# AUTHENTICATION OF DATA STORAGE USING DECENTRALIZED ACCESS CONTROL

Battaladinne Charan[1], V. Sujatha[2]
[1]*M.Tech student, CSE, Kottam college of Engineering,*
[2]*Assistant Professor, CSE , Kottam college of Engineering,*
*Chinnatekuru(V),Kurnool,Andhra Pradesh, India*

***Abstract-*** **Cloud computing is a rising computing standard in which assets of the computing framework are given as a service over the Internet. In this paper, we propose the secure data storage in clouds for a new decentralized access. The cloud verifies the authenticity of the series without knowing the user's identity in the proposed scheme. Our feature is that only valid users can able to decrypt the stored information. It prevents from the replay attack. This scheme supports creation, modification, and reading the data stored in the cloud and also provide the decentralized authentication and robust. It can be comparable to centralized schemes for the communication of data, computation of data, and storage of data.**

***Index Terms-*** **Access control, authentication of user, attribute-based signatures, attribute-based encryption, and cloud storage.**

## I. INTRODUCTION

Now a days cloud computing is a rationally developed technology to store data from more than one client. Cloud computing is an environment that enables users to remotely store their data. Remote backup system is the advanced concept which reduces the cost for implementing more memory in an organization. It helps enterprises and government agencies reduce their financial overhead of data management. They can archive their data backups remotely to third party cloud storage providers rather than maintain data centers on their own. An individual or an organization may not require purchasing the needed storage devices. Instead they can store their data backups to the cloud and archive their data to avoid any information loss in case of hardware / software failures. Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Even cloud storage is more flexible, how the security and privacy are available for the outsourced data becomes a serious concern. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the user.The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and privacy, there is also a need for law enforcement. Access control in clouds is gaining attention because it is important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often be related to health, important documents (as in Google Docs or Dropbox) or even personal information (as in social networking). design.

In UBAC, the access control list contains the list of users who are authorized to access data. This is not possible in clouds where there are many users. In RBAC users are classified based on their own roles. Data should be accessed by users who have matching roles. The roles are declare by the system. For an example, only faculty members and senior secretaries might have access to data but not the junior secretaries.

To achieve secure data transaction in cloud, suitable cryptography method is used. The data owner must encrypt the file and then store the file to the cloud. If a third person downloads the file, he/she may view the record if he/she had the key which is used to

decrypt the encrypted file. Sometimes this may be failure due to the technology development and the hackers. To overcome the problem there are lot of techniques introduced to make secure transaction and secure storage as shown in fig.1

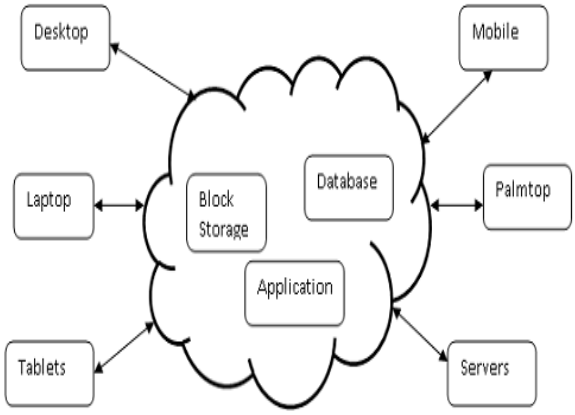


Fig1: Example diagram for data sharing with cloud storage.

## II. RELATED WORKS

[1] In 2006 A. Sahai and B. Waters, worked on "Fuzzy Identity-Based Encryption" In Identity Based Encryption scheme, A user has a set of attributes in addition to its unique ID. A Fuzzy IBE scheme can be applied to enable encryption .In Fuzzy scheme biometric input used as identity.

Advantages:-Error-tolerant , Secure against collusion attacks.

[2] In 2006 V. Goyal, O. Pandey, A. Sahai, and B. Waters, worked on "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data "This paper, the sender has an authorization to encrypt information. A revoked attributes and keys of userscannot write again to stale information. The attribute authority receives attributes and secret keys from the receiver and he/she is able to decrypt information if it has matching attributes.

Advantages:- Distribution of audit-log information and screen out encryption.

[3] In 2007 J. Bethencourt, A. Sahai, and B. Waters, worked on "Cipher text-Policy Attribute-Based Encryption". By using this approach the receiver has the access policy in the form of a tree. The tree contain attributes as leaves and monotonic access structure with AND, OR and other threshold gates

Advantages:- Encrypted information can be kept confidential even if the storage server is untrusted; Secure against collusion attacks.

