Attribute Based Encryption with Privacy Preserving and User Revocation in Cloud

[1]Ms. P.Ranjima, [2]Ms. Sumathi. D, [3]Ms.Minimol Mathew, [3]Ms.Anisha Viswan[4]

[1,3,4] PG Scholar,[2]Assistant Professor,
[1,2,3,4]Computer Science and Engineering, PPG Institute of Technology, Coimbatore, 641035, India

***Abstract*—Cloud computing is an emerging IT service that can create, configure and manipulate applications online. It is a computing in which large groups of remote servers are networked to allow centralized data storage and online access to computer services or resources. Cloud data security plays major role in the cloud computing. Many privacy preserving and auditing system have implemented earlier but those systems hardly support security and data access control. Here, a new decentralized access control scheme for secure data storage in cloud is introduced, that supports anonymous authentication. It verifies the authenticity of the user without knowing users identity before storing data. Also an additional feature like access control is added, in which only valid users are able to decrypt the stored information. This may prevent replay attack and support creation, modification, and reading of data stored in the cloud. Like that it addresses user revocation. Moreover, authentication and access control scheme is robust and decentralized, unlike other access control schemes designed for clouds which are centralized.**

***Keywords*—Cloud computing; Security; Attribute Based Encryption; Replay Attack; Authentication; Access control**.

I. INTRODUCTION

Cloud Computing is a computing platform for sharing the application and data in the remote server as service to other user which been networked. The risks in cloud computing can be quite different from on-premises computing. CSP have to secure our systems from various attacks which are from the internet, tenants and cloud CSP's staff.

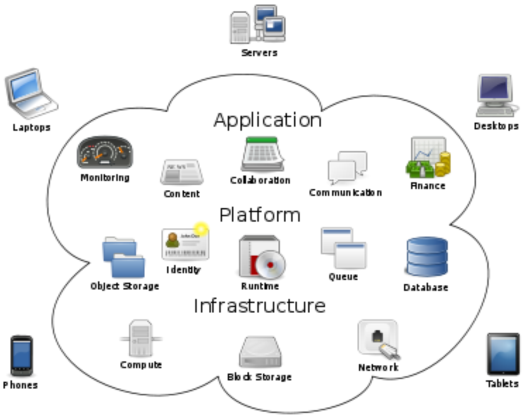

Fig 1.1 Cloud computing

Cloud data faces a lots of security issues. Hence various data security mechanisms are used to tackle these problems that are listed below:

- Access Control
- Auditing
- Authentication
- Authorization

Research in cloud computing is receiving a lot of attention through employment of above mentioned areas. Much of the data stored in clouds is highly sensitive, example, medical records and social networks. Hence cloud data have both security and privacy as important issue. So before initiating any transaction user should authenticate itself, also it should check whether cloud interferes with the data that is outsourced. Likewise privacy of user should be protected, so cloud does not reveals the identity of user. The cloud keeps an account that shows the data it outsources, similarly, the cloud is itself accountable for the services it provides.

Cloud servers are vulnerable to Byzantine attack, where the storage server may collapses in random ways. The cloud is also vulnerable to server colluding attacks and data modification. In server colluding attack, the opponent can compromise storage servers; hence it can modify data files that are consistent for a long time. So the encrypted data provides a secure data storage. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques.

The cloud always concerns about search on encrypted data. It does not know the query to search but it returns the records that satisfy the query. This is known as searchable encryption. The keyword used for the search in encrypted data that returns the result without knowing the actual keyword. The search with exact keyword delivers correct document. Many researchers examined about security and privacy issues in cloud. The homomorphism encryption techniques are suggested, that ensure the data is not able to read while performing computation. The homomorphic encryption that performs computation on ciphertext of data and returns encoded value of the result. The users can decode the result and the cloud does not know anything about data and operation done on it. In those situations, user can verify the correctness of results that cloud returns.

Accountability of clouds is a very challenging task and involves technical issues and law enforcement. It is important to have log of the transactions performed; however, it is an important concern to decide how much information to keep in the log.

II. SYSTEM ANALYSIS

Existing work on access control in cloud are centralized in nature. All other schemes use attribute based encryption (ABE). The scheme in uses a symmetric key approach and does not support authentication. Earlier work by Zhao *et al* [19], provides privacy preserving authenticated access control in cloud. Here, they take a centralized approach, it has a single key distribution centre (KDC) that distributes secret keys and attributes to all users. Unfortunately, a single KDC leads to single point of failure and also difficult to maintain because of the large number of users that are supported in a cloud environment. Hence a decentralized approach can be introduced for distributing secret keys and attributes to users. It is more efficient for cloud to have many KDCs in different locations in the world.

