Data Access Privilege With Attribute-Based Encryption and Users Revocation.

Amol Dagu Shelkar[1], Prof. Rucha Ravindra Galgali [2]

Department of Computer and Science Engineering
Shreeyash College of Engineering, Aurangabad, Maharashtra, India

Abstract—Cloud Computing Providers tremendous advantages, like flexibility, low cost on usage, on demand accessibility. But various privacy problems are related to the privacy, because data are stored on cloud server. To solve the problem related to the data privacy various schemes are proposed based on the attribute based encryption techniques, still more attention is on privacy of the data content and the access control of the data and less attention is on the privilege control and the privacy of user's identity. In these papers presents Anony Control scheme which address data privacy as well as users identity privacy also presents Anony Control-F for fully preventing the identity problems. In proposed scheme we add user revocation in users to enable activating and deactivating users to enhance efficiency of system and adding more feasibility. Revoked users are maintained in the revoke user list, will decide which user should may in cloud storage server to access data or which will remove. The data access privilege will be depending upon misbehavior of user in cloud server.

Keywords— Cloud computing, revocation, attribute-based-encryption.

1. INTRODUCTION

Cloud Computing has great benefits in today's IT Business system and industries. It provides computing resources through witch various computations are performed dynamically. Also there are many challenges regarding to the cloud computing. Some of these are the data privacy, user's identity and security. Data privacy is related to the contents of data which is outsource to the cloud server and the access control for granting privileges about the manipulation of data. Also the user identity privacy, because the authentication is done based on the user's personal information. So any one does not know about the identity of users. Personal information should be protected.

Also existing system does not provide facility of user revocation so integrity of data is not maintained. Revoked user also able to access and modified the shared data in existing system. So to avoid this there is need of revocation.

Various techniques are there to protect the data contents privacy. Identity-Based-Encryption which is introduced by Shamir [1] tells that, Sender of message can specify an identity which is match with receiver of message then and then only receiver can decrypt the message.After that Fuzzy Identity-Based Encryption [2] is proposed, soon after, more general Key-Policy Attribute-Based Encryption (KP-ABE) [3] have some problems associated with this scheme and this problems are overcome in the scheme named Cipher text-Policy Attribute-Based Encryption (CP-ABE) [4]

More efforts given to the data confidentiality while less effort is given to protect users' identity privacy. Users identities, are described through the attributes, like ph no, address, name etc and are allow to be seen to the key issuers. But a user wants to keep their identities secret while they get their private keys. So, this paper propose AnonyControl and AnonyControl-F to allow cloud servers to control users' access privileges without knowing their identity information

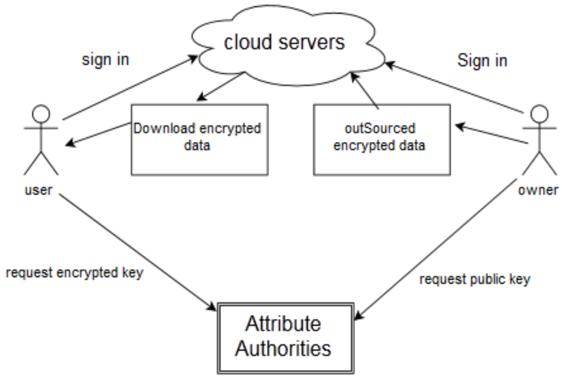


Fig.1.System Architecture

Related Work

Chase [5] gave a multi-authority ABE scheme using the concepts of a trusted central authority and global identifiers many attribute based encryption schemes are proposed having multiple authorities [7] .Authenticated access control for providing data security in the cloud is proposed which provides access to only valid users [8].

[9]In this secure data sharing among the dynamic groups without disclosing the identity information of the users. Lewko [10] and Muller [11] work of this both are the much

same in that they decentralize the central authority in the cipher text attribute based encryption into multiple ones.

Wang [12] proposes a secure and dependable cloud storage service, to address the security problems for the correctness of the data in cloud. They proposes a flexible distributed storage integrity auditing mechanism, this allows users benefit as lightweight communication and computation cost.

Lin[13] presents multi authority attribute based encryption without central authority. In ABE user is identified by attributes, and some of attributes are required to at the time of decryption to decrypt the cipher text and Chase proposed a scheme for that required central authority.

2. POBLEM STATEMENT

- Existing System:

To solve the problem related to the data privacy various schemes are proposed still more attention is on privacy of the data content and the access control of the data and less attention is on the privilege control and the privacy of user's identity. Existing system presents AnonyControl scheme which address data privacy as well as users identity privacy also presents AnonyControl-F for fully preventing the identity problems.

A System Architecture for Existing System

In Existing system, fig.1 shows that there are four types of entities-
Attribute Authorities, Cloud Server, Data Owners and Data Consumers.
A user can be a Data Owner and a Data Consumer simultaneously.
1) Authorities:

- It is assumed that they have powerful computational abilities, attributes contains users personal information which is identifiable.
- Attribute set is divided into N disjoint sets and is controlled by each authority.

