Accepted Manuscript

Compulsory traceable ciphertext-policy attribute-based encryption against privilege abuse in fog computing

Huidong Qiao, Jiangchun Ren, Zhiying Wang, Haihe Ba, Huaizhe Zhou

PII: S0167-739X(17)32882-0
DOI: https://doi.org/10.1016/j.future.2018.05.032
Reference: FUTURE 4207

To appear in: *Future Generation Computer Systems*

Received date : 15 December 2017
Revised date : 13 April 2018
Accepted date : 15 May 2018

Please cite this article as: H. Qiao, J. Ren, Z. Wang, H. Ba, H. Zhou, Compulsory traceable ciphertext-policy attribute-based encryption against privilege abuse in fog computing, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.05.032

Compulsory traceable ciphertext-policy attribute-based encryption against privilege abuse in fog computing

Huidong Qiao[a,b,*], Jiangchun Ren[a], Zhiying Wang[a], Haihe Ba[a], Huaizhe Zhou[a]

[a] College of Computer, National University of Defense Technology, Changsha 410073, China

[b] College of Computer and Communication, Hunan Institute of Engineering, Xiangtan 411100, China

Abstract. Due to the structure of fog systems, ciphertext-policy attribute-based encryption (CP-ABE) is regarded as a promising technique to address certain security problems present in the fog. Unfortunately, in most traditional CP-ABE systems, a user can deliberately leak his attribute keys to others or use his private key to build a decryption device and provide a decryption service with little risk of being caught (untraceable). We refer to this behavior as privilege abuse. The privilege abuse problem will seriously hinder the adoption of CP-ABE. To address the problem, we propose a novel black-box traceable CP-ABE scheme that is much simpler than the existing white-box traceable schemes. A malicious user who builds a decryption black-box can be tracked and exposed by our scheme. Due to its scalability and relatively high efficiency, the scheme could be practical for fog systems. Furthermore, we point out that, if the adversary can distinguish the tracing ciphertext from the normal ciphertext, he can frustrate tracking by outputting incorrect decryption results. Thus, the traceability must be *compulsory*, so as to ensure that the adversary cannot distinguish between the tracing ciphertext and the normal ciphertext. Therefore, we present a formal definition of compulsory traceability with a new security game, and our scheme is proved to be secure and compulsory traceable under the generic group model.

Keywords: ciphertext-policy attribute-based encryption; fog computing; black-box traceability; compulsory traceability

1. Introduction

Fog computing extends the cloud computing paradigm to the edge of the network, thus enabling a new breed of applications and services [1]. The concept of fog computing was proposed by Cisco, and it is thought to be a promising computing paradigm. Fog devices are heterogeneous devices such as access points, routers, set-top box, roadside units, base stations and so on. These fog nodes are usually deployed as a layered structure between cloud computing and end users. While the central cloud