Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

SECO: Secure and scalable data collaboration services in cloud computing

Xin Dong [a], Jiadi Yu [a,*], Yanmin Zhu [a], Yingying Chen [b], Yuan Luo [a], Minglu Li [a]

[a] Department of Computer Science and Engineering, Shanghai Jiao Tong University Shanghai, 200240, PR China

[b] Department of Electrical and Computer Engineering, Stevens Institute of Technology Hoboken, 07030, USA

ARTICLE INFO

Article history:
Received 3 April 2014
Received in revised form
21 November 2014
Accepted 12 January 2015
Available online 28 January 2015

Keywords:
Data collaboration
Data security
HIBE
One-to-many encryption
Cloud computing

ABSTRACT

Cloud storage services enable users to remotely store their data and eliminate excessive local installation of software and hardware. There is an increasing trend of outsourcing enterprise data to the cloud for efficient data storage and management. However, this introduces many new challenges toward data security. One critical issue is how to enable a secure data collaboration service including data access and update in cloud computing. A data collaboration service is to support the availability and consistency of the shared data among multi-users. In this paper, we propose a secure, efficient and scalable data collaboration scheme SECO. In SECO, we employ a multi-level hierarchical identity based encryption (HIBE) to guarantee data confidentiality against untrusted cloud. This paper is the first attempt to explore secure cloud data collaboration services that precludes information leakage and enables a one-to-many encryption paradigm, data writing operation and fine-grained access control simultaneously. Security analysis indicates that the SECO is semantically secure against adaptive chosen ciphertext attacks (IND-ID-CCA) in the random oracle model, and enforces fine-grained access control, collusion resistance and backward secrecy. Extensive performance analysis and experimental results show that SECO is highly efficient and has only low overhead on computation, communication and storage.

1. Introduction

Cloud computing (Armbrust et al., 2009), the long-held dream of computing as a utility, is rapidly evolving to revolutionize the way how data is stored/used. Cloud computing benefits data users in that it allows convenient access and use of storage resources offered by a cloud server provider (CSP). Challenges in security, however, posed by outsourcing data to the cloud, come along with benefits. Upon loss of physical possession of the outsourced data, users no longer control their data. But, CSPs may be untrusted and could monitor at will, lawfully or unlawfully, the data stored in the cloud and the communication between users and cloud. As a result, outsourcing users' data to the cloud initiates a series of problems about security and privacy. Examples of security breaches never stop showing up (Arrington, 2006; Wilson, 2008; Ren et al., 2012; Ateniese et al., 2007). Therefore, maintaining data availability and confidentiality becomes critical to

* *Corresponding author*. Tel./fax: +86 21 3420 5856.
E-mail address: jiadiyu@sjtu.edu.cn (J. Yu).

http://dx.doi.org/10.1016/j.cose.2015.01.003
0167-4048/© 2015 Elsevier Ltd. All rights reserved.

enable wide deployment of CSP-based data service with high quality.

One important security issue is how to ensure secure data storage service when utilizing cloud services (Arora et al., 2013; De Capitani di Vimercati et al., 2010; Samarati and De Capitani di Vimercati, 2010). For instance, enterprises can outsource their data into the cloud and then enable their employees to access these data. However, cloud servers are untrusted and they may disclose the confidential information about an enterprise to their business competitors or even hide data leakage to maintain their reputations. In order to ensure data security, companies and enterprises usually have to encrypt the data before outsourcing it into the cloud. Recently, the notion of secure cloud storage services has been proposed in the content of ensuring remotely stored data under different systems and security models (Ateniese et al., 2007; Yu et al., 2010; Wang et al., 2010a; Dong et al., 2013). These existing works addressed secure cloud storage and data access issue either by introducing attribute-based encryption (ABE) (Goyal et al., 2006) for fine-grained access control (Wang et al., 2010b; Dong et al., 2014), or by utilizing owner-write-user-read mechanism (Wang et al., 2009) to achieve cryptography-based access control and only support coarse grained access control. ABE-based schemes are data-read sharing services, while owner-write-user-read mechanism is a one-to-one encryption paradigm meaning encrypted data can only be decrypted by a particular recipient. Consequently, existing solutions mainly focus on how to afford secure data access control (read) for cloud users. None of these works considers that multiple users operate (read/write) encrypted data collaboratively in cloud computing, i.e., data collaboration services.

