Cloud based EDos attack prevention system using dual access control mechanism

Deepa s. Deulkar[1] Vijaya Kamble[2]

1(Currently pursuing masters' degree program in computer science engineering in Guru Nanak Institute of Engineering and Technology Kalmeshwar Road, Dahegaon, Nagpur, Maharashtra,India-441501)

2(Professor,Computer Science and Engineering Department in Guru Nanak Institute of Engineering and Technology kalmeshwar Road, Dahegaon ,Nagpur,Maharashtra,India - 441501)

ABSTRACT

*Cloud based data storage is becoming very popular nowadays as one can easily download any document from anytime and anywhere. However documents security is very important in cloud storage as cloud is a third party server which can be accessed by administrators. There are many literatures available to improve document security on cloud and most of the literatures proposed various data encryption techniques. However, simply encrypting data (e.g., via AES) cannot fully address the practical need of data management. Besides, an effective access control over download request also needs to be considered so that Economic Denial of Sustainability (EDoS) attacks cannot be launched to hinder users from enjoying service. In this project, we consider the dual access control, in the context of cloud-based storage, in the sense that we design a control mechanism over both data access and download request without loss of security and efficiency. Along with dual access control we also focus on document security by using modified AES algorithm***.***

keywords*- cloud-based data sharing, access control, cloud storage service, Intel SGX, attribute-based encryption.*

INTRODUCTION

Cloud computing technology consists of the use of computing resources that are delivered as a service over a network. In cloud computing model users have to give access to their data for storing and performing the desired business operations. Hence cloud service provider must provide the trust and security, as there is valuable and sensitive data in huge amount stored on the clouds. There are concerns about flexible, scalable and fine grained access control in the cloud computing. For this purpose, there have been many of the schemes, proposed for encryption. Such as simple encryption technique that is classically studied. We are going to discuss about the Attribute-Based Encryption (ABE) schemes and how it has been developed and modified further into Key Policy Attribute based encryption (KP-ABE), Cipher-text Policy Attribute Based Encryption (CP-ABE). In a cloud-based storage service, there exists a common attack that is well-known as resource-exhaustion attack. Since a (public) cloud may not have any control over download request, a malicious service user may launch the denial-of-service (DoS)/distributed denial-of-service (DDoS) attacks to consume the resource of cloud storage service server so that the cloud service could not be able to respond honest users' service requests. As a result, in the "pay-as-you-go" model, economic aspects could be disrupted due to higher resource usage. The costs of cloud service users will rise dramatically as the attacks.

In this project we focus on dual access control and document security to secure the documents from administrators. To improve security of the documents store on cloud, we proposed multi-cloud document storage system in which

documents will be stored on application cloud and their details will be stored on key manager server. Key manager server only has the document details in encrypted format and the application server will have encrypted documents therefore the cloud administrator will not be able to decrypt any document and thus the documents will remain secured. We proposed modified CP-ABE technique for secure document encryption along with AES algorithm. For dual access control we proposed identity key verification technique.

Economic denial of sustainability (EDoS)

- Economic denial of sustainability (EDoS) is a new menace in cloud computing, EDoS attackers steadily send request to access cloud resources like decryption, encryption, database access etc. which may scale cloud resource price for particular users whose account has been hacked. It is very dangerous attack and need to prevent by adding some security features in cloud. Therefore in our proposed system, we introduce identity key verification technique. Using identity key verification technique, we will be able to check requester's identity and authenticity and access permission.

LITERATURE REVIEW

- To apply fine-grained policy-based control over encrypted data, ABE [1] has been introduced in the literature. Concretely, ABE has two main research branches: one is CP-ABE, and the other is KP-ABE which refers to as key policy ABE. This paper mainly deals with the former. In a CP-ABE, decryption key is associated with attribute set and cipher text is embedded with access policy. This feature makes CP-ABE quite suitable for secure cloud data sharing (compared to KP-ABE). Note this is so because KP-ABE requires decryption key to be associated with access policy which yields heavy storage cost for cloud user. Since the introduction of seminal CP-ABE [1], many works have been proposed to employ CP-ABE in various applications, e.g., accountable and traceable CP-ABE [5], multi-authority[2],outsourced CP-ABE[15], and extendable variants.
- Although being able to support fine-grained data access, CP-ABE, acting as a single solution, is far from practical and effective to hold against EDoS attack [3] which is the case of DDoS in the cloud setting [3], [8]. Several countermeasures to the attack [4], [6] have been proposed in the literature. But Xue et al. [7] stated that the previous works could not fully defend the EDoS attack in the algorithmic (or protocol) level, and they further proposed a solution to secure cloud data sharing from the attack. However, [7] suffers from two disadvantages.

