A Privacy Preserving Authenticated Access Control Mechanism In Distributed Environment For Cloud Storage

[1]Sneha Lihite ,[2]Prof. Sagar Bhakre

[1]M.tech Student, Department Of Computer Science And Engineering, Ballarpur Institute Of Technology, Ballarpur, Maharashtra, India.

[2]Professor,Department Of Computer Science And Engineering, Ballarpur Institute Of Technology, Ballarpur, Maharashtra, India

***Abstract*—Cloud Computing is the emerging technology where we can get platform as a service, software as a service and infrastructure as a service. When it comes to storage as a service, data privacy and data utilization are the primary issues to be deal with. Security and privacy are very important issues in cloud computing. Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. Users are authenticated who store and modify their data on the cloud. The identity of the user is protected from the cloud during authentication. The architecture is decentralized, meaning that there can be several KDCs for key management. Revoked users cannot access data after they have been revoked. The proposed scheme is resilient to replay attacks. The protocol supports multiple read and writes on the data stored in the cloud. It proposing privacy preserving authenticated access control scheme. According to the scheme a user can create a file and store it securely in the cloud. The cloud verifies the authenticity of the user without knowing the user's identity before storing data. The scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. The work proposes a new decentralized access control scheme for secure data storage in clouds, which supports anonymous authentication .Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized.**

***Index Terms*— Cloud Storage, Decentralised Access, Key Distribution Center, Attribute Based Encryption, Access Control.**

I. INTRODUCTION

Cloud computing is a promising computing model which currently has drawn far reaching consideration from both the educational community and industry. By joining a set of existing and new procedures from research areas, for example, Service-Oriented Architectures (SOA) and virtualization, cloud computing is viewed all things considered a computing model in which assets in the computing infrastructure are given as services over the Internet. . Numerous services like email, Net banking and so forth are given on the Internet such that customers can utilize them from anyplace at any time. Indeed cloud storage is more adaptable, how the security and protection are accessible for the outsourced data turns into a genuine concern. The three points of this issue are availability, confidentiality and integrity. The data possessor must encrypt the record and then store the record to the cloud. Assuming that a third person downloads the record, they may see the record if they had the key which is utilized to decrypt the encrypted record. Once in a while this may be failure because of the technology improvement and the programmers.

To overcome the issue there is lot of procedures and techniques to make secure transaction and storage. Recently experts addressed Anonymous authentication for data archiving to clouds[2]. Anonymous authentication is the procedure of accepting the client without the details of the client. So the cloud server doesn't know the details of the client, which gives security to the clients to conceal their details from other clients of that cloud. 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 related to health, important documents (as in Google Docs or Dropbox) or even personal information (as in social networking).Access control is also gaining importance in online social networking where users (members) store their personal information, pictures, videos and share them with selected groups of users or communities they belong to. It is not just enough to store the contents securely in the cloud but it might also be necessary to ensure anonymity of the user. For example, a user would like to store some sensitive information but does not want to be recognized. The user might want to post a comment on an article, but does not want his/her identity to be disclosed. However, the user should be able to prove to the other users that he/she is a valid user who stored the information without revealing the identity.

II. LITERATURE SURVEY

[1] Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds (2014)

Author :SushmitaRuj , Milos .S , Amiya Nayak

In this proposed scheme the cloud verifies the authenticity of any user without having knowledge of his /her identity before storing the Data over Cloud. The authentication and access control scheme of this paper in centralized and the user are given rights which also can be revoked later, also it allows data to be written multiple times. They have used attributed based signature scheme for authentication. The scheme is resilient to replay attacks. The drawback here is that the data stored in Cloud is in a centralized location. Also the Decryption of database takes place as users end which leads to lag at system.

[2] Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control (2014)

This paper proposes access control scheme for data storage, which supports anonymous authentication and performs decentralized key management. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against replay attacks.