A ***Data Collaboration*** service is to support the availability and consistency of the shared cloud data among multi-users. Let's consider a typical data collaboration service scenario: Alice, who is the boss of a company, pays a CSP for a secure data collaboration service, and assigns her two colleagues, Jack and Bob, to work collaboratively on a project. Alice first encrypts the project data and stores the encrypted data into the cloud. Then, Alice authorizes Jack and Bob to access the encrypted data so that they can modify the data. After modifying the data, Jack or Bob re-encrypts the data and sends it to the cloud. Within these three members, anyone who modifies the data, then determines the access privilege of the data. In total, three members work together and share data in a collaborative way. To avoid information leakage, the data have to be restrained within the reach of these three members. Thus the access policy of the above scenario is: authorized users can access the encrypted data while CSP and other unauthorized users know nothing about the data in data collaboration services.

To realize secure data collaboration services in cloud computing, we face the following challenges. Firstly, since a confidential data involves more than one recipient, the encryption paradigm should be one-to-many that indicates multiple recipients can decrypt the encrypted data. Secondly, authorized users have the privilege to operate the cloud data, so the encryption paradigm should support data writing operation. Thirdly, in order to ensure data security among users, the system should provide fine-grained access control to the users. To the best of our knowledge, there is no existing solution to tackle the problems of secure data collaboration services in cloud computing.

In this paper, we propose a scalable scheme (**SECO**) to enable secure cloud data collaboration with explicit dynamic data/users. For cloud data security, we employ a multi-level hierarchical identity-based encryption (HIBE) scheme, which contains a root private key generator (PKG), a series of lower-level PKGs and independent domains. The root PKG only generates private keys for lower-level PKGs, and lower-level PKGs in turn generate private keys for entities in their next level. A domain consists of a D-PKG and a number of individual users who cooperate to complete a project. During data collaboration, to achieve one-to-many encryption paradigm, a user in a domain encrypts data with the public parameters and multiple recipients' public keys so that only the intended domain recipients are able to decrypt the data. To support writing operation, every authorized user can encrypt the decrypted data after modifying (read/write) it, and then sends it into the cloud to share with other domain users. The data writing operation does not introduce security problems. To realize fine-grained access control, each authorized user which encrypts data can decide on the intended decryption recipients.

Specifically, the main contributions of this paper can be summarized as following three aspects:

- We propose a data collaboration service, SECO, which enables secure, efficient and scalable data collaboration in cloud computing, which realize one-to-many encryption paradigm, writing operation and fine-grained access control simultaneously without any information leakage. Our work is the first attempt to explore secure data collaboration in cloud computing.
- We prove that SECO is semantically secure against adaptive chosen ciphertext attacks (IND-ID-CCA) in the random oracle model under the Bilinear Diffie-Hellman assumption (Boneh and Franklin, 2001), and SECO also enforce collusion resistance and backward secrecy for cloud data collaboration services.
- We have conducted extensive theoretical analysis and real experiments to evaluate the performance of SECO. The result indicates that SECO introduces low overhead on computation, communication and storage while improves the effectiveness and efficiency.

The remainder of this paper is organized as follows: Section related work discusses related works; Section 3 introduces the system model, threat model and our design goals; Section 4 presents the detail design of SECO; Section 5 provides the security definition and security proof of SECO; Sections 6 and 7 analyze the theoretical and experimental performance of SECO, respectively; finally, Section 8 concludes the whole paper.

2. Related work

Identity-based encryption (IBE) is an encryption choice in cloud computing (Li et al., 2013a; Guo et al., 2013). The concept