ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

An Efficient & Secure Access Control System by Combining Data Owner Side User Side for Encrypted Cloud Computing

Sthitipragnya Sabat[1], Prof. H. A. Hingoliwala[2]

P.G. Student, Department of Computer Engineering, JSCOE, Pune, India [1]

Assistant Professor, Department of Computer Engineering, JSCOE, Pune, India [2]

ABSTRACT: Data access control is a challenging issue in public cloud storage systems. To share the encrypted files with other users, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has been adopted as a promising technique to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers. A malicious attacker can download thousands of files to launch Economic Denial of Sustainability (EDoS) attacks, which will largely consume the cloud resource. The payer of the cloud service bears the expense. Besides, the cloud provider serves both as the accountant and the payee of resource consumption fee, lacking the transparency to data owners. These concerns should be resolved in real world public cloud storage. In this paper, we propose a solution to secure encrypted cloud storages from EDoS attacks and provide resource consumption accountability. It uses CP-ABE schemes in a black-box manner and complies with arbitrary access policy of CP-ABE. We present remove the problem of single-point performance bottleneck and provide a more efficient access control scheme with an auditing mechanism.

KEYWORDS: Ciphertext-Policy Attribute-based Encryption (CP-ABE), Access Control, Public Cloud Storage, Privacy-Preserving

I. Introduction

Cloud storage is a promising and important service paradigm in cloud computing. Benefits of using cloud storage include greater accessibility, higher reliability, rapid deployment and stronger protection, to name just a few. Despite the mentioned benefits, this paradigm also brings forth new challenges on data access control, which is a critical issue to ensure data security. Since cloud storage is operated by cloud service providers, who are usually outside the trusted domain of data owners, the traditional access control methods in the Client/Server model are not suitable in cloud storage environment. The data access control in cloud storage environment has thus become a challenging issue. Many storage systems use server-dominated access control, like password based and certificate-based authentication. They overly trust the cloud provider to protect their sensitive data. The cloud providers and their employees can read any document regardless of data owner's access policy. Besides, the cloud provider can exaggerate the resource consumption of the file storage and charge the payers more without providing verifiable records, since we lack a system for verifiable computation of the resource usage. To address the issue of data access control in cloud storage, there have been quite a few schemes proposed, among which Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques. A salient feature of CP-ABE is that it grants data owners direct control power based on access policies, to provide flexible, fine-grained and secure access control for cloud storage systems. In CP-ABE schemes, the access control is achieved by using cryptography, where an owner data is encrypted with an access structure over attributes, and a user's secret key is labeled with his/her own attributes. Only if the attributes associated with the users secret key satisfy the access structure, can the user decrypt the corresponding ciphertext to obtain the plaintext. So far, the CP-ABE based access control schemes for cloud storage have been developed into two complementary categories, namely, single-authority scenario, and multi-authority scenario.

DOI: 10.15680/IJIRCCE.2019. 0705011

II. Problem Definition

Here lists the two problems in Efficient Two Sided Access Control System in Cloud Storage:

- Resource-exhaustion attack
- Resource consumption

III. Goals & Objectives

Goals

- Malicious user is to convince the cloud server that he is a legitimate data owner.
- To design a dynamic collaboration environment utilizing the benefits of cloud storage while ensuring strong data security and fine-grained data access.
- To improve our skills and knowledge with regards to designing systems that leverage the benefits of the cloud, improve our ability to research a scientific subject from different perspectives, and to contribute to the scientific community.

Objectives

- Improving data confidentiality in cloud storage environments while enhancing dynamic sharing between users.
- Indeed, the proposed security mechanisms should ensure both robustness and efficiency, namely the support of flexible access control, efficient user revocation and performances.

Addressing the issue of provable data possession in cloud storage environments for data integrity verification support, following three substantial aspects: security level, public verifiability, and performance, and considering the limited storage and processing capacities of user devices.

