ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

A Secure Scalable and Efficient Access Control Using Public Verifiable Schema in Cloud Computing

Y. Samreen Begum, Dr. S.Vasundra,

M. Tech, Dept. of CSE, JNTUA, AP, India

Professor, Dept. of CSE, JNTUA, AP, India

ABSTRACT: Several data hiding methods have been recently proposed which can provide the security by hiding the data. Integrity of the data is having risk in the cloud. The Cloud Server (CS) could plan to hide the data, when data loss caused by server hacks or failures to keep up reputation. The randomization is predictable to increase the security of the system and also increase the capacity. One of the good cryptographic solutions to this problem is Cipher text Attribute Based Encryption (CP-ABE). Key technology is one of the significant factors in information sharing. In proposed system by applying encryption the information system presents an additional challenge with regard to the user revocation. Dynamic revocation of cipher policy attribute based encryption mechanism is potential to eliminate access from users without delivering new keys to other users. In this proposed system users individually request the owner to add, update, and modify or remove the value of one attribute freely without knowledge of other attribute.

KEYWORDS: CP-ABE, Removing threads, Revocation, Dataprivacy, Fine-grained accesscontrol.

I. INTRODUCTION

Data distribution is the records of making data used for network and calculating power to many people for sharing their data with external storages easily. People can contribute their enthusiasm with friends by uploading their personal things like data, pictures or messages into the online social network. The Security management is difficult when number of users increase and communicating with resources is typical and non trivial. Over the years, numerous, complex access control mechanisms have been proposed to make sure the authorized access. These approaches are based either on a cryptographic technique or on any non-cryptographic mechanisms. Among the cryptographic approaches, the popular approach is Attribute-Based Encryption Cipher text Policy (ABE-CP).
In CP-ABE, a user‘s secret key is based on a set of attributes (i.e. credentials of that user) and the cipher text is created based on the defined policy [1] [2]. Therefore, a customer is able to decrypt the cipher if the attributes in the secret key of user satisfy the policy defined in the cipher text. In data sharing system CP-ABE has many conflicts. In CP-ABE, the key generation Center (KGC) generates personal keys of customers by making use of the KGC‘s master secret key. The main goal of this method is to reduce the processing and storing public key certificates using traditional public key communications.

Different versions have been introduced to afford more meaningful attribute based encryption systems. The two important ABE’s are.

1. Key Policy ABE (KP-ABE).
2. Cipher Policy ABE (CP-ABE).

KP-ABE and CP-ABE cooperate together by which CP-ABE reverses the execution of Key Policy ABE. The encryption is associated to access structure. The key generation center distributes the private keys to the users. Users can decrypt only if attributes satisfies the access structure. In this context full control goes to the data owner.
The remaining paper is organized as follows. In section 2, related works are discussed. Our future scheme is obtained in section 3 contains proposed methodology and the results are presented in section 4. Finally the paper is concluded in section 5.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

II. RELATED WORK

CP- ABE, a user secret key is connected with set of attributes, and the encrypted data is correlated to access policy. The user can decrypt the cipher text when the attribute set satisfies the access strategy of the secret key. In many distributed systems a user can access the data if a user obtains a certain set of attributes. Bettencourt et al.'s [2] proposed a policy to deploy a trusted server to save the data and access control. They are created public key revocation encryption systems with small cryptographic private and public keys. Their systems have two important features related to size of public and private key. In this public keys are short and enable a user to create an encrypted message that revokes an unbounded number of users.

Wang, Q et al.'s [3] calculated the cryptographic key that must be saved securely on the receiving device. The devices like sensor nodes have little memory and they are high in cost. So that storing private key in the devices is not benifitable. A. Sahi et al.'s [4] proposed Identity-based encryption which is an alternative to public-key encryption. This encryption removes the necessity for Public Key Infrastructure. Pandey et al.'s [6] proposed a method which proposed fine-grained access control of public data. In this method each user has a set of attributes and the data in encrypted form. It is potential for the user to decrypt a cipher message individual, if attributes meets the access policy.