PROPOSED WORK

Identity key **,**We proposed identity key verification technique for dual access control in which every user will receive unique identity key at the time of registration, if he wants to download any document he have to submit his identity key. System will send that identity key to key manager server automatically; key manager server will verify user's identity with access attributes associated with the document

Modified CP-ABE Technique for Documents encryption

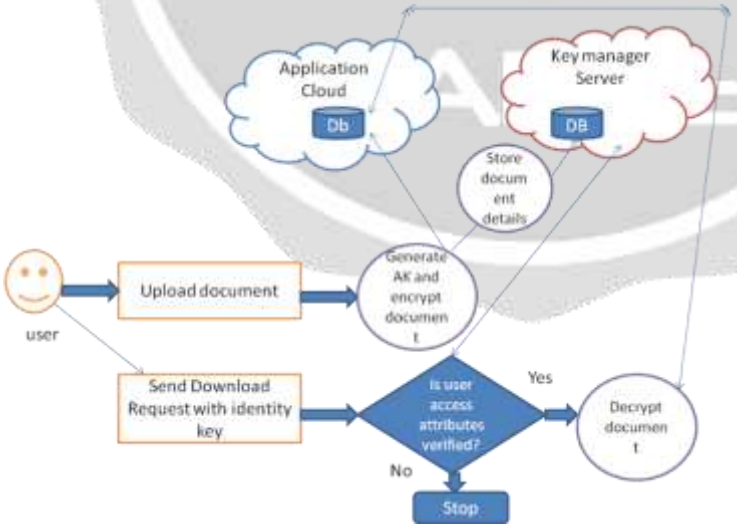
In Attribute Based Encryption scheme both the user secret key and the cipher-text are associated with a set of attributes. A user is able to decrypt the cipher-text if and only if at least a threshold number of attributes overlap between the cipher-text and user secret key. Different from traditional public key cryptography such as Identity-Based Encryption [1], ABE is implemented for one-to many encryption in which cipher-texts are not necessarily encrypted to one particular user, it may be for more than one number of users. In Sahai and Waters ABE scheme, the threshold semantics are not very expressive to be used for designing more general access control system. Attribute-Based Encryption (ABE) in which policies are specified and enforced in the encryption algorithm itself. The existing

ABE schemes are of two types. They are Key-Policy ABE (KP-ABE) scheme and Ciphertext-Policy ABE (CP-ABE) scheme.

Existing CP-ABE depends how attributes and policy are associated with cipher texts and users' decryption keys. In a CP-ABE scheme, a ciphertext is associated with a monotonic tree access structure and a user's decryption key is associated with set of attributes. However, basic CP-ABE schemes are still not fulfilling the enterprise requirements of access control which require considerable flexibility and efficiency. CP-ABE has limitations in specifying policies and managing user attributes. In a CP-ABE scheme, decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies. In CP-ABE, all the attributes are associated with the secrete key and it takes more computation time in case of any changes in attributes. Therefore to improve CP-ABE technique, we proposed attribute key concept. Using attribute key concept, system will generate unique attribute key for every document and the document will be encrypted using attribute key. The user's attributes will be managed in key manager server with reference to attribute key

