International Journal of Latest Trends in Engineering and Technology
Special Issue SACAIM 2016, pp. 164-168
e-ISSN:2278-621X

EVOLUTION OF INTERNET OF THINGS (IOT): SECURITY CHALLENGES AND FUTURE SCOPE

Prajwal Fernandes, Avinash Monteiro and Suman Antony Lasrado
AIMIT (St. Aloysius), Mangaluru, Karnataka, India

Abstract- Internet of Things (IoT) is the next breakthrough in the field of Networking. The main aim of Internet of Things is to connect to frequently used objects which have the ability of sensing and having access to the Internet, with or without the involvement of humans. IoT field is still at its early stage and has many open issues. We take up on the security issues, as the devices have low computational power and low memory the existing security mechanisms (which are a necessity) should also be optimized accordingly or a direct approach that needs to be followed. This is a survey paper to focus on the security aspects of IoT. We further also discuss the future scope in this field.

Keywords – IoT, breakthrough, computational, necessity, network layer.

I. INTRODUCTION

Internet of things (IoT) is more than device to device communication, it is a collection of many services, objects, humans and devices that are interconnected that can communicate as well share data and information in order to attain a common goal in different areas and applications. IoT has agriculture, transportation, healthcare, distribution and energy production as its implementation domainsIn a gathering of comparative and heterogeneous gadgets, gadgets in IoT take after an Identity Management way to deal will be distinguished.Thus, a district in IoT can be characterized by an IP address however inside every locale every substance has an interesting. [1] Changing the way, we live today by making keen gadgets around us perform day by day errands and tasks is the center motivation behind IoT. Smart homes, smart cities, smart transportation and infrastructure etc. are the terms which are used in relevance with IoT. The application spaces of IoT, range from individual to big business situations. IoTclients can communicate with their encompassing surroundings, and human userscan keep up and manufacture social connections through the applications in individual and social space. On top of this security is another big challenge in IoT implementation. Main challenge of IoT is to reduce power consumption and minimize the utilization of resources. IoT finds application in many fields like medicine (e.g. monitoring pulse rate of patient and keeping track of the data and with raw data it will specify or send the information to doctor about it), Home automation (e.g. controlling room temperature), Industrial plants (e.g. Quality control), Fitness equipment (e.g. calories to be burnt), Smart cities (e.g. bus on way signal to daily commuters) etc. Wireless sensor networks which are connotations of IoT can show us some solutions. Wireless sensor networks are used to sense the object and transmit the information, for sensing it doesn't need much computation power but transmitting the sensed data needs some communication path

which may lead to security issue. The basic contemplations of the IoT gadgets are security and protection. Tragically, the exceptionally differences of figuring gadgets, the many-sided quality of their structures and correspondence foundation, and their novel organization models make security a test for registering frameworks in IoT's[1].
The rest of the paper is organized as follows. IoT Architecture are explained in section II. IoT Security Issues areExplained in section III. Future Scopes are explained in section IV and Conclusion are given in section V.

II. IOT ARCHITECTURE

Each layer in IoTis defined by its functions and the devices that are used in that layer. There are different opinions regarding the number of layers in IoT.This architecture consists of three layers: Perception Layer, Network Layer, and Application layer. A brief description of each layer is given as per multiple researches [3-4] and the figure 1 graphically represents the Architecture:

A. Perception Layer:

The main task of the perception layer is to perceive the physical properties of things around us that are part of the IoT. This process of perception is based on several sensing technologies (e.g. RFID, WSN, GPS, NFC, etc.). In addition, this layer is in charge of transforming the information to digital signals. However, some objects might not be perceived directly. Thus, microchips will be appended to these objects to enhance them with sensing and even processing capabilities. Nanotechnologies and embedded intelligence will play animportant role in the perception layer. The first one will make chips smaller into the objects used in our everyday life. The second one will enrich them with processing capabilities that are required for applications [3].

B. *Network Layer:*

The network layer is responsible for processing the received data from the Perception Layer. In addition, it is in charge of transmitting data to the application layer through various network technologies, such as wireless/wired networks and Local Area Networks (LAN). The main media for transmission include FTTx, 3G/4G, Wifi, bluetooth, Zigbee, UMB, infrared technology, and so on. Huge quantities of data will be carried by the network. Hence, it is crucial to provide a sound middleware to store and process this massive amount of data. This technology offers a reliable and dynamic interface through which data could be stored and processed. Indeed, research and development on the processing part is significant for the future development of IoT [4].

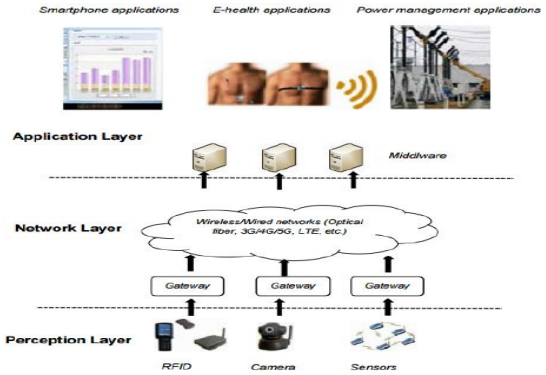

Figure.1: Three Layer IoT Architecture

C. *Application Layer:*

The application layer uses the processed data by the previous Layer. In fact, application layer constitutes the front end of the whole IoT architecture. Moreover, this layer provides the required tools for developers to understand the IoT vision. In this vision, the range of possible applications is impressive (e.g. Intelligent transportation, logistics management, identity authentication, location based services, safety, etc.).

To suit IoT specificities, the three-layer architecture provides a high level framework through which di erent approaches might be implemented.