In order to eliminate threats related to private key sharing, single trusted authority is made available to generate the private by using master secret information. Chase et al. [8] proposed KP-ABE scheme that explains the key Escrow problem in a multi-authority scheme. In this method, all attributes which are not combined, with key generation protocol. So that they cannot collect belongs to the similar user. Major disadvantage here is the performance degradation. Because there is no centralized authority with master secret information, where all attribute authorities should communicate with the other authorities to generate a user's secret key. This results in $O(N^2)$ communication overhead on any rekeying phase, and requires each user to store $O(N^2)$ additional auxiliary key components in addition to the attributes keys, where N is the number of authorities in the system.

Recently, Chow [9] proposed an unspecified private key generation protocol which can copy a private key to an authenticated user without knowing the list of user's identities. It seems that unspecified private key generation procedure works properly in ABE systems when an attribute is an identity. However, we this cannot be modified to ABE systems due to two reasons. First is, in Chow's protocol, identities of customers are not public anymore, atleast to the KGC, because the KGC can make user's secret keys otherwise. Since public keys (attributes in the ABE setting) are no longer public, it requests additional secure protocols for customers to get the attribute information from attribute authorities. Second, as the collusion attack among customers is the main security threat in ABE, the KGC issues modified key components to users by blinding them with a random secret even if they are associated with the same set of attributes.

III. PROPOSED SYSTEM

In this proposed system, CP-ABE method is used for verification. The functioning of the proposed system is as shown in the fig:1

Fig: 1. Data sharing system Architecture.

The structural design of records distribution system includes the following entities:

Data Owner: It is a client who keeps data, and needs to upload it into the external records storing center for ease of sharing or cost saving. It is the duty of a data owner to defining (attribute based) access policy and make sure on its own data by encrypting the data under the policy before distributing it. Data Owner encrypts the file which is to be sent using the key which is generated by key generation center.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Data Storing Centre: This is an entity which provides data sharing services. It is used to controlling the accesses from outside users. The data storing center has ability that generates modified user key along with key generation and revoke attribute group keys to effective users.
User: This is an entity that needs permission to access the data encrypted by data owner. User can decrypt only when satisfies the access polices of attributes defined by the data owner. It is impossible to revoke in any of the attribute groups, to the user. Then user will be able to decrypt the cipher text and obtain the data.
Key Generation Policy: This is a responsibility of key generator to generate public key and secret keys for CP-ABE. The main role of key generation center are issuing, revoking, and updating attribute keys for users. It grants accessing to individual users on the basis of their attributes. Key generation is the procedure of generating keys meant for encryption and decryption purposes.

IV. RESULTS

The performance evaluation of proposed work is evaluated and compares it with CP- ABE. This provides security by preventing key and cipher text components exchange. The results are shown in fig: 2

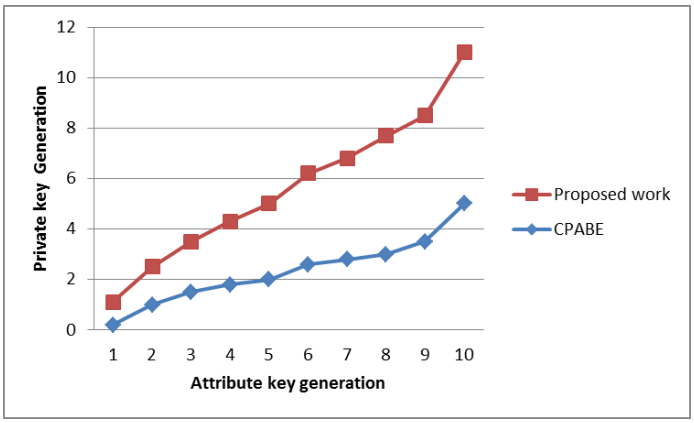

Fig: 2. Key generation

In fig: 2, Attribute keys are generated for one user. By using one key the users should wait until his or her session completes. In CP_ABE uses individual key for every user. The quantity of keys generated by Attribute key is less when compared with CP_ABE.

