Cloud-based data storage and sharing with dual access Control

Dr. D. Bujji Babu[1], Mr. K. Jaya Krishna[2], Miss. Abburi Jaya Sree[3], Miss. Bikkam Venkata Prasanti [4], Miss. Deevi Srivalli[5], Miss. Kurnool Sahithi[6]

[1], Professor, [2] Asst.Professor, [3,4,5,6] PG. Scholars
Department of MCA, QIS College of Engineering & Technology (Autonomous) Ongole, AP, India.

Abstract:
Due to its effective and affordable administration, cloud-based data storage has recently attracted growing attention from academia and business. Since services are delivered via an open network, it is critical for service providers to adopt secure data storage and sharing mechanisms to protect user privacy and the confidentiality of data. The most popular technique for preventing the compromise of sensitive data is encryption. The actual necessity for data management, however, cannot be completely met by just encrypting data (for instance, using AES). Additionally, a strong access control over download requests must be taken into account to prevent Economic Denial of Sustainability (EDoS) assaults from being performed to prevent users from using the service. This study takes into account dual access control in the context of cloud-based storage in the sense that we create a control mechanism over both data access and download requests without sacrificing security and effectiveness. This article presents the design of two dual access control systems, one for each intended environment. There is also a presentation of the systems' experimental and security analyses.

1. INTRODUCTION

Utilizing computer resources that are offered as a service across a network is the basis of cloud computing technology. Users must provide access to their data in the cloud computing paradigm in order to store and carry out the necessary business processes. Since there is a vast quantity of sensitive and important data kept in the clouds, the cloud service provider must provide trust and security. There are issues with the scalability, flexibility, and fine-grainedness of access control in cloud computing. Numerous encryption techniques have been developed for this purpose. like a straightforward encryption method that has been traditionally examined. The Attribute-Based Encryption (ABE) schemes will be discussed, along with how they have been further improved and adapted into Key Policy Attribute based encryption (KP-ABE) and Cipher-text Policy Attribute based encryption (CP-ABE). A frequent exploit known as a resource-exhaustion attack occurs in cloud-based storage services. Since a (public) cloud may not have any control over download requests, a malicious service user may execute DoS/DDoS attacks to deplete the server's resources, preventing the cloud service from responding to legitimate users' service requests. Due to increased resource demand, the "pay-as-you-go" approach runs the risk of upsetting the economy. As a result of the assaults, cloud service prices will skyrocket. In this project, we emphasise document security and dual access control to protect the papers from administrators. We suggested a multi-cloud document storage system in which documents would be kept on application clouds and their details would be saved on key management servers in order to increase the security of documents stored in the cloud. A cloud administrator won't be able to decode any documents since the key management server only has the document metadata in encrypted format and the application server will have encrypted documents. As a result, the documents will stay safe. Along with the AES method, we suggested the modified CP-ABE approach for safe document encryption. We suggested an identity key verification mechanism for dual access control.

Economic denial of sustainability (EDoS)

- A new threat to cloud computing is economic denial of sustainability (EDoS). EDoS attackers repeatedly submit requests to access cloud services like decryption, encryption, database access, etc., which may increase the cost of cloud resources for specific users whose accounts have been compromised. This assault is very hazardous, thus it has to be stopped by adding certain security elements to the cloud. As a result, we include an identity key verification approach in our proposed system. We may verify the requester's identity, reliability, and authorization using the identity key verification approach.

2. LITERATURE REVIEW

ABE [1] has been presented in the literature to implement fine-grained policy-based control over encrypted data.

ABE specifically has two primary research branches: CP-ABE and KP-ABE, also known as key policy ABE. The first is the major topic of this essay. In a CP-ABE, encrypted text is incorporated with the access policy and the decryption key is linked to the attribute set. Because of this characteristic, CP-ABE is a great choice for secure cloud data exchange (compared to KP-ABE). Note that this is the case because KP-ABE mandates that the decryption key be linked to the access policy, which results in high storage costs for cloud users. Numerous publications have suggested using CP-ABE in a variety of applications since the introduction of the original CP-ABE [1], including responsible and traceable CP-ABE [5], multi-authority[2], outsourced CP-ABE[15], and expandable variations.

