Accepted Manuscript

Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things

Qi Han, Yinghui Zhang, Hui Li

PII: S0167-739X(17)31868-X
DOI: https://doi.org/10.1016/j.future.2018.01.019
Reference: FUTURE 3926

To appear in: *Future Generation Computer Systems*

Received date : 19 August 2017
Revised date : 7 December 2017
Accepted date : 7 January 2018

Please cite this article as: Q. Han, Y. Zhang, H. Li, Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.01.019

Efficient and Robust Attribute-based Encryption Supporting Access Policy Hiding in Internet of Things

Qi Han[a,*], Yinghui Zhang[b,c], Hui Li[a]

[a] *State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China*
[b] *National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China*
[c] *Westone Cryptologic Research Center, Beijing 100070, P.R. China*

Abstract

The term of Internet of things (IoT) remarkably increases the ubiquity of the Internet by integrating smart object-based infrastructures. How to achieve efficient fine-grained data access control while preserving data privacy is a challenge task in the scenario of IoT. Despite ciphertext-policy attribute-based encryption (CP-ABE) can provide fine-grained data access control by allowing the specific users whose attributes match the access policy to decrypt ciphertexts. However, existing CP-ABE schemes will leak users' attribute values to the attribute authority (AA) in the phase of key generation, which poses a significant threat to users' privacy. To address this issue, we propose a new CP-ABE scheme which can successfully protect the user's attribute values against the AA based on 1-out-of-n Oblivious Transfer technique. In addition, we use *Attribute Bloom Filter* to protect the attribute type of the access policy in the ciphertext. Finally, security and efficiency evaluations show that the proposed scheme can achieve the desired security goals, while keeping comparable computation overhead.

Keywords: IoT, Privacy, CP-ABE, Oblivious Transfer, Bloom Filter

1. Introduction

Internet of Things (IoT) is a term coined by Ashton [1] who conceived a system of ubiquitous sensors connecting the physical world to the Internet. The three core components of IoT are things (or named as smart devices), Internet, and connectivity, however, the real value that IoT creates is at the intersection of gathering data and leveraging it.

For smart devices are usually resource-constricted, one of the most important challenges for IoT is the unprecedented amount of data, which exceeds the

*Corresponding author
Email addresses: hanqiwildginger@gmail.com (Qi Han), yhzhaang@163.com (Yinghui Zhang), lihui@mail.xidian.edu.cn (Hui Li)