ARTICLE IN PRESS

Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Towards leakage-resilient fine-grained access control in fog computing

Zuoxia Yu [a], Man Ho Au [a,*], Qiuliang Xu [b], Rupeng Yang [b], Jinguang Han [c,d]

[a] Department of Computing, Hong Kong Polytechnic University, Hong Kong

[b] School of Computer Science and Technology, Shandong University, Jinan 250101, China

[c] Jiangsu Provincial Key Laboratory of E-Business, Nanjing University of Finance and Economics, Nanjing, 210003, China

[d] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

HIGHLIGHTS

- Provide access control in fog computing secure against side-channel attacks.
- Develop a generic framework of leakage-resilient functional encryptions, a basic tool.
- Present many new fully secure leakage-resilient functional encryptions.

ARTICLE INFO

Article history:
Received 15 June 2016
Received in revised form
19 December 2016
Accepted 21 January 2017
Available online xxxx

Keywords:
Fog computing
Functional encryption
Leakage Resilient Cryptography
Dual system methodology
Pair encoding

ABSTRACT

Fog Computing, a technology that takes advantage of both the paradigms of Cloud Computing and the Internet of Things, has a great advantage in reducing the communication cost. Since its introduction, fog computing has found a lot of applications, including, for instance, connected vehicles, wireless sensors, smart cities and etc. One prominent problem in fog computing is how fine-grained access control can be imposed. Functional encryption, a new cryptographic primitive, is known to support fine-grained access control. However, when it comes to some new threats in the fog computing scenario, such as side channel attacks, functional encryption cannot maintain its security. Therefore, we need new cryptographic primitives that not only provide a way to securely share data with a fine-grained access control but also are able to resist those new threats.

In this paper, we consider how to construct functional encryption schemes (FEs) adaptively secure in continual memory leakage model (CML), which is one of the strongest models that allows continuous leakage on both user and master secret keys. Besides providing privacy and fine-grained access control in fog computing, our scheme can also guarantee security against side channel attacks. More concretely, we propose a generic framework for constructing fully secure leakage-resilient FEs (LR-FEs) in the CML model results from leakage-resilient pair encoding, which is an extension of pair encoding presented in the recent work of Attrapadung. In this way, our framework simplifies the design and analysis of LR-FEs into the design and analysis of predicate encodings. Moreover, we discover new adaptively secure LR-FEs, including FE for regular languages, attribute-based encryption (ABE) for large universe and ABE with short ciphertext. Above all, leakage-resilient adaptively secure functional encryption schemes can equip fog computing with higher security and fine-grained access control.

1. Introduction

A variety of new information technologies are gradually making our lives more convenient. For instance, thanks to the introduction of the new computing model, namely, cloud computing [1–8], which delivers common computational tasks like storing, managing and processing data from remote servers, people can

* Corresponding author.
E-mail addresses: zuoxia.yu@gmail.com (Z. Yu), csallen@comp.polyu.edu.hk (M.H. Au), xql@sdu.edu.cn (Q. Xu), orbbyrp@gmail.com (R. Yang), jghan22@gmail.com (J. Han).

http://dx.doi.org/10.1016/j.future.2017.01.025
0167-739X/

Please cite this article in press as: Z. Yu, et al., Towards leakage-resilient fine-grained access control in fog computing, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.01.025

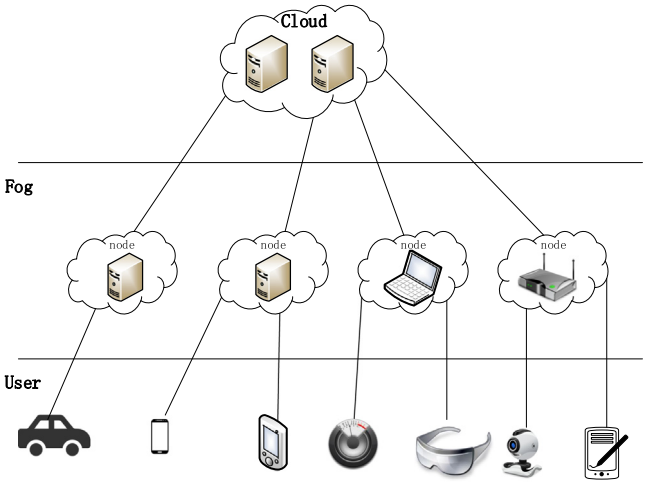

Fig. 1. The concept of fog computing.

outsource complex computational tasks to the cloud and thus complete these tasks with higher efficiency but at a lower cost.

Another new technology that changes our daily lives is the Internet of Things [9,10], which connects physical objects and enables these objects to collect and exchange data. This new technology can broaden the scope of computation to everything. What if we combine these two new techniques? Fog Computing is just the combination which can take advantage of both the cloud computing and the Internet of Things.