Modified AES Algorithm

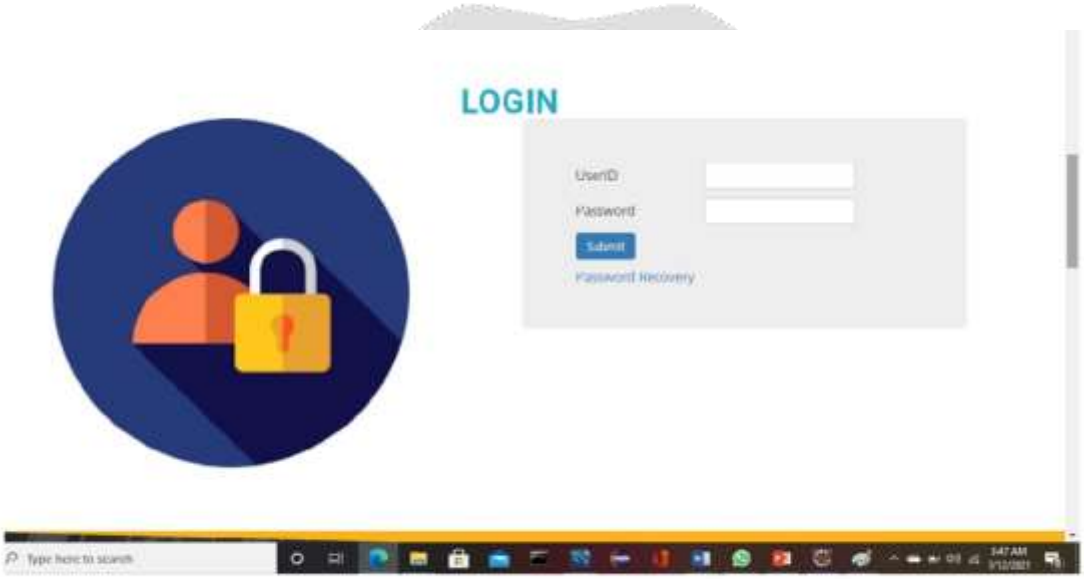
- Read document in byte array in b[]
- Divide b[] into 4 parts
- Shuffle parts b1[] b2[] b[3] and b[4]
- Generate secrete key k1, k2,k3,and k4 using Attribute key AK
- Encrypt each part with different key
- Combine all the parts
- Store encrypted document on cloud server

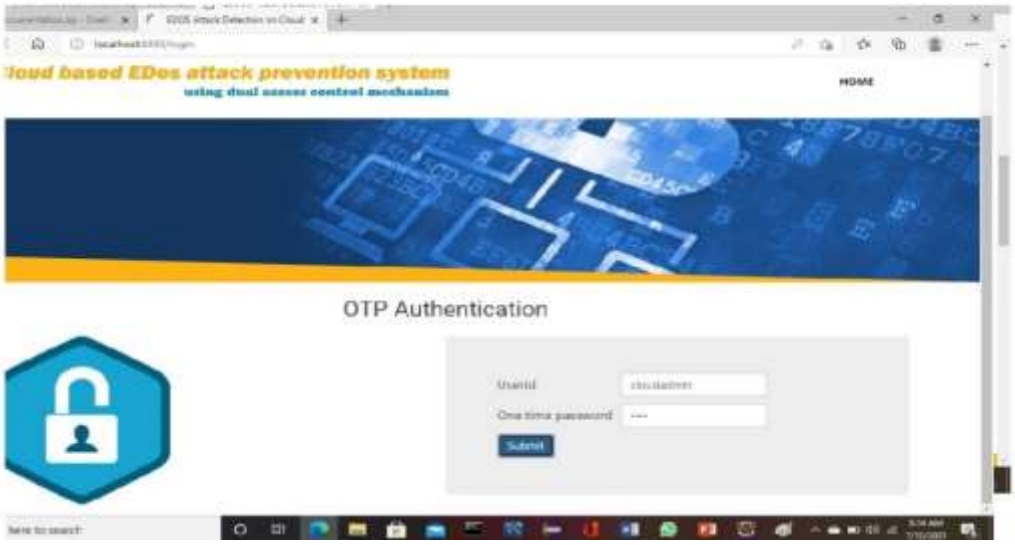


(Fig. 1)

