IJARST
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
ISSN: 2457-0362
www.ijarst.in

Efficient and Secure Cloud Storage Using Revocable Multi-Authority Attribute-Based Encryption

M.Anitha[1],K.Pavani[2], K.Mahendra [3]
#1 Assistant Professor & Head of Department of MCA, SRK Institute of Technology, Vijayawada.
#2 Assistant Professor in the Department of MCA,SRK Institute of Technology, Vijayawada.
#3 Student in the Department of MCA, SRK Institute of Technology, Vijayawada

ABSTRACT_ As is known, attribute-based encryption (ABE) is usually adopted for cloud storage, both for its achievement of fine-grained access control over data, and for its guarantee of data confidentiality. Nevertheless, single-authority attribute-based encryption (SA-ABE) has its obvious drawback in that only one attribute authority can assign the users' attributes, enabling the data to be shared only within the management domain of the attribute authority, while rendering multiple attribute authorities unable to share the data. On the other hand, multi-authority attribute-based encryption (MA-ABE) has its advantages over SA-ABE. It can not only satisfy the need for the fine-grained access control and confidentiality of data, but also make the data shared among different multiple attribute authorities. However, existing MA-ABE schemes are unsuitable for the devices with resources-constraint, because these schemes are all based on expensive bilinear pairing. Moreover, the major challenge of MA-ABE scheme is attribute revocation. So far, many solutions in this respect are not efficient enough. In this paper, on the basis of the elliptic curves cryptography, we propose an efficient revocable multi-authority attribute-based encryption (RMA-ABE) scheme for cloud storage. The security analysis indicates that the proposed scheme satisfies indistinguishable under adaptive chosen plaintext attack assuming hardness of the decisional Diffie-Hellman problem. Compared with the other schemes, the proposed scheme gets its advantages in that it is more economical in computation and storage.

1.INTRODUCTION

Cloud storage is a cloud computing application pattern, facilitates the storage of large volumes of data, which has led to a rising trend among both persons and organizations to move their data from local computers to the cloud. But, this shift raises concerns about privacy, as there is a risk that cloud service providers could access and analyze users' data for unauthorized or commercial purposes. To address this risk, various approaches have been developed. One common method involves utilizing old public key encryption technology for data encryption, although this often results in data owners lacking flexible and fine-grained access to their data. In response to this challenge, alternative approaches have been explored. Nevertheless, data owners continue to encounter limitations in accessing their data with flexibility and granularity. As a result, a novel encryption method has emerged: attribute-based encryption (ABE), which is widely regarded as a promising technology on the horizon

2.LITERATURE SURVEY

2.1 The NIST definition of cloud compute, Nati. Inst. Standards Tech.

Author: P. Mell and T.

Description: Cloud computing facilitates global, suitable, and on-demand access to a shared pool of the configurable computing resources over a network. These resources include networks, servers, storage, applications, and services. Users can quickly provision and release these resources with minimal management effort or interaction with service providers. The cloud computing model is characterized by five essential features, encompasses three service models, and includes four deployment models.

2.2 Ciphertext-policy attribute-based encryption.

Author: J. Bethencourt, A. Saha

Description: In numerous distributed systems, access to data should only be granted if a user possesses specific credentials or attributes. Currently, the main approach for enforcing such policies involves utilizing a trusted server to store data and manage access control. However, if any server storing the data is compromised, it jeopardizes the confidentiality of the data. In this paper, we propose a system for achieving sophisticated access control on encrypted data, termed ciphertext-policy attribute-based encryption (CP-ABE). With our techniques, encrypted data can maintain confidentiality even if the storage server is untrusted, and our methods are resilient against collusion attacks. Unlike previous attribute-based encryption systems, which used attributes to describe encrypted data and integrated policies into user keys, our system employs attributes to define user credentials. Furthermore, the entity encrypting data determines the decryption policy. As a result, our methods align more closely with traditional access control approaches such as role-based access control (RBAC). Additionally, we provide an implementation of our system and offer performance measurements.

