International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 05, May 2017
www.ijates.com
ijates
ISSN 2348 - 7550

DECENTRALIZED ACCESS CONTROL WITH ANONYMOUS AUTHENTICATION AND AUTO FILE PUBLISHING IN CLOUD.

Madhubala Chandak[1], Harsha Kumble[2], Sanjana Prasad[3]

Akshata Kulkarni[4], Prof. A.N. Banubakode[5]

Department of IT, S. P. Pune University, Pune (India)

ABSTRACT

In today's world, the communication network is widely developed. You can send the texts as well as files, also it can be shared in one or many forms. While communicating with the other person via medium, the registered details become transparent to the third party. What if we could demolish the transparency?

We propose a cloud system where user can upload, download, view and also share data by keeping his identity anonymous. The application can be an anonymous sharing system for government where user can bring into notice the certain issues of government by keeping his identity secured. It is also important to ensure that respective file is delivered to the authorities in any case.

Keywords - anonymous sharing center, access control, decentralized.

I. INTRODUCTION

Now-a-days, in Online social networking access control is very important. Only valid user must be allowed to access and store personal information, images and videos and all this data is stored in cloud. The goal is not just to store the data securely in cloud, it is also important to make secure that anonymity of user is ensured. In the proposed system, the cloud verifies the authenticity of the user without knowing the user's identity before storing data. In Existing System, existing work on access control in cloud are centralized in nature except that all other schemes use attribute based encryption. The scheme uses a symmetric key approach and does not support authentication.

Suitable cryptography method is used, to achieve secure data transaction in cloud. 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 has the key which is used to decrypt the encrypted file. Sometimes this may lead to failure due to the technology development and the hackers. A lot of techniques have been introduced to make secure transaction and secure storage and to overcome the problem. The encryption standards are used for transmitting the file securely. To maintain the secrecy, the encryption technique was implemented with set of key operations.

Security of data and privacy of users is more important and has to be preserved. Cloud should make sure that the users trying to access data and services are authorized users. Authentication of users can be achieved using many public key cryptographic techniques. Users should also ensure that the cloud is not tampering with their data and computational results. Sometimes, it can also be important to hide the users identity for privacy reasons. For example, while storing some medical records, the cloud should not be able to access records of a

particular patient, given the identity. Users should also ensure that the cloud is able to perform some computations on the data, but without knowing the actual data values.

1.1 Objectives

There are three main objectives:

- Privacy
- Reliability
- Accessibility

The goal is not just to store the data securely in cloud but it is also important to make sure that anonymity of user is ensured.

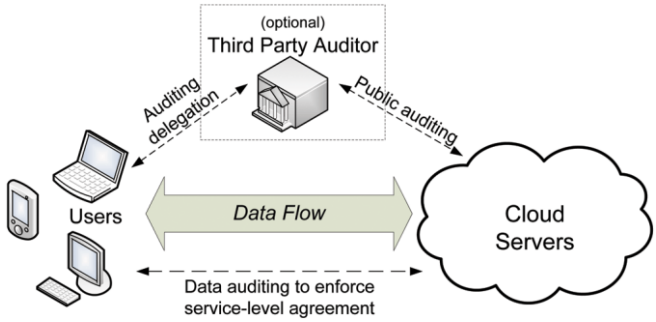

Fig 1-Cloud Storage Service Architecture

II. LITERATURE SURVEY

ABSs were introduced by Maji et al, to ensure anonymous user authentication. This was also a centralized approach. A recent scheme by Maji et al takes a decentralized approach and provides authentication without disclosing the identity of the users.

In this system we are going to use KDC for generation of encrypted Tokens and encrypted keys. Key distribution is done in a decentralized way. There is KDC which generates encryption and decryption keys and keys for signing. On presenting token to KDC, the creator will provide secret keys and keys for signing. The cloud takes decentralized approach in distributing secret keys and attributes to user.

Ruj et al proposed a distributed access control mechanism in clouds. However, the scheme did not provide user authentication. The other drawback was that a user can create and store a file and other users can only read the file. Write access was permitted to users other than the creator.

Although Yang et al proposed a decentralized approach. Their technique does not authenticate the users, who want to remain anonymous while accessing the cloud. ABS(Attribute-based signature) is a protocol which was proposed by Maji et al.

