Authentication of user Data in Clouds Computing with Multiple Key Generation of Decentralized Manner

Ms. Shruthi J[1], Mr. Avinash[2] ,Ms. Aswini[3],Mrs. Swathi Priya[4]
[1,2&3]Departmet of Computer Science and Engineering, RajaRajeswari College of Engineering, Bangalore, India.[4]Asst. Professor Department of Computer Science and Engineering, RajaRajeswari College of Engineering, Bangalore, India.

Abstract-Cloud computing method is used for storing the necessary information and retrieve information whenever it need to user. For storing information in cloud Access control is one of important tackle with security of user .It done through Authentication method without having User identification. In this paper proposes new way of Authentication that cloud verify the data present in storage without knowing the user identification which known as anonymous Authentication in cloud. This paper have ability to decrypt the data present in cloud And helps user for creation, modification and can access data in cloud. Access control of data and Anonymous Authentication of Data Stored in Clouds done in decentralized manner. So computation,, communication ,storage capacity is enhanced.

Keywords- **Cloud computing , *access control*, *Anonymous* Authentication,**

1.INTRODUCTION

Cloud computing is most demanded technologies used for storing data in both academic and Indusial
Worlds. User can store the data in Cloud Computing offers including usage of resources. Data stored in cloud is very sensitive like Military information, social network and Medical Records. So data can be misuse. To avoid this, security and privacy It should provided in cloud computing. For purpose, user must authenticated itself before going any computation and data fixed that cloud does not recognized with other out sides users.
Privacy of user is validity is verified, who stored data in cloud, so for this reason it's required for other users do not know identify of user. The cloud provides many services user who stored data. The cloud provides responsibility of it's services and validity is verified, who stored data in cloud.
The cloud is reduced the server users can stored their computation and storage to servers (also called clouds) using Internet co inside attack. Data should be encrypted to provide security for cloud's data.. The cloud can able to return record that satisfy requirements. Cloud Computing represents a major conceptual shift, introducing new elements in programming models and development environments that are not covered in traditional technologies. Responsibility of clouds is a very challenging task and involves technical concept and follow the rules. User or cloud can reject the operation performed by cloud. It should have important to log of the inter changing information performed; however, it is an important task to decide how much information to keep in the log. Access control in cloud is different from other because only related user can access who are authorized. Cloud have more storage space so more information can be stored , and much of this is sensitive information. This kind of access control mainly used in health care. AS it mention in easier, Clouds can used to store sensitive information related to patients that gives access permission to medical professionals, hospital staff, researchers, and policy makers. It have access control in manner of only valid user can access information.
Stored record can be encrypted using ABE Protocol . Set of Key and corresponding Keys are generated by user. Using encrypted data only valid user can enable to decrypted the data stored in cloud. Access control in health care has been studied in [1] and [2].
However, exiting method take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. Single KDC is difficult for storing more data. We, therefore, more important that clouds should take a decentralized approach while give secret keys and attributes to users in distributed manner. clouds to have many KDCs in different locations in the world as naturally. Although proposed a decentralized approach. The main drawback was that a user can create and store a file and other users can only read the file. Write access was not permitted to users other than the creator. our scheme is resistant to reply attacks, in which a user can replace fresh data with stale data from a previous write. This is an important property because a user, revoked of its attributes, might no longer be able to write to the cloud. We, therefore, add this extra feature in our scheme and modify appropriately. Our scheme also allows writing multiple times which was not permitted in our earlier work [5].

2.REALTED WORK

The older one is take centralized approach and has only one KDC for encryption and decryption operation. To make operation easy and more convent to the user multi authority is implemented using ABE, that has more number of KDC for encryption and decryption process. Recently, Proposed schema is fully decentralized ABE .In this approach user can have one or more attributes form from each user's authority. In this approach decryption process is done at end so, it might be time consuming process . So, this technique may be diffirent and inefficient in User's mobile device..

3 BACKGROUND

In this section, We present advance and modern method is used.
We make the following assumptions in our work:
1. Cloud admin should be available to user to check validity of User.
2. Cloud can able to read or write the data.
3. Secure shell protocol, SSH is used to secure the data communication between user and cloud.