2.3 “Fuzzy identity-based encryption,’’ in Advances in Cryptology – (EUROCRYPT)

Author: A. Sahai and B. Waters

Description

We introduce a new form of Identity-Based Encryption (IBE) scheme termed Fuzzy Identity-Based Encryption. In Fuzzy IBE, an identity is represented as a set of descriptive attributes. This scheme allows a private key for an identity, ω, to decrypt a ciphertext encrypted with another identity, ω_0, only if the identities ω and ω_0 are closely related based on the "set overlap" distance metric. Fuzzy IBE can support encryption using biometric inputs as identities, leveraging its error-tolerance property to handle the inherent noise in biometric samples. Additionally, we showcase the utility of Fuzzy IBE in attribute-based encryption. We present two constructions of Fuzzy IBE schemes in this paper, which can be viewed as Identity-Based Encryption of a message under multiple attributes constituting a fuzzy identity. Our IBE schemes are both error-tolerant and resilient to collusion attacks. Moreover, our core construction does not depend on random oracles. We establish the security of our schemes under the Selective-ID security model.

3.PROPOSED SYSTEM

In proposed system on the basis of the elliptic curves cryptography, we propose an efficient revocable multi-authority attribute-based encryption (RMA-ABE) scheme for cloud storage. The security analysis indicates that the proposed scheme satisfies indistinguishable under adaptive chosen plaintext attack assuming hardness of the decisional Diffie-Hellman problem.

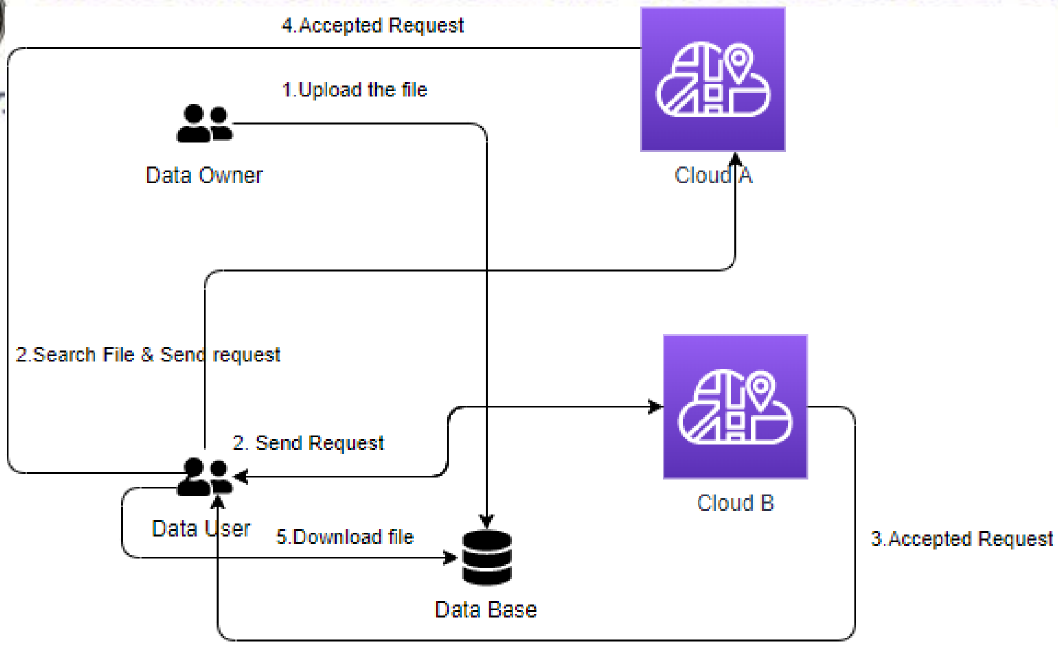


Fig 1:ARCHITECTURE

3.1 IMPLEMENTAION

- **Data owner:**
- **Register:**
- Data owner can register by entering valid details.
- **Login:**
- Data owner can login with their valid identification.
- **Upload:**
- Data owner can upload a file entering its title, keywords, description.
- **Files:**
- Data owner can view the files which he had uploaded.
- **Data user:**
- **Register:**

