International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

# COPY RIGHT



IJIEMR Transactions, online available on 30th June 2020. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-06

Title: **EFFICIENT TWO SIDED ACCESS CONTROL SYSTEM IN CLOUD STORAGE**

Volume 09, Issue 06, Pages: 158-163

Paper Authors

**LINGUTLA HARSHINI, S.SUNITHA**


USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

# EFFICIENT TWO SIDED ACCESS CONTROL SYSTEM IN CLOUD STORAGE

**LINGUTLA HARSHINI, S.SUNITHA**
PG SCHOLAR.DEPT OF CSE, SIR C.V. RAMAN INSTITUTE OF TECHNOLOGY & SCIENCE, AP, INDIA
ASSOCIATE PROFESSOR, DEPT OF CSE, SIR C.V. RAMAN INSTITUTE OF TECHNOLOGY & SCIENCE,, AP, INDIA

**Abstract:** People endorse the great power of cloud computing, but cannot entirely trust the cloud suppliers to host privacy sensitive information, because of the absence of user-to-cloud controllability. to form certain confidentiality, information owners supply encrypted information instead of plaintexts. To share the encrypted files with different users, Ciphertext-Policy Attribute based secret writing (CP-ABE) is also accustomed conduct fine-grained and owner-centric access management. but this does not sufficiently become secure against different attacks. many previous schemes did not grant the cloud provider the ability to verify whether or not or not a downloader can decipher. Therefore, these files have to be compelled to get on the market to everyone accessible to the cloud storage. A malicious wrongdoer can transfer thousands of files to launch Economic Denial of property (EDoS) attacks, that is ready to principally consume the cloud resource. The money dealer of the cloud service bears the expense. Besides, the cloud provider serves every as a result of the capitalist and conjointly the recipient of resource consumption fee, lacking the transparency to information owners. These issues have to be compelled to be resolved in real-world public cloud storage. throughout this paper, we tend to tend to propose a solution to secure encrypted cloud storages from EDoS attacks and provide resource consumption answerability. It uses CP-ABE schemes in associate degree passing black-box manner and complies with impulsive access policy of CP-ABE. we tend to tend to gift two protocols for varied settings, followed by performance and security analysis.

## 1. INTRODUCTION

CLOUD storage has many benefits, such as always-online, pay-as-you-go, and cheap [1]. During these years, more data are outsourced to public cloud for persistent storage, including personal and business documents.It bring sasecurity concern to data owners [2]–[4]: the public cloud is not trusted, and the outsourced data should not be leaked to the cloud provider without the permission from data owners. Many storage systems use server-dominated access control, like password-based [5] and certificate-based authentication [6]. They overly trust the cloud provider to protect their sensitive data. The cloud providers and their employees can read any document regardless of data owners' access policy. Besides, the cloud provider can exaggerate the resource consumption of the file storage and charge the payers more without providing verifiable records [2], [7], [8],

since we lack a system for verifiable computation of the resource usage.Relying on the existing server-dominated access control is not secure. Data owners who store files on cloud servers still want to control the access on their own hands and keep the data confidential against the cloud provider and malicious users. Encryption is not sufficient. To add the confidentiality guarantee, data owners can encrypt the files and set an access policy so that only qualified users can decrypt the document. With Ciphertext-Policy Attribute-based Encryption (CP-ABE) [9], [10], we can have both fine-grained access control and strong confidentiality [11]–[16]. However, this access control is only available for data owners, which turns out to be insufficient. If the cloud provider cannot authenticate users before downloading, like in many existing CP-ABE cloud storage systems [14], [15], the cloud has to allow everyone to download to ensure availability. This makes the storage system vulnerable to the resource-exhaustion attacks. If we resolve this problem by having data owners authenticate the downloaders before allowing them to download, we lose the flexibility of access control from CP-ABE. Here lists the two problems should be addressed in our work: Problem I: resource-exhaustion attack. If the cloud cannot do cloud-side access control, it has to allow anyone, including malicious attackers, to freely download, although only some users can decrypt. The server is vulnerable to resource-exhaustion attacks. When malicious users launch the DoS/DDoS attacks to the cloud storage, the resource consumption will increase. Payers (in pay-as-you-go model) have to pay for the in creased consumption contributed by those attacks, which is a considerable an un reason able financial burden. The attack has been introduced as Economic Denial of Sustainability (EDoS) [17]–[20], which means payers are financially attacked eventually. In addition, even files are encrypted, unauthorized downloads can reduce security by bringing convenience to to offline analysis and leaking information like file length or update frequency. Problem II: resource consumption accountability. In the pay-as-you-go model, users pay money to the cloud provider for storage services. The fee is decided by resource usage. However, CP-ABE based schemes for cloud storage access control does not make online confirmations to the data owner before downloads.It is needed for the cloud service provider to prove to the payers about the actual resource usage.

