DUAL ACCESS CONTROL FOR CLOUD-BASED DATA STORAGE AND SHARING USING MULTILEVEL SECURITY

Y.Siva Prasad[1], Assistant Professor, Dept. of Computer Science and Engineering, DVR &Dr. HS MIC College of Technology,Kanchikacherla, Andhra Pradesh, India
Ch.Vinay Santhosh[2], Assistant Professor, Dept. of Computer Science and Engineering, DVR &Dr. HS MIC College of Technology,Kanchikacherla, Andhra Pradesh, India
Vamsi Krishna Arepalli[3], UG Student, Dept. of Computer Science and Engineering, DVR &Dr. HS MIC College of Technology,Kanchikacherla, Andhra Pradesh, India
Prasanna Devi Dangeti[4], UG Student, Dept. of Computer Science and Engineering, DVR &Dr. HS MIC College of Technology,Kanchikacherla, Andhra Pradesh, India
Shailu Chintalacheruvu[5], UG Student, Dept. of Computer Science and Engineering, DVR &Dr. HS MIC College of Technology,Kanchikacherla, Andhra Pradesh, India
Rakesh Dasaripalli[6], UG Student, Dept. of Computer Science and Engineering, DVR &Dr. HS MIC College of Technology,Kanchikacherla, Andhra Pradesh, India

1.Abstract

The effective cost management of cloud-based data storage has attracted increasing attention from academics and industry in recent years. In order to safeguard user privacy and the confidentiality of the data, service providers must develop secure data storage and sharing techniques because services are given through an open network. to prevent the compromise of sensitive information.

The method that is used the most frequently is encryption. Encrypting data alone, however, falls short of entirely satisfying the true need for data management (for instance, using AES). In order to prevent Economic Denial of Sustainability (EDoS) attacks from being carried out to prevent users from using the service, a robust access control on download requests must also be taken into consideration. The dual access is examined in this article.

Keywords: One time password, denial of sustainability

2.Introduction

Cloud-based storage services have received a lot of interest in present era from both academia and business. Due to its extensive list of advantages, which includes access freedom and the lack of local data administration, it may be widely employed in many Internet-based commercial applications (such as Apple iCloud). Nowadays, a growing number of people and businesses prefer to outsource their data to faraway clouds in order to avoid having to upgrade their local data management facilities or devices. However, one of the biggest barriers preventing Internet users from embracing cloud-based storage services generally may be their concern about breach of security involving outsourced data. Outsourced data may need to be subsequently shared with others in many practical scenarios. , a Dropbox member, might share pictures with her companions. Without employing data encryption, Prasanna must first create a sharing link and then distribute it to others in order to share the images. The sharing link might be viewable from the Dropbox administration level, even while it guarantees some level of access control over unauthorised users (for example, those who are not Prasanna friends) (e.g., administrator could reach the link). In order to protect data security and privacy, it is typically advised to encrypt the data before uploading it to the cloud (which is deployed on an open network). One of the comparable options is to immediately utilise an encryption technique (such as AES) on the outsourced data before uploading to the cloud, so that only authorized cloud users (with legal decryption keys) can access the data after it has been encrypted.

A simple solution to prevent shared photographs from being accessed by system "insiders" is to specify the group of permitted data users before encrypting the data. In other circumstances, nevertheless, Prasanna may have no information about swho the photo receivers/users are going to be. Prasanna might only be aware of attributes related to photo receivers. Traditional public key encryption, like Paillier encryption, cannot be used in this situation since it requires the encryptor to know in advance who the data receiver is. In order to ensure that only a select group of authorised

DOI: 10.36893.JK.2023.V13I04N16.00103-00106

users can access the encrypted images, it is desirable to provide a policy-based encryption mechanism over the outsourced photos. Prasanna may then utilise the mechanism to define access control over the encrypted photos.

A frequent exploit known as a resource-exhaustion attack exists in cloud-based storage services. A malicious service user may launch denial-of-service (DoS)/distributed denial-of-service (DDoS) attacks to consume the resource of the cloud storage service server in order to prevent the cloud service from being able to respond to honest users' service requests. This is because a (public) cloud may not have any control over download requests (namely, a service user may send an unlimited number of download requests to cloud server). Due to increased resource demand, the "pay-as-you-go" model runs the risk of upsetting the economy. Users of cloud services will experience a sharp increase in charges as the attack spreads. This is a so-called Economic Denial of Sustainability (EDoS)

In addition to financial loss, unrestricted downloads themselves could provide network intruders access to encrypted download data. It may lead to some potential information leakage (e.g., file size). Hence, there is also a need for an efficient control over download requests for external (encrypted) data.