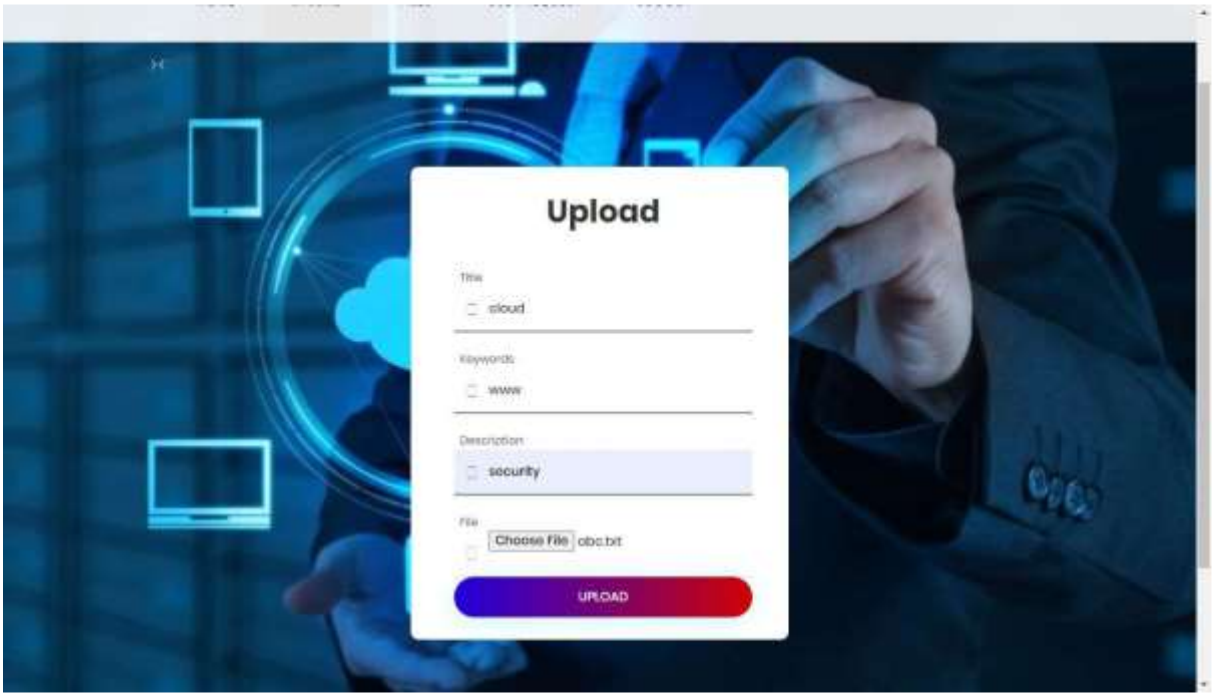
User can register into the application by providing their details

- **Login:**
- User can login into the application by authenticating his own credentials.
- **Search:**
- Data user can search a file by entering its keyword and he can send a request to data possessor to download that folder.
- **Download:**
- If the data possessor accepts the request, the user can download that specific folder
- **Cloud A:**
- **Login:**
- Cloud A can login with their valid identification.
- **Owner details:**
- Cloud A can view all the data owner details.
- **Cloud A:**
- **View User Details:**
- Cloud A has access to view all user details.
- **View All Files:**
- Cloud A can access and view all files uploaded by the owner.
- **User Requests:**
- Cloud A can view user requests and respond to them.

- **Cloud B:**
- **Login:**

- Cloud B can log in using valid credentials.
- **View Owner Details:**
- Cloud B can access and view all data owner details and has the authority to accept, ensuring only data owners can log in.
- **View User Details:**
- Cloud B has access to view all user details and has the authority to accept, allowing only data users to log in.
- **View All Files:**
- Cloud B can access and view all files uploaded by the owner.
- **User Requests:**
- Cloud B can view user requests and respond to them.

