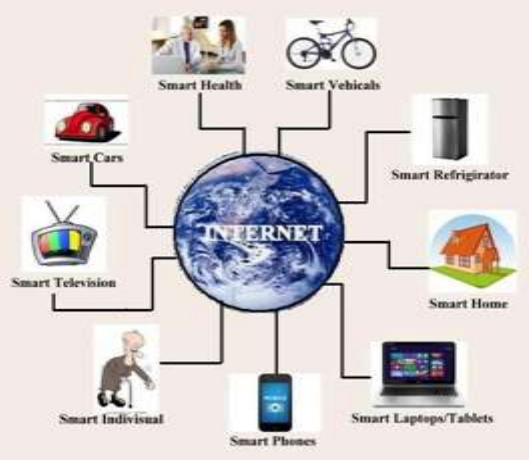

Fig. 1 Application of IoT

IOT is one of the upcoming concepts of technological innovation in the field of networks which will help not only in the industrial development but also in the day to day life of a human being, hence nowadays IOT is being the research emphasis topic for the researchers and for the enterprises. The typical scenario of IOT is shown in figure 1, depicting the interconnection among things like smart television, phones/laptops, smart refrigerator and smart individual etc. via internet.

The main objective of this paper is to provide the understanding of security issues of IOT which needs to be studied along with their countermeasures. This paper presents a brief idea of IOT which includes the architecture of IOT, security issues at each layer and countermeasures. These issues would be studying theoretically using parameters like authenticity, integrity, availability, confidentiality etc.

The remainder of this paper is organized as follows. In section 2 the architecture of IOT have presented. Section 3 gives main emphasis on security parameters and issues faced by IOT with its countermeasures. Finally, concluded the paper along with the direction for further work in section 4.

.

.

II ARCHITECTURE OF IOT

Internet of things is composed of two words i.e. "Internet" which give a look of interconnected networks and "Things" which clearly shows some objects. But when these two words put together gives a means of "a world-wide network of interconnected objects, uniquely addressable, based on standard communication protocols" [4]. Below it present the architecture and security of IOT.

Real time working of IOT is possible through the integration of various technologies together In this paper, a layered architecture of IOT is presented that gives an idea about basic architecture of IOT. Generally, IOT is divided into three layers: Perception layer, Network layer, and Application layer [5] [6] . Xiong Li, Zhou Xuan in [7] described the general architecture of trusted security system based on IOT security system such as trusted perception module, trusted terminal module and trusted network module. All of these three layers have large scale of information with different enabling technologies and features as shown in figure 2.

A. *Perception layer:*

The main working of IOT i.e. collection of information is done at the perception layer with the help of different devices like smart card, RFID tag, reader and sensor networks, etc. It has a feature of comprehensive sensing through the RFID system to get object's information anytime and anywhere. Each RFID electronic tag has a unique ID called Electronic Product Code (EPC) which is the only searchable ID allocated for each physical target. Extra information about the product is given by a string of figures imposed on it such as manufacturer and product category with its manufacturing date and expiry date etc. [2].

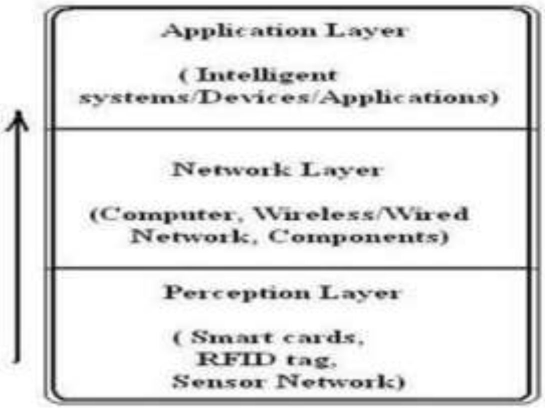
Application Layer
(Intelligent systems/Devices/Applications)
Network Layer
(Computer, Wireless/Wired Network, Components)
Perception Layer
(Smart cards, RFID tag, Sensor Network)

Fig. 2. Architecture

B. *Network layer:*

The data gathered by sensors used to be sent to the internet via network layer with the help of computers, wireless/ wired network and other components. Hence network layer is mainly responsible for the transmission of information with the feature of reliable delivery hence this layer also includes the functionality of transport layer.. Application layer: Analyzing the received information and making the control decisions to achieve its feature of intelligent processing by connection, identification and control between objects and devices. Intelligence means makes use of intelligent computing technology such as cloud computing and process the information for intelligent control like what to do and when to do things hence this layer is also called as process layer.

