Internet of Things: Security Issues

Ramanpreet Kaur
Dept of Computer Science
GGN Khalsa College, Ludhiana

Abstract- *The Internet of Things (IoT) is an emerging paradigm in which wide variety of objects are interrelated over internet like computing devices, machines, animals or people in such a way that they can communicate with each other without requiring human interaction.The Internet of Things (IoT) opens opportunities for wearable devices, home appliances, and software to share and communicate information on the Internet. The shared data contains a large amount of private information and preserving this private information in a secure way is an important issue that cannot be neglected. This paper focuses on the security problems and challenges in IoT environment.*

Keywords- Internet of Things,privacy, sensitive, security concerns

I. INTRODUCTION

The term, internet of things (IoT) that refers to uniquely identifiable objects, things, and their virtual representations in an internet-like structure, was first proposed in 1998 [1].IoT is based on the concept of wireless sensor networks and machine to machine communication where each device is recognized by a unique identifier which is used to transfer data over a network. Internet of Things can be seen as a framework which allowsintegration and data exchange between the physical world and computer systems over existing network infrastructure. It includes the interaction between cars, home devices, electronic appliances, lamps, security systems etc. The reality of internet of things is based on following components:

Hardware-Making physical objects active with the capability to respond to instructions

Software-Enabling the data collection, storage, processing, manipulating and instructing

Communication Infrastructure-consists of protocols and technologies which enable two physical objects to exchange data

The practical realization of IoT requires the development of a number of new versions of platforms and technologies including device and process identification and tracking, sensing and actuation, communication, computational sensing, semantic knowledge processing, coordinated and distributed control, and behavioral, traffic, and user modeling [3].

IoT transpires a vision of a future Internet where any object having computing and sensing capabilities can communicate with other devices using Internet communication protocols. This framework requires a lot of sensing and actuating devices which places constraint on cost, memory, energy and power. Overall, such factors motivate the design and adoption of communications and security mechanisms optimized for constrained sensing platforms, capable of providing its functionalities efficiently and reliably[2].

As the advancements in telecommunication sector are becoming more efficient, broadband internet is widely available. With the advent of new technologies it is now much cheaper to produce necessary sensors with built-in Wi-Fi capabilities making connecting devices less costly.

Most important, the smart phone usage has surpassed all the predicted limits and telecommunication sector is already working on its toes to keep their customers satisfied by improving their infrastructure. As IoT devices need no separate communication than the existing one building IoT tech is very cheap and highly achievable. The interconnection of a large number of smart devices opens the door for new research challenges and issues.

As to the security, the IoT will be faced with more severe challenges. The following are the reasons for the need of secure IoT

1) The IoT extends the ‘internet’ through the traditional internet, mobile network and sensor network and so on,
2) Every ‘thing’ will be connected to this ‘internet’
3) These ‘things’ will communicate with each other. Therefore, the new security and privacy problems will arise. We should pay more attention to the research issues for confidentiality, authenticity, and integrity of data in the IOT.

II. CHALLENGES IN IOT DEVELOPMENT

As with any disruptive innovation, the IoT will present multiple challenges to adopting enterprises. For example, due to the explosion of data generated by IoT machines,Gartner(2014) suggested that data centers will face challenges in security, the enterprise, consumer privacy, data itself, storage management, server technologies, and data center networking. According to a report by Gartner there will be 30% increase in the number of connected devices in 2016 as compared to 2015 with 6.4 billion IoT devices entering the realm of internet of things. The number is further expected to increase to 26 billion by 2020.

1. Data Management:

With the advancements in telecommunication a huge amount of sensing devices connecting through IoTgive rise to data management challenge. The internet is full of smart devices these days which generates massive amount of data. The storage and processing of this bulk data requires data centers with capability to handle voluminous data, backup procedures efficiently. Data centers will become more distributed to improve processing efficiency and response time as IoT devices become more widely used and consume more bandwidth [4].

2. Data Mining:

While keeping in mind the usage of this huge amount of data in business perspective, the use of data mining tools becomes a necessity to process and analyze the data available. Advanced data mining tools are used to analyze the data from sensor networks.

3. Interoperability and Standardization:

In order to achieve better communication between different connected devices, IoT infrastructure should be based on some standard rules and protocols that must be followed to connect different and wide variety of devices over the internet.

4. Information Privacy:

IoT is concerned with connecting daily life smart objects in such a way that the quality of lifestyle of an individual gets improved to a great extent. This quality improvement needs protecting individual's privacy.IoT devices collect and handle one's very sensitive and personal data which are stored in cloud servers using third party vendors or cloud service providers. Thus this private data needs to be protected from unauthorized access because it creates a lot of damage if it will fall into hands of wrong people. According to the 2014 TRUSTe Internet of Things Privacy Index, only 22% of Internet users agreed that the benefits of smart devices outweighed any privacy concerns (TRUSTe, 2014). In this scenario the fundamental challenge in growth IoTis of protection of private data.