4.RESULTS AND DISCUSSION



Upload

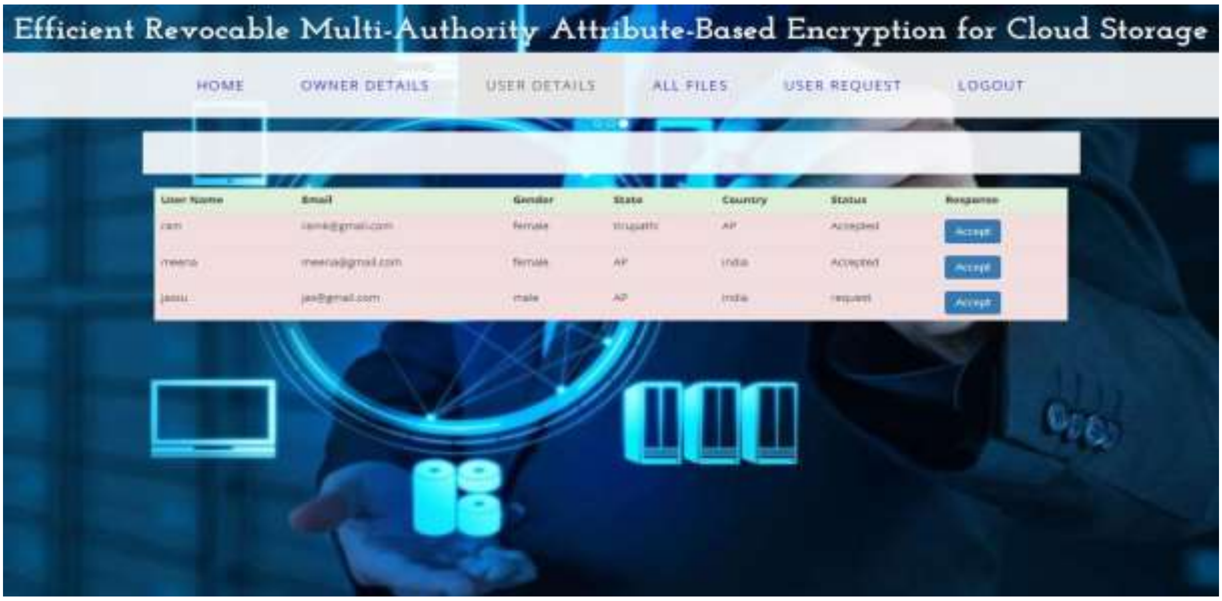
Title: cloud

Keywords: www

Description: security

File: Choose File abc.txt

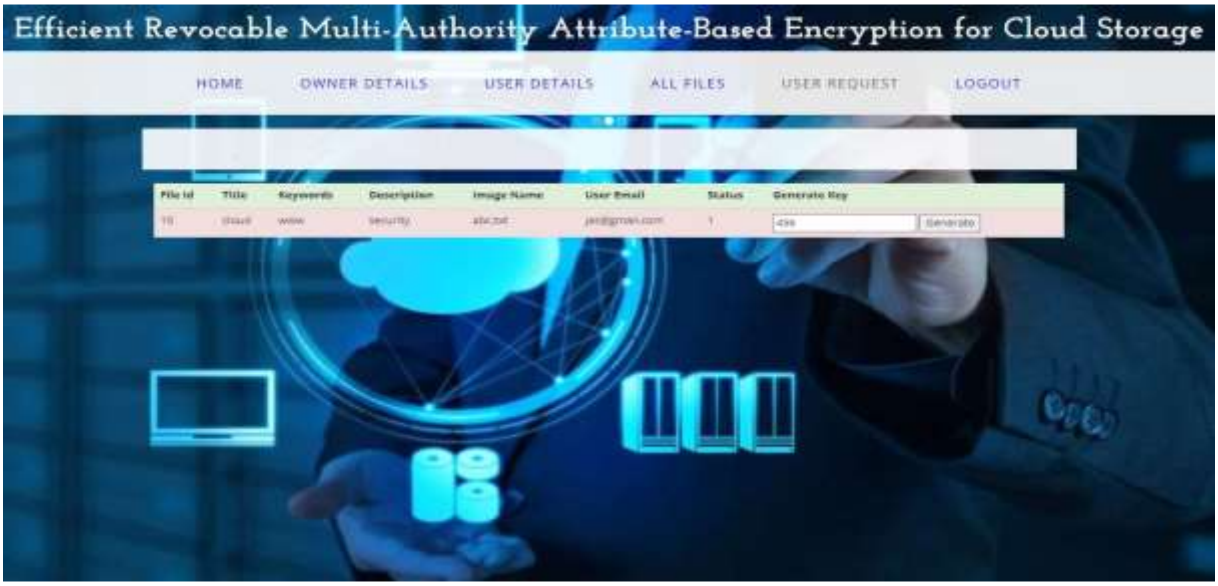
Fig. owner uploading the file



Efficient Revocable Multi-Authority Attribute-Based Encryption for Cloud Storage

User Name	Email	Gender	State	Country	Status	Response
ram	ram4@gmail.com	female	tirupathi	AP	Accepted	Accept
meena	meena@gmail.com	female	AP	india	Accepted	Accept
jassu	jas@gmail.com	male	AP	india	request	Accept

Fig. User sent the request for the file.



Efficient Revocable Multi-Authority Attribute-Based Encryption for Cloud Storage

File Id	Title	Keywords	Description	Image Name	User Email	Status	Generate Key
19	cloud	www	security	abc.txt	jas@gmail.com	1	456 Generate

Fig. CloudA Accepted the user Request and generate the key

5.CONCLUSION

Utilizing elliptic curve cryptography, the document introduces an efficient MA-ABE system designed specifically for cloud storage. It incorporates a version key into attributes to facilitate attribute revocation. Furthermore, a security proof validates that the future system ensures confidentiality.

REFERENCES

[1] P. Mell and T. Grance, ''The NIST definition of cloud computing,'' Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep., Sep. 2009, no. 53, pp. 267–269.

[2] A. Sahai and B. Waters, ''Fuzzy identity-based encryption,'' in Advances in Cryptology– (EUROCRYPT). Berlin, Germany: Springer, Jan. 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ''Attribute-based encryption for fine-grained access control of encrypted data,'' in Proc. 13th ACM Conf. Compute. Communication. Secure. (CCS), 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-policy attribute-based encryption,'' in Proc. IEEE Symp. Secure. Privacy (SP), Berkeley, CA, USA, May 2007, pp. 321–334.

[5] S. Yu, K. Ren, and W. Lou, ''FDAC: Toward fine-grained distributed data access control in wireless sensor networks,'' IEEE Trans. Parallel Distribute. Syst., vol. 22, no. 4, pp. 673–686, Apr. 2011.

