International Journal of Advanced Smart Convergence Vol.5 No3 27-31 (2016)
http://dx.doi.org/10.7236/IJASC.2016.5.3.27

IJASC 16-1-3

IoT Industry & Security Technology Trends

*Se-Hwan Park, **Jong-Kyu Park†

**Dept. of ReSEAT Program, KISTI, Seoul Korea*
***Dept of Scientometric Research, KISTI, Seoul Korea*
e-mail: world0017@reseat.re.kr, jkpark@kisti.re.kr

Abstract

High-tech industries in a state well enough to troubleshoot hacking information introduction a big barrier to delay the growth of the market related to IoT(Internet of Things) as is likely to be on the rise. This early on, security issues introduced in the solution, a comprehensive solution, including the institutional laws/precautions needed. Recent examples of frequent security threats while IoT is the biggest issue of introducing state-of-the-art industry information due to the vulnerable security hacking. This high-tech industries in order to bridge the information responsible for the target attribute, target range, and the protection of security and how to protect the subject, IoT environment (domestic industrial environment) considering the approach is needed. IoTs with health care and a wide variety of services, such as wearable devices emerge. This ensures that RFID/USN-based P2P/P2M/M2M connection is the implementation of the community. In this study, the issue on the high-tech industrial information and the vulnerable security issues of IoT are described.

Key words: IoT security issue, wearable devices, security risk, encryption, RFID/USN, internet governance

1. INTRODUCTION

Each of the companies(including public authorities) of Korea IoT technology introduced on the biggest issue is vulnerable to security issues. In order to address the scope and characteristics of the target, and security is responsible for the protection of the subject, including on security issues of equality, such as how to protect access strategy is needed. In addition, in order to build an effective network of IoT supply chain(creation, collection, distribution, management, leverage) to a vulnerable to security threats should be followed to build the infrastructure to protect against. IoTs(Internet of Things) with health care and a wide variety of services, such as wearable devices emerge. This ensures that RFID/USN-based P2P/P2M/M2M connection is the implementation of the community[1][2][3][4]. IoT sector status of the products and services are as follows[4][5][6][7]:

Manuscript Received: July 17, 2016 / Revised: July 28, 2016 / Accepted: August 05, 2016
Corresponding Author: world017@empal.com
Tel:+82-31-718-8009
ReSEAT Program, Korea Institute of Science and Technology Information(KISTI)
66, Hoegi-ro, Dongdaemun-gu, Seoul, Korea

- NIKE(US) have smart-phones and the movement of the user can manage the situation systematically terminals(NIKE+FuelBand).
- Fitbit(US) food intake can do tracking information terminals(Fitbit Flex).
- HapiLabs(Hongkong) takes time, and the user has to inform the frequency of ingestion intelligent dishwasher tool(HAPIfork).

2. Introducing Difficulty of IoT Technology

2-1. Domestic IoT Industry Environment

Each of the companies and public authorities in Korea and things got to the introduction of IoT technology, the hot issue is vulnerable due to privacy issues, security, life safety issues such as threats to this issue. Especially in recent years with regard to the introduction of security threats to the IoTs is being exposed to more frequent cases of disability are being a factor. This is in contrast to that, in order to bridge the current cyber environment and protected range, the target attribute, and how the security is responsible for the protection of the subject, considering the new security environment issues IoT can solve the following access strategy[8]:

- Safety threats and invasion of privacy in a state well enough to troubleshoot IoT is a big barrier to delay the introduction of the relevant market growth is likely to be. This solution of security issues since the early days, the introduction of IoT act in terms of the institutional framework in this study is a comprehensive solution, including the preemptive need to foster and protect.
- IoT introduction stage being the most efforts, security and privacy issue to solve the problem you need a strategy.
- In order to build an effective network of IoT “creation-collection-distribution-management-leverage” supply chain to a vulnerable to security threats should be followed to build the infrastructure to protect against.

2-2. Security Threats and Practices of IoT

(1) Security Threats

Digital devices connected to the Internet things, 70 percent of the information that is collected or sent unencrypted in the local network, and 60 percent of the IoT, the security appliance and the web interface vulnerable to. Software update does not use encryption, even 60 percent of users access rights, such as encryption, or seems to have a vulnerability. As a result, security-related IoT survey 2/3 of the respondents the following concerns about security, and that is in response to[9]:

- There is a vulnerability in the IoT is 17.2 percent almost seems to be concerned about the level of disaster.
- 48.8 percent of the population of about other existing applications and systems such as security issues are concerned.
- IoT security risks was a big device, smart phone 41.3%, tablet PC 10.7%, cars 9.4%, appliances/home automation system 8.8%, wearable devices 8.2%, medical equipments 7.2%.

(2) Security Practices

Distribution of personal information through the IoT network following invasion of privacy can also cause problems[3]:

- Private medical records being leaked by hackers on the outside can result in enhanced medical informatization strategy than is needed.
- Smart-grid networks to hack through communication and power can occur, which is completely down strains than is necessary for security-enhanced grid strategy.
- Traffic lights control of hacking and losing the control of traffic accidents or traffic is paralyzed can lead to situations where more than ITS(Intelligent Traffic System) security strategy is needed.

