ONLINE LIBRARY
(www.onekhmer.org/onlinelibrary)

Title: THE SECURITY PROBLEMS IN THE INTERNET OF THINGS

Name of Author	
Name of University	Deakin
Country of Study	Australia
Major	Business
Degree	Bachelor
Course Title	SIT 382
Type of Document	Assignment
Year	2018

DEAKIN UNIVERSITY

SIT382

THE SECURITY PROBLEMS IN THE INTERNET OF THINGS

An innovation of new information technology has invented a virtual world and provided helpful functions. However, there was a problem of joining the virtual world and the real world. The Internet of Things (IoT) is the solution for helping these issues. The definition of the Internet of Things is a structure of combining computing devices, mechanical machines and digital, physical objects, humans or animals that are supported with unique identifiers that data can be transmitted over a network. In this case, the communication between man to machine and man to man are not used or preferred. All parts work naturally. Even if this has developed better for the business and communication, there are also challenges that must be provided. There are several problems that Internet of Things has to meet ("IEEE Internet of Things Journal", 2017).

- Enterprise- in the Internet of Things, the security issues can cause highly risk for the organization.
- Security- the using an automation of devices and the digitization providing new security issues.
- The customers privacy- the security problems affect privacy of the customers.
- Increased amount of data- The storage will be raising when the personal and public data are increasing.
- Servers costing- highly payment to save and store the data.

THE CHALLENGES IN THE INTERNET OF THINGS

These challenges are the problems which the Internet of Things has to meet today, and the developers have to solve these mentioned problems to the users. There are many problems related to the security.

The data encryption issue- the Internet of Things collects a huge data in the application. The processing and the retrieval of the information are the fundamental part of the Internet of Things environment. These data need to be protected from hackers. The process of encryption is the solution of this security problem. The SSL or Secure Socket Layers protocol can be used to provide this security problem. This is available when the data is online. The SSL is used to protect and encrypt the user's data on website which is in online ("4 critical security challenges facing IoT", 2016).

The authentication of data is the next problem. It is unsure a 100 percent safe to protect the data from the processing of encryption. The hackers have chance to hack

successful. Authentication of the data should be provided to communicate in the system otherwise there is a risk on the security data.

The side channel attacks are problem for the security of the Internet of Things. Valuable data are protected by data encryption and data authentication, but it is not fully secure from the hackers. Many security problems are from side channel attacks. In this process, the hackers concern on how the data is presented rather than paying their attention on the data (“Internet of Things: Security Analysis & security Protocol CoAP", 2017).

INVESTIGATION OF THE SECURITY PROBLEMS IN THE INTERNET OF THINGS

Hardware problems can affect the security of the Internet of Things. There are chipmakers that reinforce and update their processors regularly such as ARMS and Intel. It causes the hardware issues which they cannot address the security gap. The invention of the new architecture of chips are designed for the Internet of Things devices so, the price will be increased as they have made it more complex. Most of the Internet of Things devices are complex devices. This cause the devices to use more power and expensive. Many customers cannot afford it as it is expensive.

There are several concepts to help the security problems in the Internet of Things. The first concept is secure booting. The respective software has to undergo a digital process of verification when an Internet of Things device is launched at the initial phase (Dicxon, 2015). In the future, it makes sure that there are no other programs run on that device. The second concept is access control. It is used to build up the security of the Internet of things. In this process, certain mandatory controls are inserted into the operating system and the both Internet of Things and device activities are restricted. In this case, there are only essential components can be accessed. Authentication solution is the third concept of the security issue of the Internet of Things. In this technique, the embedded devices must be connected to the network and secure machine authentication mechanisms are employed. The local firewalls are used to maintain the security of the Internet of Things. These local firewalls are important. The parent network does not need filtering the traffic, but local filters are useful to figure out which data is going to be processed in the Internet of Things environment.

In the field of Internet of Things, hardware issues cause a significant problem. In the Internet of Things market, there are many organizations that focus on making and developing advanced hardware to support the devices in the Internet of Things environment. ARM and Intel chips are developed to improve their products every year. Each generation is getting larger segment of the respective market by making the new products. The new chips run better and faster in processing and efficient processors in

the Internet of Things. In this process, the Internet of Things environment can be highly improved by using new hardware (Grengouh, 2016).

The generation of new chips do much good work than the previous generation. They do a good job in data encryption and authentication. In the Internet of Things environment, users face many security issues and other disasters. The help of new advanced devices provides the risk can be minimized and make it properly secured in the entire Internet of Things environment. The new chips provide the machines to work more powerful and save much time. There will be problems for users to switch to the modern devices as the price of a new device is more expensive. This issue will decrease the number of customers of using new devices. The cost of the product is the issue for customers, so it is better to find solutions and means to manufacture. This will help customers to be able to afford the products.

The increasing efficiency devices help users to get the advantage of the Internet of Things environment than in the past. In this situation, the consumption of power is the issue for the producers. The battery issue is caused from the modern and complex device. It consumes more power when it is used by the users. The producers have to find solution to solve this issue as all users want to save the power and keep it for a longer time. The long-life batteries solution can be considered as a solution to this issue (“Internet of Things: Security Analysis & Security Protocol CoAP”, 2017).

DISCUSSION

The modern devices provide users with the better advantages of using various area without leaking any information. Even if the products are expensive, but it can support the user in a few aspects. The new components can increase the authenticity, functions and efficiency. However, there are limitations such as expensive, complexity and power consumption. It is better to purchase or install the new advanced devices in Internet of Things environments.

CONCLUSION

The real world and the virtual world of the information technology are linked by the Internet of Things. All devices are connected automatically and work together in the same network with the help of advanced technology. The user performances provide several challenges in security system. To get the maximum use of the Internet of Things, users have to be identified properly and well handled. There are many benefits in different fields. However, this has given many benefits to users but there also have disadvantages such as security issues and the improvement of quality and efficiency.

Hardware issue is the highly effective issue to achieve of the performances in the Internet of Things environment. There are advantages and disadvantages, but it is a must to follow to modern and upgrade devices to get the better of the process.

REFERENCES

4 critical security challenges facing IoT. (2016). CIO. Retrieved 05 September 2018, from http://www.cio.com

Dickson, B. (2015). Why IoT Security Is So Critical?. TechCrunch. Retrieved 05 September 2018, from https://techcrunch.com

Grengouh, J. (2017). How the 'Internet of Things' will impact consumers, businesses, and governments in 2016 and beyond. Business Insider. Retrieved 05 September 2018, from http://www.businessinsider.com

IEEE Internet of Things Journal. (2017). IEEE Internet Of Things Journal, 4(1), C2-C2. http://dx.doi.org/10.1109/jiot.2017.2662259

Internet of Things (IoT): Security Analysis & Security Protocol CoAP. (2017). International Journal Of Recent Trends In Engineering And Research, 3(3), 417-425. http://dx.doi.org/10.23883/ijrter.2017.3126.6ibua