4 .PROPOSED PRIVACY PRESERVING AUTHENTICATED ACCESS CONTROL SCHEME

By proposed work, privacy is provide to user data which is stored in cloud. For this purpose two protocol are used there are ABE and ABS. According to fig1 three User are present three are creator, reader and writer. Creator can create data in cloud. Reader can read the data present in cloud storage. Writer can able to update the information. Creator able to receives a token from the trustee. Trustee are more Honest to the work. A trustee can be like the federal government who manages social insurance numbers etc. Trustee can generated token by using user id like insurance number. Here are multiple KDCs are used which are which scattered in Cloud storage. For example, servers can present in different parts of the world. By using token User can have encrypted/decrypted key, by providing token to one or more KDC . In the Fig. 1, SKs are secret keys given for decryption, Kx are keys for signing. Permission of Accessing the data can be provided by Access Policy. The claim policy Y decides by creator. under this claim her authenticity and signs the message can be checked. It generates ciphertext C with signature is c, and is sent to the cloud storage. Signature and stores the ciphertext C can be verified by cloud. In the same way reader can read Data presenting in cloud by using Ciphertext C. User is verified at every step in designing the verification method so user.
Should present in the process so, it can time consuming. The Decryption is done using the secret keys it receives from the KDCs When a reader wants to read some data stored in the cloud . If more than one attributes matching with the access policy, then Secrete Key can be decrypts the information stored In the cloud. in the same way as file creation is done in write process. By designating the verification process to the cloud, it relieves the individual users from time consuming verifications.

4.1 Data Storage in Clouds

User can stored the data using the clouds. If revocation process is proceeded for any user, then it is not possible to Access the data present in cloud.

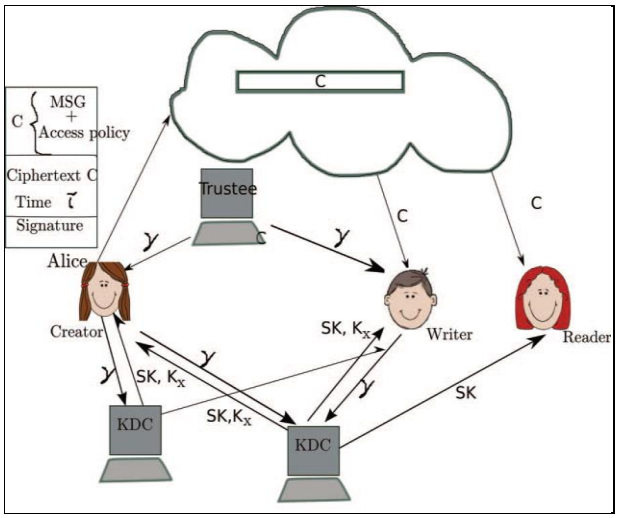

Fig. 1. Our secure cloud storage model.

.

4.2 Reading from the Cloud

The cloud sends the ciphertext C using SSH protocol when user want to read the data. Decryption process with done by using algorithm ABE and the message MSG.

4.3 Writing to the Cloud

To updated or modify write an already existing file, the user must send its message with the claim policy as done in file creation. The claim policy verified by cloud only if the user is valid, then it allowed to write or modifies file details.

4.4 User Revocation

In this schema user revocation will provided. As in above operation like reading, writing from cloud will done by only valid user, who are registered in admin.
If user is revoked from any organization he have no rights to access the data present in cloud storage.

5. SYSTEM ARCHITECTURE

The process of defining and designing the different components, modules, interfaces and data form a system to satisfy user specified requirements is known as System architecture.

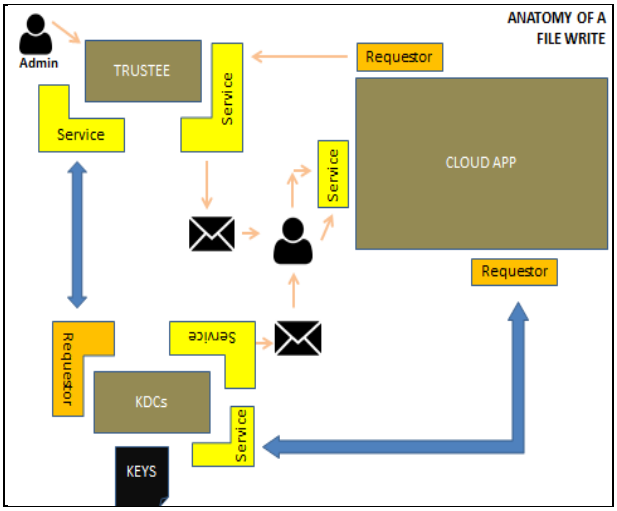

Fig. 2 The architecture of decentralized access control in anonymous authentication of data in cloud