The devices connected to the IoT network are very easily can find hacking threats are being increased. Through IoT network security threats are invasion of privacy, attack of smart home control systems, network and control system hacking, medical/transportation/broadcast system hacking, cyber crime, etc.

3. IoT Security Technology Trends

3-1. Domestic and Global IoT Security Technology Development Trends

Currently, the initial market entry step in the security market yet IoT leader in the absence of domestic and foreign companies and has launched a competition for a market preemption. Table 1 shows IoT security technical development trends.

Table 1. IoT Security Technical Development Trends

		Technical Development Trends
Domestic	KTB SOLUTION	- Easy to carry as a small/low-power/light weight - IoT for wearable firewall development
	SECU-i	- IoT security hardware/software modular security gateway development - IoT security platform that is configured as a security sensor development
	ICTK	- PCP(Physical Copy Protection) method of electronic fingerprint security chip development
	SGA	- Secure OS based wearable and medical equipment security solution development
	PENTA SECURITY	- DB encryption solution extends the data encryption solution for IoT
	MARKANY	- IoT supported electronic signature technology development

Global	SYMANTEC	- IoT devices embedded OS monitoring technology development - Intrusion detection/blocking/access control features such as CSP development
	TREND MICRO	- Home gateway security solution development jointly with BROADCOM
	INFINEON TECHNOLOGY	- Confidential data authentication and encryption solution development such as smart home etc.

* source : Comprehensive Security Technology IoT Related Data /reconstruction.

3-2. Privacy Protection Measures of IoT Network

Security issue of IoT network is need to access in a new light for security target, scope, characteristics, security principals etc.. Especially for appliances connection IoT, networking, various environmental conditions, such as the properties of an object, because the more attention is needed per each access point. In addition, public and private networks, RFID-based sensor network, 3G/4G-LTE(A), as well as a variety of network, simple, low-cost small power/signal processing capabilities of the sensor, a commercial OS depending on the specific system and terminal security strategy is needed. In other words, in order to respond to security threats IoT sensors and devices, telecommunications and networks, platforms, separated by an application as a service, as follows: there is a need to establish their respective security system [10][11].

IoT devices is not easy to manage because CPU or memory, etc, depending on the price range of the performance of the software update and it is. Therefore, the difficulty to apply the existing security technologies security vulnerable. This can build a security system to solve strategy is needed. In terms of communication and network incompletely defined standard rooms and excessive SSL(Secure Sockets Layer) is vulnerable to security to rely on. This can build a security system to solve strategy is needed. Therefore, in order to protect the privacy of information sensing, processing, processing, storage and utilization from the step by step, it is necessary to provide the privacy protection. In addition, in response to security violations for the IoT system follows the front need to improve:

- A new security vulnerability or malware related to IoT occurred for quick detection and analysis, it is necessary to arrange for the system to respond.
- Related companies to share information than the competition between the cooperation through the configuration of the system is also very important.

4. CONCLUSION

In this study, the issue on the high-tech industrial information and the vulnerable security issues of IoT are described. IoT systems communicate information via RFID/USN-based arbitrary changes in the connected to implement at tipping point early on. IoT technology ICT infrastructure and are climate change

and disaster/disaster response, including many vulnerable security, energy savings, you will be able to solve global issues. In order to activate the IoT industry that system/platform/network is user authentication and access control, key management, such as management, reputation management, privacy, an identifier for a variety of security technologies to enhance the future of internet governance, there is a need to respond to. This ensures that RFID/USN-based P2P/P2M/M2M connection is the implementation of the community. In this study, the issue on the high-tech industrial information and the vulnerable security issues of IoT are described.

5. ACKNOWLEDGEMENT

This research was supported by the ReSEAT Program funded by the Korean Ministry of Science ICT & Future Planning through, the National Research Foundation of Korea and the Korea Lottery Commission grants.

REFERENCES

[1] Kyung-Sik Min, “Internet of Things”, NET Term, KISA, June 2012.
[2] "The Internet of Things Is Poised to Change Everything“, IDC, Oct. 2013.
[3] Se-Hwan Park, “IoT Core Technologies and Marketability Analysis”, Weekly Technology Trends, Vol.1630, NIPA, Jan. 29. 2014.
[4] “Core Trends of IoT Industries”, Global ICT R&D Strategy Trend, NIPA, June 2013.
[5] Mashable, "Nike Unveils FuelBand for Tracking All Physical Activity", 2012. 1.
[6] http://www.fitbit.com
[7] Se-Hwan Park, “IIoT Security System Construction Scheme”, 2015 IIoT Market Prospect Seminar_Keynote Speech Data, CCTV NEWS, May 28. 2015.
[8] "ARM Brings the Internet of Things To Life On Its Campus", Data Center Knowledge, 2013. 7.
[9] IoT Security-related Poll Results(SANS Institute Data).
[10] “IoT Status and Key Issues”, IITP, Dec. 2014.
[11] D. Gessner et al., “Trustworthy Infrastructure Services for a Secure and Privacy-respecting Internet of Things”, IEEE Conference on Trust, Security and Privacy, 2012.