2) Data Owner:

- He has to register himself to Multi-authority system with various attributes.
- They want to outsource encrypted data file to the Cloud Servers.
- For outsourcing data file 1st he has to get public key from Multi-authority system to upload it on cloud server

3) Cloud Server:

- It is assumed to have big storage capacity.

4) Data Consumers:

- They request for their private keys from all the authorities.
- Authorities then create corresponding private key and send it to them.
- After that Data Consumers are able to download any of the encrypted data files, but only those for which its private keys satisfy the privilege tree.
- Proposed System:

For security reasons, when a user leaves the group or misbehaves, this user must be revoked from the group. As a result, this revoked user should no longer be able to access and modify shared data, and the signatures generated by this revoked user are no longer valid to the group. New keys are generated and broadcasted among the valid users.

A System Architecture for Proposed System

Different users may leave or join the group and different blocks are signed by different users. When any user leaves the group or misbehaves then this user must be revoked from the group and after that this user should not able to access and modify the data. Also signature generated by this user is not valid, that means user does not able to access or modify the shared data and the contents of shared data is not altered during the process of user revocation.

Now there is need to resign the blocks by existing user which were previously signed by the revoked user. So revoked user will not be able to access or modified the data, as new signatures will be generated for existing users and that will be broadcasted to the all remaining user. As a result integrity of data is maintained. But as in existing system user revocation is not used which can make unsecure environment.

Following fig.2 shows that the general flow of Proposed System.

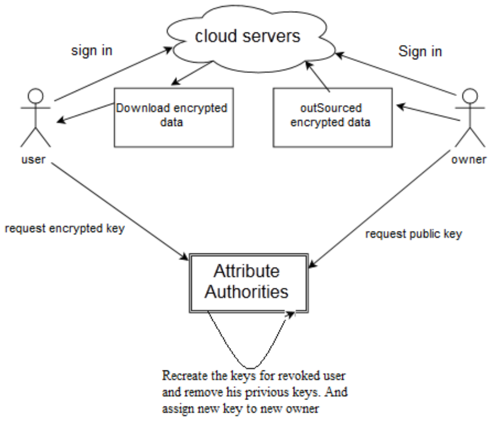

cloud servers
sign in
Sign in
Download encrypted data
outSourced encrypted data
user
owner
request encrypted key
request public key
Attribute Authorities
Recreate the keys for revoked user and remove his privious keys. And assign new key to new owner

Fig.2. System Architecture of Proposed System

3. MATHEMATICAL MODEL

Set Theory:

User Model:

Set of user entities U€{Do,Dc}

Do= {Do1, Do2, ……Don}→Set of Data Owner

Dc= {Dc1, Dc2, …….Dcn}→Set of Data Consumer

Each data owner and data consumer have attribute set

A(Do) → {Attr0, Attr1,……………….,AttrN}

A(Dc) → {Attr0, Attr1,……………….,AttrN}

Authority Model:

Each user of type Do, Dc has to register with N attribute authorities.

Authorities Au = {A0, A1, A2………………..AN}→ There are N authorities

Each authority Ai has to kept attribute of user U.

User can upload multiple files F= {f1, f2 …fn}

S={ O, U, MA, C, Pb, Pr}

S: System

O: {Set of owners O1, O2, ..., On, who requests public key , encrypt data and upload it on cloud}

U: {Set of users U1, U2, …,Un, who requests private key

from MA then using that private key decrypts encrypted data downloaded from cloud}

MA: {multi authority server who generates keys for respective end users}

C: {All the data stored in cloud}

Pb: {Public key from multi authority server requested from

owner}

Pr: {Private Key from multi authority server requested from

user}

Venn Daigram:

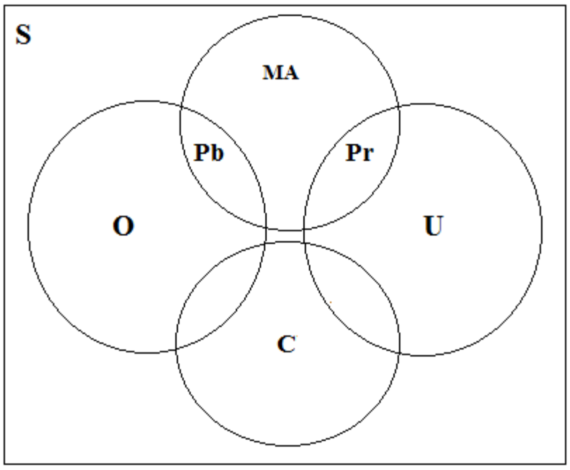


Fig.3. Venn Daigram

4. Algorithms

To implement the existing system we use the ABE and AES

Algorithms

1. End users i.e. owner {O1,O2,..,On} and consumer {C1,C2, . . ., Cn}will register themselves with the system with his own attributes{AT1,AT2,…,ATn}.
2. Multi Authority system uses ABE for generating key *PK* and *PrK*.
3. Data owner uploaded encrypted file done by AES to server *S* by using public key *PK* from Multi Authorities *MA*.
4. Consumer downloaded File by requesting private key *PrK* from Multi Authorities *MA* and decrypted it.

Algorithm for proposed invocation System:

When some revocation happened in group then again new keys generated by multi authority and broadcast it to the users.

