Contemporary Engineering Sciences, Vol. 7, 2014, no. 31, 1715 - 1721
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2014.411230

A Study on the Development Method for Trust-Based Activation in Internet of Things

Kyong-jin Kim

Dept. of Computer Science
Graduate School, Sungshin Women's University
2 Bomun-ro 34da-gil, Seongbuk-gu
Seoul 136-742, Korea

Seng-phil Hong

School of Information Technology
Sungshin Women's University
2 Bomun-ro 34da-gil, Seongbuk-gu
Seoul 136-742, Korea

Abstract

The IoT is to connect a variety of things between the physical world and the digital one. Such environment has raised concerns about security challenges in the IoT, though. In our work, we consider it necessary to develop the standardization applying multiplicative security factors for possible threats.

Keywords: Internet of Things, IoT environment, Trust-based activation

1 Introduction

The aim of advanced concept about Machine-to-Machine (M2M) is to connect not only people and computer devices but also everyday objects in the real world by expanding services on the Internet [3, 6]. It can be defined as the Internet of Things (IoT) [1, 4]. In our work, we can define, M2M is a core technology for developing the IoT infrastructure, and IoT is to interconnect a large number of networked smart machines and to share necessary information by equipping things with computing and communication abilities.

Governments in leading countries are implementing various policies for prior occupation of the market and boosting technology competitiveness as the IoT activity is expecting to increase [5]. But this environment does not yet fully develop the innovation technologies, and international standardizations for the IoT are still insufficient. Therefore, the capabilities of the IoT leave much to be desired that as its services can be not useful more than expected. Such IoT-based platform involves various threats to traditional environments, and it has potential pitfalls by offering new services as well. Now the IoT paradigm is in its infancy; it is a time to develop an approach to IoT-related standardization that supports security capabilities such as interoperability, authorization, monitoring.

Our approach to reliability in this paper consists of three categories for connecting in all its aspects, and we are also focused on the method of security capabilities to be depended on the IoT environments.

2 Background and Key Challenges

2.1 Related Works

Many researchers [1, 5, 7] are studying how intelligent services for the IoT can be provided to the smart objects securely. There are a number of specific capabilities with regard to security related challenges in the IoT. As summarized in Table 1, we examined here the aforementioned researches if it meets all aspects that address this requirement according to [1].

Table 1. Examining security related requirements

	Requirements	CASAGRAS	iCore	CapBAC	GAMBAS
Trust	Lightweight PKI and key management		✓	✓	✓
	Quality of information to ensure confidence	✓	✓	✓	✓
	Decentralised and self-configuring systems				✓
	Access control to prevent intrusions	✓	✓	✓	✓
	Proposed novel methods for warranting objects			✓	
Security	Mechanisms to ensure important facilities	✓	✓	✓	✓
	General attack detection and recovery			✓	
	Context awareness techniques to be able to monitor	✓	✓	✓	✓
	Associated accounting structure for supporting devices	✓	✓		✓
	New approaches without intervening humans				✓
Privacy	Privacy assuring method using cryptography	✓	✓	✓	✓
	Support for privacy by design concepts	✓		✓	✓
	Fine-grain access control to emulate real world		✓	✓	✓
Non-func.	Enforcing security related laws/regulations	✓			
	Suggested principles that apply to private data	✓		✓	

Almost the whole research is reinforcing safety by multiple level of existing security features such as authentications, access control methods, etc. There are also mutually benefit from a trusted IoT that is establishing suitable provisions for security capabilities. But still there is much to be resolved.

2.2 Possible Security Threats in IoT

In the IoT, smart applications and services are increasingly exposed to significant security risks. In addition to this, there are still existing threats on traditional networks such as wireless and wired infrastructures, mobile communications, and so on. And the actual damages caused by possible threats to the IoT can range from loss and exposure of general information to life-threatening for humans in the automated system. The result from recent survey [1, 2, 4] has raised concerns about privacy and security to build the IoT as shown in Figure 1. That means these issues were seen as the key technical and architecture building IoT related blocks needed.

