International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Providing Efficient Cloud Resources Using Dual Access Control Mechanism

A. Vinitha

M.Tech. Scholar, Department of Computer Science and Engineering, Ananthalakshmi Institute of Technology and Sciences, Andhra Pradesh, India

ABSTRACT

AWS Cloud-based data storage service has drawn increasing interests from both academic and industry within the recent years thanks to its efficient and low-cost management. It provides services in an open network it's urgent for service providers to form use of secure data storage and sharing mechanism to confirm data confidentiality and repair user privacy. To guard sensitive data from being compromised, the foremost widely used method is encryption. Two dual access control systems are designed during this project, where each of them is for a definite designed setting. The safety and experimental analysis for the systems are presented. A replacement mechanism, dubbed dual access control, to tackle the above aforementioned two problems. To secure data in cloud- based storage service, attribute-based encryption (ABE) is one in every of the promising candidates that allows the confidentiality of outsourced data further as fine-grained control over the outsourced data

Keywords: Attribute based encryption, Amazon web Services, Encryption, and Cloud based data sharing

INTRODUCTION

In the recent decades, cloud-based storage service has attracted considerable attention from both academia and industries. It'sgoing to be widely employed in many Internet-based commercial applications (e.g., Apple could) thanks to its long-list benefits including access flexibility and free from of local data management. Increasing number of people and corporations nowadays opt to outsource their data to remote cloud in such how that they will reduce the value of upgrading their local data management facilities/devices. However, the concern of security breach over outsourced data is also one amongst the most obstacles hindering Internet users from widely using cloud-based storage services.

LITERATURE SURVEY

1. Alexandros Bakas, AntonisMichalas:

We have seen some interesting approaches that are based either on the promising concept of Symmetric Searchable Encryption (SSE) and the well-studied field of Attribute-Based Encryption (ABE). A revocation mechanism is implemented on the functionality offered by SGX (SoftWare Guard Extensions).

2. Antonis Michalas:

In olden days the data is maintain in files and begin shared among people by this data is at un- protected and the time for writing the files will take the more so. They implement the cloud service provider to

overcome the problems. They implemented the symmetric searchable encryption in this we can internally and externally we exchange the data

3. P. Han, H. Pan:

Two layered encryption scheme which is combination of identity-based encryption & public key encryption is simply called as IDcrypt.This is used for sharing the secrete -key among users. It's also provided security to the sensitive data from miss leading during encryption

4. JiananHong, PeilinHong:

People endorse the good power of cloud computing, but cannot fully trust the cloud providers to host privacy-sensitive data, rather than the absence of user-to-cloud controllability. To make sure confidentiality, data owners outsource encrypted data instead of plaintexts. To share the encrypted files with other users, cipher text-policy attribute-based encryption (CP-ABE) could even be utilized to conduct fine-grained and owner-centric access control.

5. Xiaolei Dong, Kaitai Lian:

As a classy mechanism for secure fine grained access control over encrypted data, cipher text- policy attribute-based encryption (CP-ABE) is one amongst the highly promising candidates for cloud computing applications. However, there exist two main long-lasting open problems of CP- ABE that will limit its wide deployment in commercial applications. One is that decryption yields expensive pairing cost which regularly grows with the rise of access policy size

6. Alexandros Bakas, Antonis Michalas:

The dual access control Mechanism, within the context of cloud-based storage, within the sense that we design an bearing mechanism over both data access and download request without loss of security and efficiency. Two dual access control systems are designed during this project, where each of them is for an actual designed setting. The Protection and experimental analysis for the systems also are presented.

1. PROPOSED SYSTEM

We used a brand-new mechanism, dual access control Mechanism, to tackle the above aforementioned two problems. To secure data in cloudbased storage service, attribute-based encryption is one amongst the promising candidates that allows the confidentiality of out sourced data still as fine-grained control over the outsourced data using AWS cloud.

2. BLOCK DIAGRAM

The block diagram of our dual access control systems for cloud data sharing are shown in fig concretely, the systems consist of the following entities:

Authority:

Authority is responsible for configure the system parameters and data user registration. Also, it handles the call request from the cloud in the first proposed constructions**.**

Data owner:

Data owner holds the information and wants to outsource his information to the cloud. In particular, data owners want to share their information those who satisfy certain conditions. Once they will be offline their data have been uploaded to the cloud.

