International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 2, Mar-Apr-2019, ISSN (Online): 2395-566X

Data Sharing With CP-ABE to Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage

M.Tech. Scholar Diguvasadum Deepika
Dept. of Computer Science & Engg.
MJR College of Engg. & Technology
Piler, AP, India

Asst. Prof. G.Varaprasad
Dept. of Computer Science & Engg.
MJR College of Engg. & Technology
Piler, AP, India

Asst. Prof. Karamala Suresh
Dept. of Computer Science & Engg.
MJR College of Engg. & Technology
Piler, AP, India.

***Abstract*- People support the great power of cloud computing, but cannot completely trust the cloud providers to host privacy-sensitive information, due to absence of user-to-cloud controllability. To ensure confidentiality, data owners outsource encrypted data instead of plaintexts. To distribute the encrypted files with other users, Ciphertext-Policy Attribute-based Encryption (CP-ABE) can be utilized to carry out fine-grained and owner-centric access control. But this does not adequately become make safe against other attacks. Many earlier schemes did not grant the cloud providers potential to verify whether a downloader can decrypt. Therefore, these files have to be available to everyone accessible to the cloud storage. A malicious attacker can download thousands of files to launch Economic Denial of Sustainability (EDoS) attacks, which will mostly consume the cloud resource. The customer 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 two protocols for different settings, followed by performance and security analysis.**

***Keywords* - Cipher text-Policy Attribute-based Encryption (CP-ABE), access control, public cloud storage, accounting, privacy-preserving.**

I. 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 brings a security 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 excessively 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.

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 Cipher text-Policy Attribute-based Encryption (CP-ABE), we can have both fine-grained access control and strong confidentiality. However, this access control is only available for data owners, which turn out to be insufficient. If the cloud provider cannot authenticate users before downloading, like in many existing CP-ABE cloud storage systems, 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 downloader's 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 accomplish 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.

Problem II: resource consumption accountability. In the pay-as-you-go model, users pay money to the cloud provider for storage services. The payment 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 download. It is needed for the cloud service provider to prove to the payers about the actual resource usage. Otherwise, the

© 2019 IJSRET

cloud provider can charge more without being discovered.

1. CP-ABE- Cipher text-Policy Attribute-based-Encryption

CP-ABE is a public key encryption scheme with fine-grained access control. In CP-ABE, each user has some attributes and data owners encrypt their files with an access policy over attributes. Users in the system hold their own secret keys associated with their attribute sets. If and only if the user satisfies the access policy, the user can decrypt.

2. Authenticated Encryption with Associated Data

Authenticated Encryption with Associated Data (AEAD) is a symmetric-key encryption that provides both confidentiality and integrity. The security and correctness of the two constructions are the same. But the latter has a benefit in performance the CP-ABE encryption and decryption, which rely on heavy pairing, are reduced to one. The two pieces of the AEAD encrypted messages can still be sent in arbitrary order.

3. Digital Signature

The system uses a public-key signature scheme for message integrity. Assumed the secure distribution of public keys, any data recipient can verify the message integrity. For succinct- ness of signatures, we can use ECDSA. When a readjustment is needed, both the Sink and the sensor calculate the error between the real transmitted measurement and the last prediction that exceeded exam and triggered the transmission.

II. GOALS & OBJECTIVES

1. 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.

2. 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.

III. LITERATURE SURVEY

Cong wang ,member of IEE-the security in cloud sharing in this study enabling public audit ability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user.

Wenjing lou senior member of IEE- the security in cloud storage in this study provides flexible distributed storage integrity auditing mechanism, utilizing the homomorphism token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server.

Devi Parvathy Mohan, Gnanamani college of engineering- this study provides a traditional approach developed a dynamic audit service for verifying the integrity of an un trusted and outsourced storage. An audit service is constructed based on the techniques, fragment structure, random sampling, and index-hash table, supporting provable updates to outsourced data and timely anomaly detection. The method based on probabilistic query and periodic verification for improving the performance of audit services. The audit service is performed by TPA monitoring.

Priya J. Khindre, Matoshri Pratishthan Group of Institutions, this study proposed an essential security requirement that can be attained by combining both the cryptographic cloud storage along with searchable encryption scheme. In cloud system overall cost of data storage is less as it does not require managing and maintaining expensive hardware. In which data owners firstly encrypt all data before storing on a cloud in such way that only user whom having decryption keys can be decrypt or fetch the data.

IV. EXISTING SYSTEM

Cloud storage has many benefits, such as always-online, pay-as-you-go, and cheap. During these years, more data are outsourced to public cloud for persistent storage, including personal and business documents. It brings a security concern to data owners: 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 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 owners' access policy. Besides, the cloud provider can

© 2019 IJSRET

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. 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.

V. PROPOSED SYSTEM

We combine the cloud-side access control and the existing data owner-side CP-ABE based access control, to resolve the aforementioned security problems in privacy- preserving cloud storage. Our method can prevent the EDoS attacks by providing the cloud server with the ability to check whether the user is authorized in CP-ABE based scheme, without leaking other information. For our cloud-side access control, we use CP-ABE encryption/decryption game as challenge-response.

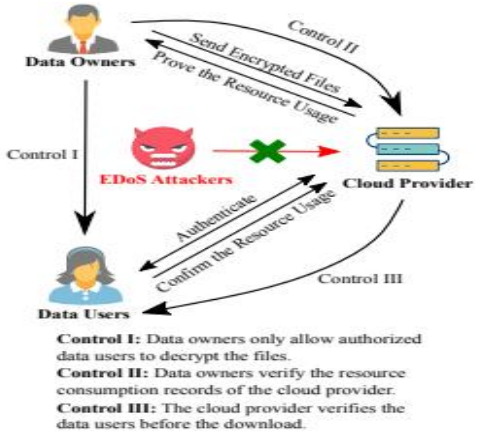

Fig.1 System model of the encrypted cloud storage with mitigation of EDoS attacks and transparency of resource consumption accounting.

while upload an encrypted file, the data owner firstly generates some random challenge plaintexts and the corresponding cipher texts. The cipher texts are related to the same access policy with the specific file. For an incoming data user, the cloud server asks him/her to decrypt randomly selected challenge cipher text. If the user shows a correct result, which means he/she is authorized in CP-ABE, the cloud-side access control allows the file download.

VI. 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.

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, "Cipher text-policy attribute based 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.

Author's Profile

Diguvasadum Deepika Pursuing M.Tech at MJR College of Engineering & Technology, Department of CSE, Piler, Chittoor Dist.

Varaprasad Gajjala Working as a Assistant Professor in MJR College Of Engineering And Technology, Piler, A.P. and he obtained Graduation Degree in Computer Science and Engineering from JNTUA university in 2012, and obtained his Master's degree in 2014 specialized in Artificial Intelligence under Department of Computer Science & Engineering JNTUA college of Engineering, Anantapuramu, India. He made robot based on Artificial Intelligence while pursuing Master's. His research interest includes Web Designing, Information Security, Image Processing, Natural Language Processing, Robotics, and Artificial Intelligence, **Email:**gajjala.varaprasad@gmail.com.

Karamala Suresh Working as a Head of the Department in MJR College Of Engineering & Technology, Department Of CSE, Piler, Chittoor dist. He is having 14 years of teaching experience in engineering colleges, he received B.Tech (CSE) from JNTU Hyderabad in 2002,Received M.E(CSE) from satyabama university Chennai in 2006, and Received M.Tech(CSE) in 2015 from JNTU Anantapuramu, he published several research papers in various national and international journals. He is interested in Computer Networks.