[3] Privacy Preserving Access Control with Authentication for Securing Data in Clouds (2012)

Author :SushmitaRuj , Milos .S , AmiyaNayak

This is the Base paper for Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds by the same authors. The papers discusses on user authentication who store and modify their data on cloud. The identity of user is protected from cloud during authentication. The architecture is decentralized meaning there are multiple KDC for key management. The protocol Supports multiple read and write on the data stored in the cloud .The cost is comparable to the existing centralized approaches. The only drawback was the authentication of validating the message without revealing the identity of the user who has stored the information.

[4] Toward Secure and Dependable Storage Services in Cloud Computing (2012)

Auhtor : C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou

Cloud allows users to store data in a remote location and enjoy on demand high quality cloud resources ,even if the benefits are clear ,such a service is also relinquishing usersmindset towards their stored data which brings in new security risks. This paper proposes a design of distributed storage integrity, using the homomorphic token and distributed erasure coded data. It allows detecting misbehaving server's .It also allows operation like block modification, deletion and append. This scheme is highly efficient against Byzantine failure, malicious data modification and server colluding attacks.

III. PROPOSED SYSTEM

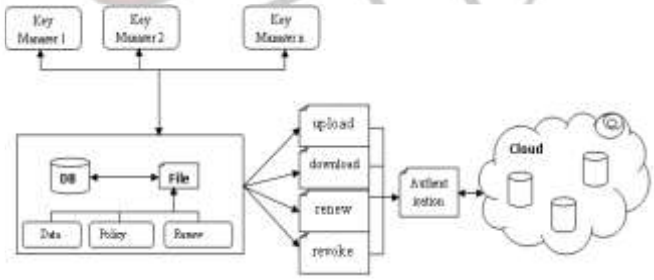


Fig1: Overall system diagram.

First the client was authenticated with the username and password, which is provided by the user. Then the user was asked to answer two security levels with his/her choice. Each security levels consist of 5 user selectable questions. The user may choose any one question from two securitylevels. The private key for encrypt the file was generatedwith the combination of username, password and the answers for the security level questions. After generating theprivate key the client will request to the key manager for thepublic key. The key manager will verify the policy associated with the file. If the policy matches with the filename then same public key will be generated. Otherwise new public key will be generated. With the public key andprivate key the file will be encrypted and uploaded into thecloud. If a user wants to download the file he/she would be authenticated. If the authentication succeeded, the file will be downloaded to the user. Still the user cant able to read the file contents. He / she should request the public key to the key manager. According to the authentication, the keymanager will produce the public key to the user. Then theuser may decrypt the file using the login credentials given by the user and the public key provided by the key manager.
The client can revoke the policy and renew the policy due to the necessity.

The proposed scheme consists of four algorithms which isdefined as follows

- Setup :This algorithm takes as input security parameters and attribute universe of cardinality N. It then defines a bilinear group of prime number. It returns a public key and the master key which is kept secret by the authority party.
- Encryption:It takes a message, public key and set of attributes. It outputs a cipher text.
- Key Generation:It takes as input an access tree, master key and public key. It outputs user secret key.
- Decryption: It takes as input cipher text, user secret key and public key. It first computes a key for each leaf node. Then it aggregates the results using polynomial interpolation technique and returns the message.

IV. SYSTEM DESIGN

➢ **Key Management**

In our project following are the cryptographic keys to protect data files stored on the cloud.

- Public Key: The Public key is a random generated binary key, generated and maintained by the Key manager itself. Particularly used for encryption/ decryption.
- Private Key: It is the combination of the username,password and two security question of user's choice. The private key is maintained by client itself. Used for encrypt / decrypt the file.
- Access key: It is associated with a policy. Private access key is maintained by the client. The access key is built on attribute based encryption. File access is of read or write.
- Renew key: Maintained by the client itself. Eachhas its own renew key. The renew key is used to renew the policy of each necessary file at easy method.

➢ **Encryption / Decryption**

We used ECC algorithm for encryption/Decryption. This algorithm is the proven mechanism for secure transaction. Here ECC algorithm has key size of 128.

