사물 인터넷망에 기반한 산업 시설의 보안 요구 사항 해석

김정태
목원대학교

Analyses of Security and Privacy Challenges in Industrial Based on Internet of Things

Jung Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

Abstract

Today, embedded, mobile, and cyber-physical systems are ubiquitous and used in many applications, from industrial control systems, modern vehicles, to critical infrastructure. Current trends and initiatives, such as “Industry 4.0” and Internet of Things (IoT), promise innovative business models and novel user experiences through strong connectivity and effective use of next generation of embedded devices. We survey an introduction to Industrial IoT systems, the related security and privacy challenges, and an outlook on possible solutions towards a holistic security framework for Industrial IoT systems in this paper.

Keyword

Security, IoT, Gateway, Privacy, WSN

Ⅰ. Introduction

The technologies of the Internet of Things can effectively facilitate the integration of material production and service management, the integration of the physical world and the digital world. With development of IoT technologies, the most important IoT application includes infrastructure construction, public security, environment protection, modern agriculture, intelligent industry, urban management, business service and other fields. To understand the importance of exploring security and privacy issues in the domain of IoT, we first take a look at the existing state of the IoT device deployments in the world. A 2014 study by Hewlett-Packard on commercialized IoT deployments found that 80% of such devices violate privacy of personal information. There are several cases where researchers showed the successful take-over of smart things [1].

Ⅱ. IoT Architecture

The field of Internet of Things (IoT) is apprehensive with such complications which involves interfacing and integrating of smart electronic devices and other such hardware devices with their adjacent surroundings. Muhammad Usman and Nazar Abbas analyzed application of IoT for securing industrial threats. In proposed system, different types of nine sensors are connected to increase the security level at its best. The results are very helpful in the desire to achieve an efficient and reliable solution contributing in the field of IoT, considering different various aspects which include fast processing, system cost, robustness and precision for the modern, technological and corporate need [2].

Ⅲ. Security and Privacy

Special security threats of IoT in terms of the architecture of IoT, in addition to traditional threats of TCP/IP networks, wireless networks and mobile communications networks and other traditional network, IoT still have its own special security issues, and most of these peculiarities stem from sensing layer Include the following several aspects [3]:

- Privacy security
- Security of Intelligent nodes
- Attack in the way of Faking
- Denial of Service

Adjustment for IoT is tuned mainly According to the architecture and specificity of its application. Things perception layer, layer-aware network interface with the main part of the following security defense technologies rely primarily on traditional knowledge of information security [4].

- Encryption mechanism
- Identification mechanism of node
- Access control technology
- Trend analysis and others

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. Among those challenges are [5]:

- User privacy and data protection:
- Authentication and identity management:
- Trust management and policy integration:
- Authorization and access control:
- End-to-End security:
- Attack resistant security solution:

Several IoT centric critical security issues might be unnoticed or poorly addressed by the security researchers, as this paradigm is not full-fledged yet. Therefore, we organize this section with some of the prominent security issues [1, 6].

- Trust management:
- Governance:
- End-to-end security:
- Fault tolerance:
- Identity management:
- Energy efficient security:
- Key management:
- Data transparency:
- Group membership:
- Security of handling IoT big data:
- IoT forensics:

Ⅳ. Conclusion

The advances in the smart objects systems and Internet of Things approach are remarkable developed. To realize this application in industrial field, we surveyed the research status in this field from encryption mechanism, communication security, protecting sensor data, and encryption algorithm.

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: 2015-071892)

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] Muhammad Usman and Nazar Abbas, "On the Application of IOT (Internet of Things) for Securing Industrial Threats", 12th International Conference on Frontiers of Information Technology, 2014, pp.37-40.

[3] Chenghua Yan, Kun Feng and Zhiming Zhang, "Impact of Internet of things on security grade evaluation", 2012 International Conference on Computer Science and Electronics Engineering, pp.289-292.

[4] Romano Fantacci, Tommaso Pecorella, Roberto Viti and Camillo Carlini, "Short Paper: Overcoming IoT Fragmentation

Through Standard Gateway Architecture", 2014 IEEE World Forum on Internet of Things (WF-IoT), pp.181-182

[5] Hui Suo, Jiafu Wan Caifeng Zou and Jianqi Liu, "Security in the Internet of Things: A Review", 2012 International Conference on Computer Science and Electronics Engineering, pp.648-651

[6] 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