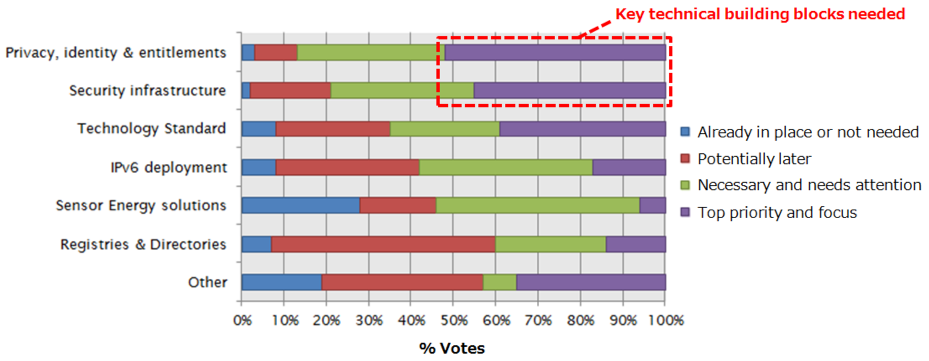

Figure 1. Concerns about security

It is concerned with issues of importance for the accessibility and use of sensitive information captured by IoT related things such as devices and sensors. As a result, some related studies are currently underway to ensure provide confidence. According to preceding studies by the IoT, the IoT era has raised concerns about security and privacy, and a primary security will be consolidated as researches of such approach.

3 Method for Trust-Based Activation

Even though several studies and developments have been performed over recent years, it is still insufficient to meet the needs of the IoT service. And the IoT related standardization that has not yet been released by industry is one of the reasons. There is a complication that may occur, compatibility. It is important to connect and communicate things that they are all connected to each other in the

Internet. Although there are a number of challenges in the IoT, we have focused on providing trusted service above all. This is depicted in Figure 2, which represents three categories for connecting by challenge aspects.

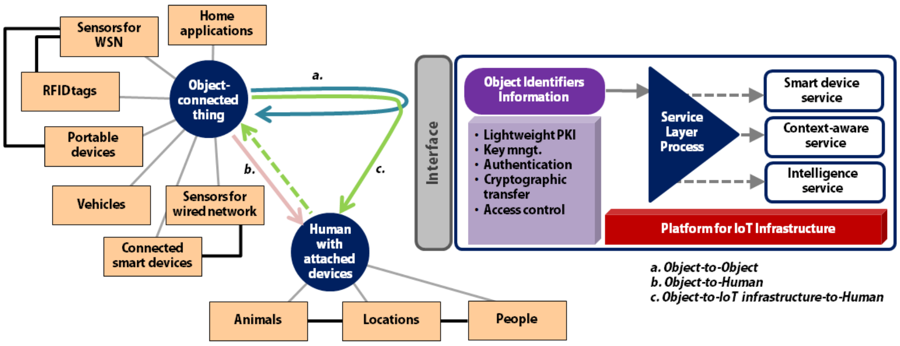

Figure 2. Development method for providing trust-based activation

a. Object-to-Object

Objects here can mean the physical components of the IoT that is capable of being identified and integrated into the communication networks, and it includes RFID, sensors, a variety of devices and platforms, and so on. These objects have computational and power restrictions, and it is not sufficient to provide consolidated security functionalities by the IoT networks. Above all, RFID seems to be the most vulnerable as it allows objects (such as a person, the goods for shipping) tracking to services offered. Sensors for data collection and actuators can be tampered with to provide incorrect data to the nodes against insider attack, to address which non-cryptographic means are needed, particularly in WSN. Then we will need the following requirements at this stage:

- It should identify and authenticate smart objects which include equipments required for network communications;

- Compatible cryptographic protocols (or chips) are a good way of ensuring data confidentiality to defend outsider attacks without relying on human control;

- Many IoT devices have got the resource constrained nature, and for that reason there should be have lightweight security solutions.

b. Object-to-Human

At the IoT space, the surrounding communication device such as sensors can monitor the individual life style from personal smart devices to balance people needs.