In this research, we provide a novel dual access control system to address the two issues mentioned above. To protect data stored in a cloud-based service,

One of the promising alternatives that permits the confidentiality of outsourced data as well as fine-grained control over the outsourced data is attribute-based encryption (ABE) [9].

Particularly, Ciphertext-Policy ABE (CP-ABE) [5] offers a reliable method of data encryption that enables the specification of access policies, which specify the access privilege of prospective data receivers, over encrypted data. Please take note that in this research, we consider the use of CP-ABE in our mechanism. Nevertheless, using the CP-ABE technique alone is insufficient to create a sophisticated mechanism that ensures the control of both data access and download requests.

SYSTEM ARCHITECTURE AND SECURITY MODEL

System Architecture The architectures of our dual access control systems for cloud data sharing are shown in Fig. 1. Concretely, the systems consist of the following entities:

The image part with relationship ID rId6 was not found in the file.

• Authority is responsible for initializing system parameter and data user registration. Also, it handles the call request from the cloud in the first proposed construct

• Data owner holds the data and wants to outsource his data to the cloud. In particular, data owners (only) want to share their data with those who satisfy certain conditions (e.g., professors or associate professors). They will be offline once their data have been uploaded to the cloud.

• Data user wants to download and decrypt the encrypted data shared in the cloud. Those who are authorized can download the encrypted file and further decrypt it to access the plaintext.

. Cloud provides convenient storage service for data owners and data users. Specifically, it stores the outsourced data from data users and handles the download requests sent by data users

Security Assumptions The security assumption of each entity is described as follows.

• Authority is fully trusted by other entities.

• Data owner is honest in the sense that she/he encrypts the outsourced data and uploads the encrypted data to the cloud honestly.

• Data user is malicious in the sense that she/he may try to download the shared file which is not authorized for her/him and launch the EDoS attacks.

• Cloud is honest-but-curious in the sense that it may gather sensitive information curiously by observing the transcript but will not deviate from the specification. Specifically, it will store the outsourced data and handles the access control on the download request honestly. However, it may try to infer more information (they are not supposed to know) than what is revealed by the transcript.

3.PROPOSED SYSTEM

To protect the data, we use a hybrid system, which combines the effectiveness of symmetric-key systems with the practicality of public-key systems and also One Time Password into a text format. The suggested dual access control systems, in particular, are both in setting for the Key/Data Encapsulation Mechanism (KEM/DEM). An effective symmetric-key encryption strategy is employed to encrypt the message, while the CP-ABE, an inefficient public-key scheme, is only used to encrypt and decrypt a small key value.

We use the CP-ABE technique as the fundamental building block to fulfil the security requirements of anonymous data sharing, confidentiality of shared data, and access control on shared data. Due to the efficiency and elegance of the CP-ABE scheme's construction, we specifically provide it here. To fulfil the security requirements of anonymous download request and access control on download request we create an efficient system so the cloud may determine if a data user is authorised or not without disclosing any sensitive information (including the identity of the data user, the plaintext of the outsourced data), anonymous download requests, and access control on download requests. In the first method, the cloud need assistance from the authorities while making a decision on the download request (sent by a data user). Thus, the authority must constantly be online.

4.Working Method

1.Registration

Both the client and the owner must sign up before they can do anything in the cloud. For enrollment, the client and the owner will send a request to the comparing space authority. The new component's compliance with the agreements is then confirmed by the space authority. The local authority will send the request to the trusted space if they are willing to accept the terms. The thought power will then issue an extremely long-lasting ID to all of the owners and customers. After that, they'll be able to make them a secret key.

2. Document Upload

The owner of the information must first encrypt it using his private key before sending it to the next higher level. That is the authority that has jurisdiction. The proprietor's registration will then be checked by the space authorities. The space authority will transmit that encrypted record to the trusted authority if he is a registered proprietor.

