The International Journal of Engineering and Science (IJES)
|| Volume || 6 || Issue || 12 || Pages || PP 45-50 || 2017 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Internet of Things: Security & Privacy Nightmare

Kamiya shrivastava
Assistant professor, IT DepartmentSBIIMS, Pune
Kamiya04@gmail.com

ABSTRACT

Internet of Things (IOT) has provided an Opportunity to build powerful industrial system and applications by leveraging the growing ubiquity of RFID, wireless, mobile and sensor devices. Many industrial IOT applications have been increasingly developed and deployed in recent years. Now-a-days, controlling and monitoring plays a main role in our day to day life. Everything we can monitor and control using advanced technologies. Remote access is a wonderful feature that came because of high speed internet. The main objective of proposed system is to provide a technology oriented and low cost system to make an advanced industry for those who away from their industry and want to control devices

Date of Submission: 24-11-2017 Date of Publication: 05-12-2017

I. INTRODUCTION

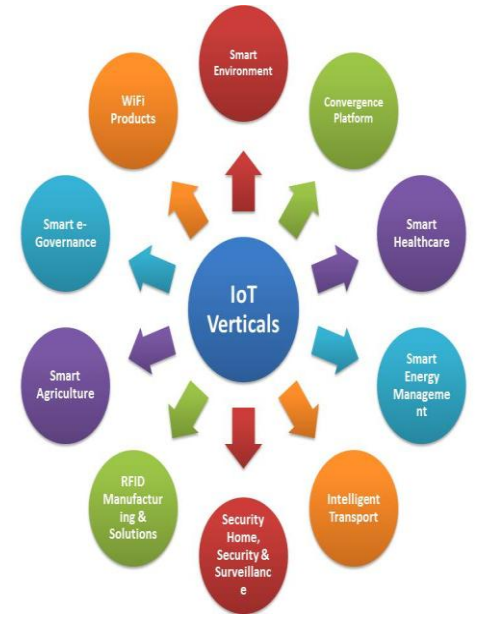
The Internet of Things (IoT) is the "network of interconnected sensor-equipped electronic devices that collect data, communicate with each other, and can be monitored or controlled remotely over the Internet" (Ahrens, "Making Sense of The Internet of Things"). The main goal of the IoT's development is to connect the physical world and the environment to the Internet or to wireless networks; this would allow making objects, machines and work environments interactive. By using sensors, objects will be capable of exchanging data with other machines without the need of human intervention.

Earlier there was a simple manual way of handling machines. However, with the advancement of technology, new ways are introduced for controlling the machines like automation. At the touch of a button, we can access large amount of information due to capability of computers and the Internet. Everybody wants an affordable and secure way to control their machines from any smart mobile device or Internet connection. The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator or other connected devices. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure.

The IoT includes different technology infrastructure, devices and services such as the cloud, computing, data analytics and mobile communications. The IoT is not a prediction; it is a plausible trend that is moving forward, rapidly. It is estimated that by 2020, 50 billion devices around the world will be connected to the Internet. "A third of them will be computers, smartphones, tablets and TVs… The remaining two-thirds will be other kinds of things: sensors, actuators, and newly invented intelligent devices that monitor, control, analyze, and optimize our world. There are major platforms and discoveries that have had a rich wage of complexity, global reach and novelty. But the IoT is for sure a trend that takes the development of interconnectivity to another level, one that once was only imaginable.

Since the IoT is a rapidly growing trend, most major companies are seeking to get involved, there are enormous efforts to trigger this trend as something positive in the forthcoming future. A frequent discourse that is present in the media mentions the major positive technological improvement that the IoT represents. "Capitalist societies generally educate people to appreciate the conveniences and choices of modern consumer technologies". Who wouldn't want a refrigerator that could tell you when you are running out of milk or that you need to replace one of its pieces? How fantastic it would be that your car could save information about what routes you take every day? Who would not want a house that can monitor and regulate the temperature to save

energy? Or a watch that can save your sleep pattern information? These are all conveniences that are presented to potential consumers about the IoT, however little is said about what happens to all these information that is saved by the devices and whether this is safe or could be a treat for the consumers´ privacy.



