Computers and Electrical Engineering 72 (2018) 266–273

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Towards decentralized IoT security enhancement: A blockchain approach☆

Yongfeng Qian[a], Yingying Jiang[b], Jing Chen[c], Yu Zhang[b], Jeungeun Song[d], Ming Zhou[e,g,*], Matevž Pustišek[f]

[a] School of Computer Science, China University of Geosciences, Wuhan, China
[b] School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China
[c] School of Cyber Science and Engineering, Shenzhen Institute of Wuhan University, Wuhan University, Wuhan 430072, China
[d] Department of Electrical and Computer Engineering, The University of British Columbia, Canada
[e] Insititue of New Energy, Wuhan, China
[f] Laboratory for Telecommunications, Faculty of Electrical Engineering, University of Ljubljana, Slovenia
[g] School of Energy and Power Engineering, Huazhong University of Science and Technology, Wuhan 430074, China

ARTICLE INFO

Article history:
Received 8 January 2018
Revised 31 August 2018
Accepted 31 August 2018

Keywords:
IoT
Blockchain
Security management

ABSTRACT

With the rapid development of internet of things (IoT), it has brought great convenience to users in different fields, such as smart home, smart transportation and so on. However, it also carries potential security risks. In order to solve this challenge, in this paper, we first introduce three layers of IoT, i.e., perception layer, network layer and application layer, then corresponding security problems of three layers are introduced. Second, we propose a high-level security management scheme based on blockchain for different IoT devices in the full life cycle. Finally, we give open research problems and future work.

1. Introduction

In recent years, with constant upgrade of terminal devices and development of new network technologies [1], internet of things (IoT) has become popular [2]. It is estimated that the scale of IoT will reach 50 billion devices in 2020. The interconnections of massive terminal devices bring great convenience to people, such as smart transportation, smart home [3] and battlefield environments [4], etc. However, there are potential risks that are also brought by IoT. For instance, moving vehicles that are connected via advanced cooperative communication are expected to form an open internet of vehicles (IoV) [5], which is a representative IoT system. Without proper protection of security measures, the deployment of IoT will not be realized [6].

Due to the profound influence, we should pay more attention to the security problems of IoT [7]. At present, the research on IoT security is heating up [8]. Kim et al. [9] introduced the security protocol problem in the IoT, described the encrypted DoS attack strategy, and implemented it in multiple IoT protocols. However, with the help of encryption, it is likely not suitable for mobile devices which do not have enough storage and computing resources. Thus, the lightweight security measures are required. Usman et al. [10] designed a lightweight encryption method, which called SIT. When used in another scenario, however, there will be different security problems. Mejri et al. [11] summarized the security problems appeared

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. M. M. Hassan.

* Corresponding author.
E-mail address: mingzhou.hust@gmail.com (M. Zhou).

https://doi.org/10.1016/j.compeleceng.2018.08.021
0045-7906/

Table 1
Existing work.

Exsisting Work	Asset Tracking	Specific Application	Communication Platform Security	(Lightweight) Blockchain-based architecture for IoT	Managing IoT devices
[16]	*	–	–	–	–
[17]	–	*	*	–	–
[15]	–	–	–	*	–
[18]	–	*	–	–	–
[19]	–	–	–	*	–
[21]	–	*	–	–	–
[22]	–	–	–	*	–
[23]	–	–	–	–	*
[24]	–	–	–	–	*

in the Internet of vehicles, and gave the possible encryption solutions. Zhang et al. [12] described the security problems in smart city, and introduced the possible solution. The security and privacy problems of wireless mobile networks were summarized in [13].

According to the above discussion, much work has been made for the research on IoT security. However, the research on IoT security is still in the early stages, and research on asset management for IoT terminal devices in full life cycle has not fully been taken into consideration. In the meantime, as an emerging technology, blockchain technology gradually arouses attention of academia and industry. Blockchain technology is based on a decentralized peer-to-peer network, combines encryption technology, time-series data, and consensus mechanisms, and thus realizes the traceability and verification of data. In the meantime, privacy protection and sharing are realized [14]. Currently, many researchers have begun to study blockchain technology applied for IoT. However, most of the research is based on establishment of protocol, blockchain has not been applied specifically to the full life cycle of IoT. The work in [15] described a lightweight blockchain-based IoT architecture. There are some more work in allusion to application of blockchain in IoT. For example, according to the work of Christidis et al. [16] and Biswas et al. [17], the applications of blockchain in IoT were put forth, however, only one application, i.e., automatic contract execution, was considered in application scene. How to solve safe asset management and traceability has not been taken into consideration yet. The blockchain based lightweight safety and privacy protection problem was put forth in allusion to a smart home in [18]. Similarly, only one specific case (i.e., smart home) is taken into consideration. Other IoT scenarios (significantly different from smart home, such as smart power grids) are not covered. Dorri et al. [19] put forth the optimized blockchain to relieve complicated computation and bandwidth overhead brought by traditional blockchain, and requirements on privacy protection and security were guaranteed. However, there has been no consideration of security problems of IoT terminals in the life cycle [20]. In [21], the realization mode of E-business was introduced based on blockchain and P2P trade, however, security problems applied to this type of IoT E-business have not been taken into consideration. In [22], IoT services driven by blockchain were given along with four typical frameworks. However, IoT database storage and IoT terminal management have not been taken into consideration. In [23], the IoT system was built on blockchain, and the blockchain is adopted to control and configure IoT devices. However, the blockchain ledger problem of IoT devices has not been taken into consideration. In [24], blockchain technology was adopted to realize ownership authentication for IoT devices under cloud computing, however, traceability management on data of IoT devices has not been taken into consideration. In [25], the authors utilized blockchain to realize supply chain.

From the Table 1, we can see that blockchain has been applied to the IoT in the last two years. Most of these exciting works focus on how to make use of blockchain to manage assets, ensure the security of communication platform, build lightweight architecture for IoT and managing IoT devices or specific applications (e.g., intelligent services, smart city and intelligent medica). These works use the advantage of blockchain centralization to design a fair and credible management platform or key distribution platform without third party. It break through the limitations of the third party centered, and achieve the high efficiency of processing. However, these works do not consider the threat traceability of IoT terminal life cycle. Furthermore, the life cycle of IoT terminal devices (e.g., different sensors or mobile devices) is different. Thus, in the life cycle of these terminals, how to achieve effective threat traceability can help to avoid unnecessary leakage of security and privacy issues in the actual deployment of devices for IoT. However, due to the different terminal life cycle, centralization is usually used to trace the source, which leads to the waste of resources. Therefore, how to use blockchain to deal with it is a challenge problem.

We first introduce the services acquisition of IoT device. The IoT device include vehicles, cameras, mobile phones, bracelets and other devices. These IoT devices can be accessed to the network through cellular network or WiFi, and obtain services at remote cloud [26,27]. In fact, service providers can use fog computing or edge computing to provide users with low latency services in order to ensure the quality of experience (QoE) of users [28]. For example, in the internet of vehicles, roadside units (RSUs) can be regarded as a fog node to provide services for vehicle users [29]. Though the IoT provides convenient services for users, it will also bring security problems.

Utilizing blockchain to enhance the security of IoT is shown in Fig. 1. From the Fig. 1, we can see that the blockchain is applied to the threat traceability of the IoT devices, which involves the interaction between IoT devices and network transmission, as well as between IoT devices and cloud. For the IoT devices and network transmission, the problems include