5. Compatibility and Longevity Challenge:

IoT is growing in many different directions, where number of devices with different technologies is connected together for machine to machine interaction. In order to make this interaction efficient and fruitful, IoT requires the deployment of extra hardware and software while connecting these heterogeneous devices. But the point here is that the technologies used in these devices obsolete very soon, so it becomes very difficult to handle compatibility issues.

6. Data Security:

IoTnetwork introduces a large number of connected devices which give rise to a new challenging area related with security concerns. Iot make use of personal information of users which needs to be protected from hackers .IoT devices do not use data encryption techniques, authorization, software protection. It is desired to make every effort to reduce the complexity of connected systems, enhance the security and standardization of applications, and guarantee the safety and privacy of users anytime, anywhere, on any device.

7. Naming and Identity Management:

IoT Network introduces billions of connected objects to enhance the living standard and provide a variety of services. Each object needs some identification mechanism to have a unique identity over the Internet. Thus, an efficient naming and identity management system is required that can dynamically assign and manage unique identity for such a large number of objects.

8. Data confidentiality and encryption:

The sensor devices perform independent sensing or measurements and transfer data to the information processing unit over the transmission system. It is necessary that the sensor devices should have proper encryption mechanism to guarantee the data integrity at the information processing unit.

9. Connectivity Challenge:

Networking environment is based on centralized or client server models these days. These types of models are well suited where number of connected components is limited,

as the count of devices increase the complexity of connectivity becomes difficult to handle.Thus in order to manage and tackle billion and trillions of connected devices, it will require huge investments, efficient cloud servers that can handle such large amounts of information exchange.

10. Network security:

The data from sensor devices is sent over wired or wireless transmission network. The transmission system should be able to handle data from large number of sensor devices without causing any data loss due to network congestion, ensure proper security measures for the transmitted data and prevent it from external interference or monitoring.

12. GreenIoT:

Due to increasing growth of internet in every sphere of life and use of internet enabled services, there will be huge amount of connected devices which give rise to the demand of increased power and energy consumption. The future IoT will cause significant increase in the network energy consumption. Thus, green technologies need to be adopted to make the network devices energy efficient.

III. CONCLUSION

This paper introduced the emerging future of Internet called "Internet of Things" that will connect everything and everyone. The IoT embeds intelligence in the sensor devices to autonomously communicate, exchange information and take intelligent decisions. This paper finally addressed some key challenging areas concerned with the IoT technology. The IoT deployment could be hard and require large research efforts to tackle with the challenges but it can provide significant personal, professional and economic benefits in the near future.

REFERENCES

[1] R. H. Weber, “Internet of things – new security and privacy challenges,” Computer Law & Security Review, vol. 26, pp. 23-30, 2010.
[2] Jorge GranjalSecurity for the Internet of Things: A Survey of Existing Protocols and Open Research issues”
[3] A. Juels, “RFID security and privacy: A research survey,” IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 381–394, 2006.
[4] The Internet of Things (IoT): Applications, investments, and challenges for enterprises In Lee a, Kyoochun Lee b” Business Horizons (2015) 58, 431—440
[5] https://www.sitepoint.com/4-major-technical-challenges-facing-iot-developers/
[6] S. Haller, S. Karnouskos, and C. Schroth, "The Internet of Things in an Enterprise Context," in Future Internet – FIS 2008 Lecture Notes in Computer Science Vol. 5468, 2009, pp 14-28.
[7] Roberto Minerva, AbiyBiru, "Towards a Definition of the Internet of Things," IEEE IoT Initiative white paper.
[8] Wan, J., Zhang, D., Sun, Y., Lin, K., Zou, C., &Cai, H. (2014). VCMIA: A novel architecture for integrating vehicular cyberphysical systems and mobile cloud computing. ACM/Springer Mobile Networks and Applications, 19(2), 153–160.
[9] D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, 1662Springer, 2010. ISBN: 978-1-4419-1673-0. 1663
[10] L. Tan and N. Wang, “Future Internet: The Internet of Things,” in 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), August 2010.
[11] T. Fan and Y. Chen, “A Scheme of Data Management in the Internet of Things,” in 2nd IEEE International Conference on Network Infrastructure and Digital Content, Sept. 2010.
[12] M. Conti, V. T. N. Nguyen, and B. Crispo, "Crepe: context-related policy enforcement for android," in Information Security, Springer, 2011, pp. 331–345.
[13] H. S. Ning, H. Liu; Y, L.T. "Cyberentity Security in the Internet of Things," Computer, vol.46, no.4, pp.46,53, April 2013
[14] Wang, K., Bao, J., Wu, M., & Lu, W. (2010). Research on security management for internet of things. In Proceeding of the IEEE international conference on computer application and system modeling (ICCASM) (vol. 15, pp. 133–137)
[15] Z. Yang, M. Yang, Y. Zhang, G. Gu, P. Ning, and X. S. Wang, "Appintent: Analyzing sensitive data transmission in android for privacy leakage detection," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013, pp. 1043–1054.