INTERNET OF THINGS

The Internet of Things (IoT) foresees the interconnectionof billions to trillions [1, 2], of smart things around us– uniquely identifiable and addressable everyday thingswith the ability to collect, store, process and communicateinformation about themselves and their physical environment [3]. IoT systems will deliver advanced servicesof a whole new kind based on increasingly fine-graineddata acquisition in an environment densely populated withsmart things. Examples of such IoT systems are pervasivehealthcare, advanced building management systems, smartcity services, public surveillance and data acquisition, orparticipatory sensing applications [4, 5].

The increasingly invisible, dense and pervasive collection, processing and dissemination of data in the midsof people's private lives gives rise to serious privacyconcerns. Ignorance of those issues can have undesiredconsequences, e.g. non-acceptance and failure of new services, damage to reputation, or costly law suits. The publicboycott of the Italian retailer Benetton in 2003 [6, 7], therevocation of the Dutch smart metering bill in 2009 [8],or the recent outcry against the EU FP7 research projectINDECT [9, 10] are only three examples of IoT relatedprojects that experienced huge problems due to unresolvedprivacy issues.

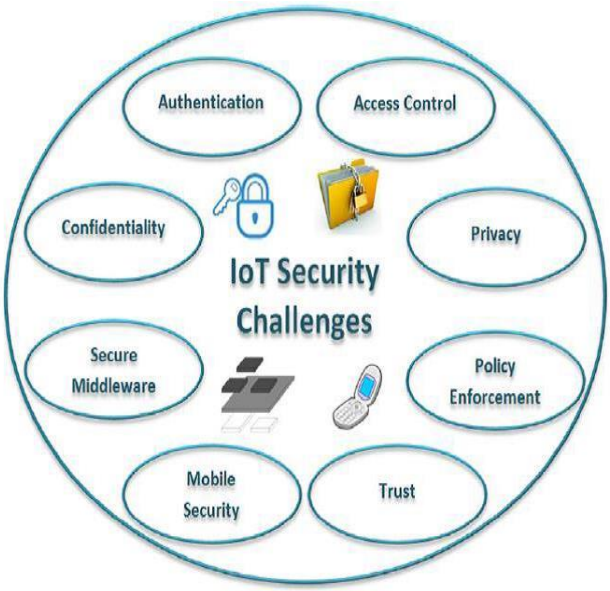
Privacy has been a hot research topic in different technology and application areas that are important enablers of the IoT vision, e.g. RFID, wireless sensor networks (WSN), web personalization, and mobile applications and platforms. Despite considerable contributions from these communities a holistic view of arising privacy issues in the IoT is missing, since the IoT is an evolving concept that comprises a growing number of technologies and exhibits a range of changing features.

II. SECURITY REQUIREMENTS

In IoT, all the devices and people are connected with each other to provide services at any time and at any place. Most of the devices connected to the internet are not equipped with efficient security mechanisms and are vulnerable to various privacy and security issues e.g., confidentiality, integrity, and authenticity, etc. For the IoT, some security requirements must be fulfilled to prevent the network from malicious attacks [11], [12], [13]. Here, some of the most required capabilities of a secure network are briefly discussed.

A)Resilience to attacks:
The system should be capable enough to recover itself in case if it crashes during data transmission. For an example, a server working in a multiuser environment, it must be intelligent and strong enough to protect itself from intruders or an eavesdropper. In the case, if it is down it would recover itself without intimation the users of its down status.

B)Data Authentication:
The data and the associated information must be authenticated. An authentication mechanism is used to allow data transmission from only authentic devices.



C) Access control:
Only authorized persons are providedaccess control. The system administrator must control access to the users by managing their usernames and passwords and by defining their access rightsso thatdifferent users can access only relevant portion of the database or programs.