The concept of fog computing was first introduced by Bonomi in [11,12], which extends the cloud computing paradigm to the edge of the network. In particular, users in the fog computing model will outsource computation tasks to servers that are geographically close to them. The fog computing model has the characteristics of location awareness, geo-distribution, low latency, mobility support etc. [12]. The abstract concept of fog computing is shown in Fig. 1.

Based on the advantages mentioned above, many applications have been discussed in the paradigm of fog computing. Examples include connected vehicle [11,12], wireless sensors and actuators Networks [12], smart grid [13,14,12], smart cities [12], and health fog [15–17].

Similar to that in the area of cloud computing and Internet of Things, security [18–26] and forensics [27–41] are primary concerns in fog computing [42]. In the following, we illustrate security issues with health fog [15], one of the prominent applications of fog computing. Health Fog aims at promoting and assisting users with a healthy lifestyle via fog, an intermediary layer between cloud and end users. Compared with the original cloud-based healthcare service, Health Fog enjoys the benefits of fog computing, for instance, edge location, low latency, geographical distribution and etc. as mentioned in [43]. In such a system, the personal health information, such as heart rate, pulse, body temperature, BMI index, weight and so on, is gathered by sensors at first. Then fog devices upload data to cloud from user's side as per individual needs or operate real-time analytic. Precisely, those large computation tasks are transferred to remote cloud, while the fog device can also directly conduct some small computation task, such as real-time reply via extracting data. Usually, the fog device is some electronic device with processing ability, such as smart gateway in [43]. For example, if the smart gateway finds the heart rate of user "BOb" is abnormal via extracting information from his health data, it makes immediate warning to him. Consider the case where the data has to be shared or transmitted to different entities. For instance, in order to analyze whether her heart rate is normal, data owner "Alice" chooses to share her physical data to those users with attribute "institution = hospital $\bigwedge$ role = doctor $\bigwedge$ gender = female".

Next, we analyze the security requirements in the above system. To ensure the privacy of user's health data, encryption should be done before data is outsourced to the cloud. Moreover, it is obvious that the access control of the health data of per user should also be assured. Then in order to support fine-grained access control and maintain the data privacy simultaneously, the natural choice is to employ a cryptographic primitive known as "functional encryption". Here we briefly recall the syntax of functional encryptions and discuss how it can be used to achieve access control. In functional encryption, the secret user key and ciphertext are both associated with a set of attributes, and the decryption operation succeeds if and only if the key attribute matches the ciphertext attribute. Furthermore, in a Health Fog, the Department of Health of a city could act as the authority center for the functional encryption scheme. More precisely, once a user with concrete attribute joins in this system, Department of Health generates a corresponding key for this user. The encryption of health data of each user is done by fog device via functional encryption. This idea can be seen as a natural extension of the similar case in cloud computing [44–47], where functional encryption is deployed to impose access control to data. However, the two environments, in terms of potential threats, are different and thus applying the same technique directly could lead to potential vulnerabilities. Specifically, fog node is in close proximity to the users and is thus very often operated in a public environment, the attacker may launch some physical attacks (a.k.a. side channel attacks) against fog devices. For instance, attacker may gain additional information based on the power consumption and running time of devices in the smart gateway. Therefore, the traditional functional encryption may not provide sufficient security guarantee in the fog computing environment.

In a nutshell, functional encryption is a natural candidate cryptographic technique in providing access control in the fog computing environment. However, its traditional definition may not be secure enough against threats that could arise in the fog computing environment.

1.1. Related work

Leakage-resilient cryptography. Traditionally, security of a cryptographic scheme relies on the secrecy of its secret states. In practice, however, state information could be revealed from measurements of the physical attributes of the device on which the cryptographic system is deployed. Attacks based on this extra information, such as timing attacks [48], power attacks [49], cold-boot attacks [50], etc., are grouped under the umbrella term of side-channel attacks.

Leakage-resilient cryptography was developed to address side-channel attacks. To model the additional capability in side-channel attacks, an attacker is allowed to submit an efficiently computable leakage function f to obtain the output of f on the current secret states of the cryptographic system. Many leakage models, differ in the restrictions imposed on f, have been proposed. Among them, the continual memory leakage (CML) model [51,52] is believed to best describe those real world attacks. In this model, the entire lifetime of a scheme is divided into periods. At the end of each period, the secret state of the scheme is updated. The amount of leakage information in each time period is bounded, but the total amount of leakage during the lifetime of the scheme is unbounded. Since then, many cryptographic primitives have been designed in this model, include signatures [53], public-key encryption [54,55], identity-based encryption (IBE) [56,57], attribute-based encryption (ABE) [57], multiparty computation [58], etc.

Please cite this article in press as: Z. Yu, et al., Towards leakage-resilient fine-grained access control in fog computing, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.01.025