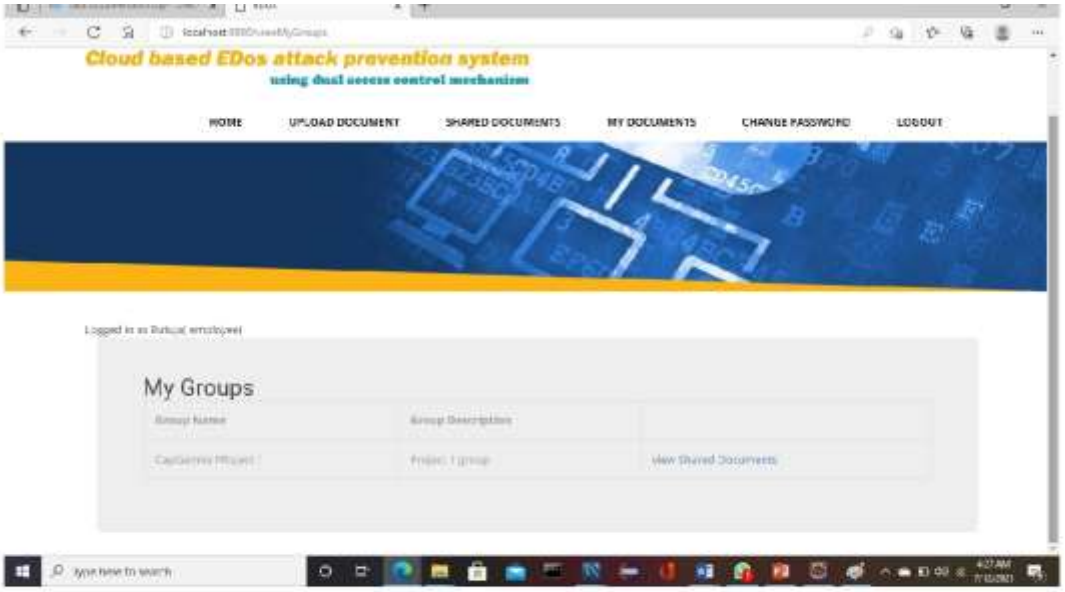
- EDos Prevention due to identity key verification

- Constant cipher text of the document (Size of the Encrypted document will remain same after attributes modification)
- Execution Time comparative result
- Comparative result of existing CPABE and Modified CPABE
- CPABE technique is modified using Attribute key
- Cipher text size is constant as the attributes will be maintained in database and attribute key is maintained in cipher text
- Proposed Encryption algorithm (Modified AES) is more secure and unbreakable
- Dual access control using OTP and identity key hence EDOS prevented





otp and identy key send by email



Empolyee home page

CONCLUSION

- In this paper we focus on security policies to prevent EDOS attack on cloud. We proposed Identity key verification technique to prevent EDOS attack. In Identity key verification technique, system will generate unique identity key for every user in such a way that the identity key will be able to prove user's authenticity as well as authorization. As the key generation server will check user's authenticity and authorization for every request, EDOS attack will be automatically get prevented.

- In addition to EDOS attack we focus on cloud documents security. In this paper we proposed modified AES algorithm and modified CPABE technique to improve security of the document. In this paper we proposed a concept of reference attribute key based security key generation in CPABE technique. Therefore the size of cipher text will remain constant for n number of attributes.

- Therefore we can conclude that our proposed system is very efficient and unbreakable,Here we provide extra security by using CPABE technique which maintained confidentiality of authorized user.it also reduced exicution time .

REFERENCES

[1] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In ACM CCS 2006, pages 89–98. ACM, 2006.

[2] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and Man Ho Allen Au. Improving privacy and security in decentralized ciphertext-policy attribute-based encryption. IEEE transactions on information forensics and security, 10(3):665–678, 2015.

[3] Christofer Hoff. Cloud computing security: From ddos (distributed denial of service) to edos (economic denial of sustainability). http://www. rationalsurvivability.com/blog/?p=66.

[4] Joseph Idziorek, Mark Tannian, and Doug Jacobson. Attribution of fraudulent resource consumption in the cloud. In IEEE CLOUD 2012, pages 99–106. IEEE, 2012.

[5] JiantingNing,ZhenfuCao,XiaoleiDong,andLifeiWei. White-box traceable CP-ABE for cloud storage service: How to catch people leaking their access credentials effectively. IEEE Transactions on Dependable and Secure Computing, 15(5):883–897, 2018.

[6] Mohammed H Sqalli, Fahd Al-Haidari, and Khaled Salah. Edosshield-a two-steps mitigation technique against edos attacks in cloud computing. In UCC 2011, pages 49–56. IEEE, 2011.

[7] Kaiping Xue, Weikeng Chen, Wei Li, Jianan Hong, and Peilin Hong. Combining data owner-side and cloud-side access control for encrypted cloud storage. IEEE Transactions on Information Forensics and Security, 2018.

[8] Shui Yu, Yonghong Tian, Song Guo, and Dapeng Oliver Wu. Can we beat ddos attacks in clouds? IEEE Transactions on Parallel and Distributed Systems, 25(9):2245–2254, 2014.