ARTICLE IN PRESS

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

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry

Meikang Qiu [a,b,*], Keke Gai [b], Bhavani Thuraisingham [c], Lixin Tao [b], Hui Zhao [d]

[a] School of Computer Science and Information Technology, Hubei Engineering University, Hubei, 432000, China

[b] Department of Computer Science, Pace University, New York, NY 10038, USA

[c] Department of Computer Science, The University of Texas at Dallas, Richardson, TX 75083-0688, USA

[d] Software School, Henan University, Kaifeng, Henan, 475000, China

HIGHLIGHTS

- Proactive user-centric data protection scheme for the financial industry.
- Use the attribute-based semantic access control to restrict the data accesses.
- Achieve high level security by avoiding unexpected operations on the cloud side.

ARTICLE INFO

Article history:
Received 19 September 2015
Received in revised form
6 December 2015
Accepted 13 January 2016
Available online xxxx

Keywords:
Proactive secure scheme
Privacy protection
Mobile cloud computing
Cyber security
Financial industry

ABSTRACT

As one of the most significant issues in the financial industry, customers' privacy information protection has been considered a challenging research over years. The constant emergence of the novel technologies often leads to dynamic threats from both internal and external service providers. We consider the implementations of mobile cloud-based financial services an important approach of service provisions, which also causes risks to privacy protections due to the data sharing with the unknown third parties. The data generated by mobility are usually associated with mobile users' personal privacy information. This paper addresses this issue and proposes an approach proactively protect financial customers' privacy information using *Attributed-Based Access Control* (ABAC) as well as data self-deterministic scheme. The proposed approach is called *Proactive Dynamic Secure Data Scheme* (P2DS), which aims to guarantee the unanticipated parties cannot reach the privacy data. There are two main algorithms supporting the proposed scheme, which are *Attribute-based Semantic Access Control* (A-SAC) *Algorithm* and *Proactive Determinative Access* (PDA) *Algorithm*. The main contributions of this paper have three aspects. First, we propose a semantic approach for constraining data accesses. Second, we propose a user-centric approach that proactively prevents users' data from unexpected operations on the cloud side. Finally, the proposed scheme has a higher-level secure sustainability since it can deal with dynamic threats, including the emerging and future hazards. We have examined that our proposed scheme had a quality performance matching our expected goal.

© 2016 Elsevier B.V. All rights reserved.

1. Introduction

The recent dramatic growth of the electronic and digital technologies has provisioned a variety of novel approaches for service offerings in financial industry. Along with the new service approaches, the *Financial Service Institutes* (FSIs) also face diverse threats caused by new techniques or within new technical circumstances. Traditional threats had been addressed by the prior researches to govern the risks within an anticipated scope, such as malware attacks, network-traveling worms, and data abuse [1–3]. However, the new hazards generated by the emerging techniques are usually unanticipated. The masked operations in the clouds increase the chances of information leaks [4,5]. Contemporary deployed security approaches cannot effectively deal with threats. This paper concentrates on this issue and proposes a proactive user-centric secure data scheme that implements *Attributed-Based Access Controls* (ABAC) and a data self-deterministic scheme in

* Corresponding author at: Department of Computer Science, Pace University, New York, NY 10038, USA. Tel.: +1 914 773 3253; fax: +1 914 989 8111.
E-mail addresses: qiumeikang@yahoo.com (M. Qiu), kg71231w@pace.edu (K. Gai), bxt043000@utdallas.edu (B. Thuraisingham), ltao@pace.edu (L. Tao), zhh@henu.edu.cn (H. Zhao).

http://dx.doi.org/10.1016/j.future.2016.01.006
0167-739X/© 2016 Elsevier B.V. All rights reserved.

Please cite this article in press as: M. Qiu, et al., Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.01.006

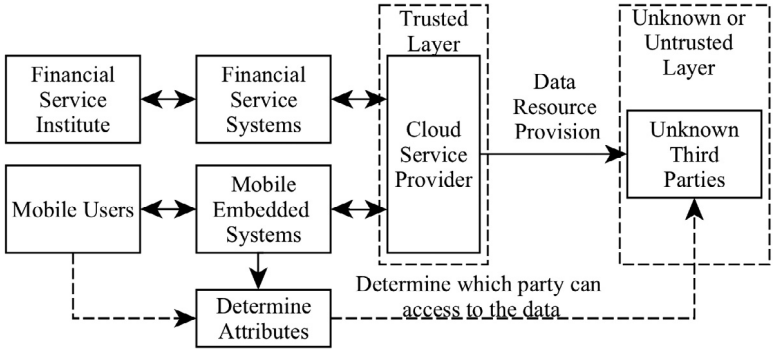

Fig. 1. Architecture of Proactive Dynamic Secure Data Scheme (P2DS).

mobile clouds to achieving the prevention of all potential threats in the financial industry.