➢ **File Upload / Download**

i. File Upload

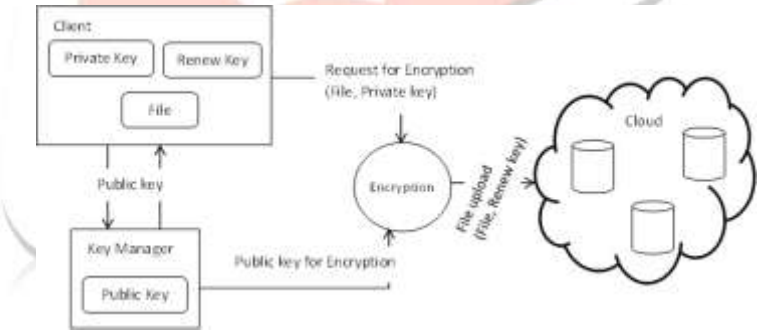


Fig.2: File uploading process

The client made request to the key manager for the public key, which will be generated according to the policy associated with the file. Different policies for files, public key also differs. But for same public key for same policy will be generated. Then the client generates a private key by combining the username, password and security credentials. Then the file is encrypted with the public key and private key and forwarded to the cloud.

ii. File Download

The client can download the file after completion of the authentication process. As the public key maintained by the key manager, the client request the key manager for public key. The authenticated client can get the public key.Then the client can decrypt the file with the public key and the private key. The users credentials were stored in the client itself. During download the file the cloud will authenticate the user whether the user is valid to download the file. But the cloud doesn't have any attributes or the details of the user.

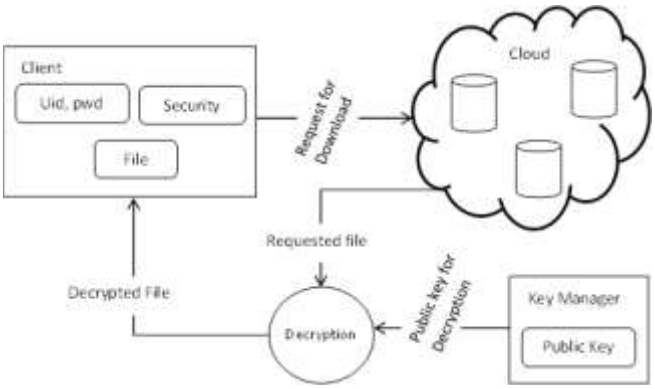


Fig 3: File downloading process

- **Policy Revocation for File Assured Deletion**

The policy of a file may be revoked [8] under the request by the client, when expiring the time period of the contract or completely move the files from one cloud to another cloudenvironment. When any of the above criteria exists the policy will be revoked and the key manager willcompletely removes the public key of the associated file.So no one recover the control key of a revoked file in future.For this reason we can say the file is assuredly deleted. Automatic file revocation [12] scheme is also introduced to revoke the file from the cloud when the file reaches the expiry and the client didn't renew the files duration.

- **File Access Control**

Ability to limit and control the access to host systems and applications via communication links. To achieve, access must be identified or authenticated. After achieved the authentication process the users must associate with correct policies with the files. To recover the file, the client must request the key manager to generate the public key. For that the client must be authenticated. The attribute based encryption standard is used for file access which is authenticated via an attribute associated with the file. With file access control the file downloaded from the cloud will be in the format of read only or write supported.Each user has associated with policies for each file. So the right user will access the right file. For making file access the attribute based encryption scheme is utilized.