[4 In 2007 M. Chase, worked "MultiAuthority Attribute Based Encryption". This scheme describes several Key Distribution Authorities (coordinated by a trusted authority) which distribute attributes and secret keys to users. Multi authority Attribute Based Encryption protocol which requires no trusted authority which requires every user to have attributes from at all the KDCs.

Advantages:- Allows a more number of attributes.

[5] In 2011 A.B. Lewko and B. Waters, worked on "Decentralizing Attribute-Based Encryption," This paper where users could have zero or more attributes from each authority and did not require a trusted server.

Advantages: Collusion resistant.

[6] In 2011 M. Green, S. Hohen berger, and B. Waters, worked on "Outsourcing the Decryption of ABE Ciphertexts," .This paper subcontract the decryption task to a proxy Server, so that the user made computation on minimum resources like hand held devices.

Advantages:- The user significantly saves bandwidth, without raising the number of transmission.

[7] In 2008 H.K. Maji, M. Prabhakaran, and M. Rosulek, worked on"Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance,".In this paper to ensure anonymous user authentication ABSs were introduced. This was also a centralized approach.

Advantages: The user significantly saves decryption time, without raising the number of transmissions

[8] In 2011 H.K. Maji, M. Prabhakaran, and M. Rosulek, worked on "Attribute-Based Signatures," This method takes a decentralized approach and provides authentication without disclosing the identity of the users.

Advantages:- secure against a malicious attribute authority

## III. PROPOSED PRIVACY PRESERVING AUTHENTICATED ACCESS CONTROL SCHEME

The architecture of proposed system depicted in Fig.1.There are three users, a creator, a reader, and writer. Creator Alice receives a token _ from the trustee, who is assumed to be honest. A trustee can be someone like the federal government who manages social insurance numbers etc. On presenting her id (like health/social insurance number), the trustee

gives her a token _. There are multiple KDCs (here 2), which can be scattered. For example, these can be servers in different parts of the world.

A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing. In the Fig. 2, SKs are secret keys given for decryption, Kx are keys for signing. The message MSG is encrypted under the access policy X. The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove her authenticity and signs the message under this claim. The cipher text C with signature is c, and is sent to the cloud. The cloud verifies the signature and stores the cipher text C. When a reader wants to read, the cloud Sends C. If the user has attributes matching with access policy, it can decrypt and get back original message.

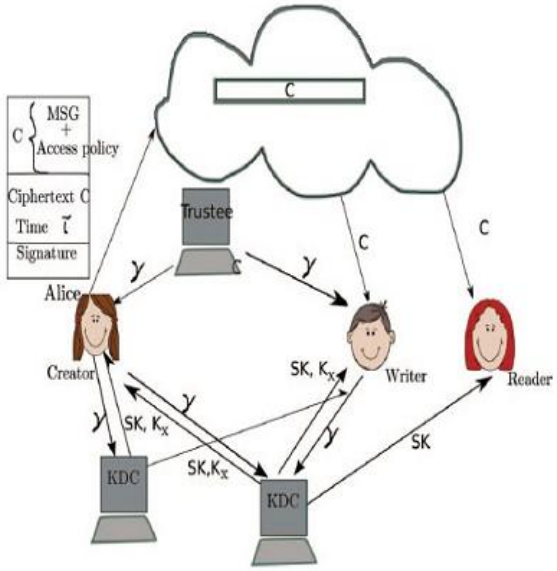


Fig. 2. Our secure cloud storage model.

**Advantages**

Our access control scheme is secure which means no outsider or cloud can decrypt cipher texts.

- Collusion resistant
- Authorized users only can access.
- Resistant to replay attacks
- Protects privacy of the user.

The cloud is honest-but-curious, such that the cloud administrators can be able to view user's content, but cannot modify data/information.

- Honest-but-curious model of adversary do not tamper with data so that they can keep the system functioning normally and remain undetected.
- Users have rights like either read or write or both accesses to a file stored in the cloud.

The communications between users/clouds are secured by secure shell protocol, SSH.

**Data Storage in Clouds:**

A user $U_u$ have one or more trustees. This is used to prevent to the replay attacks. In this time data is not sent, then the user can write previous stale message back to the cloud with a valuable signature, even when its claim policy and attributes have been revoked.

**Reading from the Cloud:**

The user requests data from the cloud, the cloud sends the ciphertext using SSH protocol. Decryption proceeds using algorithm ABE.

**Writing to the Cloud:**

The user must send its message with the claim policy as done during file creation. The cloud verifies the claim policy, and only if the user is authentic is allowed to write on the file.

**User Revocation:**

It should be ensured that users must not have the ability to access data, even if they possess matching set of attributes.

### A. SECURITY OF THE PROTOCOL

We will explain that our scheme authenticates a user who wants to write to the cloud. A user should only write provided the cloud is able to validate it access to the claim. An invalid user cannot receive the attributes from a KDC, if it do not have the credentials from the trustee. If a user's credentials are revoked, then it cannot replace data with previous data, thus preventing replay attacks.

