ISSN 2319-2720
Volume 7, No.4, October - December 2018
International Journal of Computing, Communications and Networking
Available Online at http://www.warse.org/ijccn/static/pdf/file/ijccn01742018.pdf
https://doi.org/10.30534/ijccn/2018/01742018

INTERNET OF THINGS (IoT): AN OVERVIEW BASED ON SECURITY CHALLENGE

Zeyad Halabi[1], Dr. Abdelrahman Karrar[2]
[1]Saudi Arabia, zrh_z7@hotmail.com
[2]Saudi Arabia, akarrar@taibahu.edu.sa

ABSTRACT

The internet of things is facing a lot of security and privacy related issues, which creates challenges to protect data and information in the IoT network. The resilience to attacks, data authentication, and access control and client privacy are the main aspects of the IoT. In the context of IoT not just users, but some of objects that are authorized may have the right of entry to the data. The Data security is make sure by a variety of technologies of encryption which prevent the stealing threats of the data in the IoT networks.

Key words: IoT, Security, privacy, network, Data protection.

1. INTRODUCTION

The internet of things (IoT) is very vast topic, and in the today's global world with the extensive use of internet and web the security issues and challenges of IoT also increasing. The IoT is basically the network of interconnected entities that can be human, cars, books, computers etc. there is always a communication channel between all of the entities in IoT that help them to exchange the information and develop a good network [1].

The IoT has some security issues, privacy issues, diverse authentication and issues related with the information storage and management and access control network configuration and so on. In the case of IoT the data and privacy protection is the application challenges. In IoT, WSNs sensors in the RFID systems distinguish for information technology end, which is likely to defend the integrity and privacy of overall information by using the technology of password encryption.

In IoT there are a lot of ways for encryption of information and data, for example the hash chain protocol, random hash lock protocol, Encrypted identifier etc. The access control and Identity authentication can settle on the communication involving both sides and corroborate true identity of each other, to prevent any sort of attacks to make sure the validity and authenticity of information etc. [2]

1.1 Figures

Shows many kind of technologies connected as IoT devices.

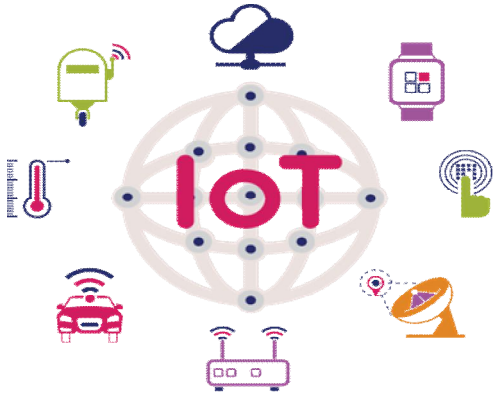

Figure 1.1: Some of IoT devices

2. SECURITY AND PRIVACY NEEDS

The technological architecture of IoT also affects the security and privacy of stakeholders. The Privacy comprises the personal information concealment and also the capability control the information later on. The privacy right in the IoT can be measured as either an essential and absolute human right, or some personal right. In case of IoT the ascription of tags to items might not know by users, and there is not any visual signal in the IoT entities to draw object's user attention. In that way, some of the individuals can be following it without any of knowledge and also leave information or at least cyberspace traces.
Additionally, for aggravation of the problems, it is not the state interested in gathering the individual data, however also some private actors for example the marketing enterprises also have get effected by IoT security issues. There are many of security requirements are there that must be followed in the IoT. The resilience to attacks, data authentication, and access control and client privacy are the main aspects of the IoT that must be consider while managing the security of IoT network. [3]

2.1 DATA CONFIDENTIALITY

The data confidentiality stands for a primary issue in IoT set-up, demonstrating the assurance that just certified entities can access and adapt the data. This is mainly significant in the context of business; the data may symbolize an asset that must be protected to guard market values and competitiveness. In the context of IoT not just users, but some of objects that are authorized may have the right of entry to the data. This is also likely to necessitate address the two significant aspects: primary, the description of control mechanism access control mechanism and following the description of authentication process of object with a connected system of identity management [4].

3. SECURITY ISSUES IN IOT SYSTEM

The security is the main challenges that have to overcome to move forward the Internet of Things in real world. The architectures of IoT are deal with a probable to billions of objects population, that is likely to interrelate with some of the other entities, for example the virtual entities and human beings. In addition to all these connections should be protected someway, for information protection and provisioning of service for all significant actors and limiting the incidents that have an effect on whole IoT [5].