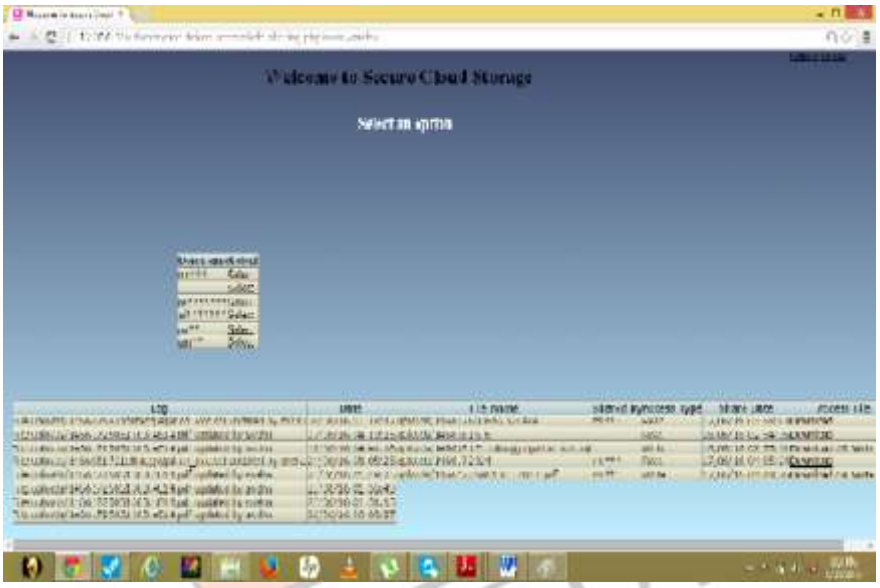
- **Policy Renewal**

Policy renewal is a tedious process to handle the renewal of the policy of a file stored on the cloud. Here we implement one additional key called as renew key, which is used to renew the policy of the file stored on the cloud. Therenew key is stored in the client itself.

