SCIREA Journal of Agriculture

http://www.scirea.org/journal/Agriculture

December 21, 2016

Volume 1, Issue 2, December 2016

SECURITY AND PRIVACY ISSUES IN IoT

S.ANKITHA[1], M.BALAJEE[2]

[1]B.Tech(CSE), 3rd year Student, GMR Institute of Technology, Rajam

seepanaankitha@gmail.com

[2]Sr. Asst. Prof., Dept. of CSE, GMRIT, Rajam, INDIA

balajee.journal@outlook.com

ABSTRACT

Internet of Things (IoT) involves creating network of everyday items embedded with electronics, software and network connectivity. For any technology to be successful and achieve widespread use, it needs to gain the trust of users by providing adequate security and privacy assurance. Some of the devices used by IoT can accommodate only very basic security mechanisms, the likes of which are incapable of maintaining the integrity and confidentiality of the users' data. The IoT developed the concepts of smart cities and smart health concept(s-Health), understood as a context-aware healthcare paradigm for smart environments, improves the quality of healthcare systems within smart cities. Data security in IoT is one of substantial issues and security protocols provided by communication technologies used in IoT such as: ZigBee. The combination of the Internet and emerging technologies such as near- field communications, real-time localization, and embedded sensors lets us transform everyday objects into smart objects that can understand and react to

their environment. Such objects are building blocks for the Internet of Things and enable novel computing applications.

Keywords: security, privacy, smart-health, ZigBee, IoT

1. INTRODUCTION

Now-a-days the technology environment has engaged with different new concepts of technology issues has moved beyond fostering only connections between humans, and now facilitates both the linkage of people to things and indeed, things to one another, to achieve a common goal; this being termed "The Internet of Things (IoT)".Many technologies are slowing down due to hurdles of security and privacy concerns, and many are failed to provide adequate mechanisms of security and privacy issues. Thus ,our new technology Internet of Things(IoT) have solved the problems caused by many technologies regarding security and privacy conditions by gaining the trust of users in many useful and best ways. Smart Objects as Building Blocks for the Internet of Things, which is now widely used for tracking objects, people, and animals. *Smart objects* — that is, autonomous physical/digital objects augmented with sensing, processing, and network capabilities. In contrast to RFID tags, smart objects carry chunks of application logic that let them make sense of their local situation and interact with human users. *Smart*-Health(s-Health) utilizes the smart city infrastructures to provide a more comprehensive medical care to citizens. Privacy is the fundamental right that has to be guaranteed for citizens and it is most important factor in health industry compared to other sectors. We analyse the privacy issues and explore potential risks of the s-Health approach in each of those privacy dimensions in the context of 5-Dimentional privacy issues. Considering security protocols in communication technologies ZigBee is one of the application. ZigBee is a specification for a suite of high level communication protocols, intended for devices equipped with small and low-power digital radios. ZigBee Specification provides two security models.

1) Standard Security Mode and

2) High Security Mode.

2. LITERATURE SURVEY

2.1 SECURITY AND PRIVACY IN HEALTH SECTOR

For smart environments s-Health may encounter some privacy and security issues by improving the health conditions of many people. Mart´ınez-Ballest´proposed the 5D (five dimensions model) for citizen's privacy in smart cities. They identified the following dimensions:

1) Identity privacy,

2) Query privacy,

3) Location privacy,

4) Footprint privacy, and

5) Owner privacy.

IDENTITY PRIVACY:

This privacy helps in recognizing to identify the citizens who are suffering from severe health problems.

QUERY PRIVACY:

This privacy helps to solve the queries raised by user to a database system. For this privacy dimension, the main purpose is to avoid the correlation between citizens and queries, and current PIR solutions.

LOCATION PRIVACY:

This privacy is guaranteeing the physical location of the citizens. When citizens try to obtain optimal routes, they send their location to CCC and allow the LBS provider to track them.

FOOTPRINT PRIVACY AND OWNER PRIVACY:

These privacy issues are related to the protection of data collected by the city infrastructure.

2.2 SECURITY CONSIDERATIONS IN ZIGBEE NETWORKS

ZigBee is a standard for personal-area networks developed by the ZigBee Alliance, which includes companies such as Samsung, Philips Motorola and many others, with the goal of providing low-cost, low-power consumption, as well as reliable, two-way, wireless communication standard for short range applications.

1) On supporting forward security

2) On supporting backward security.

2.3 SMALL OBJECTS AS BUILDING BLOCKS

1) Awareness is a smart object's ability to understand (that is, sense, interpret, and react to) events and human activities occurring in the physical world.

2) Representation refers to a smart object's application and programming model — in particular, programming abstractions.

3) Interaction denotes the object's ability to converse with the user in terms of input, output, control, and feedback.

3. METHODOLOGY

3.1 SECURITY AND PRIVACY CHALLENGES OF USE-CASES

Due to heterogeneous nature, the IoT poses many security and privacy challenges. To overcome these challenges by formulating the security and privacy by providing the several use-cases .Some of the case-based security analysis, and formulate the security and privacy are:

1) Power Management,

2) Smart Car, and

3) Smart Healthcare System.

