International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume – 04, Issue – 04, April 2019, PP – 06-10

Internet of Things Security Management Policies and Procedures

Dr. Abdelrahman Karrer, Mohammed Saif
Kingdom of Saudi Arabia, Madinah
Taibah University
College of Computer Science and Engineering
Department of Information System

Abstract: Internet of thing is an advanced concept in information technology that benefit the society thorough providing solutions for several kinds of problems. Internet of thing (IOT) require strong security system and securities management policies. Considering the importance of security systems, policies and procedures for IOT security management are discussed in detail. In this paper, major components, challenges, and applications of IOT are discussed in the light of information and knowledge collected from research and literature review. Secondary data analysis presented information about the key threats of IOT and FTC policies for security management that is also presented in this paper. After discussing the all challenges and applications of IOT recommendations are presented for security system of IOT. In the light of research, it can be recommended that experts of IOT should follow up the guidelines and policies to avoid security related issues.

Introduction

The aim of this paper is to provide deep insights regarding the security management policies & procedures regarding the internet of things (IOT). IOT has gain immense importance in the 21st century because of the technological advancement. IOT has revolutionized the world and have provided solution to a lot of problems. IOT can be defined as the network of various devices connected with each other to interact & share data with each other [1]. Through IOT the internet connectivity has been expended beyond the traditional devices which include smartphones, desktops and laptops. Today the IOT is connecting devices such as cars, ovens and other electronic equipment's. Since the number of devices increased the usage and challenges related to IOT have also increased as a result. One of the biggest challenges is related to the security policies of IOT. The data of the users contain sensitive information which can be used for wrong purposes [2]. The paper will discuss various security related challenges and how those challenges can be overcome through proper policies. The paper is divided into four main sections. The first section is the introductory section, second section discuss the components & key challenges in IOT, third section discuss the management policies & procedures and in the end the paper provides recommendations & conclusion.

IOT Practices to Large Companies

Internet of things (IOT) can be defined as the network of devices. Different devices are connected with each other so that they can interact and share data with each other. In the past the devices like laptops, desktops and smartphones were connected with internet to exchange information [3]. However, IOT has allows individuals to connect other electronic devices with the internet as well. Today the experts believe that everything that is around us can be connected such as vehicles, home appliances etc. IOT has lots of applications and can provide more convenience to the society. IOT can be used in Medical health care, creation of Smart homes and for modernizing the current industrial processes [4]. It can be said that IOT has lots of advantages and have many applications for the future however there are lots of challenges that needs to be addressed in order to make this technology more beneficial for the users. One of the major challenges is the security concern that should be addressed to enhance the benefit [5].

Components of IOT

Following are the key components of the IOT that are discussed in detailed below:

Sensors & Physical Devices

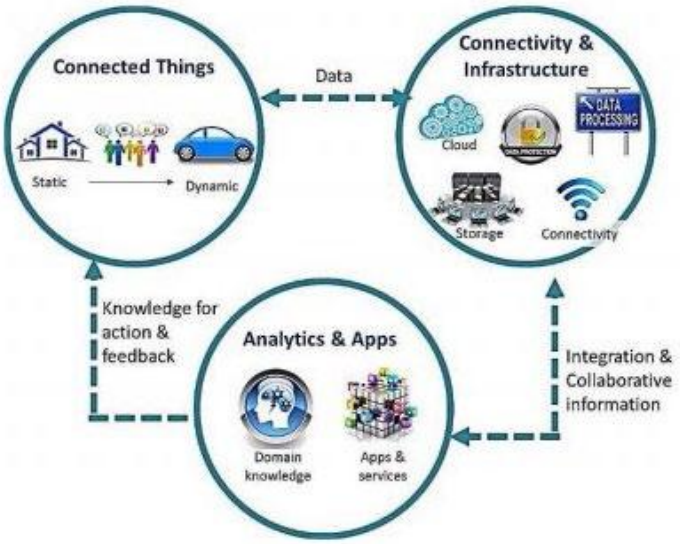
IOT ecosystem consist of analytics, cloud application and all the aspects related to the internet. The physical devices & sensor have the ability to gather the information [6]. After gathering the information, the devices react accordingly. The devices or sensors are programed to perform various functions according to the information provided. The devices are the most important part of the IOT mechanism and without devices IOT system would not work [7].