3. Document Download

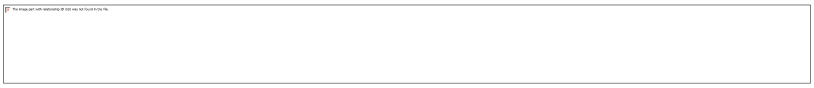
The information client must first request the appropriate space authority before downloading any record from the cloud. The local government will then

conduct a check on the client. The request will be forwarded to the trusted in power if the client is legitimate. This request will then be forwarded to the owner of the relevant data by the presumed power. The client's trait set will then be examined by the proprietor. The owner will give the client a key if the client possesses a lot of traits. When the owner hands customer a key, the clock will start to tick. After a predetermined amount of time has passed, that key ceases to be valid.

Consequently, the client must finish the requested paper within the allotted time.

4. Deletion of Documents

Only the person who owns the data can delete it from the cloud. The believed power will assign an identification number to each information owner during the enlistment period. These ID numbers are extremely durable, Forthem. In a similar vein, the secret key that each of them uses isn't particularly long-lasting. To erase a report, the data proprietor should initially record a solicitation to his comparing space


The image part with relationship ID rId6 was not found in the file.

5.Authority

This solicitation includes the document name and proprietor id. The proprietor's secret word will then be the subject of an inquiry from the area administration. If the owner provides the correct secret word, the local authority will forward the request for deletion to the trusted authority. The document will then be removed from the cloud by the believed pow

5.LITERATURE SURVEY

[1] Alexandros Bakas and Antonis Michalas. Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX. In SecureComm 2019, pages 472–486, 2019.

Secure cloud storage is considered as one of the most important issues that both businesses and end-users take into account before moving their private data to the cloud. Lately, we have seen some interesting approaches that are based either on the promising concept of Symmetric Searchable Encryption (SSE) or on the well-studied field of Attribute-Based Encryption (ABE). In this paper, we propose a hybrid encryption scheme that combines both SSE and ABE by utilizing the advantages of both these techniques. In contrast to many approaches, we design a revocation mechanism that is completely separated from the ABE scheme and solely based on the functionality offered by SGX

[2] Antonis Michalas. The lord of the shares: combining attributebased encryption and searchable encryption for flexible data sharing. In SAC 2019, pages 146–155, 2019

Secure cloud storage is considered one of the most important issues that both businesses and end-users are considering before moving their private data to the cloud. Lately, we have seen some interesting approaches that are based either on the promising concept of Symmetric Searchable Encryption (SSE) or on the well-studied field of Attribute-Based Encryption (ABE). In the first case, researchers are trying to design protocols where users' data will be protected from both internal and external attacks without paying the necessary attention to the problem of user revocation. On the other hand, in the second case existing approaches address the problem of revocation. However, the overall efficiency of these systems is compromised since the proposed protocols are solely based on ABE schemes and the size of the produced ciphertexts and the time required to decrypt grows with the complexity of the access formula. In this paper, we propose a protocol that combines both SSE and ABE in a way that the main advantages of each scheme are used. The proposed protocol allows users to directly search over encrypted data by using an SSE scheme while the corresponding symmetric key that is needed for the decryption is protected via a Ciphertext-Policy Attribute-Based Encryption scheme.

[3] G. Wang, C. Liu, Y. Dong, P. Han, H. Pan, and B. Fang, "Idcrypt: A multi-user searchable symmetric encryption scheme for cloud applications," IEEE Access, vol. 6, pp. 2908–2921, 2018.

Searchable Encryption (SE) has been extensively examined by both academic and industry researchers. While many academic SE schemes show provable security, they usually expose some query information (e.g., search and access patterns) to achieve high efficiency. However, several inference attacks have exploited such leakage, e.g., a query recovery attack can convert opaque query trapdoors to their corresponding keywords based on some prior knowledge. On the other hand, many proposed SE schemes require significant modification of existing applications, which makes them less practical, weak in usability, and difficult to deploy. In this paper, we introduce a secure and practical searchable symmetric encryption scheme with provable security strength for cloud applications, called IDCrypt, which improves the search efficiency, and enhances the security strength of SE using symmetric cryptography. We further point out the main challenges in securely searching on multiple indexes and sharing encrypted data between multiple users. To address the above issues, we propose a token-adjustment search scheme to preserve the search functionality among multi-indexes, and a key sharing scheme which combines identity-based encryption and public-key encryption. Our experimental results show that the overhead of the key sharing scheme is fairly low.