D)Client privacy:
The data and information should bein safe hands. Personal data should only be accessed by authorized person to maintain the client privacy. It means that no irrelevant authenticated user from the system or any other type of client cannot have access to the private information of the client.

III.IOT SECURITY, PRIVACY, THREATS ANDCHALLENGES

The era of IoT has changed our living styles [14]. Although the IoT provides huge benefits, it is prone to various security threats in our daily life. The majority of the security threats are related to leakage of information and loss of services. In IoT, the security threats straightforwardly are affecting the physical security risk. The IoT consists of different devices and platform with different credentials, where every system needs the security requirement depending upon its characteristics. The privacy of a user is also most important part because a lot of personal information is being shared among various typesof devices [15], [16]. Hence a secure mechanism is needed to protect the personal information. Moreover, for IoT services, there are multiple types of devices that perform communication using different networks. It means there are a lot of security issues on user privacy and network layer. User privacy can also be uncovered from different routes. Some security threats in the IoT are as follows:

A) E2E Data life cycle protection:
To ensure the security of data in IoT environment, end-to-end data protection is provided in a complete network. Data is collected from different devices connected to each other and instantly shared with other devices. Thus, it requires a framework to protect the data, confidentiality of data and to manage information privacy in full data life cycle.

B) Secure thing planning:
The interconnection andcommunication among the devices in the IoT vary according to the situation. Therefore, the devices must be capable of maintaining security level. For example, when local devices and sensors used in the home-based network to communicate with each other safely, their communication with external devices should also work on same security policy.

C) Visible/usable security and privacy:
Most of the security and privacy concerns are invoke by misconfiguration of users. It is very difficult and unrealistic for users to execute such privacy policies and complexsecurity mechanism. It is needed to select security and privacy policies that may apply automatically.

IV.SECURITY ISSUES

The security concern is the biggest challenge in IoT. The application data of IoT could be industrial, enterprise,consumer or personal. This application data should be secured and must remain confidential against theft and tampering. For example, the IoT applications may store the results of a patient's health or shopping store. The IoT improve the communication between devices but still, there are issues related to the scalability, availability and response time. Security is a concern where the data is securely transmitted over the internet.While transporting the data across international border, safety measure act may be applied by government regulation such as Health Insurance Portability and Accountability (HIPA) act. Among different security challenges, the most important challenges relevant to IoT are discussed.
A)Data Privacy: Some manufacturers of smart TVs collectdata about their customers to analyze their viewing habits so the data collected by the smartTVs may have a challenge fordata privacy during transmission.

B) DataSecurity: Data security is also a great challenge.While transmitting data seamlessly, it is important to hide from observing devices on the internet.

C) Insurance Concerns: The insurance companies installing IoT devices on vehicles collect data about health and driving status in order to take decisions about insurance.

D) Lack of Common Standard: Since there are many standards for IoT devices and IoT manufacturing industries. Therefore, it is a big challenge to distinguish between permitted and non-permitted devices connected to the internet.

E) Technical Concerns: Due to the increased usage of IoT devices, the traffic generated by these devices is also increasing. Hence there is a need to increase network capacity; therefore, it is also a challenge to store the huge amount of data for analysis and further final storage.

F) Security Attacks and System Vulnerabilities: There has been a lot of work done in the scenario of IoT security up till now. The related work can be divided into system security, application security, and network security [17].
a) System Security: System security mainly focuses on overall IoT system to identify different security challenges, to design different security frameworks and to provide proper security guidelines in order to maintain the security of a network.
b) Application security: Application Security works for IoT application to handle security issues according to scenario requirements.

c) Network security: Network security deals with securing the IoT communication network for communication of different IoT devices.

V. CONCLUSION

Security in IoT is a need of the time. Security must provide Integrity,Confidentiality, non-repudiation and authentication of the information flows. Security of IoT communications can be addressed in the context of the communication protocol, or on the other end by external mechanisms. Other security requirements should be considered for the IoT and in particular regarding communications with sensing devices.