III SECURITY OF IOT

There are many challenges involved while building IoT. In this section, major security related challenges while building IoT are described in brief.

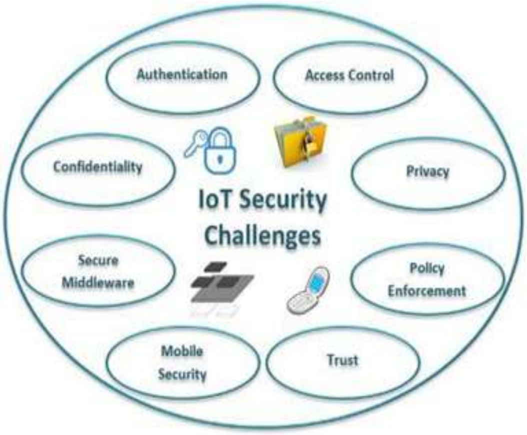

Fig. 3. Major security issues in IoT [8]

A. *Access Control*

Access control deals with access rights given to the things/devices in IoT environment. In traditional database systems, processing of discrete data is done, however in IoT, processing of flowing data is done. Two terminologies are described for Access Control [9]: 1) data holders (Users), who send/receive data to things. They must send data to authenticated things 2) data collectors (things), which must authenticate users. [10] presents an identity based system for personal location in emergency situation. Authentication problem for outsourced data stream is found in [11]. Access control of streaming data is specified in [12].

B. Privacy

A data tagging for managing privacy in IoT is proposed in [13]. A user-controlled privacy-preserved access control protocol, based on k-anonymity privacy model is proposed in [14]. [15] defines k-anonymity model by changing quasi-identifiers to preserve sensitive data. The privacy risk that occurs when astatic domain name is assigned to a specified IoT node is analyzed in [16]. Only some of the privacy issues related to IoT are covered in recent work, there is still a large scope to create privacy preserving mechanisms in IoT context.

C. Policy Enforcement

Policy enforcement implies to the approaches used to cause the application of a set of defined efforts in a system. Policies are performing rules which desire to be acted for the purpose of acknowledging order, security, and consistency on data. Only few works from literature describe how to control policies enforcement.

D. Trust

Trust is a complicated concept about which no explanatory acquiescence endures in the scientific literature, [9] furthermore its importance is dimensionally identified. A core problem with many applications towards trust description is that they do not contribute themselves to the demonstration of metrics and computation methodologies. The gratification of trust constraints are exactly related to the identity negotiation and access control effects.

E. Mobile Security

Mobile nodes in IoT frequently move from one cluster to another, in which cryptography based protocols are used to allow expeditious identification, authentication, and privacy protection. An ad hoc protocol is demonstrated in [18] which is useful when a mobile node joins a new cluster. This protocol also accommodates a valid demand message and an answer authentication message, which speedily implements identification, authentication, and privacy protection. It will be useful to safeguard against replay attack, eavesdropping, and tracking or location privacy attacks.

3.1 Security Issues in each layer

The growing use of IOT system needs a powerful protection against all possible attacks or vulnerability. Hence security is needed at each layer (Perception layer, Network layer, and Application layer) of the IOT system; each layer either consists of devices, applications or networks. Some classified security issues at each layer are as given below:

3.1.1 Security at Perception Layer

Perception layer mainly includes: Smart card, Reader, RFID tag, Sensor network. Each of these devices has following vulnerability which leads to be a security issue of IOT such as sensor attacks, sensor abnormalities, radio interference.

3.1.1.1 Terminal security issues

For perception of things it needs a large number of terminals. Terminals are used for real-time data collection to be presented to the user. This process needs an authentication and data integrity. Due to the wireless nature of communication, IOT can face threat from the hackers, virus attacks etc. The main problems existed in perception terminals include leakage of confidential information, tampering, terminal virus, copying and other issues.

3.1.1.2 Sensor network security issues

The sensor nodes are responsible for data transmission, data acquisition, integration and collaboration. As they operate on their own battery with less security protection, they can face complex security issues.

3.1.2 Security at Network layer

Network layer mainly including Computers, Wireless or wired network, faces security issues such as network content security, hacker intrusion, illegal authorization

3.1.2.1 Data transmission security issue

The security of the network layer is of two main types: The first is from the security risks of the IOT itself; the second is from the related technologies and protocol defects during design and implementation [5]. In wireless networks, nodes can move freely, they can join or leave the network at any time without any prior authentication. This makes wireless networks to be more malicious or vulnerable for the security concern.