III. EXISTING WORK

Cloud computing, helps the users to outsource their computation, applications and storage to servers (also called clouds) using Internet. This frees users from the hassles of maintaining resources on-site. Clouds provide services like application as a service (e.g., Google Apps, Microsoft online), infrastructure as a service (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g., Amazon's S3,

Windows Azure). Since services are outsourced to a remote server, security and privacy are of immense concern in cloud computing.

Now-a-days, access control in clouds is gaining more attention because only authorized users have access to valid service. While ensuring access control of the sensitive information care should be taken as the information can be related to health, important documents (as in Google Docs or Dropbox) or even personal information (as in social networking). Access control also gains 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. Such data are being stored in clouds. Only authorized users are given access to those information. A similar situation arises when data is stored in clouds, for example when data is stored in Dropbox, and shared with certain groups of people.

In many applications, it is essential to use a common secret key for secured communication among multiple devices. Granting access rights to certain users and forbidding other users to access the data, is called access control. One way to achieve this is to attach a list of all valid users to the data. In cloud computing scenario, such lists can be extremely long and often dynamic, which will make handling such lists extremely difficult. Each time the list has to be checked to see if the user is valid. This results in a huge computation and storage costs. Another way to encrypt data is by using public keys of valid users, so that only they are able to decrypt data using their secret keys. However the same data then must be encrypted several times (individually for each user), which may result in huge storage costs. Hence we use the cryptographic technique called Attribute Based Encryption(ABE) to achieve access control in clouds.

IV. TECHNOLOGIES TO BE USED

Our system uses the following technologies:

- **Java**

Java is designed for applications that are portable and also have high-performance for the widest range of computing platforms .By making applications available across heterogeneous environments, businesses can provide more and more services and boost end-user productivity, communication, and collaboration—and dramatically reduce the cost of ownership of both enterprise and consumer applications.

All the implementation of Java compilers, virtual machines, and class libraries were released by Sun under proprietary licenses. As of May 2007, in compliance with the specifications of the Java Community Process, Sun relicensed most of its Java technologies under the GNU that is General Public License. Others have also developed some alternative implementations of these Sun technologies, such as the GNU Compiler for Java (byte code compiler), GNU Classpath (standard libraries), and IcedTea-Web (browser plugin for applets).

- **Token generation**

In this method, we will generate encrypted token by KDC. A security token provided by KDC is given to an authorized user of computer services is given to ease authentication. The term may also refer to software tokens. Security tokens are used to prove one's identity electronically. The token is used in place of a password to prove that the customer is who they claim to be. The token acts like an electronic key to access information.

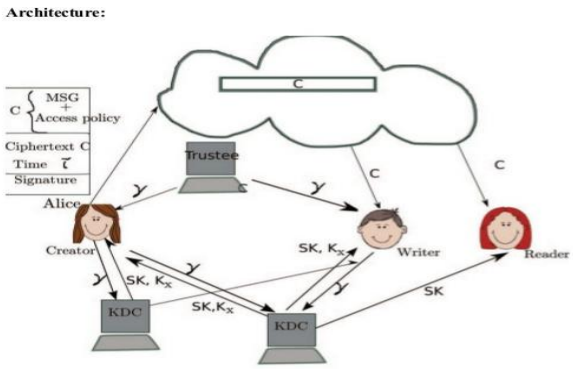

Fig 2-Token Genertaion

- **Key generation**

After Validating the tokens we will generate the encrypted key to the user. Key generation is the process of generating keys in cryptography. An electronic key that is provided to the user is used to encrypt and decrypt whatever data is being encrypted/decrypted.

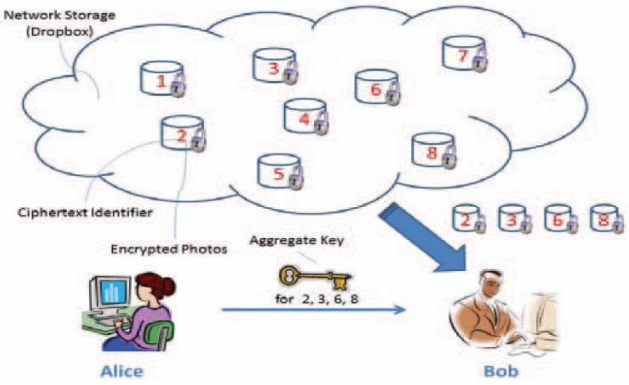

Fig 3-Key Generation

V. PROPOSED SYSTEM

In the proposed system, the cloud verifies the authenticity of the user without knowing the user's identity before storing data. In the existing system, RSA algorithm is used. We are now using AES encryption algorithm which is of 256 bit key length. A user can create and store a file and other users can only read the file. The write access is only permitted to the creator not to the other users. To authenticate the user, OTP is sent to the user's email-id. Multiple files can also be uploaded. The file should be delivered to the right authorities in any case. A pre-defined deadline is scheduled after which the file will be automatically posted even without the provider's permission.