The security of the IoT has an extremely broad scope in four dimensions. As far as the scope of security it comprises rarely address responsibilities for example computation, trusted sensing, privacy, communication and digital forgetting. It also ensures the better method for the hardware protection, data and software that believe the likelihood of physical access to the devices of IoT. In the IoT devices the sensors and actuators are general mechanism of and pose more than a few unique challenges related to the security as well as the reliability of physical sign and events actuation. At last, throughout collected data processing, one can imagine a lot of semantic attacks. There are many of the IoT security techniques for example CAD security techniques that can be used to have protected IoT network.

4. DIFFERENT LAYERS SECURITY

There are a lot of researches being conducted to offer a dependable distinct architecture of security which can assure the security and privacy of data. [6]

4.1 PERCEPTION LAYER

Perception Layer is IoT architecture bottom layer which offer a variety of hardware security features. It provides four essential principles which are Data Privacy, verification, sensitive information Privacy and Assessment of Risk.

4.2 NETWORK LAYER

The network layer that can be wired or wireless is also having the risk of various types of attacks. Because of the openness of wireless waterway, infrastructure can be observed without difficulty by the hackers. The security of the network layer is divided into 3 categories [7].

5. ATHUNTICATION

With appropriate process of authentication and encryption, unlawful access to the nodes sensor to increase false information could be disallowed strategy. Initially it is likely to under goes the process of authentication which avoids the miscreant user access by incorporated identity identifications. This is same as the identification process in all of the layers excluding that it support some authentications by cooperate services it means that the users can select the associated information to share with services [9].

6. ROUTING SECURITY

After process of Authentication, algorithms of routing are implementing to make sure the data privacy to replace between the nodes of sensor and processing systems. The routing security is also likely to guaranteed by providing the numerous pathways for routing of data which develop the ability of the system to notice any mistake and performing any sort of system failure.

7. DATA PRIVACY

The mechanisms of safety control examine the method for any sort of interruption and lastly the methods of data integrity are executed to ensure the received data [8].

8. INTRUSION DETECTION

Its techniques of intrusion detection offer solutions form a variety of security intimidation by producing an apprehension on happening of any doubtful action in the system because of the continuous check and keeping intruder's activities log which could assist to draw the intruder. There are diverse existing interruption techniques of detection as well as the approach of data mining and anomaly exposure [10].

9. DATA SECURITY

The Data security is make sure by a variety of technologies of encryption which prevent the stealing threats of the data in the IoT networks. Furthermore, to avoid other malevolent

activities from troublemaker users, the AntiDos firewalls and advanced spywares and malwares are set up.

10. CONCLUSION

Summing up the discussion, it can be said that the The IoT has some security issues, privacy issues, diverse authentication and issues related with the information storage and management and access control network configuration and so on. The access control and Identity authentication can settle on the communication involving both sides and corroborate true identity of each other, to prevent any sort of attacks to make sure the validity and authenticity of information. In case of IoT the ascription of tags to items might not know by users, and there is not any visual signal in the IoT entities to draw object's user attention.

In the context of IoT not just users, but some of objects that are authorized may have the right of entry to the data. In addition to all these connections should be protected someway, for information protection and provisioning of service for all significant actors and limiting the incidents that have an effect on whole IoT. Perception Layer is IoT architecture bottom layer which offer a variety of hardware security features. With appropriate process of authentication and encryption, unlawful access to the nodes sensor to increase false information could be disallowed strategy.

REFERENCES

1. Suma M , Sushma S V , Swathi S Poojari , Sanjana R , Prof. Kiran M, " A novel technique for automatic detection of earthquake and landslide using iot " International Journal of Computing, Communications and Networking, 2018.
2. Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu, "Security of the Internet of Things: perspectives and challenges," 2014.
3. Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan, "Future Internet: The Internet of Things Architecture,Possible Applications and Key Challenges," IEEE, pp. 257-260, 2012..
4. M.U. Farooq, Muhammad Waseem, Anjum Khairi, and Sadia Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," International Journal of Computer Applications, vol. 111, no. 7, 2015.
5. Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues," IEEE, 2015.
6. Rolf H. Weber, "Internet of Things – New security and privacy challenges," c o m p u t e r l a w & s e c u r i t y r e v i e w, vol. 26, pp. 23-30, 2010
7. Huansheng Ning and Hong Liu, "Cyber-Physical-Social Based Security Architecture for Future Internet of Things ," Advances in Internet of Things, pp. 1-7, 2012.
8. Docs.microsoft.com. (2018, June) Internet of Things security architecture. [Online]. https://docs.microsoft.com/en-us/azure/iot-fundamentals /iot-security-architecture
9. Mahmud Hossain, Maziar Fotouhi, and Ragib Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," June 2015. [Online]. file:///C:/Users/Pk/Downloads/mahmud2015scc-iotsecuritysurvey.pdf
10. Gary Eastwood. (2017, February) 4 critical security challenges facing IoT. [Online]. https://www.networkworld.com/article/3166106/internet-of-things/4-critical-security-challenges-facing iot.html