3.1.3 Security at Application layer

Application layer mainly includes the intelligent devices for effective decision making. Each of these has some vulnerability which leads to be an issue of the security of IOT.

3.1.3.1 Application safety issues

Application layer mainly contains a variety of applications for example, industrial monitoring, smart grid, monitoring services, or any other intelligent system. The main security problem can be its own design flaws that can attract any attacker to attack. Malicious code or software vulnerabilities can be introduced in such defected systems. Another issue can be the integration of various areas of techniques and business needs which can cause a bottleneck for the massive data processing and on operation control [30]. This can lead to the security issues of reliability and safety for IOT. Some of the issues could be privacy protection technology, database access control, protection technology of secure electronic products, information leakage tracking technology and intellectual property of software [31].

3.3 Security Countermeasures

The Xu Xiaohui [5] talked about the countermeasures for the security issues of IOT. Some of them as certification, access control, data encryption and cloud computing are discussed in this subsection.

3.3.1 Certification

Certification is a secure way of confirming the true identity of both the parties which communicate with each other. Hence by using Public Key Infrastructure (PKI), it is possible to achieve the strong authentication by two way public key certification for protecting authenticity and confidentiality of the IOT system. Notarization is another solution for security purpose. Notarization is a trusted third party i.e. a certificate authority that facilitates interactions between the users to assure the properties of data exchange

3.3.2 Access Control

Access control is another mechanism which gives secure environment of IOT by limiting the access control for machines, objects or people which are illegal to access the resources. Certification and access control technology are correlated with each other. Access control can be implemented on the area such as: Encrypt password, confidential directories or files, configuration and update rights etc.

3.3.3 Data Encryption

Encryption technique is used to prevent the information from tampering and to maintain confidentiality as well as integrity of the information. When data is intercepted by an attacker, encryption prevents that data from being deciphered. There are two ways of Encryption:

1) Hop by Hop Encryption provides cipher text conversion on each node to make it more secure for network layer.

2) End to End Encryption in which encryption-decryption performed at sender-receiver end only.

According to the business needs, one can choose different encryption methods. Using more secure key exchange and key management schemes one can prevent attacks on IOT such as eavesdropping, fabrication, record and replay etc

3.3.4 Cloud Computing

Cloud is a name for huge data storage capacity, high performance with affordable low cost. In the essential working of IOT i.e. large number of sensor nodes that collect and analyze huge amount of data, storing and processing of data where cloud computing can be used very effectively. Another use of cloud computing is providing third party security. IOT security can be enhanced using cloud’s security at minimum cost, as cloud provides the feature of “pay for how much you use”. While using cloud computing it needs to make sure that the “Scale” of IOT is large for example in areas such as, earthquake monitor, smart grid, industrial applications etc.

IV . CONCLUSION AND FUTURE WORK

In this paper, a summarized view of IOT including its architecture has been presented. IOT is an upcoming technology of innovation but still at its early stage of research and development. IOT cannot be used widely if it is not safe. Therefore, the paper has discussed security issues of IOT and some countermeasure for required security parameters. Even though in recent years, an active research on IOT is going on, but still some issues can be further focused on: 1) Use and evaluation of Wi-Fi, Ethernet, Bluetooth for networking of IOT or ZigBee protocol;

2) Application oriented study is needed for different industrial application in which IOT can be used in order to initiate a new technological revolution; 3) New security challenges and application of lightweight cryptographic protocol need to be studied further.

REFERENCES

[1] Conner, Margery "Sensors empower the "Internet of Things" ISSN 0012-7515 pp. 32–38, 2010.
[2] Shao Xiwen "Study on Security Issue of Internet of Things based on RFID" Fourth International Conference on Computational and Information Sciences, 2012.
[3] Xu Xiaohui Study on Security Problems and Key Technologies of The Internet of Things", International Conference on Computational and Information Sciences, 2013.
[4] Yan L, Zhang Y, Yang L T" The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems", Auerbach Publications, 2008.
[5] Xiong Li, Zhou Xuan, Liu Wen "Research on the Architecture of Trusted Security System Based on the Internet of Things".
[6]. S. Sicari, A. Rizzardi, L.A Grieco and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead", Comput. Netw. 76, 146–164, 2015.
[7].A. Alcaide, E. Palomar, J. Montero-Castillo and A. Ribagorda, "Anonymous authentication for privacy-preserving iot targetdriven applications", Comput. Secur. 37, 111–123, 2013.