Infrastructure & Connection

In the internet of things the devices needs to be connected with each other which means that necessary infrastructure is required for the connectivity of the devices. It means that internet infrastructure, storage, could, security and data processing facilities would be needed for the IOT system [8]. In the IOT system it is important that the information should be stored and secured for the users [9]. The data security is important because data breaches can cause financial loss of the individuals. Various technologies can be used for enhancing the security and privacy of the network [10].

Applications & Analytics

Various applications and analytics are developed to provide various benefits to the users. Through various applications the users can perform various tasks such as finding various locations, perform payments and sharing important data. The applications & analytics are developed by keeping the preferences and needs of the customers in mind. Specific applications are made for providing convenience to the users however they also raise security & privacy concerns as well [11]. It is important for the App manufacturers to enhance the security of the user data otherwise various issues Can arise in future which will not only affect the users but also to the business which are related to App manufacturing



Source: https://wikisites.cityu.edu.hk/sites/netcomp/articles/Pages/InternetofThings.aspx

Key Challenges & Threats to IOT

Security & Privacy

The privacy and security is a major challenge for the IT experts and in the growth of IOT ecosystem. Since more devices are connected with the internet the level of security concern has increased up to lot of extent. Today the users of the devices share sensitive data that can be used for inappropriate purposes through which the users can face financial loss [12]. Therefore, it is important to develop such security management policies which allow IT organizations to improve the security of the whole IOT ecosystem [5].

Ecosystem

The IOT ecosystem consist of all the aspects of internet, devices and connectivity infrastructure. AS the IOT is experiencing growth over time more things are started entering into IOT ecosystem like everyday objects. It means that the level of complexity will increase up to lot of extent which would arise a lot of other problems from the security & privacy point of view [13]. In future more advance mechanism would be needed for the management of such a complex IOT ecosystem which can only be done through strong management policies [14].

Data & Information

The data & information would be a great challenge in the future. It is evident that more storage would be needed for storing and protecting the data. When huge amount of devices are going to be connected than the amount of data would be in large number and it is up to the IOT experts to manage the data efficiently [15].

Man in the middle attack

The man in the middle attack would be one of the major threats for the IOT in the future. Man in the middle attack means that the third individual can intervene between two individuals when they are sharing information. Through this the third individual can hack the information and can use it for its own benefit. It means that the other two persons can face severe consequences due to this data breach [16]. Over the years IOT experts have taken necessary actions to improve

DoS Attack

Denial of Services (DoS) Attack is among the most common cyber-attack and is major threat for IOT mechanism. The attack can cause the devices to become unavailable for use for the users. In order to mitigate or control such attacks necessary measures have to be taken for improving the security of the IOT system [17].

	Manufacturing	Installation/ Commissioning	Operation
Transport Layer		Eavesdropping & Man-in-the-middle	Eavesdropping & Man-in-the-middle
Network Layer			DoS attack Routing attacks
Physical Layer	Device Cloning	Substitution	DoS attack Privacy threat Extraction of security parameters

Source: https://www.ijcsmc.com/docs/papers/June2016/V5I6201699a9.pdf

Security Management policies & Procedures for IOT

Following are the main Security Management policies & Procedures which have been implemented to improve the security & privacy:

Attack Counter Measure Policy

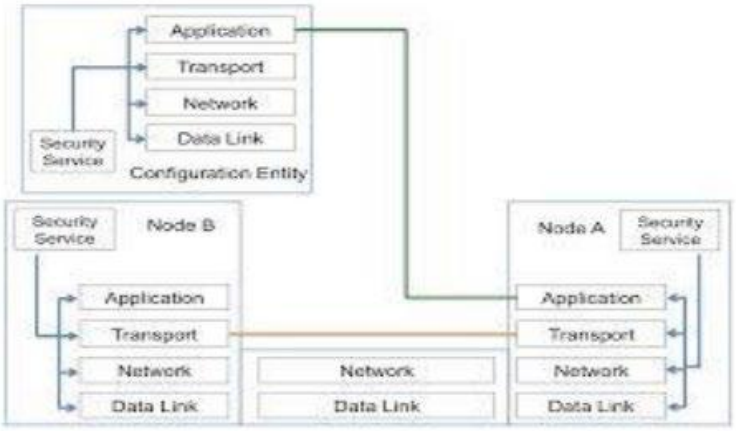
The cyber attackers can get information about the security information keys and through this they might be able to reprogram the devices according to their own preferences. If group key has been implemented than the entire IOT network can get effected. The policy of forming unique keys can mitigate or control such cyber-attacks [10].