A. Disadvantages of Existing System

- Uses a symmetric key Encryption
- does not support authentication
- A centralized access control architecture
- Use single KDC for key distribution
-

III. PROPOSED WORK

A decentralized approach is modelled with access control mechanism to control the data integrity against the data violation attacks .Multiple Key distribution centres used with distributing secret keys and attributes to users. An attribute based signature scheme can be modelled to achieve authenticity and privacy. The identity of the user is protected from the cloud during authentication. The access control and authentication are both collusion resistant, it means no two users can collude and access data or authenticate themselves, if they are individually not authorized. The revoked users cannot access data after they have been revoked based on authorization rules. Using attribute based encryption user revocation can be achieved.

A. Advantages

- Provides a distributed access control of data stored
- Only authorized user can store or modify data
- Identity of user is protected
- Decentralized architecture provide several KDC for key management
- Revoked user cannot access data
- Tough to replay attacks

B. System Initialization

Cloud storage has to be modeled which is to be used as storage service that provides resizable compute capacity in the cloud. Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations of the hard drive), and the physical environment is typically owned and managed by an application server which utilizes the hard disk or computer or laptop. These cloud storage are responsible for keeping the data available and accessible, and the physical environment protected and running. Cloud storage services can be utilized from an off-premises service or deployed on-premises. Cloud Architecture is been allowed to provision the security mechanism and technique against the data and user identity.

The users for the data access mechanism are

1. Creator
2. Reader
3. Writer
4. Trustee –Trustee issues the token
5. KDC – KDC obtain the token and issues the public and private key for encryption and decryption, signing.

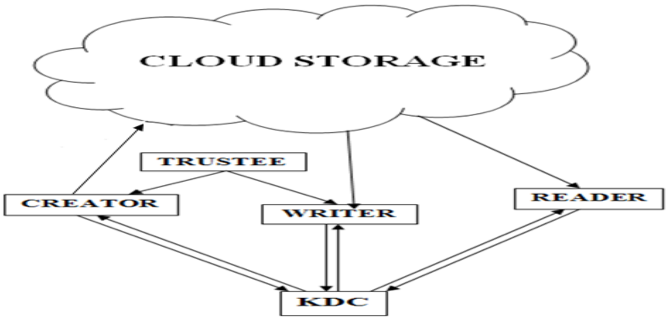

Fig 3.1 System Model

D. Decentralized Access Control Mechanism

Attribute based encryption is used to secure the data and to make only authorized user to get access to the data. Using ABE, the records are encrypted under some access policy and stored in the cloud. Each user has set of attributes and their corresponding keys. For decrypting the information stored in cloud, user's set of attributes should match with access policy.

1) Attribute Based Signature

It is used to secure the identity of the user against the authenticity and privacy, who creates the data. Users have a claim predicate associated with a message, that makes easier to recognize the user as an authorized one, without revealing its identity. Similarly other users can verify authorization and validity of information stored. Usage of ABS with ABE helps to achieve authenticated access control without disclosing the identity of the user to the cloud.

Algorithm of ABS

1. ABS is also uses the hash function for data encryption , Private key and public key for message sign and verification
2. KDC is used to generate token as signing key and signature
3. Token verification algorithm utilized for signature verification
   ABS.sign = for message signing
   ABS.verify = for message authentication without revealing the identity of the user

Encryption Process

Encryption function is modeled as sender decides the access tree through Boolean access structure.

Decryption process

Decryption function takes cipher text, group; secret key, access matrix. Access matrix compares the attributes for similarity.

2) Attribute Based Encryption

KP-ABE, the sender has an access policy to encrypt data. Here, once a writer having attributes and keys have been revoked cannot write back stale information. The attribute authority distributes attributes and secret keys to the receiver and can decrypt the message if it matches with access policy.

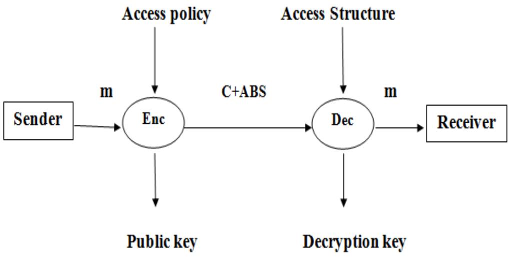

Fig 3.2 Attribute Based Encryption and Decryption

Condition for reading and writing a data in the cloud

To write an already existing file, simply the user sends message with claim policy. Then the cloud confirms the claim policy, and only if the user is authenticated, is allowed to write on the file.

When a user requests data from the cloud, the cloud sends the ciphertext C using SSH protocol. Decryption proceeds using algorithm.

E. Performance Evaluation

The protocol supports multiple read and writes on the data stored in the cloud. In this paper, cost of various existing centralized approaches is comparable. System developed is computation intensive. Time taken for computation is two scalar multiplications time and based on pairing operation .Both of this, gives the minimized time. Scheme supports many features that the other schemes did not support. 1-W-M-R means that only one user can write while many users can read. M-W-M-R means that many users can write and read.

