사물인터넷 통신의 시장성 및 기술 동향 분석

장창환, 조성호, 김정태
목원대학교

Analyses of Technology Trend and marketability in Internet of Things

Chang-Whan Jang, Sung-Ho Jo, Jung Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

Abstract

The idea of Internet of Things (IoT) and the challenges is developed and growing rapidly. The general layered architecture of IoT along with its constituent elements is analyzed and described. Further, the paper provides for a secure construction of the IoT architecture, by tackling security issues at each layer of the architecture. We survey an introduction to industrial IoT systems, the related security and privacy challenges, and an outlook on possible solutions towards security framework for Industrial IoT systems.

Keyword

Security, IoT, Gateway, Privacy, WSN

Ⅰ. Introduction

In the last decade, network technology has dramatically been developed. Recently, more and more network technologies have been applied to control systems[1]. This kind of control systems in which a control loop is closed via communication channel is called networked control systems. Now, networked control is a new area in control systems. Particularly, Internet based control systems allow remote monitoring and adjustment of plants over the Internet, which makes the control systems benefit from the ways of retrieving data and reacting to plant fluctuations from anywhere around the world at any time. The concept of cloud control systems is discussed in this paper, which is an extension of networked control systems (NCSs). With the development of Internet of Things (IOT), the technology of NCSs has played a key role in IOT. At the same, cloud computing is developed rapidly, which provides a perfect platform for huge mass data processing, controller design and performance assessment. Cloud control will give new contribution to the control theory and applications in the near future. Despite the wide use of WSNs in the IoT architectures, there are a few limitations that should be taken into consideration. First of all, SOs are still severe-resource constrained devices, despite the technological advancements in this domain. Many IoT applications are supported by battery-operated SO(Smart Objects)s; hence, there is always the risk of operation disruption when one or more SOs fail to properly function due to energy shortage [1]. The IoT paradigm has increasingly received attention from both academia and industry as a key enabler for the emergence of new applications and systems with a significant influence in the daily lives of human beings. Recently, we have witnessed the convergence of this paradigm with Cloud Computing largely

motivated by the need of IoT infrastructures and applications to be enhanced in terms of computational resources, scalability, and performance [2]. Survey on IoT security and privacy, a great deal of research is needed in order to make the IoT paradigm become reality.

Ⅱ. IoT Architecture

In 2005, the International Telecommunications Union(ITU) proposed that "Internet of Things" will connect the real world objects in both a sensory and intelligent manner. The IoT can find its applications in almost every aspect of our daily life. Below are some of the examples [3].

1) Prediction of natural disasters:
2) Industry applications:
3) Water Scarcity monitoring:
4) Design of smart homes:
5) Medical applications:
6) Agriculture application:
7) Intelligent transport system design:
8) Design of smart cities:
9) Smart metering and monitoring:
10) Smart Security:

Ⅲ. Security and Privacy

The Internet of Things is a multi-domain environment with a large number of devices and services connected together to exchange information. Each domain can apply its own security, privacy, and trust requirements. In order to establish more secure and readily available IoT devices and services at low cost, there are many security and privacy challenges to overcome [4].

1) User privacy and data protection:
2) Authentication and identity management:
3) Trust management and policy integration:
4) Authorization and access control:
5) End-to-End security:
6) Attack resistant security solution:

The IoT can change the shape of the Internet and can offer enormous economic bene fits but it also faces many key challenges. Some of them are briefly described below [5].

1) Naming and identity management:
2) Interoperability and Standardization:
3) Information privacy:
4) Objects safety and security:
5) Data confidentiality and encryption:
6) Network security:
7) Spectrum:
8) Greening of IoT:

Ⅳ. Conclusion

The IoT in the future will realize the interconnection between individuals and the expansion between things at any time and in any place, by which a lot of exposed information in public places will be transmitted to the network layer and application layer. Along with the rapid development of the IoT industry, the importance of the security in the IoT is gradually emerging and IoT is one of the most promising network technologies in the new network. We analyzed security and privacy in IoT system.

Acknowledgments. This research was supported by Basic Science Research Program through the National Re-search Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (grant number: 2015R1D1A09061435)

Reference

[1] Md. Mahmud Hossain, Maziar Fotouhi, and Ragib Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", 2015 IEEE World Congress on Services, 2015, pp.21-28.

[2] Everton Cavalcante, etat, "On the interplay of Internet of Things and Cloud Computing: A systematic mapping study", Computer Communications, 89-90, 2016, pp.17-33

[3] Rafiullah Khan, etat, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges", 2012 10th International Conference on Frontiers of Information Technology, pp.257-260

[4] Quandeng GOU, etal, "Construction and Strategies in IoT Security System", 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, pp.1129-1132.

[5] Chibiao Liu and Jinming Qui, “Study on a Secure Wireless Data Communication in Internet of Things Applications”, International Journal of Computer Science and Network Security, Vol.15, No.2, 2015, pp.18-23