Namely, the foundation of IoT applications is sensitive data provided by users and their devices. It means anyone can access to personal data, especially in open networks, and it also may permit attackers who have gained unauthorized access to private/confidential information. To overcome these issues, it is necessary to establish standardization which achieves the following requirements:

- It should assort the authority to access depending on the purpose of services, including the way, the place and the time for activities;

- As much of the information in the IoT system may be personal data, there is a requirement to protect privately owned devices by e.g. based on anonymity and restrictive handling, preserving location privacy;

- New techniques (e.g. from introducing 4G and LTE) for supporting high speed and quality are required to ensure trust in objects and humans, particularly using mobile communications.

c. Object-to-IoT infrastructure-to-Human

The ultimate purpose of the IoT should provide intelligent services to the smart objects without intervening humans. And it can provide the virtual infrastructure for utility application using the IoT to support a large number of users. Security in the cloud on the other hand is important to this area to make it a bigger threat from attackers. They are able to access devices or data sources with unreliable connectivity in wired and wireless network environments. There is exposed to significant privacy and security risks, and it is still the major issue with existing threats on traditional network. There are a number of security implications arising from intelligence services where advances are required:

- For providing advanced intelligence services, objects have to get many of these information and data to support context-awareness. This would strengthen security capabilities (such as assurance methods for trusted platform) for controlling it;

- Sharing and using data should be impossible to trace back and to identify it again. For example, highly confidential data can be stored on locally managed network storage devices;

- With the advent of cloud computing and the continued growth of storages, preserving over time in the context of IoT can lead to many security issues as the data collected can be used for providing intelligent services. It is important to suggest alternatives capable of forgetting irrelevant details.

4 Conclusion

As mentioned above, the IoT environment involves various threats to existing environments, and it also has potential risks by offering new services. To solve these issues, we suggested that our approach is to develop the standardization applying multiplicative security factors. It is represents three categories for connecting, and we discussed about security and privacy issues. And then for providing reliability, we suggested trusted requirements to establish standardization/framework. In the future, the IoT systems that our standard approaches can be applied will reduce these problems and provide to better services in the IoT.

Acknowledgements. This work was supported by the Sungshin Women's University Research Grant of 2014.

References

[1] Ovidiu Vermesan and Peter Friess, Internet of Things - From Research and Innovation to Market Deployment, *River Publishers*, 2014.

[2] Israa Alqassem, Privacy and Security Requirements Framework for the Internet of Things (IoT), *Proceedings of ICSE Companion'14*, May 31 – June 7 (2014), 739 - 741. http://dx.doi.org/10.1145/2591062.2591201

[3] Daeyong Joo, Industrial Revolution Series: Ⅱ. A Study on the Significant Facotrs Affecting the Internet of Things (IoT) of Hyperconnectivity, *KIET Indeustrial Economic Report* (2014), 16 - 24.

[4] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic and Marimuthu Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, *Future Generation Computer Systems*, Elsevier, vol. 29 no. 7 (2013), 1645 – 1660. http://dx.doi.org/10.1016/j.future.2013.01.010

[5] Ovidiu Vermesan and Peter Friess, Internet of Things - Converging Technologies for Smart Environments and Integrated Ecosystems, *River Publishers*, 2013.

[6] Asma Elmangoush, Adel Al-hezmi and Thomas Magedanz, Towards Standard M2M APIs for Cloud-based Telco Service Platforms, *Proceedings of MoMM*, 2 - 4 December (2013), http://dl.acm.org/citation.cfm?id=2536892.

[7] CASAGRAS, Final Report: RFID and the Inclusive Model for the Internet of Things, *CASAGRAS an EU Framework 7 Project*. http://www.grifs-project.eu/, 2009.

[8] Rajneesh Kumar, Shekhar Verma and Geetam Singh Tomar, Thwarting Address Resolution Protocol Poisoning using Man In The Middle Attack in WLAN, *International Journal of Reliable Information and Assurance*, vol.1 no.1 (2013), 8 - 19.

Received: October 1, 2014; Published: December 2, 2014