Performance of the proposed system has been evaluated and proved its efficiency. The special features of the cloud security system modelled is as follows

- Execution time to data preserving is less compared to public key cryptosystem as it is supported by the attribute based scheme and processing speed is balanced by implementation of multiple KDC.

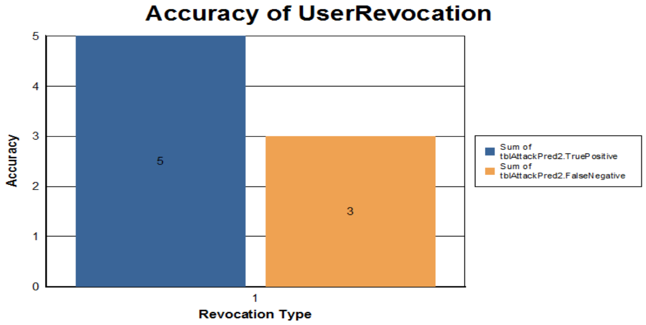

Fig 3.3 Performance of the system is measured with accuracy against the revocation

- Revocation of user is strictly maintained through access policy generation

User authorization and authentication is maintained with attribute based signature scheme

III. CONCLUSION

A cloud system has been modelled and implemented a storage space for data storage through a decentralized access control technique with anonymous authentication with process of attribute based signature scheme, which provides user revocation and prevents replay attacks. And a cloud is unaware about identity of user who stores data, but it can only check the user's credentials through access policies generated by the attribute based encryption. Key distribution is done in a decentralized way with claim policy generation. It achieves privacy and security in the cloud storage using ABE and ABS.

REFERENCES

[1] Amiya Nayak, Milos Stojmenovic & Sushmita Ruj, (2014), "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", in IEEE transactions VOL:25 NO:2.

[2] C. Wang, J. Li, K. Ren, N. Cao, Q. Wang & W. Lou, (2010), "Fuzzy keyword search over encrypted data in cloud computing," in IEEE INFOCOM., pp. 441–445.

[3] G. Wang, J. Wu & Q. Liu, (2010),"Hierarchical attribute-based encryption for fine -grained access control in cloud storage services," in ACM CCS., pp.735–737.

[4] A. Sahai, B. Waters, O. Pandey & V. Goyal, (2006), "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on Communications Security, pp. 89–98.

[5] Kan Yang, Kui Ren & Xiaohua Jia, (2012), "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems", IACR Cryptology ePrint Archive, 419

[6] A. Nayak, I. Stojmenovic & S. Ruj, (2011), "DACC: Distributed access control in clouds," in IEEE TrustCom.

[7] A. Nayak, M. Stojmenovic & S. Ruj,(2014),"Privacy Preserving Access Control with Authentication for Securing Data in Clouds", IEEE/ACM International Symposium on Cluster, pp. 556–563.

[8] K.Maji, M.Prabhakaran & M.Rosulek, (2008),"Attribute-based signatures: Achieving attribute-privacy and collusion-resistance," IACR Cryptology ePrint Archive.

[9] C.Wang, K.Ren, N.Cao, Q. Wang & W. Lou, (2012), "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE T. Services Computing, vol.5, no.2, pp. 220–232

[10] C.Wang, K.Ren, S.Yu & W.Lou, (2010), "Attribute based data sharing with attribute revocation," in ACM ASIACCS, pp. 261–270

[11] H.K. Maji, M. Prabhakaran & M. Rosulek, (2008), "Attribute-based signatures: Achieving attribute-privacy and collusion-resistance," IACR Cryptology ePrint Archive.

[12] K. Lauter & S. Kamara, (2010), "Cryptographic cloud storage," in Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol. 6054. Springer, pp. 136–149.

[13] N. Borisov, P. Mittal & S. Jahid, (2011),"EASiER: Encryption-based access control in social networks with efficient revocation," in ACM ASIACCS.

[14] M. Chase, (2007), "Multi-authority attribute based encryption," in TCC, ser. Lecture Notes in Computer Science, vol. 4392. Springer, pp. 515–534.

[15] M. Chase & S.S.M. Chow, (2009), "Improving privacy and security in multi- authority attribute-based encryption," in ACM Conference on Computer and Communications Security, pp. 121–130.

[16] A. B. Lewko & B. Waters, (2011), "Decentralizing attribute-based encryption," in EUROCRYPT, ser. Lecture Notes in Computer Science, vol. 6632. Springer, pp. 568–588.

[17] Brent Waters, Matthew Green & Susan Hohenberger, (2011) "Outsourcing the Decryption of ABE Ciphertexts," in USENIX Security Symposium.

[18] A. Sahai & B. Waters, (2005), "Fuzzy identity-based encryption," in EUROCRYPT, ser. Lecture Notes in Computer Science, vol. 3494. Springer, pp. 457–473.

[19] F. Zhao, K. Sakurai & T. Nishide, (2011), "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in ISPEC, ser. Lecture Notes in Computer Science, vol.6672,Springer,pp.83–97.