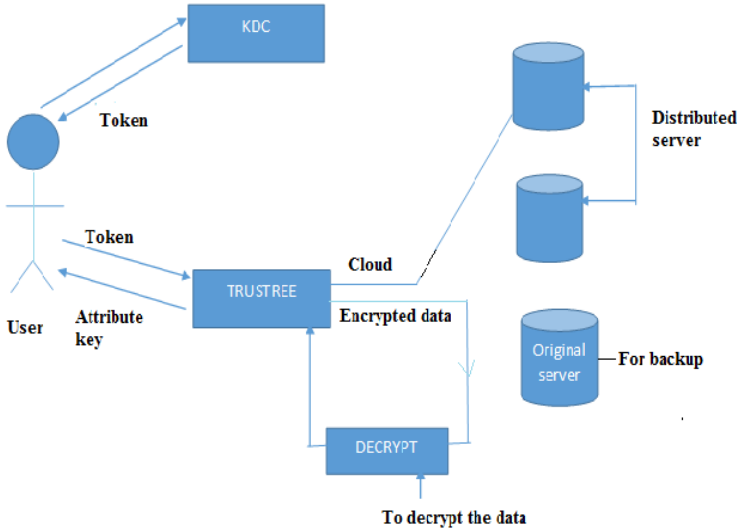

Fig 4-Proposed system

5.1. PRODUCT PERSPECTIVE

The perspective of this application to maintain security and unauthorized person who wants to access the data on the cloud. This was also a centralized approach. A recent scheme by Maji et al. Takes a decentralized approach and provides authentication without disclosing the identity of the users.

In this system we are going to use KDC for generation of encrypted tokens and encrypted keys. Key distribution is done in a decentralized way. There is KDC which generates encryption and decryption keys and keys for signing. Creator will present token to KDC and it will provide secret keys and keys for signing.

5.2. PRODUCT FUNCTION

- Registration:-Register user with name, email, Date of Birth and address. Token will be sent to specified email to authenticate user. If token is correct, then user will again get key on email, thereafter email and key will be the log-in credentials.
- After Logging In, user can upload files on Cloud and see list of uploaded files if uploaded before. Also user can share files from his uploaded file list through email.

5.3. USER CHARACTERISTICS

Proposed system involves important role for the User-

- User will able be to Register with system with credentials -Name, Email, Date of Birth, Address.
- User will be able to Login with Email and Key which will sent on email.
- User Able to Upload File. File sharing via Email interface.

VI. ALGORITHM

1. Register User

    1.1: Sent all user details to Web Service.

    1.2 : Validate fields.

    1.3 : Sent OTP to mobile number.

1.4 : Sent Login key on Mail if OTP correct.

2. Login User

3. Home page

3.1 : Uploaded files.

3.2 : Show list of uploaded files.

3.3 : Send files

4. Stop

VII. IMPLEMENTATION AND DISCUSSION

In this proposed system, we briefly discuss the existing works about Decentralized Access control system.

1. In this the additional feature of a timer has been added in order to assure file publishing in any case.
2. The earlier 2 step user authentication has been advanced into a three step authentication system .
3. In the existing system only single files can be uploaded. In this system the user is able to upload multiple files into the cloud.
4. The authentication is done via the email and phone number of the user.
5. The uploaded file is stored on a backup server and also into the main cloud.
6. Advanced key encryption methods like 256 bit key is used improving the security provided.

VIII. CONCLUSION

Here, we have presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. Key distribution is done in a decentralized way. The proposed system provides a Anonymous Authentication of Decentralized Access Control of Data Stored in Cloud. It prevents replay attacks and addresses user revocation. The user credentials are verified by cloud who store the data but cloud does not know who the user is.

IX. ACKNOWLEDGEMENTS

This project aims at providing a quality of service at the traffic junctions. We are profoundly grateful to **Prof. Dr.A.N.Banubakode** for his expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion. We are also grateful to **Head of Department Dr.A.N.Banubakode** for his support and guidance that have helped us to expand my horizons of thought and expression.

X. 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. 556563, 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. 14th Int'l Conf. Financial Cryptography and Data Security, pp. 136149, 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.