The proposed scheme focuses on the emerging threats appearing in multiple manners. The varied threats manners often raise financial crisis, disruptions, and execution obstacles [6]. Kaspersky Lab ZAO, for example, asserted that a large number of banks were facing a serious problem of online robbing and the amount of the stolen money could be over million dollars [7]. The losses are also made for other financial organizations due to the impacts of the technical development [8,9]. When investigating the cases of the information leakage, it is noticed that one of the major causes is applying mobility and data mitigations. The vulnerabilities can take place when the users' data can be reached by other service institutions offering lower-level security.

Moreover, there is no ubiquitous approach solving the problem above, even though the issue can be successfully identified. Data mitigations to the clouds result in unawareness when other organizations use customers' privacy data [10,11]. Financial users are unaware of the hazards behind the operations masked in the clouds. This paper focuses on avoiding untrusted parties reaching the data stored on the cloud side and proposes an approach, named as *Proactive Dynamic Secure Data Scheme* (P2DS). This scheme is designed to protect sensitive financial data within a dynamic operational context. The research work is mainly based on the prior research work [12].

Fig. 1 represents the architecture of P2DS provisioning a user-centric data protection approach. Shown in the figure, the proposed P2DS architecture addresses the demands of financial mobile customers and FSIs. The financial business parties, including FSIs and financial mobile users, communicate data transfer via the services offered by the cloud service providers. Mobile users are data owners who determine the attribute constraints. A higher-level security can be achieved by determining sets of the attributes possessed by the data users. Two layers of the data users identified in the architecture are *Trusted Layer* (TL) and *Unknown/Untrusted Layer* (UL). The attribute constraints mainly constrain or limit the accesses on UL. The proposed P2DS paradigm can ensure the data are encrypted as well as initiatively determine who has the authority to access the data.

For the expected goal of P2DS, we propose three main algorithms. First, the *Static Decryption Attribute Algorithm* (SDAA) is designed to the authorizations of the decryptions from which the status of the trusted parties will be determined based on the *Static Decryption Attributes* (SDA). Next, the *Corresponded Decryption Attribute Algorithm* (CDAA) is to assign the *Corresponded Decryption Attributes* (CDA) along with the decryption authorizations. Furthermore, we generate the *Attribute-based Semantic Access Control* (ASAC) algorithm that constrains the data accesses using semantic access control techniques. Finally, we propose the *Proactive Determinative Algorithm* (PDA) to purpose whether the attributes need to be encrypted.

The main contributions of this paper are threefold:

- We produce an attributed-based data protection approach using semantic access techniques.
- We propose a user-centric approach proactively avoiding unexpected operations or unanticipated parties on the cloud side for the purpose of the data protections.
- The proposed scheme provides a higher-level secure sustainability due to the limitations of the data accesses based on configuring user attribute constraints.

The remainder of this paper is organized by the follows. In Section 2, recent related work in the field are reviewed. Section 3 gives a motivational example explaining the implementation of the proposed scheme. Section 4 exhibits the concepts and models of our proposed mechanism. Next, Section 5 represents the main algorithms. The experimental results are represented in Section 6 and the conclusions are stated in Section 7.

2. Related work

This section focuses on reviewing recent academic achievements of the data protections in clouds as well as data secure approaches in the financial industry. The differences between the prior related work and our proposed scheme are stated in this section via comparisons.

First, a proactive secure data scheme [12] was proposed to protect financial customers' data from untrusted parties' usage in mobile clouds. This approach concentrated on the controls of the data owners and mainly used SDA and CDA. Our paper is an extended work of this scheme by adding semantic constrains of the access controls. Moreover, the extended contents also include formulating the mechanism by mathematical representations and new algorithms.

Next, as a secure approach offering high level security, *Attribute-Based Encryption* (ABE) has been explored by researchers over years. The implementations of ABE have been applied in tele-health field for securing patient privacy information in cloud systems [13–15]. For example, the policy-based ABE has been examined to being a proper approach of preventing personal health records from unexpected usages [16]. Another example was that combining ABE with healthcare social networks can enable an efficient emergency management [17]. However, the attempts in the tele-health fields did not solve the problems caused by the unconstrained data accesses.

In addition, using ABE approaches in the financial industry was also explored by the previous researches [18,19]. An investigation was done for examining the effect of the innovation attributes and knowledge-based trust in the mobile banking field [20]. In general, role-based solutions are treated as an optional solution constraining the access from different role perspectives [21]. Nevertheless, rare prior researches had addressed controlling the access constrains from the unknown data users for dealing with unanticipated risks.

Please cite this article in press as: M. Qiu, et al., Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.01.006

Download English Version:

https://daneshyari.com/en/article/6873338

Download Persian Version:

https://daneshyari.com/article/6873338

Daneshyari.com