## 2. LITERATURE SURVEY

[1] TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud

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 cipher text 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 users at different time, according to a well-defined access policy over attributes and release time. We further studied 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.

[2] "Semantic aware Searching over Encrypted Data for Cloud Computing"

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] "Data Security Enhancement in Public Cloud Storage using Data Obfuscation and Steganography"

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.

[4] "RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage"

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

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

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.

## 3.EXISTING SYSTEM

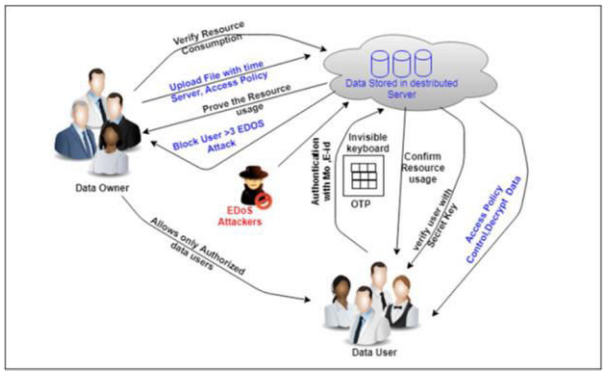
Some existing works try to mitigate EDoS attacks. In the authors proposed a mitigation technique by verifying whether a request comes from a cloud user or is generated by bots. The authors proposed an attribute based way to identify malicious clients. They treat the underlying application in a black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

## 4. 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.

## 5. ARCHITECTURE




## 6.IMPLEMENTATION

Data Owners

Data owners are the owner and publisher of files and pay for the resource consumption on file sharing. As the payers for cloud services, the data owners want the transparency of resource consumption to ensure fair billing. The data owners require the cloud provider to justify the resource usage. In our system, the data owner is not always online.

Data Users

Data users want to obtain some files from the cloud provider stored on the cloud storage. They need to be authenticated by the cloud provider before the download (to thwart EDoS attacks). The authorized users then confirm (and sign for) the resource

consumption for this download to the cloud provider.

Cloud Server

Cloud provider hosts the encrypted storage and is always online. It records the resource consumption and charges data owners based on that record. The cloud is not public-accessible in our system as it has an authentication based access control. Only data users satisfying the access policy can download the corresponding files. The cloud provider also collects the proof of the resource consumption to justify the billing.

## 7.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.

## 8.FUTURE WORK

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] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," Journal of Internet Services and Applications, vol. 1, no. 1, pp. 7–18, 2010.

[2] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, no. 1, pp. 69–73, 2012.

[3] L. Zhou, Y. Zhu, and A. Castiglione, "Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner," Computers & Security, vol. 69, pp. 84–96, 2017.

[4] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, "Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data," IEEE Transactions on Image Processing, vol. 25, no. 7, pp. 3411–3425, 2016.

[5] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 651–663, 2012.

[6] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," IEEE Transactions on Wireless Communications, vol. 10, no. 7, pp. 2372–2379, 2011.

[7] V. Sekar and P. Maniatis, "Verifiable

resource accounting for cloud computing services," in Proceedings of the 3rd ACM workshop on Cloud computing security workshop. ACM, 2011, pp. 21–26.

[8] C. Chen, P. Maniatis, A. Perrig, A. Vasudevan, and V. Sekar, "Towards verifiable resource accounting for outsourced computation," in ACM SIGPLAN Notices, vol. 48, no. 7. ACM, 2013, pp. 167–178.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in 2007 IEEE Symposium on Security and Privacy (SP'07). IEEE, 2007, pp. 321–334.

[10] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography– PKC 2011. Springer, 2011, pp. 53–70.

[11] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013.

[12] S. Yu, K. Ren, and W. Lou, "Attribute-based content distribution with hidden policy," in Proceedings of 4th Workshop on Secure Network Protocols (NPSec2008). IEEE, 2008, pp. 39–44.