For that following steps followed:

Step 1: ReKeyGen(°,MK) It takes as i/p an attribute set ° that includes attributes for update, and current master key MK. It gives o/p new master key MK′,also new public key PK'.

Step 2: ReEnc(CT, rk, ¯) It takes as input a cipher text CT, the setof proxy re-key's rk having the same version with CT, a set of attributes ¯ which includes all the attributes in CT's access structure.

Step 3: ReKey(¯D, rk, µ) It takes as input the component ¯D of a user secret key SK, the set of proxy re-key's rk has the same version SK, and a set of attributes μ.

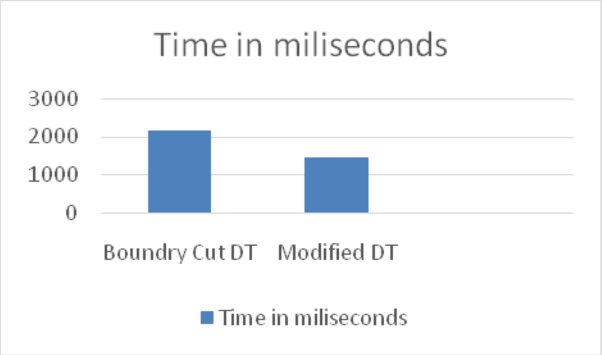
Step 4: Dec (CT, PK, SK) It takes as input a cipher text CT, public parameters PK, and the user secret key SK. It outputs the message M if the attribute set of SK satisfies the cipher text access structure.

Proposed algorithm for DT:

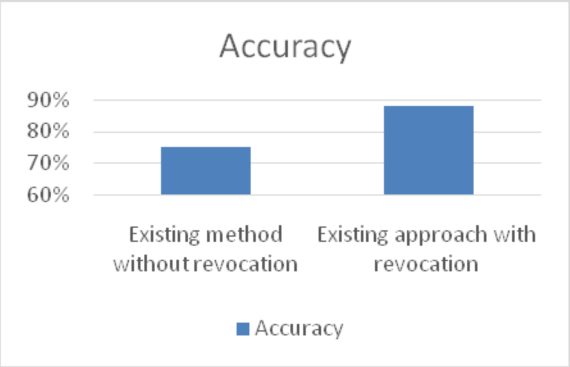
```
Build_DT

1. Single-node tree initialize as root contains all filters:
2. While (current storage <= the predefines storage budget AND some current leaf nodes have > 3 filters)
   {   let S3 = set of leaf nodes have > 3 filters;
       Select v ϵ S3 which requires the longest time to searching a filter in worst case.
       Split node v to produce the CSTs and new child DT nodes
   }
```

5. Expected Results

1) Time Graph:
This graph shows that time required for boundary cut DT is more than the modified DT.



2) Accuracy Graph:
Accuracy of existing system without revocation is less. While in proposed system will be with revocation and it gives more accuracy than the existing system. In short revocation allows access only to the authorized users.



6. Conclusion

Here we are implementing a semi-anonymous attribute-based privilege control scheme to solve the user's identity privacy problem in a cloud storage server.In proposed system for security reasons, when a user leaves the group or misbehaves, this user must be revoked from the group and then this revoked user should not able to access and modify shared data. Also signature generated by this user is not valid, that means user does not able to access or modify the shared data and the contents of shared data is not altered during the process of user revocation.

ACKNOWLEDGMENT

I take this opportunity to express my profound gratitude to my guide Prof. B.Padmavathi and PG Co-coordinator Prof. T.A.Wakade, for her personal involvement and constructive criticism provided beyond technical guidance and model direction, important input and consistent consolation all through the span of the venture. Her important recommendations were of huge help all through my undertaking work. Her insightful feedback kept me attempting to make this venture in a greatly improved manner. Working under her was a greatly learned experience for me. She has been keen enough for providing me with the invaluable suggestions from time to time. Above all, her keen interest in the project helped me to come out with the best.

REFFERENCES

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1985, pp.47–53.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2005, pp 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th CCS*, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE SP*, May 2007, pp. 321–334.

[5] M. Chase, "Multi-authority attribute based encryption," in *Theory of Cryptography*. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.

[6] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proc. 16th CCS*, 2009, pp. 121–130.

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," *Inf. Sci.*, vol. 180, no. 13, pp. 2618–2632, 2010.

[8] S. Ruj, M. Stojmenovic and A. Nayak, ―Privacy Preserving Access Control with Authentication for Securing Data in Clouds‖, 2012:

[9] Kanya Devi J, Kanimozhi S,"Efficient User Revocation for Dynamic Groups In The Cloud", International journal of Engineering And Computer Science ISSN, Vol 3,2014:

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.

[11] S. Müller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," *Bull. Korean Math. Soc.*, vol. 46, no. 4, pp. 803–819, 2009.

[12] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou,―Toward Secure and Dependable Storage Services in Cloud Computing‖, 2012

[13] H. Lin, Z. Cao, X. Liang, and J. Shao, ―Secure threshold multi authority attribute based encryption without a central authority,‖, 2010