IV. Literature Survey

This paper aims at fine-grained access control for time sensitive data in cloud storage. One challenge is to simultaneously achieve both flexible timed release and fine granularity with lightweight overhead, which was not explored in existing works. In this paper, we proposed a scheme to achieve this goal. Our scheme seamlessly incorporates the concept of timed-release encryption to the architecture of at different time, according to a well-defined access policy over attributes and release time. We further studied ciphertext policy attribute-based encryption. With a suit of proposed mechanisms, this scheme provides data owners with the capability to flexibly release the access privilege to different user’s access policy design for all potential access requirements of time sensitive, through suitable placement of time trapdoors. The analysis shows that our scheme can preserve the confidentiality of time-sensitive data, with a lightweight overhead on both CA and data owners. It thus well suits the practical large-scale access control system for cloud storage. [1]

In this paper, to address the problem of semantic retrieval, we propose effective schemes based on concept hierarchy. Our solutions use two cloud servers for encrypted retrieval and make contributions both on search accuracy and efficiency. To improve accuracy, we extend the concept hierarchy to expand the search conditions. In addition, a tree-based index structure is constructed to organize all the document index vectors, which are built, based on the concept hierarchy for the aspect of search efficiency. The security analysis shows that the proposed scheme is secure in the threat models. Experiments on real world dataset illustrate that our scheme is efficient. [3]

Cloud Storage provides cost-effective services to individual users as well as organization. It provides huge amount of space to outsource the data to the cloud. Organization and enterprises do not possess full infrastructure to maintain their data with their premises. Data outsourcing helps to effectively maintain their data in cloud storage. Whenever user moves their data to the cloud, there are many possibilities to attack the data at rest as well as transit. This paper discusses confidentiality enabled obfuscation and steganography technique to enhance the security of data in cloud storage. When the masked data is stored in the cloud, hackers are tried to attack the data. But, when embedding the obfuscated data inside the image it is difficult to identify whether it is a cover image or stego image. Experimental results show that the proposed technique can be used to hide much more information than the existing method and the visual quality of the stego images is also to be improved. So, the proposed technique will improve the data storage security. [3]

In this paper, we proposed a new framework, named RAAC, to eliminate the single-point performance bottleneck of the existing CP-ABE schemes. By effectively reformulating CPABE cryptographic technique into our novel framework, our proposed scheme provides a fine-grained, robust and efficient access control with one-CA/multi-AAs for public cloud storage. Our scheme employs multiple AAs to share the load of the time-consuming legitimacy verification and standby for serving new arrivals of users requests. We also proposed an auditing method to trace an attribute authority's potential misbehavior. We conducted detailed security and performance analysis to verify that our scheme is secure and efficient. The security analysis shows that our scheme could effectively resist to individual and concluded malicious users, as well as the honest-but-curious cloud servers. Besides, with the proposed auditing & tracing scheme, no AA could deny its misbehaved key distribution. [4]

Privacy-preserving outsourcing of image feature extraction offers the promise of obtaining feature descriptors dependent on private data without exposing the data owner's privacy, while enjoying the abundant cloud computation resources. However, previous solutions for secure SIFT outsourcing have both security or efficiency issues, and none can well preserve the important characteristics of the original SIFT in terms of distinctiveness and robustness. In this work, we presented a new and novel privacy-preserving SIFT outsourcing protocol based on newly proposed secure interactive protocols BSMP and BSCP. We both carefully analyze and extensively evaluate the security and effectiveness of our design. Our experimental results shows that our protocol outperforms the state-of-the-art and performs comparably to the original SIFT and are practical for real-world applications. [5]

The proposed system uses a cryptographic protocol which is used to allow federated organizations which use attribute based access control policies and preserving the privacy of users to identity attributes. It ensures integrity of access control components which is responsible for evaluating and enforcing access control policies. Users will use the secret to reconstruct the key from the encrypted data and access the data with integrity. [6]

EDoS mitigation approach referred to as the EDoS Attack Defense Shell (EDoS-ADS) is proposed. The EDoSADS approach avoids false negatives and allowing the legitimate clients to access the cloud services. EDoS-ADS use an average CPU utilization threshold as a parameter to trigger the auto scaling condition. [7]

Here an outsourced file is divided into n blocks. Each block generates a verification metadata. They propose a sampling strategy on blocks in the cloud. The scheme reduces the computational cost of the user. [8]