 Even though it can allow fine-grained data access, CP-ABE operating as a standalone solution is unable to effectively fend off an EDoS assault, which is what happens when DDoS occurs in a cloud environment [3], [8].

In the literature, a number of defences to the assault [4], [6] have been suggested. But according to Xue et al. [7], the prior works could not completely protect against the EDoS attack at the algorithmic (or protocol) level, and they further suggested a strategy to safeguard cloud data sharing from the assault. Nevertheless, [7] has two drawbacks.

3. SYSTEM DESIGN

3.1 EXISTING SYSTEM

Although CP-ABE can provide fine-grained data access, it is neither practicable or effective to defend against EDoS attacks, which is the situation when DDoS occurs in a cloud environment. The literature has suggested a number of defences against the onslaught. However, Xue et al. claimed that the prior works could not completely protect against the EDoS attack at the algorithmic (or protocol) level, and they further provided a remedy to secure cloud data sharing from the assault.

Nevertheless, it has two drawbacks. To defend against the attack, the data owner must first create a series of challenge ciphertexts, which adds to the computing work necessary. Second, as a test, a data user must decode one of the challenge ciphertexts, which requires several costly operations (e.g., pairing). Here, both sides' computing complexity necessarily rises, and in addition, ciphertext transmission necessitates a large amount of network capacity. The significant computing capacity of the cloud is not completely taken into account in. In this work, we will outline a novel method for halting an EDoS assault that uses minimal compute and communication resources.

A data sharing protocol that combines symmetric searchable encryption with ABE, enabling users to directly search through encrypted data, was recently suggested by Antonis Michalas. The

protocol makes use of SGX to host a revocation authority in order to provide key revocation capability in ABE. Later, Bakas and Michalas expanded the protocol and introduced a hybrid encryption method that simplifies the issue of data sharing across several users to that of a single user. In particular, the ABE-encrypted SGX enclave contains the symmetric key that is used to encrypt data. Similar to, it uses the SGX enclave to address the revocation issue in the context of ABE. In this study, we use SGX to provide download request control (so that DDoS/EDoS assaults may be avoided). In this regard, our methodology and goal vary from those of the procedures in.

3.2 PROPOSED SYSTEM

In this research, we provide a novel dual access control system to address the two issues described above. Attribute-based encryption (ABE), which permits the secrecy of outsourced data as well as fine-grained control over the outsourced data, is one of the potential contenders for securing data in cloud-based storage services.

Particularly, Ciphertext-Policy ABE (CP-ABE) offers a reliable method of data encryption that enables the specification of access rules, which specify the access privilege of prospective data receivers, over encrypted data. Please take note that in this research, we examine the usage of CP-ABE in our method. However, using the CP-ABE approach alone is insufficient to create a sophisticated system that ensures the control of both data access and download requests.

Dummy ciphertexts may be used to check the permissions of the data recipient to decode data as a crude solution to the control of download requests. The "testing" ciphertexts, which are the encryptions of fictitious communications subject to the same access policy as the "real" data, must be uploaded to the cloud by the data owner, say Alice, with the "actual" encryption of the data. When a user, let's say Bob, requests a download, the cloud responds by asking Bob to decode a random "testing" ciphertext. If a proper result or decryption is given (showing that Bob has legitimate decryption privileges), Alice has given Bob permission to access the "actual" data, allowing Bob to download the associated ciphertext from the cloud.

