RESEARCH ARTICLE OPEN ACCESS

A Study on Data Security in Internet of Things

G. Ambika [1], Dr.P.Srivaramangai [2]
PG & Research Scholar [1], Assistant Professor [2], Director,
Department of Computer Science
Srimad Andavan Arts & Science College, Tiruchirappalli
Tamil Nadu - India

ABSTRACT

The main aim of this paper is to enhance the security in Internet of things and services, which have the potential scope and benefits not only for the end users but also for the service providers and adaptors. Due to the invention of IPv6 and the development of Wifi networks, digitally connected devices are being developed in all the fields. Since there is an intervention of internet there are many security issues. Internet of things and data mining is the primary interest of many information researchers worldwide due to the fast booming information technology sector. This paper provides a high level review of the fundamentals of Internet of Things, a few of the key problems and issues, that can be raised from the user perspective.

Keywords:- Internet of Things, Data security, IPv6, Wifi networks, Internet of Things revolution, Information technology, Privacy, etc.

I. INTRODUCTION

The Internet of Things is a very important topic on Information technology business, policy, and engineering circles. This technology is embodied with a wide spectrum of networked merchandise, systems, security and sensors that make the most of the advancements in computing power. Science conferences, reports, and news articles discuss and analyse the possible impact of the " Internet of Things revolution". Internet of Things has the potential to develop new market opportunities and business models. At the same time security, privacy, and technical feasibility issues should also be addressed.

According to a research report, there will be 40 million wireless connected devices by 2020. More connected devices lead more attacks by hackers. Digitally connected devices such as mobile phones, cars and all other products have potential threats through the hackers, attack vectors and cyber criminals. Internet of Things security has many issues of high concern. Many researches are going on in and around the world in the field of Internet of Things security through devices using smart mobile phones. Huge repositories of Internet of Things data related to consumers, manufacturers, service providers have potential threats from the hackers and spies. More research work has to be conducted in the data security area in order to protect the privacy of the consumers and the functionality of the corporate companies. According to the HP Enterprises security products company research, 70 % of the most commonly used Internet of Things devices have vulnerability such as password security, encryption, etc.,

The number of connected devices increases and their usage becomes an important part of day to day life, security, confidential and individual safety issues will arise. Many security issues are seen to take up in the Internet of Things environment for sensitive information. The variety of sources manage and secure these vast changes the security issues. Security of Personal information is a major concern in the Internet of Things environment. Through cloud services available data security is provided.

II. REVIEW OF LITERATURE

According to Dong Chen et al. heterogeneous entities, security communication, security system and other security issues are complex and difficult. A novel security architecture for Internet of Things has been proposed to solve complexity issues.[1]. Sachin Babar et al, have proposed an embedded security framework to solve the security issues with Internet of Things and integrating the conventional security systems and embedded security system in the device itself for the better security services and also proposed a security model for the Internet of Things [2]. Wu He et al, have proposed a novel multi-layered vehicular data cloud platform. This paper deals about the vehicular data cloud services, intelligent parking cloud service and vehicular data mining cloud service in the Internet of Things environment. This paper also analyzed the Naïve Bayes model and a Logistic Regression model for the Internet of Things environment [3].

Chang Lu et al, have analyzed the security of Internet of Things based on authenticator-based data integrity verification techniques for cloud. This paper also focuses multiple aspects of the security problem and proposed security verification technique for Internet of Things [4]. Zhao et al, proposed ISSAP-Intelligence Service Security Application Protocol, which has a standard packet structure named smart business security, Internet of Things application Protocol used a custom data packet encapsulation mechanism which helped to reduce the overhead of data resources. This author also used another cross-platform communication which has a combination of secure encryption and decryption, signature and authentication algorithms. Finally developed the secure communication system for Internet of Things [5].

Liang et al. studied the security of multimedia applications on the Internet of Things, analyzed the security issues in wired, wireless sensor and actuator networks. An efficient multimedia-aware security framework for transmitting various multimedia applications in the Internet of Things are framed. A novel multimedia traffic classification, analysis method and also proposed multimedia-aware traffic security architecture based on classification. The flexibility and efficiency of the security architecture, the characteristics of multimedia traffic, security service and the Internet of Things were studied [6]. Dukas et al, presented a system to solve security issues using digital certificates and PKI data encryption [7]. Quandeng Gou studied the security problem in Internet of Things perception, network and application on the environment and proposed security strategies frameworks for Internet of Things. The theoretical basis to build up the reliable security system developed [8]. According to Marica et al, the Named Data Networking has the potential as a secured content retrieval solution both in wired and wireless networks. Its elements such as name based content, named routing and in-network caching are suitable for the heterogeneous nature of the Internet of Things [9].

III. USER NEED FOR SECURITY IN IOT

Internet generates a large volumes of data which needs scalable, huge, storing & processing capacity specifically for varied devices. Users need their data to be secured while accessing or storing or processing their data thro devices. Data authentication of the source of data is required in Internet of Things environment. M2M and the Internet of Things has huge potential, but currently comprises a heterogeneous collection of established and emerging, often competing, technologies and standards. Thus data security of internet of things devices is to be addressed to make sure that the client devices are secured for easy access & usage.

IV. ISSUES & CHALLANGES IN DATA SECURITY

- Many devies are IOT connects things there will be various challenges to organize and manage Individual devices.
- Personal data protection is required in Data retrieval and processing of large volumes of data in Internet of Things environment.
- Data authentication for source of data is required in Internet of Things environment.
- Data usage through the security channel attack need to be addressed.
- To improve performance of Internet of Things environment through increasing latency and capacity

V. CONCLUSION

Data security in Internet of Things is already seen as inhibiting the adoption of services for variety of organizations. Internet of Things are designed with protection with so much of data with less thought given to sharing. A promising approach is providing each information protection and sharing is to enhance centered access management technologies with people who specialize in the properties of the information. Providing controlled information sharing is often supported by public cloud services via secured networks.

VI. REFERENCES

[1]. Dong Chen, et al, “A novel secure architecture for the Internet of Things”, IGEC, 5th conference, IEEE Xplore, 2011

[2]. Sachin babar et al, “Proposed embedded security framework for Internet of Things”, Wireless communication, 2nd conference, IEEE Xplore, 2011

[3]. Wu He et al, “Developing vehicular Data cloud services in the Internet of Things environment”, Transactions on informatics, IEEE Xplore, 2014

[4]. Chang Lu et al, “External integrity verification for outsourced big data in cloud and Internet of Things: A big picture”, future generation computer system, ELSEVIER, 2015

[5]. Y. L. Zhao, "Research on Data Security Technology in Internet of Things", Applied Mechanics and Materials, Vols. 433-435, pp. 1752-1755, 2013

[6]. Liang Zhou et al, “Multimedia traffic security architecture for the internet of things”, IEEE Xplore, 2011,

[7]. Doukas et al, “Enabling data protection through PKI encryption in Internet of Things m-Health devices” Bioinformatics HYPERLINK "http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber= HYPERLINK "http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6387371" HYPERLINK "http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6387371"6387371

[8]. Quanden Gou, “Construction and Strategies in Internet of Things Security System”, Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social ComputingIEEE Xplore, 2013,

[9]. Marica et al, “Named data networking for Internet of Things: An architectural perspective”, Networks and Communications (EuCNC), 2014 European Conference onIEEE Xplore, 2014.