Accepted Manuscript

Research on security of information sharing in Internet of Things based on key algorithm

Pengcheng Wei, Zhen Zhou

PII: S0167-739X(18)30305-4
DOI: https://doi.org/10.1016/j.future.2018.04.035
Reference: FUTURE 4113

To appear in: *Future Generation Computer Systems*

Received date : 11 February 2018
Revised date : 22 March 2018
Accepted date : 10 April 2018

Please cite this article as: P. Wei, Z. Zhou, Research on security of information sharing in Internet of Things based on key algorithm, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.04.035

Research on Security of Information Sharing in Internet of Things Based on Key Algorithm

Pengcheng Wei[1*], Zhen Zhou[2]

1. *Chongqing University of Education, Chongqing University of Posts and Telecommunications, Chongqing, China*
2. *Chongqing University of Posts and Telecommunications, Chongqing, China*

Corresponding Author's Email: CooperyMlw@yahoo.com, +8618680853003

Abstract: With the popularization of mobile devices and the development of wireless networks, the use of mobile devices to access services is becoming more and more popular. It is becoming more and more popular for users to access servers by using mobile terminals to obtain services. At the same time, the server to obtain the user's privacy information will also become more and more, and this privacy information is obtained without the user's knowledge of the situation. Therefore, how to not only protect the confidentiality of sensitive data of users but also provide safe, reliable and convenient services is a hot issue for research.In this paper, the user privacy and security issues and solutions on the Internet are discussed. The issue generated by accessing the server to obtain the required information based on the mobile device has got in-depth study. The main work is as follows: Firstly, the common methods of privacy protection is introduced, and the methods of attribute-based encryption and homomorphic encryption are analyzed in detail. According to the existing homomorphic encryption scheme and base station knowledge applied to the mobile network model, a privacy protection scheme based on homomorphic encryption is proposed. Finally, this paper analyzes and summarizes the important problems that still exist in the interaction between mobile and access server, and points out the research direction in the next step.

Key words: Internet of Things; user privacy; encryption algorithm

1. INTRODUCTION

With the development of computer network technology, mobile users are getting more and more convenient to access network services, which makes users request services from servers more and more frequently. Therefore, the privacy protection when requesting services becomes an immediate concern of both industry and academia topic (Weber R. H. 2015) [1]. In the mobile environment, mobile devices request services from the server through the wireless network. The server provides data and resources to mobile devices according to user requirements (Sicari S et al. 2015) [2]. The server connects the available resources including storage resources and software resources to form a large-scale data center. Users only need to give the corresponding service remuneration to enjoy the service. Service data providers manage their services in a unified manner, reflecting the idea of modern services "everything as a service" (Borgohain T et al. 2015) [3]. There are mainly three architectures for the interaction between mobile devices and servers: standalone architecture, central server architecture and distributed peer-to-peer architecture (Weinberg B D et al. 2015) [4]. The independent structure means that the mobile user interacts with the server directly so that the user can obtain the corresponding information. The central server structure adds a middleware based on the independent structure, and the middleware is responsible for collecting the user's request service information responding to user's request which is credible. Distributed peer-to-peer system architecture is a two-terminal structure between mobile users and servers. Mobile users need to trust each other to collaborate, and requests services to the server at the same time. In this way, the information requested by the user request is obtained (Porambage P et al. 2016) [5]. Independent structure is structure only have client or mobile users and servers (Caron X et al. 2016) [6]. The system architecture assumes that the mobile user is a device capable of computing and storage (Mylrea M.2017) [7]. Mobile users use the service-based user privacy protection research algorithms in their secure mobile networks to achieve the necessary privacy protection according to their privacy needs (Pasquier T et al. 2017) [8].

2. STATEOFTHEART

With the rapid development of computer technology and its widespread application, people's lives are becoming more and more inseparable from computer products. However, not all networks are trustworthy, so people's information security has become a hot topic in all walks of life (Yang Y et al. 2017). While obtaining the service, it is guaranteed that the sensitive data of mobile users can be effectively protected, and the users except the requester can not obtain the service information acquired by the requester, that is, the third party can be accessed and controlled. Attribute-based encryption is an important means of encryption for data access control (Arias O et al. 2017) [10].

Scholars have proposed many attribute-based encryption (ABE) schemes so far. As a kind of public-key cryptography, attribute-based encryption firstly ensures the confidentiality of data. Secondly, the property encryption scheme can be used for user's access control, identification and withdrawal of user information.