Dual Access Control for Cloud-Based Data Storage and Sharing

ABSTRACT

Cloud-based data storage service has drawn increasing interests from both academic and industry in the recent years due to its efficient and low cost management. Since it provides services in an open network, it is urgent for service providers to make use of secure data storage and sharing mechanism to ensure data confidentiality and service user privacy. To protect sensitive data from being compromised, the most widely used method is encryption. However, simply encrypting data (e.g., via AES) cannot fully address the practical need of data management. Besides, an effective access control over download request also needs to be considered so that Economic Denial of Sustainability (EDoS) attacks cannot be launched to hinder users from enjoying service. In this paper, we consider the dual access control, in the context of cloud-based storage, in the sense that we design a control mechanism over both data access and download request without loss of security and efficiency. Two dual access control systems are designed in this paper, where each of them is for a distinct designed setting. The security and experimental analysis for the systems are also presented.

**EXISTING SYSTEM**

Although being able to support fine-grained data access, CP-ABE, acting as a single solution, is far from practical and effective to hold against EDoS attack [11] which s the case of DDoS in the cloud setting [11], [39]. Several countermeasures to the attack [12], [33] have been proposed in the literature. But Xue et al. [38] stated that the previous works could not fully defend the EDoS attack in the algorithmic (or protocol) level, and they further proposed a solution to secure cloud data sharing from the attack.

However, [38] suffers from two disadvantages. First, the data owner is required to generate a set of challenge ciphertexts in order to resist the attack, which enhances its computational burden. Second, a data user is required to decrypt one of the challenge ciphertexts as a test, which costs a plenty of expensive operations (e.g., pairing). Here the computational complexity of both parties is inevitably increased and meanwhile, high network bandwidth is required for the delivery of ciphertexts. The considerable computational power of cloud is not fully considered in [38]. In this paper, we will present a new solution that requires less computation and communication cost to stand still in front of the EDoS attack.

Recently, Antonis Michalas [20] proposed a data sharing protocol that combines symmetric searchable encryption and ABE, which allows users to directly search over encrypted data. To implement the functionality of key revocation in ABE, the protocol utilizes SGX to host a revocation authority. Bakas and Michalas [3] later extended the protocol in [20] and proposed a hybrid encryption scheme that reduces the problem of multi-user data sharing to that of a single-user. In particular, the symmetric key used for data encryption is stored in an SGX enclave, which is encrypted with an ABE scheme. Similar to [20], it deals with the revocation problem in the context of ABE by employing the SGX enclave. In this work, we employ SGX to enable the control of the download request (such that the DDoS/EDoS attacks can

be prevented). In this sense, the purpose and the technique of ours are different from that of the protocols in [3], [20].

Disadvantages

1) The system was not implemented Ciphertext-Policy Attribute-based-Encryption Method which leads less security on outsourced data.

2) The system is less security due to lack of Authenticated Encryption with Associated Data.

**PROPOSED SYSTEM**

In this paper, we propose a new mechanism, dubbed dual access control, to tackle the above aforementioned two problems. To secure data in cloud-based storage service, attribute-based encryption (ABE) [9] is one of the promising candidates that enables the confidentiality of outsourced data as well as fine-grained control over the outsourced data.

In particular, Ciphertext-Policy ABE (CP-ABE) [5] provides an effective way of data encryption such that access policies, defining the access privilege of potential data receivers, can be specified over encrypted data. Note that we consider the use of CP-ABE in our mechanism in this paper. Nevertheless, simply employing CP-ABE technique is not sufficient to design an elegant mechanism guaranteeing the control of both data access and download request.

A strawman solution to the control of download request is to leverage dummy ciphertexts to verify data receiver’s decryption rights. It, concretely, requires data owner, say Alice, to upload multiple “testing” ciphertexts along with

the “real” encryption of data to cloud, where the “testing” ciphertexts are the encryptions of dummy messages under the same access policy as that of the “real” data. After receiving a download request from a user, say Bob, cloud asks Bob to randomly decrypt one of the “testing” ciphertexts. If a correct result/decryption is returned (i.e. indicating Bob is with valid decryption rights), Bob is authorized by Alice to access the ”real” data, so that the cloud allows Bob to download the corresponding ciphertext.

**Advantages**

**(1) Confidentiality of outsourced data.** In our proposed systems, the outsourced data is encrypted prior to being uploaded to cloud. No one can access them without valid access rights.

**(2) Anonymity of data sharing.** Given an outsourced data, cloud server cannot identify data owner, so that the anonymity of owner can be guaranteed in data storage and sharing.

**(3) Fine-grained access control over outsourced (encrypted) data.** Data owner keeps controlling his encrypted datavia access policy after uploading the data to cloud. Inparticular, a data owner can encrypt his outsourced dataunder a specified access policy such that only a groupof authorized data users, matching the access policy, canaccess the data.

**(4) Control over anonymous download request and EDoS attacks resistance.** A cloud server is able to control thedownload request issued by any system user, where thedownload request can set to be anonymous. With thecontrol over download request, we state that our systemsare resistant to EDoS attacks.

**(5) High efficiency.** Our proposed systems are built on the top of the CP-ABE system. Compared with [36], they do not incur significant additional computation and communication overhead. This makes the systems feasible for real-world applications.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**Software Requirements:**

* Operating System - Windows XP
* Coding Language - Java/J2EE(JSP,Servlet)
* Front End - J2EE
* Back End - MySQL