Employee will request Cloud App for Token. Cloud App on be off of Employee forward Request to Trustee. Admin login to Trustee to acceptor Rejected Trustee, then it sends the tokens to Employee in Email upon approval from Admin. Employee Request Cloud App for keys She/he send Token for Request. Cloud App on be off of Employee requirement forward the Token to KDC to New keys generation. KDC will request the Trustee to check if token valid or not. Upon validation, KDC will generate set of keys. Pointer to keys will be return to Employee through on Email. Employee provides the Data along with key pointer to cloud for Encryption. Cloud apps forwards Data and pointer to KDC it will encrypt the Data will generate at the end.KDC forwards encrypted Data to Cloud App. Cloud App write encrypted Data to Google Cloud.

6 REAL LIFE EXAMPLE

Suppose is a law student need to send a different kind of reports about announcement of social issue . by authorities of organization A to all the professors of Organization A, Research chairs of Organization A; B;C and students present in Co-responding department Organization X.

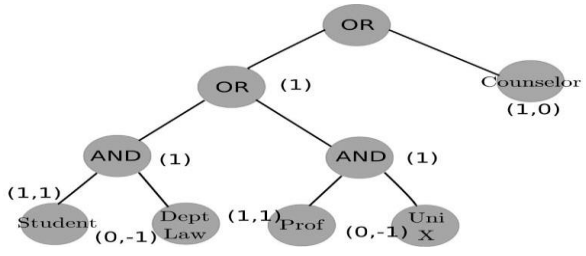

Fig. 3 Example of claim policy.

User wants to remain anonymous(Not have any identification), when realizing all proofs. All information is stored in the cloud. users should not be able to know their identity, but must trust that the information is from a valid source it is validated in admin.

7. COMPARISON WITH OTHER ACCESS CONTROL SCHEMES IN CLOUD

We compare our scheme with other access control schemes and it mentions that our scheme supports many features that the other schemes did not support
Other schema do not have writes which is present in our approach. Authentication of user is provided who store the data in cloud and this in form decentralized
Manner so only valid user can stored the data. Authentication is done in such a way that ,identity of user will not visible to out side users.
In many schema single Key Distribution Center is Used for encryption/Decryption of data in cloud. So, it is difficult to store more information in cloud. To over come this more number of KDC is used. Our scheme also supports privacy preserving authentication, which is not presented by others. One of expensive operations involving in this approach is pairings and it is done by the cloud service. This Access control can allow only valid user who are registered in admin. User revocation is done in this Access control so ,canceling of information is done when user revoked organization. The protocol used in this approach that are ABE &ABS have the ability to read and write data which is present in cloud .No limitation of on storing information in cloud. Our schema have ability to avoid the reply attack.

8.CONCLUSION

We have presented a access control in decentralized manner with anonymous(not have identity of itself to out sources) authentication. It supports user revocation in which after revoking the organization user not have ability to access data in cloud. and
Avoid replay attacks. The cloud does not know the identity of the user who stores information, but
Authentication is done in from registering information in cloud .Key are distribution in form decentralized manner. One drawback is that the
Access policy of each record will present in cloud .In future enhancement , attributes and access policy of a user will be protected by hiding process.

REFERENCES

[1] 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,"
[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information,
[3] 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
[4] F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems," 2011
[5] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. ,2011.
[6] http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cs-01-en.pdf, 2013.
[7] http://securesoftwaredev.com/2012/08/20/xacml-in the-cloud,2013

[8] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure Threshold Multi-Authority Attribute Based Encryption without a Central Authority,"Proc. Progress in Cryptology, 2008.
[9] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. 2009.
[10] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABE Ciphertexts," Symp., 2011.
[11] K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems," IACR 2012.
[12] A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), , 2011.
[13]W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and Efficient Access to Outsourced Data," Proc. ACM 2009.