3.1.1 Power management

In any sector the technology must be successful, the power consumption tool plays key role in it. The IoT-based smart system is managing the power consumption is an essential part in any private and industrial sector. In this use-case temperature sensor, location device, movement sensor are used in various examples just to consume and manage the power used by users in IoT based.

3.1.2 Smart Car

Smart Car is outstanding technology came into this automated world which makes the citizens more comfortable while they journey in this cars. It can connect to city's infrastructure to get

live updates on traffic, signals from traffic lights, and it can adjust the speed when having less fuel.

According to “Safe Kids Worldwide”, “movement sensors” helps to identify if a child or animal was left in a locked car. A smarter car can contribute to a more secure world; It can prevent unauthorized users from driving/using the car, hence, it can protect against theft. Only authorized users who belong to a “white list” are allowed to drive a car.

3.1.3 Smart Health Care System

In a smart hospital, RFIDs can be used to identify patients, items, and doctors easily and rapidly, eg in a case when an anonymous person gets in an accident and it is critical to obtain the relevant medical records without any delay. It will allow the staff to keep track of the doctors’ location to allow for better response time during emergencies.

3.2 ATTACKS IMPACT

We provide an attack analysis and address the security and privacy concerns for each device using the above use-cases.

3.2.1 Actuators

Actuators in IoT context is equivalent to the write operations in Pc’s.

Security:

It can cause damage to the user in various domains. In the above use cases

Power management scenario, unauthorized triggering of the actuator can result severe in

the smart car scenario where a malfunction in the breaks’ actuator can result in loss of lives In the smart healthcare system, an actuator can be the trigger for injecting medication to a patient monitored at home, and any mistake or malfunction in this context can result in a wrong dosage of medication which can have fatal impact.

3.2.2 Sensors

Data collected by sensors transferred to other component devices to be analyzed and resulting in response.

Security:

The collected data can be a source of an attack, such as when data is fabricated due to a physical attack, resulting in an unexpected behavior of other entities in the system.

Privacy:

The data collected from these devices can reveal information about the user's habits, even though it might not reveal secrets about the user.

3.2.3 RFID tags

The RFIDs involve the use of a reader device to identify a tag. These devices became popular due to their low cost, while maintaining the ability to track and identify objects.

Security:

In this there is no proper adoption of security mechanisms due to less power in it and limitation in hardware.

Privacy:

The ability to track can pose a huge privacy concern.

3.2.4 Network, NFC, and the Internet

The communication protocols vary according to their function, thus vary in their security and privacy levels.

Security:

IoT devices will communicate with each other via wireless channels that will increase the system's vulnerability.

Privacy:

Posing critical point for information disclosure.

4. ANALYSIS

Many of you have probably heard of the new era as the "Internet of things". The "things" concept can be connected, monitored and managed via small efficient processors to provide beneficial data and interaction with the physical world.

The power of the Internet of Things is in its ability to combine information from various devices and systems in novel way to provide unprecedented insights and convenience. Synthesizing data from various sensors and systems is what makes Internet of Things a force for major changes in that it may help us solve some biggest problems facing society, from minimizing power outages to easing traffic congestion.

Since the Internet of Things is still in the emerging phase, ensuring security and privacy is an important issue that may be addressed and resolved now. As security practitioners we are at a critical place to make a difference in the evolution of Internet of things. We can be evangelists for security-aware technologies and products in several ways:

1) Implementer: If you are installing devices in your organization, incorporate the Internet of Things into your security policies and work with vendors to evaluate and improve their security features.

2) Developer: If your product fits this category, take the necessary steps to ensure security is being built in using techniques such as secure development methods, secure operating systems and hardware security.

3) Securer: If you work for a security company, start making strides in developing new approaches to Internet of Things threat monitoring and ways to detect and remediate attacks

4) Consumer: If you are an end consumer of devices, make sure you are purchasing devices with built-in security and let companies whose product lack security know why you haven't purchased their products. Most importantly, secure the devices you are purchasing. Change the default passwords and enable the security features. At a minimum, smart devices should include the ability for a strong password and encryption.

5. CONCLUSION

However, Internet of Things(IoT) have played major role in the present world-wide technology scenario. We discussed the privacy and security issues in IoT of some use-cases .we have described an application example for s-Health, i.e., a system to support citizens affected by respiratory conditions. We referred to the 5-Dimensional model and we have analyzed the emerging privacy issues of our proposed s-Health application. We discussed an attack analysis and address the security and privacy concerns for each device using the above use-cases. We also have brief discussion about properties of security and privacy of an IoT system

REFERENCES

[1] G.Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart objects as building blocks for the Internet of things," IEEE Internet Computing, vol. 14, no.1, pp. 44–51, Jan. 2010.

[2] Gianluca Dini, Marco Tiloca, "Considerations on Security in ZigBee Networks", Dipartimento di Ingegneria dell'Informazione University of Pisa. 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing.

[3] C. Patsakis, A. Papageorgiou, F. Falcone, and A. Solanas, "s-health as a driver towards better emergency response systems in urban environments," in Medical Measurements and Applications (MeMeA), 2015 IEEE International Symposium on. IEEE, 2015, pp. 214–218.