[6] Z. Wan, J. Liu, and R. H. Deng, ''HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing,'' IEEE Trans. Inf.

[7] K. Yang, X. Jia, and K. Ren, ''Secure and verifiable policy update outsourcing for big data access control in the cloud,'' IEEE Trans. Parallel Distribute. Syst., vol. 26, no. 12, pp. 3461–3470, Dec. 2015.

[8] J. Li, X. Lin, Y. Zhang, and J. Han, ''KSF-OABE: Outsourced attribute Based encryption with keyword search function for cloud storage,'' IEEE Trans. Services Compute, vol. 10, no. 5, pp. 715–725, Sep. 2017.

[9] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, ''User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage,'' IEEE Syst. J., vol. 12, no. 2, pp. 1767–1777, Jun. 2018.

6[10] M. Chase, ''Multi-authority attribute Based encryption,'' in Proc. Theory Crypto gr. Conf. Berlin, Germany: Springer, Feb. 2007, pp. 515–534.

AUTHOR'S PROFILE

Ms.M.Anitha Working as Assistant Professor & Head of Department of MCA ,in SRK Institute of technology in Vijayawada. She done with B .tech, MCA ,M. Tech in Computer Science .She has 14 years of Teaching experience in SRK Institute of technology, Enikepadu, Vijayawada, NTR District. Her area of interest includes Machine Learning with Python and DBMS.

Ms.K.Pavani completed her Master of Compter Applications.Currently Working as an Assistant Professor in the Department of MCA at SRK Institute of Tecnology **,** Enikepadu, Vijayawada, NTR District. She is qualified for UGC Net 2023,Assistant Professor. Her area of interest include Artificial intelligence and Machine Learning with Python.

Mr.K. Mahendra is an MCA Student in the Department of Computer Application at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. He has Completed Degree in B. Sc (computer Science) from Geetham Degree College Ongole, Prakasam District. His area of interest are Java and Cloud.