Data user:

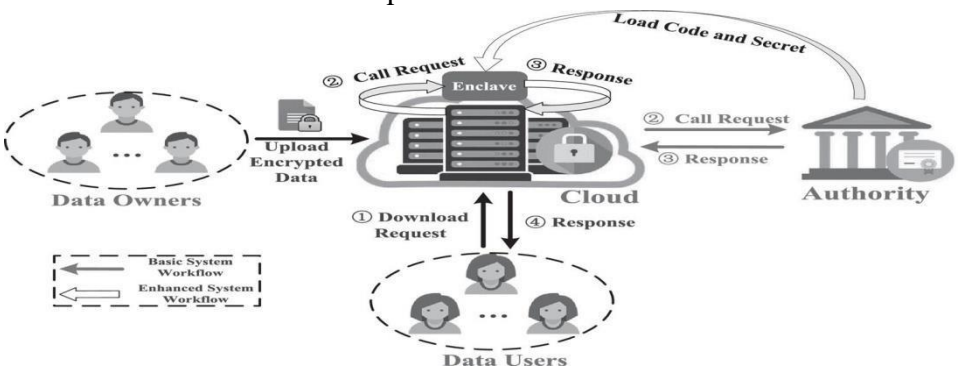
Data owner's wants to download and decrypt the encrypted data shared within the cloud. Thosethat are authorized can download the encrypted file and further decrypt it to access the plaintext.

Cloud:

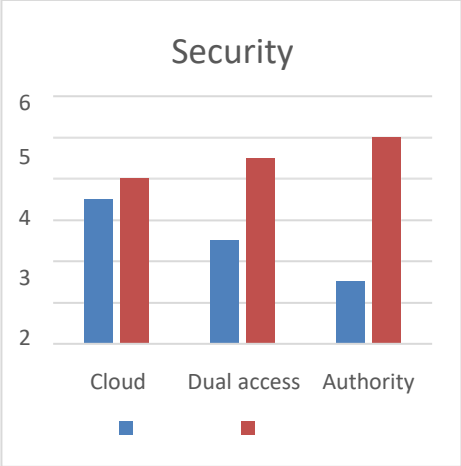
Cloud provides convenient storage service for data owners and data users. Particularly, it stores the outsourced data from data users and handles the download requests sent by data users.

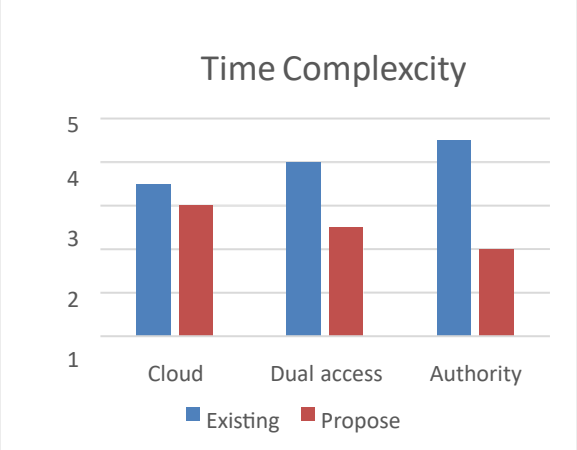
Enclave:

From the cloud Enclaves handles the decision request.



3. PERFORMANCE ANALYSIS





High Security:

At the consideration of cloud security, we offer improvement from the present system security. In side of dual access, we provide a wide range of security from existing system. At the purpose of Authority, we implement safer process for authentication and Authorization it's leads the more changes from existing system.

4. TIME COMPLEXITY

On observing the time taken by the present system for cloud we complete within the less time. Just in case of dual access we improve far better than the present system. By the Authority it's taking less time for authentication because we use the various algorithms in our project.

5. CONCLUSION AND FUTURE WORK

We addressed an motivating and long-lasting problem in cloud-based data sharing, and presented two dual access control systems. The proposed systems are proof against DDoS/EDoS attacks. We state that the technique accustomed achieve the feature of control on download request is “transplantable" to other CP-ABE constructions. Our experimental results show that the proposed systems don't impose any significant computational and communication overhead (compared to its underlying CP-ABE building block). We

utilize the actual key data in our enhanced system that loaded into the enclave cannot be extracted. However, recent work shows that enclave may leak some amount so fits secret(s) to a malicious host through the operation patterns or other related side-channel attacks. The model of transparent enclave execution is hence introduced in. Constructing a dual access system for cloud data sharing from transparent enclave can be a noteworthy problem. In our future work, we are visiting to the corresponding solution to the matter.

References

1. I. Anati, S. Gueron, S. Johnson and V. Scarlata, "Innovative technology for CPU based attestation and sealing", *Proc. Workshop Hardware Architect. Support Secur. Privacy*, 2013.
2. A. Bakas and A. Michalas, "Modern family: A revocable hybrid encryption scheme based on attribute-based encryption symmetric searchable encryption and SGX", *Proc. Int. Conf. Secur. Privacy Commun. Syst.*, pp. 472-486, 2019.
3. J. A. Akinyele et al., "Charm: A framework for rapidly prototyping cryptosystems", *J. Cryptogr. Eng.*, vol. 3, no. 2, pp. 111-128, 2013.
4. J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute-based encryption", *Proc. IEEE Symp. Security Privacy*, pp. 321-334, 2007.
5. B. Fisch, D. Vinayagamurthy, D. Boneh and S. Gorbunov, "IRON: Functional encryption using intel SGX", *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, pp. 765-782, 2017.