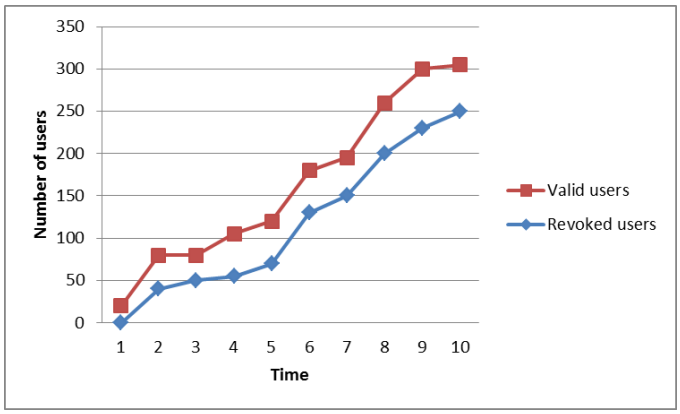

Fig: 3. Number of users in attribute group.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

In fig: 3, the attribute group contains revoked users. Where as in CP-ABE the users are more due to individual sessions for every user at the same time every user contains different policies. So, number of users is more in CP-ABE when compared with users in attribute group.

Component	Proposed Work (bytes)	CP-ABE (bytes)
Public Key	1316	1316
Master Key	152+(t+1)24	148
Private Key	128+(a+212)n	128+(a+168)n
Cipher Text	168+8i+(176+a)1	168+8i+(176+a)1
Proxy Key	24t	NA

Table: 1. Component size and Communication overhead.

Table 1 shows the sizes of the components involved in the system, considered based on group members. Elements consist of the degree of polynomial; n are the quantity of attributes in private key, and the string length of an attribute. Public Key includes a string describing the pairing used (980 bytes). Hence, conversion of a cipher text with l leaf nodes in the policy will need to transfer 124l bytes each way. Therefore, overhead is reasonable for users in proposed system.

V. CONCLUSION

To get more secure and fine-grained data access control in the data shared system, the proposed scheme is well-organized and scalable to secured user in the record sharing system. The encryption scheme is implemented and compared it with CP-ABE. The consequences show that proposed work is scalable in terms of computation and communication. In future, we are expecting to encrypt multimedia files, by improving the performance degradation of completely distributed approach. This is to avoid key expired time, by using multi Data Storing Centre, and Proxy servers to update user secret key without disclosing user attribute information.

REFERENCES

[1] Hur, J. (2013). Improving security and efficiency in attribute-based record sharing. IEEE transactions on knowledge and data engineering, 25(10), 2271-2282.
[2] Bethencourt, J., Sahai, A., & Waters, B. (2007, May). Ciphertext-policy attribute-based encryption. In Security and Privacy, 2007.SP'07. IEEE Symposium on (pp. 321-334). IEEE.
[3] Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2011). Enabling public auditability and data dynamics for storage security in cloud computing. *IEEE transactions on parallel and distributed systems*, *22*(5), 847-859.
[4] P. Traynor, P. McDaniel, and B. Waters. Secure attribute-based systems. In CCS '06: Proceedings of the 13th ACM conference on Computer and infrastructures security, pages 99–112, New York, NY, USA, 2006. ACM.
[5] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006, October).Attribute-based encryption for fine-grained access control of encrypted data.In Proceedings of the 13th ACM conference on Computer and communications security (pp. 89-98).Acm.
[6] Boldyreva, A., Goyal, V., & Kumar, V. (2008, October). Identity-based encryption with efficient revocation.In Proceedings of the 15t[4] A. Sahai, B. Waters, ―Fuzzy Identity-Based Encryption,‖ Proc. Eurocrypt 2005, pp. 457–473, 2005.
[7] A. Lewko, A. Sahai, B. Waters, ―Revocation Systems with Very Small Private Keys,‖ Proc. IEEE Symposium on Security and Privacy 2010, pp. 273–285, 2010.
[8] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. (2007, October). Provable data possession at untrusted stores.In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 598-609).Acm.
[9] Chow, S. S. (2009, March). Removing Escrow from Identity-Based Encryption.In *Public Key Cryptography* (Vol. 5443, pp. 256-276).