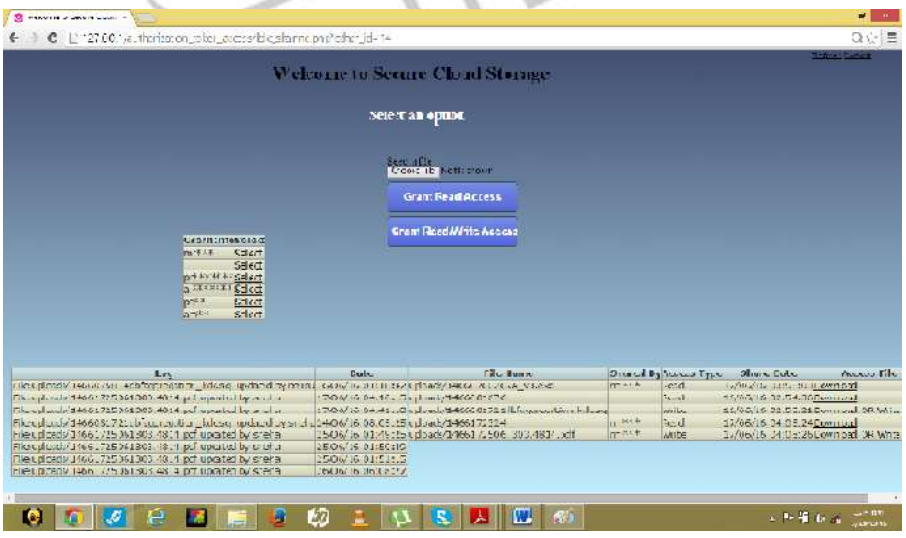
V. SCREENSHOT

Screenshot 1: Homepage of the system

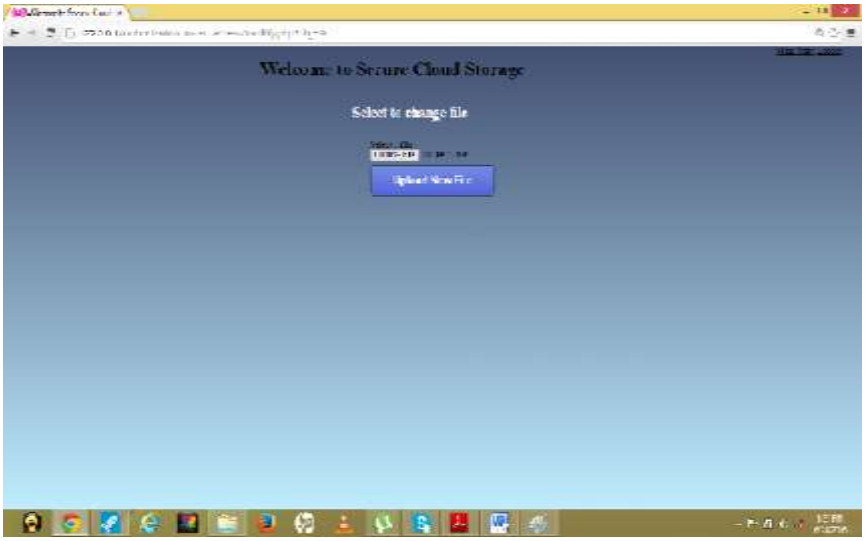
Screenshot 2: Login Page



Screenshot 3: KDC User Login



Screenshot 4: Select user and file to grant access



Screenshot 5: Upload New file Window

VI. RESULT ANALYSIS

In this sections result analysis is discuss in detail. Cloud is the virtual storage area where the user can store the data securely. The data storage is mainly consist of the security. The user must be ensure that the stored data is securely stored on the cloud. For this the user must be sure that only autherized used can access the data. Privacy and the security are the two mentioned factor for the data stored on the cloud. User authentication ensures the security. Hence the data can be only visible to the user who are successfully authenticated to the system. The user may permit the another user to access data by granting the access permission according to the choice. User Anonymity ensures the privacy of the data. The decentralized nature of the system relaxed it from the burdon of maintaining the eysabd attributes of all the user. Hence the analysis can be done according to the Authentication scheme, granting the access permission and Anonymity scheme and the decentralized environment.

VII. APPLICATION

- **Government Organization:-**The data related to a department can be shared among the same department to only people who have right to read it. Any government employee can share data related to any malpractices or corruption in the office to report to the higher authority.
- **International Security Agencies: -** Any individual person can upload data regarding terrorism on the Cloud, hiding his own information and mentioning to whom to share this data.
- **Universities: -** The data can be stored on a shared Server and can be access on any device through Internet.

VIII. CONCLUSION

We propose secure cloud storage using decentralized access control with anonymous authentication. The files are associated with file access policies, that used to access the files placed on the cloud. Uploading and downloading of a file to a cloud with standard Encryption/Decryption is more secure. Revocation is the important scheme that should remove the files of revoked policies. So no one can access the revoked file in future. The policy renewal is made as easy as possible. The renew key is added to the file. Whenever the user wants to renew the files he/she may directly download all renew keys and made changes to that keys, then upload the new renew keys to the files stored in the cloud.
In future the file access policy can be implemented with Multi Authority based Attribute based Encryption. Using the technique we can avoid the number of wrong hits during authentication. Create a random delay for authentication, so the hacker can confuse to identify the algorithm.

ACKNOWLEDGMENTS

I would like to extend my gratitude to many people who helped me to bring this paper fruition. First I would like to thank Prof. Sagar Bhakre. I am so deeply grateful for his help, professionalism, and valuable guidance throughout this paper. I would also like to thank to my friends and colleague. This accomplishment would not have been possible without them. Thank you.

REFERENCES

[1] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc. IEEE/ACM Int'l Symp.Cluster, Cloud and Grid Computing, pp.556- 563, 2012.
[2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.- June 2012.
[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM, pp. 441-445, 2010.
[4] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14thInt'l Conf. Financial Cryptography and Data Security, pp. 136- 149, 2010.
[5] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.
[6] C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/ craig, 2009.
[7] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.
[8] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Framework for Accountability and Trust in Cloud
Computing," HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/ 2011/HPL-2011-38.html, 2013.
[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.
[10] D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," Proc.15th Nat'l Computer Security Conf., 1992.
[11] D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role- Based Access Control," IEEE Computer, vol. 43, no. 6, pp. 79-81, June 2010.
[12] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 89- 106, 2010.
[13] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp.Information, Computer and Comm. Security (ASIACCS), pp. 261-270, 2010.
[14] G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.
[15] F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems," Proc. Seventh Int'l Conf. Information Security Practice and Experience (ISPEC), pp. 83-97, 2011.
[16] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.
[17] S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2011.