An advanced ABE technique is used to overcome the drawback of CP-ABE, by using our system cipher text size will remain constant. And users can update and can delete attributes without document decryption using Meta data file anytime. [9]

Access structures are defined on the attributes; control the accessibility of users in the system. Based on the association of access structure can is Key-policy attribute based encryption (KP-ABE) and Ciphertext-policy Based encryption (CP-ABE). In CP-ABE scheme, ciphertext is labeled with access structure and user's secret key is labeled with attributes, if attributes associated with user's secret key fulfill the requirement of the access structure then only the user can decipher the ciphertext. [10]

V. EXISTING SYSTEM

Some existing works try to mitigate EDoS attacks. In the authors proposed a mitigation technique by verifying whether a request comes from a cloud user or is generated by bots. The authors proposed an attribute-based way to identify malicious clients. They treat the underlying application in a black box and do not fully immunize the attack in the algorithmic and protocol level.

VI. PROPOSED SYSTEM

To achieve the security requirements, the scheme consists of two components: 1. A cloud-side access control to block users whose attribute set Ai does not satisfy the access policy A; 2. A proof-collecting subsystem where the cloud provider can collect the proofs of resource consumption from users, and present to the data owners later.

In real-world scenarios, it is reasonable to specify an expected maximal download times, and data owners can remain offline unless it wants to increase this value. This leads to our first protocol: Partially Outsourced Protocol (POP) (V-B). In some other cases where the data owner cannot set expectations of download times or would be offline for a long time, the data owner can delegate to the cloud. This leads to our second protocol: Fully Outsourced Protocol (FOP) (V-C). Performance analysis shows that the overhead of our construction is small over existing systems.

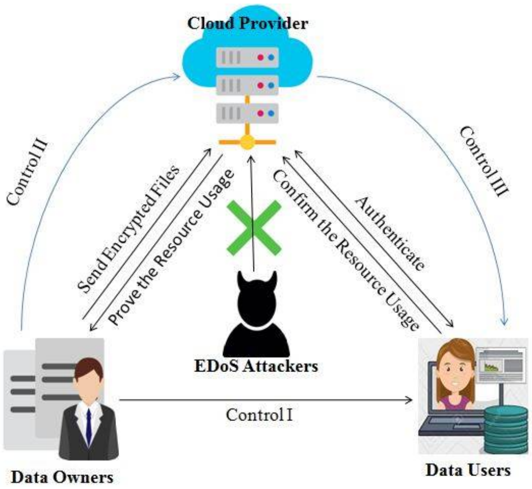


Fig 1: System Architecture

VII. Advantages

- Improving information privacy in cloud storage conditions while improving powerful sharing between clients.
- Indeed, the proposed security components ought to guarantee both robustness and efficiency, specifically the help of adaptable access control, productive client repudiation and performances.
- Addressing the issue of provable information ownership in cloud storage conditions for information honesty confirmation support, following three generous viewpoints: security level, open undeniable nature, and execution, and thinking about the limited storage and processing capacities of client devices.

VIII. Limitations

- One attack that is originated from this limitation is Distributed Denial of Services (DDoS). The power of DDoS attacks has been showed to incur significant resource consumption in CPU, memory, I/O, and network. The attacks can exist in public clouds.
- In the limitation of cloud-side static resource allocation model is analyzed, including the risk of Economic Denial of Sustainability (EDoS) attacks, which is the case of DDoS attacks in the cloud setting in, or the Fraudulent Resource Consumption (FRC) attack in.
- Despite a sizable research effort in searchable encryption, all current schemes have severe limitations.
- Several schemes do not support modifications to data once it is indexed.
- Another limitation is that no existing scheme supports the scenario of Owner-side and Cloud-side.