FTC Policies & Regulations

FTC (Federal Trade Commission) has allowed the corporations to create built in security in the devices which are being used in the IOT framework. For collecting the data FTC thinks that involving customer would be a great idea because through this not only the trust of the users can be gained but also new strategies for the improvement security can also be made.

Enhancement of data integrity

It is important to enhance the integrity of the data through encryption. When the data is going to be encrypted the man in the middle attack will be controlled up to lot extent. When the data is encrypted it becomes nearly impossible for the individual to decipher it [7].



Source: https://www.ijcsmc.com/docs/papers/June2016/V5I6201699a9.pdf

Conclusion

If all the above discussion is summarized than it is evident that IOT ecosystem consist of analytics, cloud application and all the aspects related to the internet. The physical devices & sensor have the ability to gather the information. After gathering the information the devices react accordingly. The devices or sensors are programed to perform various functions according to the information provided. The cyber attackers can get information about the security information keys and through this they might be able to reprogram the devices according to their own preferences. If group key has been implemented than the entire IOT network can get effected. The policy of forming unique keys can mitigate or control such cyber-attacks.

Recommendations

It is recommended to the IOT experts to work according to the set guidelines. It is recommended to the organizations or IT experts to use authentic or trusted IOT devices so that no privacy/security concern could arise in the future. FTC have formed various policies for the improvement of security therefore it is responsibility of the It expert to create IOT ecosystem in accordance with the policies. FTC (Federal Trade Commission) has allowed the corporations to create built in security in the devices which are being used in the IOT framework.

References

[1]. B. Russell and D. V. Duren, Practical Internet of Things Security: Design a security framework for an Internet connected ecosystem, Packt Publishing Ltd, 2018.
[2]. S. Li and L. D. Xu, Securing the Internet of Things, Elsevier Science, 2017.
[3]. S. Bhattacharjee, Practical Industrial Internet of Things Security: A practitioner's guide to securing connected industries, Packt Publishing Ltd, 2018.
[4]. Management Association, The Internet of Things: Breakthroughs in Research and Practice: Breakthroughs in Research and Practice, IGI Global, 2017.
[5]. H. Jayakumar, K. Lee, W. S. Lee, A. Raha, Y. Kim and V. Raghunathan, "Powering the Internet of Things," pp. 375-380, 2014.
[6]. P. N. Mahalle and P. N. Railkar, Identity Management for Internet of Things, River Publishers, 2015.
[7]. R. Roman, J. Zhou and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," vol. 57, no. 10, pp. 2266-2279, 2013.
[8]. M. Dawson, M. Eltayeb and O. Marwan, Security Solutions for Hyperconnectivity and the Internet of Things, IGI Global, 2016.
[9]. B. Aziz, A. Arenas and B. Crispo, Engineering Secure Internet of Things Systems, Institution of Engineering and Technology, 2016.
[10]. A. K. Rajpoot, M. Varshney and A. Nailwal, "Security and Privacy Challenges in the Internet of Things," International Journal of Computer Science and Mobile Computing, vol. 5, no. 6, p. 525 – 531, 2016.
[11]. L. Chen and S. Erfani, "A note on security management of the Internet of Things," in 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), 2017.

[12]. K. Wang, J. Bao, M. Wu and W. Lu, "Research on security management for Internet of Things," in 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), 2010.

[13]. D. Jonckers, "A security mechanism for the Internet of Things in a smart home context," KU Leuven, 2016.

[14]. B. B. Zarpelão, R. S. Miani, C. T. Kawakani and S. C. Alvarenga, "A survey of intrusion detection in Internet of Things," vol. 84, pp. 25-37, 2017.

[15]. L. Chen, "Security Management for The Internet of Things," University of Windsor, 2017.

[16]. X. Liu, M. Zhao, S. Li, F. Zhang and W. Trappe, "A Security Framework for the Internet of Things in the Future Internet Architecture," MDPI, 2017.

[17]. P. Kasinathan, C. Pastrone, M. A. Spirito and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," pp. 600-607, 2013.

