

# Research on the Architecture of Trusted Security System Based on the Internet of Things

Xiong Li, Zhou Xuan, Liu Wen

School of Management, Shanghai University, Shanghai, 200444, China  
xiongli8@shu.edu.cn; shining\_xuan@126.com; liuwen3099@163.com

**Abstract**—With the advent of Internet of Things (IoT), information security issues will be a major bottleneck of the future development of IoT. How to resolve the information security problems of IoT effectively has become an important research issue. Firstly, various potential information security issues and preventive measures in the application of IoT are summarized. Then, the general architecture of trusted security system based on IoT is first proposed based on the former researches about trusted computing, trusted network, etc. Finally, according to the general architecture of trusted security system based on IoT, a study of concrete realization of trusted security system based on IoT is made, which mainly includes trusted user module, trusted perception module, trusted terminal module, trusted network module and trusted agent module.

**Keywords**—trusted security system; IoT; trusted network; trusted computing

## I. INTRODUCTION

With the rapid development of information technology and Internet, IoT is likely to be the third wave of the information industry after computer and Internet. National Guideline on Medium- and Long-Term Program for Science and Technology Development in China (2006-2020) has explicitly included IoT in the key research areas. However, due to the full openness of its architecture, the information security of IoT has met unprecedented challenges, and a variety of new and potential problems about information security appear constantly. Therefore, to build a security and reliable system in the context of IoT becomes the focus of attention.

Traditional information security solutions, including virus checking and killing, security scanning, patch upgrades, intrusion detection and other security techniques, which are mostly proposed for only a part or a stage of the application of IoT, can hardly cope with the rapid growing of security threats and attacks, not to mention solving the security problems of IoT fundamentally. Therefore, a general architecture of trusted security system based on IoT is first proposed to deal with information security problems appearing in the application of IoT. Then, the core modules of the trusted security system of IoT, which include trusted user module, trusted perception module, trusted terminal module, trusted network module and trusted agent module, are designed to eliminate the various security threats in the application of IoT.

## II. LITERATURE REVIEW

With the growing use of IoT technology, its security problems have drawn close attention of domestic and foreign scholars. Feng Dengguo (2007) and Wu Chuankun (2010) summarized the security problems of IoT respectively from the perception layer and network layer, including sensor attacks, sensor abnormalities, radio interference, network content security, hacker intrusion and illegal authorization [1-2]. In addition, IoT also faces many security issues in the application layer, including database access control, privacy protection technology, information leakage tracking technology, secure computer data destruction technology, and protection technology of secure electronic products and intellectual property of software [3].

Facing these information security issues that may arise during the application of IoT, Juels, A (2006) proposed RFID tag encryption technology to prevent unauthorized pryer from getting and tampering electronic label information [4]. Ma Yujian (2009) proposed a construction method by using the PKI trust model and trust path to reinforce interactive security of IoT enterprises [5]. Wonnemann, C. Strucker, J (2008) put forward two password management solutions to resolve the security management problems of IoT reader [6]. Christoph P. Mayer (2009) proposed to guarantee information security and privacy in three aspects: accountability of information, encryption of tag identifier and key extraction of wireless channel characteristics [7]. Benjamin Fabian and Oliver Günther (2009) proposed the solutions of IoT security from VPN, TLS, DNSSEC, Anonymous Mixes, Private Information Retrieval, Peer-to-Peer Systems and other aspects [8].

However, these information security solutions are only for a certain aspect of the application of IoT, and can not resolve the secure problems of the whole IoT process fundamentally. Therefore, the trusted security system in the context of IoT is built to forwardly prevent various security threats during the application process of IoT, so as to make various security risks to the minimum.

## III. THE GENERAL ARCHITECTURE OF TRUSTED SECURITY SYSTEM BASED ON IOT

Trusted security system can be derived from the concepts of trust and trusted computing base, which includes structured TCB, trusted guarantee mechanism, trusted process control mechanism and other aspects [9]. Along with the development of network technology, Wei Wei designed a trusted platform [10]; Li Hongpei put forward the concept of