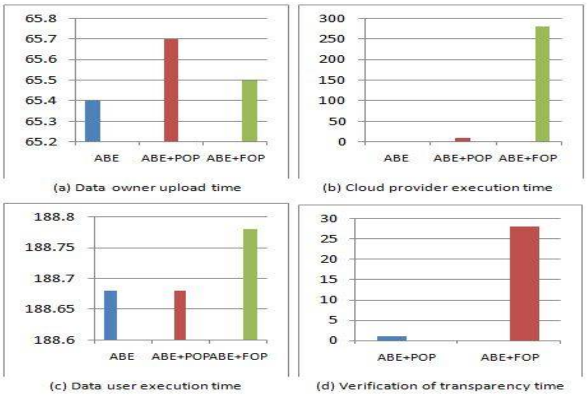
IX. Result

The trial result regarding calculation overhead is given in Fig. 2(a), 2(b), 2(c), and 2(d). Since the CP-ABE has bi-linear blending, the encryption and the decryption costs 64ms and 188ms in our test, respectively. The overhead of our development over CP-ABE is from:

- The encryption and hash for producing N = 1000 difficulties and making the bloom filter BL in POP;
- The key generation, signature, and verification from ECDSA in FOP.

For the calculation the record (as shown in Fig. 2(a)), POP and FOP has 0.3ms and 0.1ms extra execution time, separately. The expansion is little contrasted and the first ABE (with owner’s signature), as is h0.5% in Fig. 2 (a).

For the calculation overhead, when the cloud provide confirms a data user (as appeared in Fig. 2(b)), POP and FOP brings an extra overhead, 0.03μs and 279.06μs, separately. At the point when an approved data user recovers a record (as appeared in Fig. 2(c)), the data user needs to illuminate the cloud gives test. The test decryption should be possible inside a few symmetric encryptions and hashing, which is effective both in POP and FOP. For the asset utilization accounting (as appeared in Fig. 2(d)), the season of check is under 100ms, for confirming an aggregate of ± ≤1000 difficulties. This is just essential when the data owner who needs to account the asset utilization.



(a) Data owner upload time

(b) Cloud provider execution time

(c) Data user execution time

(d) Verification of transparency time

Fig 2: Data owner upload time Performance analysis of the computation cost with the illustration the communication under attacks

X. Conclusion

In this paper, we propose a combined the cloud-side and data owner-side access control in encrypted cloud storage, which is resistant to DDoS/EDoS attacks and provides resource consumption accounting. Our system supports arbitrary CP-ABE constructions. The construction is secure against malicious data users and a covert cloud provider. We relax the security requirement of the cloud provider to covert adversaries, which is a more practical and relaxed notion than that with semi-honest adversaries. To make use of the covert security, we use bloom filter and probabilistic check in the resource consumption accounting to reduce the overhead. Performance analysis shows that the overhead of our construction is small over existing systems.

XI. Future Scope

Security algorithms mentioned for encryption and decryption can be implemented in future to enhance security framework over the network. In the future, I will try to develop algorithm to make advancement to my research by providing algorithm for encryption, decryption and batch auditing to provide authentication.

References

1. Jianan Hong, KaipingXue, YingjieXue, Weikeng Chen, David S.L. Wei, Nenghai Yu and Peilin Hong, "TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud", IEEE Transactions on Services Computing, 2016.
2. Zhangjie, Fu Lili Xia, Xingming Sun, Alex X. Liu, GuowuXie, "Semantic aware Searching over Encrypted Data for Cloud Computing", IEEE Transactions on Information Forensics and Security, 2018.
3. Dr. D. I. George Amalarethinam, B. FathimaMary, "Data Security Enhancement in Public Cloud Storage using Data Obfuscation and Steganography", IEEE, World Congress on Computing and Communication Technologies (WCCCT), 2017.
4. KaipingXue,YingjieXue, "RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage", IEEE Transactions on Information Forensics and Security, 2016.
5. Shengshan Hu, Qian Wang, Jingjun Wang, Zhan Qin, KuiRen, "Securing SIFT: Privacy-preserving Outsourcing Computation of Feature Extractions over Encrypted Image Data", IEEE Transactions on Image Processing, 2016.
6. DongmahnSeo, Suhyun Kim, and Gyuwon Song, "Mutual Exclusion Method in Client-Side Aggregation of Cloud Storage", IEEE Transactions on Consumer Electronics, 2017.