4. SYSTEM ARCHITECTURE

Flow CHART

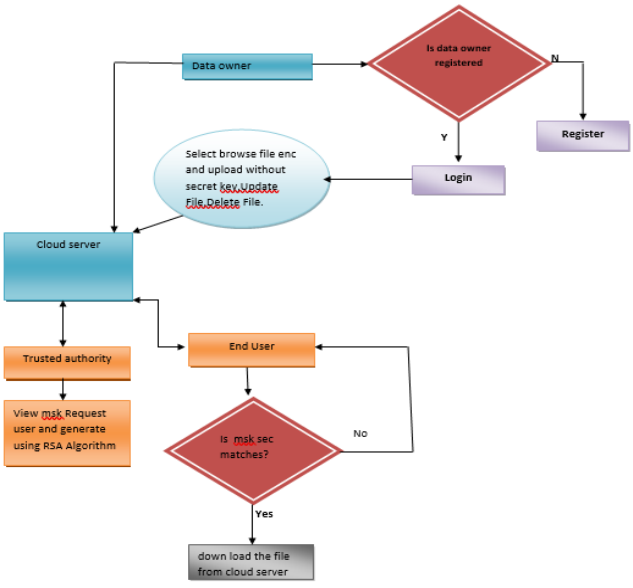

Fig4.1 Flow chart

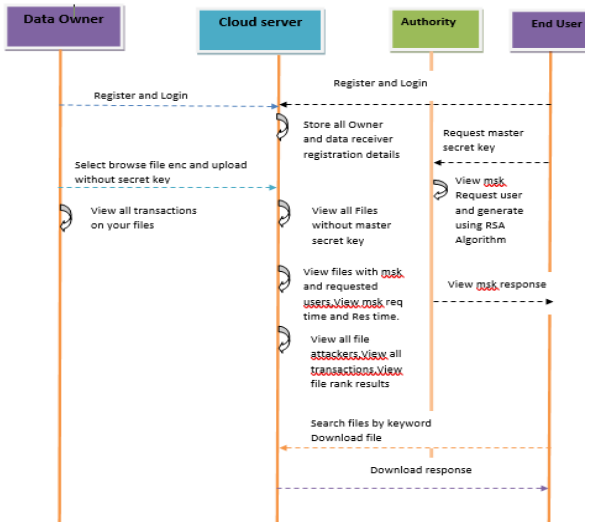

Fig4.2: Sequence diagram

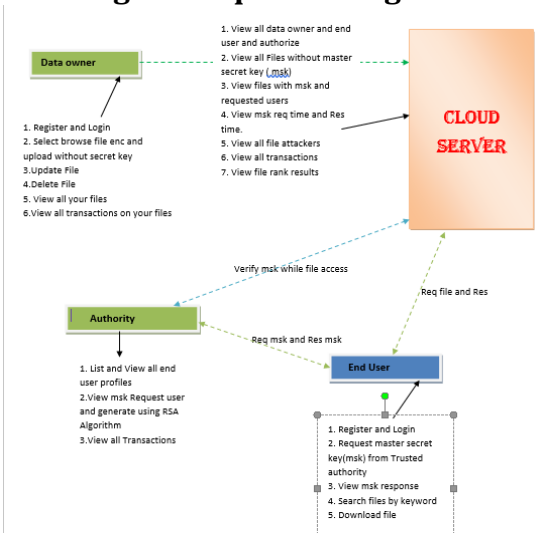

Fig 4.3: System architecture

5.RESULTS:

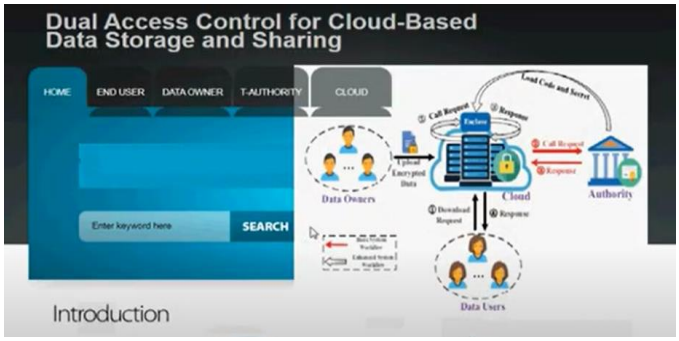

Fig 5.1: Home

Fig 5.2: Cloud login

Fig 5.3: Trusted authority login

Fig 5.4: Welcome authority

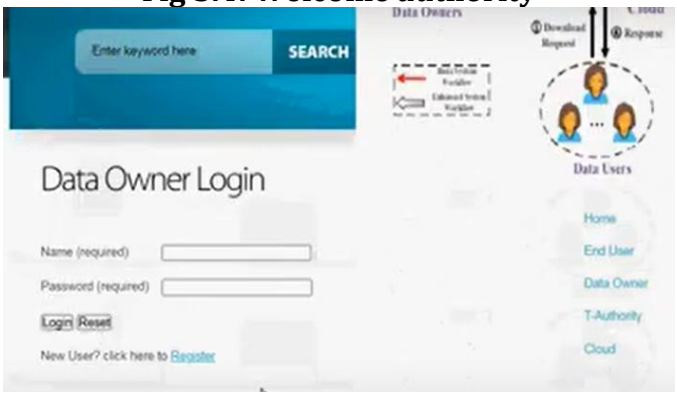

Fig 5.5: Data Owner login

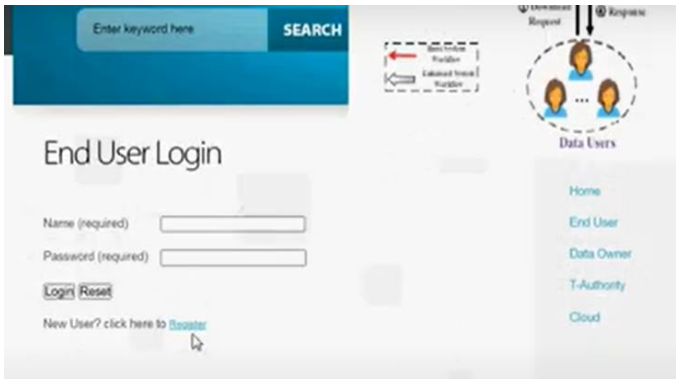

Fig 5.6: End User Login

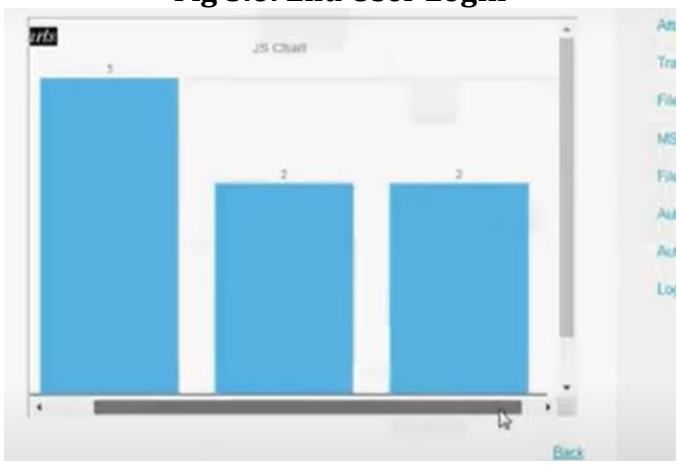

Fig 5.7: Results

CONCLUSION

We showed two dual access control systems and addressed an intriguing and pervasive issue with cloud-based data sharing. DDoS/EDoS assaults cannot be used against the suggested systems. We claim that different CP-ABE constructions may "transplant" the method utilised to accomplish the feature of control on download request. The suggested solutions don't incur a large computational or communication overhead, according to the findings of our experiments (compared to its underlying CP-ABE building block). We take use of the fact that the secret information entered into the enclave cannot be recovered in our improved system. The memory access patterns [37] or other comparable side-channel attacks [14], [30] reveal that enclave may, nevertheless, leak part of its secret(s) to a hostile host. Thus, [35] introduces the transparent enclave execution approach. An intriguing challenge is creating a dual access control scheme for cloud data sharing from a transparent enclave. We'll take into account the relevant problem-solving approach in our next work.

REFERENCES

[1] Joseph A Akinyele, Christina Garman, Ian Miers, Matthew W Pagano, Michael Rushanan, Matthew Green, and Aviel D Rubin. Charm: a framework for rapidly prototyping cryptosystems. Journal of Cryptographic Engineering, 3(2):111–128, 2013.

[2] Ittai Anati, Shay Gueron, Simon Johnson, and Vincent Scarlata. Innovative technology for cpu based attestation and sealing. In Workshop on hardware and architectural support for security and privacy (HASP), volume 13, page 7. ACM New York, NY, USA, 2013.

[3] 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.
[4] Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
[5] John Bethencourt, Amit Sahai, and BrentWaters. Ciphertext-policy attribute-based encryption. In S&P 2007, pages 321–334. IEEE, 2007.
[6] Victor Costan and Srinivas Devadas. Intel sgx explained. IACR Cryptology ePrint Archive, 2016(086):1–118, 2016.
[7] Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, and Sergey Gorbunov. IRON: functional encryption using intel SGX. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, pages 765 782, 2017.
[8] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Advances in Cryptology-CRYPTO 1999, pages 537–554. Springer, 1999.