III. IoT SECURITY ISSUES

Security objectives like Confidentiality, Integrity and Availability discover their applications in IoT too. IoT has its own particular limits and outskirts as far as the gadgets, control assets, and even the heterogonous and omnipresent nature of IoT that set up an extra concern. This section comprises of two sections. They are: The Security features (the IoT must have) and the security issues (detailed to each layer of the IoT) [5].

The security difficulties of IoT can be generally separated into two classes, Technological challenges and Security challenges. The technological challenges occur due to the mixed and omnipresent nature of IoT devices. The security challenges are associated to the principles and functionalities that should be imposed to accomplish a protected network. Technological challenges are related to wireless technologies, scalability, force, and scattered nature. Security challenges require the ability to ensure security by authentication, confidentiality, uninterrupted security, integrity etc. Security should be imposed in IoT right through the development and operational life cycle of all IoT devices [4].

The IoT can be affected by various categories of security threats which includes the following. They are:

- Common worms jumping: Generally limited to things running consumer O/S: Windows, Linux, iOS, Android
- "Script kiddies" or others targeting residential IoT: Unprotected webcams, stealing content, breaking into home control systems
- Organized crime: Access to intellectual property, sabotage, and espionage
- Cyber terrorism: Nuclear plants (For example, Stuxnet virus), traffic monitoring, railways, critical infrastructure

A. Confidentiality:

Only authorized users can make sure that data is secure and is available to them. For example, in IoT a user can be a human, service, machine and objects (internal or external). [6] Internal objects are the devices which are part of a network. Outer items are gadgets that are not a part of a system. It is vital for the IoT clients to know about information administration components. These mechanisms can be applied to persons or process who are actually responsible for the management. data is protected in this process [7].

B. *Integrity:*

The IoT exchanges data between differentdevices. It is required to ensure the data accuracy. This data comes from a sender and this ensures data tampering. This process involves data consistency and correctness, firewalls and protocols manage data traffic. There are no security issues in this process.

C. *Availability:*

The main aim of IoT is to connect smart devices. The IoT users should have all the required data. This process performs hardware repairs when needed and correctly maintains the functionalities of the Operating System.

D. *Authentication:*

Authentication is a process in which the identities provided by the users are compared. The user details are then compared with the files in a database. If the identities match the user will be granted with all authorization access [8].

IV. FUTURE SCOPE

In recent years there has been a rapid development seen in IoTin the areas of Tele medicine platforms, Intelligent Transportation systems, Logistics Monitoring, and Pollution Monitoring Systems etc. The examiners trust that number of things related will increment up to 26 billion units before this current decade's over. The security challenges identified with the IoT are managed to accomplish its development and development. The future degrees are given underneath for the examination keeping in mind the end goal to make the IoT worldview more secure [9-10].

A. Architecture Standards

An arrangement of models ought to be taken after from the miniaturized scale to full scale levels of IoT acknowledgment, to coordinate a system of IoT structures to accomplish a greater structure and the distinctive gadgets, administrations, and conventions are utilized by IoT to accomplish a shared objective which bolster an extensive variety of people, gadgets, dialects, and working framework is the present day necessity of IoT from an all-around characterized engineering.

B. Identity Management

The usage surprisingly association of Identity Management is finished by exchanging the data between the things. This procedure prompts to middle attack as a result of listening stealthily which accordingly can endanger the entire IoTstructure.Hence to prevent such threats like identity theft cryptography and many other techniques are applied.

C. Session layer

According to most analysts, the opening, shutting, and dealing with a session between two things can't be obliged by the three-layer architecture of IoT. So as to address these issues, conventions are required. These conventions are likewise required to facilitate the correspondence between gadgets. an extra layer, called the dynamic layer ought to be suited in the IoT engineering which can particularly deal with the associations, conventions, and sessions between imparting heterogeneous gadgets [9].

V. CONCLUSION

The IoT as a system is inclined to attacks at each layer henceforth there are numerous security prerequisites and difficulties that should be mulled over.The Present condition of work in the field IoT is fundamentally points on get to control and confirmation conventions, yet with the present progression of innovation it is vital to incorporate new systems administration conventions like IPv6 and 4G to accomplish the blend of IoTtopology[11]. The significant progressions saw in IoT are basically on new companies and little scale businesses. To augment the IoT structure from one substance to a gathering of elements and frameworks, various security issues should be tended to.IoT has a great potential with our day to day activities. But, security is the major concern in smart frameworks and their realization. We can foresee the near future to be

completely in sync with IoT. There is requirement for new grouping of remote programming, and equipment innovations to determine the difficulties in IoT.

REFERENCES

[1] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in Int'l Conference on Privacy and Security in Mobile Systems (PRISMS), 1-8, 2014.

[2] K. Zhao and L. Ge, "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667, 2013.

[3] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol. 56, 3594-3608, 2012.

[4] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC), 1-5, 2014.

[5] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," J. of Cyber Security and Mobility, vol. 1, 309-348, 2013.

[6] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol. 111, 2015.

[7] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," Computer, vol. 44, 51-58, 2011.

[8] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, 2266-2279, 2013.

[9] Q.Wen, X. Dong, and R. Zhang, "Application of dynamic variable cipher security certificate in internet of things," in Int'l Conference on Cloud Computing and Intelligent Systems (CCIS), 1062-1066, 2012.

[10] G. Zhao, X. Si, J. Wang, X. Long, and T. Hu, "A novel mutual authentication scheme for Internet of Things," in Int'l Conference on Modeling, Identification and Control (ICMIC), 563-566, 2011.

[11] Sandip Ray†, SwarupBhunia‡, YierJin*, and Mark Tehranipoor‡ †Strategic CAD Labs,Security Validation in IoT Space Intel Corporation .