Journal of Computer and System Sciences 80 (2014) 546–553

Contents lists available at SciVerse ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

A new definition of homomorphic signature for identity management in mobile cloud computing

Zhiwei Wang [a,b,c,*], Guozi Sun [a,b,c], Danwei Chen [a,b,c]

[a] College of Computer, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu 210003, China
[b] State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences), Beijing 100190, China
[c] Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing, Jiangsu 210003, China

ARTICLE INFO

Article history:
Received 30 November 2012
Received in revised form 30 April 2013
Accepted 14 June 2013
Available online 3 July 2013

Keywords:
Homomorphic signature
Identity management
Mobile cloud computing
GHR signature

ABSTRACT

In this paper, we define a new homomorphic signature for identity management in mobile cloud computing. A mobile user firstly computes a full signature on all his sensitive personal information (SPI), and stores it in a trusted third party (TTP). During the valid period of his full signature, if the user wants to call a cloud service, he should authenticate him to the cloud service provider (CSP) through TTP. In our scheme, the mobile user only needs to send a $\{0,1\}^n$ vector to the access controlling server (TTP). The access controlling server who doesn't know the secret key can compute a partial signature on a small part of user's SPI, and then sends it to the CSP. We give a formal secure definition of this homomorphic signature, and construct a scheme from GHR signature. We prove that our scheme is secure under GHR signature.

1. Introduction

Homomorphic signature [18] is a cryptographic primitive where, given a set of signature $\sigma_1, \ldots, \sigma_n$ on messages $m_1, \ldots, m_n$ in message space $\mathcal{M}$, a function $f : \mathcal{M}^n \to \mathcal{M}$ from a set of "admissible" functions $\mathcal{F}$, anyone can compute a signature on the pair $(f, f(m_1, \ldots, m_n)) \in \mathcal{F} \times \mathcal{M}$. If the signature is valid, then it means that the claimed value equals $f(m_1, \ldots, m_n)$. If the system is secure, then any malicious adversary cannot compute a valid signature on (f, m^*) for any $m^* \neq f(m_1, \ldots, m_n)$.

Homomorphic signature was firstly proposed by Johnson et al. [18]. In the past few years, there are about three classes the research has touched in this area: *quoting/redacting signature*, *arithmetic signature*, *transitive signature*. Quoting/redacting signature [2–6] is that given Alice's signature on some message m, anyone can derive Alice's signature on a substring of m. Quoting/redacting signature is specially applied to signed text message and signed images. Arithmetic signature [7–11] is motivated by the application of secure network coding. In transitive signature [12–16], given Alice's signature on edges in a graph G, anyone can derive Alice's signature on a pair of vertices u, v, if there exists a path from u to v in G.

In 2009, Gentry proposed a fully homomorphic encryption scheme to make it possible to analyze data without decrypting it [1]. As we all know, this property is very suitable for the encrypted date searching in cloud computing. Homomorphic signature also can be used to cloud computing, especially in identity management. Our contributions can be listed as follows: 1) We give a security definition of the homomorphic signature suitable for identity management in mobile cloud

* Corresponding author at: College of Computer, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu 210003, China.
E-mail address: zhwwang@njupt.edu.cn (Z. Wang).

0022-0000/$ – see front matter
http://dx.doi.org/10.1016/j.jcss.2013.06.010

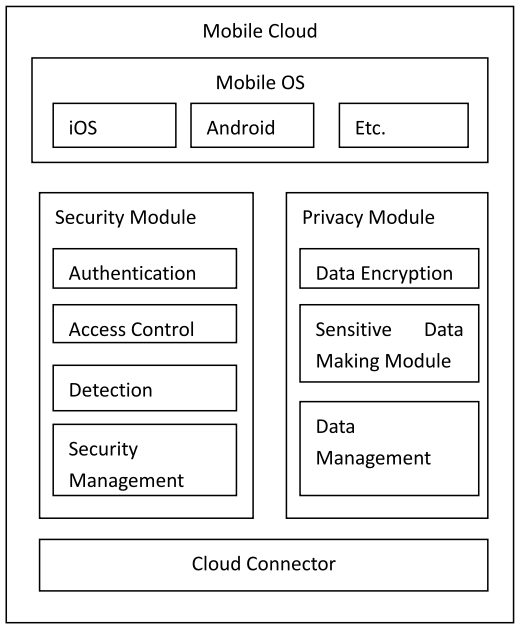

Fig. 1. Mobile cloud computing security architecture overview.

computing; 2) We construct such a homomorphic signature scheme based on the GHR signature [17]; 3) We provide a security proof to our scheme without random oracles, using GHR signature.

This paper is organized as follows: Section 2 describes the application for identity management in mobile cloud computing; Section 3 reviews some concepts related to our construction and the GHR signature; Section 4 gives the security definition of the new homomorphic signature; Section 5 designs a scheme based on GHR signature; Section 6 provides the security analysis to our scheme; Section 7 concludes the paper.

2. Application for identity management in mobile cloud computing

Cloud computing allows the use of Internet-based services to support business processes and rental of IT-services on a utility-like basis. Mobile cloud computing refers to the availability of cloud computing services in a mobile environment. It incorporates the elements of wireless mobile networks and cloud computing, thereby providing optimal services for mobile users. In mobile cloud computing, wireless mobile devices usually do not have a powerful configuration (e.g., CPU speed and memory capacity). Fig. 1 shows an overview of the mobile cloud computing security architecture.

While requesting services from the cloud, a wireless mobile user has to provide some sensitive personal information (SPI) (e.g., name, home address, credit card number, phone number, driver's license number, date of birth, etc.). Obtaining the user's SPI helps the cloud service provider (CSP) to decide whether to permit access to its service or not. However, if all SPI are disclosed, a trail is leaved that can be used to uniquely identify, contact, or locate a particular user. Thus, when requesting a cloud service, a mobile user do not want to disclose all his SPI, but only give the signature on a small part of SPI according to the requirement of the cloud service.[1] So the mobile user might hold multiple accounts with different cloud services, and each account only involves a small part of SPI. Different solutions use different ways of sending mobile user's SPI for negotiation with the CSP. The common way is to use a trusted third party (TTP), such as Privacy and Identity Management for Europe (PRIME) [20].

We assume that every mobile user has a set of SPI: $\mathbf{v} = \{v_1, \ldots, v_n\}$, and one identity ID is a subset of $\mathbf{v}$.[2] Firstly, every mobile user pre-computes the full signature $(\sigma_1, \ldots, \sigma_n)$ on all its corresponding attributes $(v_1, \ldots, v_n)$, and sends them to the access controlling server (the access controlling server as a TTP should check and verify the full signature). Each full signature has a period of validity. During the valid period of his full signature, if the user wants to request a cloud service on a special identity ID, he only needs to send a vector $(c_1, \ldots, c_n)$, where if $v_i \in ID$, then $c_i = 1$, otherwise $c_i = 0$. The access controlling server can compute a partial signature $\hat{\sigma}$ on the ID by using homomorphic signature algorithm, and then it sends $(\hat{\sigma}, ID)$ to cloud server for verification. For example, a mobile user has set of SPI: $\mathbf{v} = \{name, age, sex, credit\ card\ number, phone\ number\}$. One cloud service requires that the one who is a male and over 18

[1] If the cloud service requires to verify all or most of SPI, then mobile user can consider that the CSP is malicious to obtain his identity information.

[2] $ID \neq \mathbf{v}$, otherwise all SPI would be lost.