The main emphasis of this paper was to highlight major security issues of IoT particularly, focusing the security attacks and their countermeasures. Due to lack of security mechanism in IoT devices, many IoT devices become soft targets and eventhis is not in the victim's knowledge of being infected.

In this paper, the security requirements are discussed such as confidentiality, integrity, and authentication, etc. Moreover, to protect from any intruders or security threat, it is also recommended not to use default passwords for the devices and read the security requirements for the devices before using it for the first time. Disabling the features that are not used may decrease the chances of security attacks. Moreover, it is important to study different security protocols used in IoT devices and networks.

REFERENCES

[1]. Evans D. The Internet of Things - How the Next Evolution of the Internet Is Changing Everything. CISCO white paper 2011; .

[2]. David K, Jefferies N. Wireless visions: A look to the future by the fellows of the www.Vehicular Technology Magazine, IEEE Dec 2012; 7(4):26 –36, doi:10.1109/MVT.2012.2218433.

[3]. Mattern F, Floerkemeier C. From active data management to event-based systems and more .Springer-Verlag, 2010.

[4]. Presser M, Krco Sa. IOT-I: Internet of Things Initiative: Public Deliverables – D2.1: Initial report on IoT applications of strategic interest 2010.

[5]. Atzori L, Iera A, Morabito G. The Internet of Things: A survey. Computer Networks 2010; 54 (15):2787 – 2805, doi:10.1016/j.comnet.2010.05.010.

[6]. Benetton to Tag 15 Million Items. RFID Journal.http://bit.ly/XXe4Wi [Online. Last accessed: 2012-09-25], 2003.

[7]. Albrecht K. Boycott Benetton - No RFID tracking chips in clothing! Press Release.http://bit.ly/49yTca [Online. Last accessed: 2012-09-25], Sep 2003.

[8]. Cuijpers C. No to mandatory smart metering does not equal privacy! Tilburg Institute for Law, Technology, and Society: Webblog 2009; .

[9]. The INDECT Consortium. INDECT project.http://www.indect-project.eu/ [Online.Last accessed: 2012-10-12], 2009.

[10]. Munch V. STOPP INDECT.http://www.stopp-indect.info [Online. Last accessed: 2012-10-12], 2012.

[11]. L. M. R. Trabuco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santanna, "Internet of things in healthcare: Interoperatibility and security issues," in Communications (ICC), IEEE International Conference on . IEEE, 2012, pp. 6121–6125.

[12]. R. H. Weber, "Internet of things–new security and privacy challenges,"Computer law & security review vol. 26, no. 1, pp. 23–30, 2010.

[13]. S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposedsecurity model and threat taxonomy for the internet of things (iot),"inInternational Conference on Network Security and Applications. Springer, 2010, pp. 420–429.

[14]. Y. H. Hwang, "Iot security & privacy: threats and challenges," inProceedings of the 1st ACM Workshop on IoT Privacy, Trust, andSecurity.ACM, 2015, pp. 1–1.

[15]. M. A. Qureshi, A. Aziz, B. Ahmed, A. Khalid, and H. Munir, "Comparative analysis and implementation of efficientdigital image watermarking schemes, "International Journal of Computer and ElectricalEngineering, vol. 4, no. 4, p. 558, 2012.

[16]. M. Abdur Razzaq, R. A. Sheikh, A. Baig, and A. Ahmad, "Digital image security: Fusion of encryption, steganography and watermarking," International Journal of Advanced Computer Science and Applications (IJACSA) , vol. 8, no. 5, 2017.

[17]. H. Ning, H. Liu, and L. T. Yang, "Cyber entity security in the internet of things," Computer, vol. 46, no. 4, pp. 46–53, 2013.

Kamiya shrivastava "Internet of Things: Security & Privacy Nightmare." The International Journal of Engineering and Science (IJES), vol. 6, no. 12, 2017, pp. 45-50.