**Theorem 1.** Our access control scheme is secure, collusion resistant and allows access only to authorized users.

**Theorem 2**. Our authentication data is correct, collusion secure, resistant to the replay of attacks, and protects privacy of the user.

Next we confirm that only a valid user with valid access claim is only able to store the message in the cloud. This is taken from the functions given in [24] . A user who wants to create a file and tries to make a wrong access claim, cannot do so, since it will not have attribute keys Kx from the related KDCs. Since the message is encrypted, a user without valid access policy cannot decrypt and change the information.

### B. COMPUTATION COMPLEXITY

To calculate the computations required by users (creator, reader, writer) and that is provided by the cloud. The following Table 1 presents notations used for different operations.

Table 1

| Symbols | Computation |
|---|---|
| $E_x$ | Exponentiation in group $G_x$ |
| $\tau_H$ | Time to hash using function $H$ |
| $\tau_{\mathcal{H}}$ | Time to hash using function $\mathcal{H}$ |
| $\tau_P / \tau_{\hat{P}}$ | Time taken to perform 1 pairing operation in $e/\hat{e}$ |
| $\|G\|$ | Size of group $G$ |
| $a$ | Number of KDCs which contribute keys to user |

The creator needs to encrypt the message and sign it. Creator needs to calculate one pairing eðg; gÞ. Encryption takes two exponentiations to calculate each of C1;x. So this requires 2mET time, where m is the number of attributes.

## IV. SIMULATION RESULTS

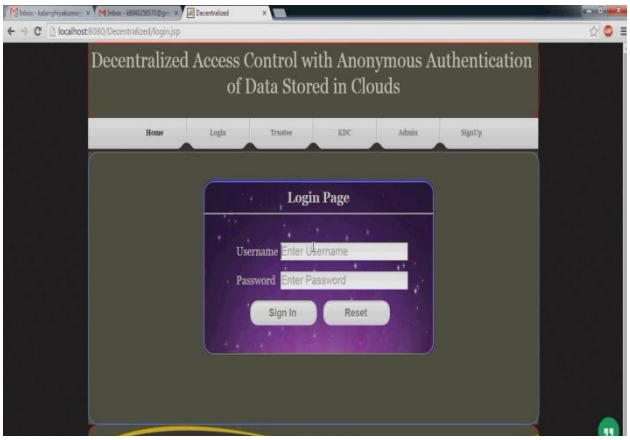


Fig. 3

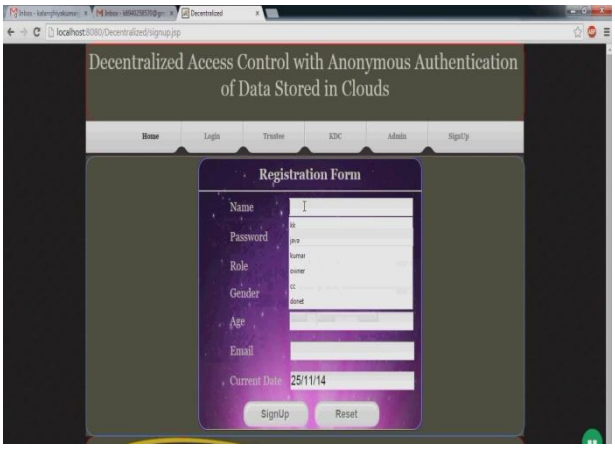


Fig. 4

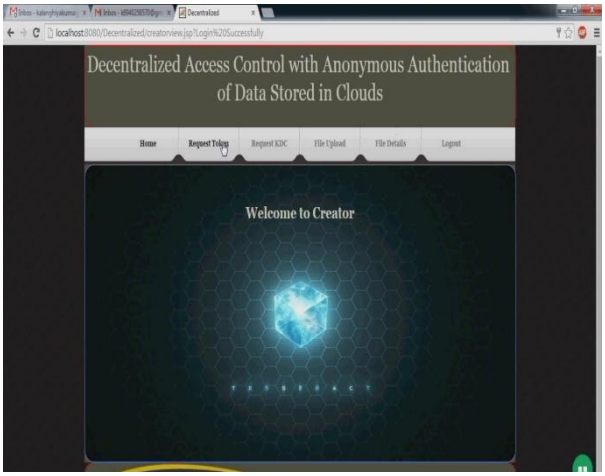


Fig. 5


Fig.6

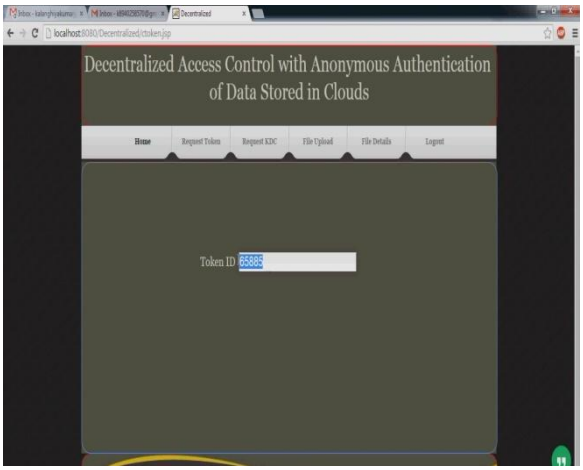


Fig. 7


Fig. 8

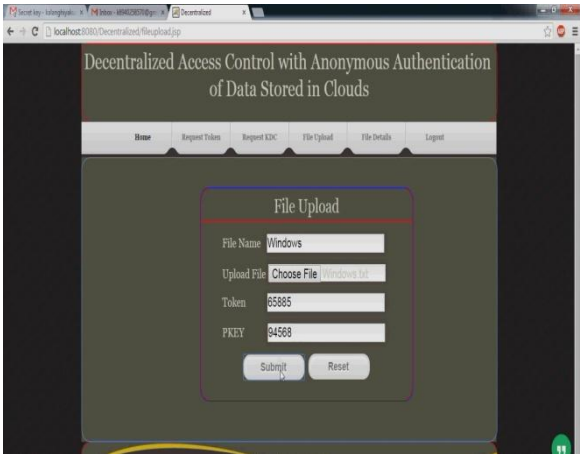


Fig. 9

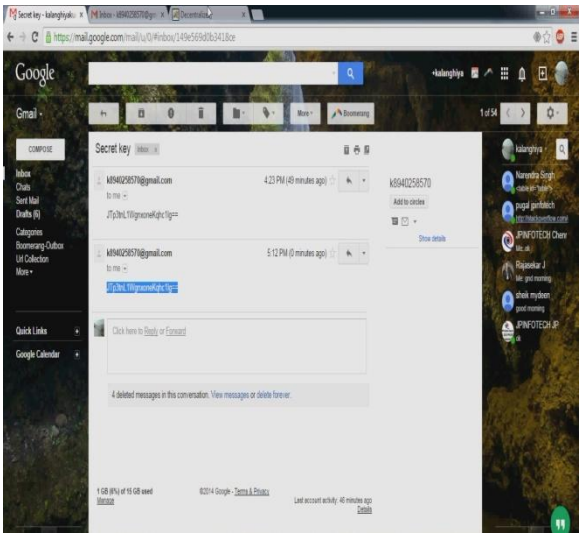


Fig. 10

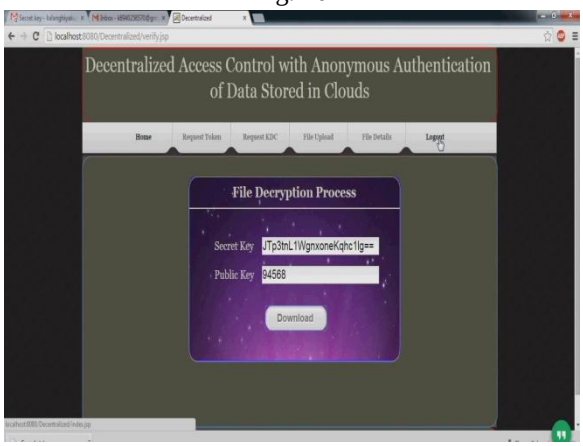


Fig.11

## V. CONCLUSION

In this paper, a decentralized access control technique with anonymous authentication is proposed, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. One limitation is that the cloud knows the access policy for each record stored in the cloud.

## REFERENCES

[1]A. Sahai and B. Waters, "Fuzzy IdentityBased Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM

Conf. Computer and Comm. Security, pp. 89-98, 2006.
[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
[4] M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf.Theory of Cryptography (TCC), pp. 515-534, 2007..
[5] A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.
[6] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABECiphertexts," Proc. USENIX Security Symp., 2011.
[7] H.K. Maji, M. Prabhakaran, and M.Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and CollusionResistance," IACR Cryptology ePrint Archive, 2008.
[8] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.

**BIODATA**

**Author**

**Battaladinne Charan** presently pursuing his M.Tech in CSE, Kottam College of Engineering, Chinnatekuru (V),Kurnool,Andhra Pradesh, India.

**Co-Author**

**V.Sujatha** received M.Tech. Presently working as Assistant Professor in Kottam College of Engineering, Chinnatekuru (V),Kurnool,Andhra Pradesh, India.