Public Auditing and User Revocation in Dynamic Cloud Environment

Ms. S. Nandhini[1], Mr. N. Premkumar[2], C. Radhakrishnan[3]
[1, 2, 3] Department of CSE
[1, 2, 3] Kongunadu college of engineereing and Technology

Abstract- *Cloud computing is one of the rising technologies. The cloud environment is a huge open distributed system. It is considerable to protect the data, as well as, privacy of users. Access Control methods make sure that authorized users access the data and the system. Access control is generally a policy or procedure that permits, denies or restricts access to a system. It may, as well, observe and record all attempts made to access a system. Hence, OPOR (Outsourced Proof of Retrievability) scheme is proposed so that it does not have pairing operations for the purpose of securely sharing sensitive information in public clouds. OPOR framework resolves both the key escrow problem and revocation problem in identity based encryption and public key cryptography. Also, it overcomes user revocation problem by utilizing a novel public key updation technique. Then it addresses this issue, and implements group signature and dynamic broadcast encryption techniques. Generally, public key updation algorithm is used so as to enable cloud users to share data anonymously with others. The storage overhead and encryption computation cost are reduced in proposed system. And this framework is implemented in NOSQL database.*

Keywords- Privacy preserving, User Revocation, Certificate less encryption, Access control

I. INTRODUCTION

The architecture of cloud security Mell and Grance [1] is effective whenever the correct defensive implementations are carried out. Such architecture of cloud security would identify the issues occurring with security management. These issues are resolved by the addresses of security management with security controls. Different access control models are in use, including the most popular Mandatory Access Control , Discretionary Access Control (DAC) and Role Based Access Control. These models are called as identity based access control models. Furthermore, in these models, the user (subjects) and resources (objects) are identified by their unique names. This identification will be carried out directly help of roles given to the users. In an unchangeable distributed system these access control methods are more effective, where the set of users are available with a known set of services. Based on Bethercourt et al. [2] attributes or characteristics are used for identifying the users and the predefined identities are not used. At this situation, the traditional identity based access control models do not work effectively and thus, the system access should be processed on decisions based on some of the attributes. In the cloud system, a unique set of security policies are used by the autonomous domains. Therefore, the various kinds of domains and policies are supported by the control Mechanism in a flexible manner.

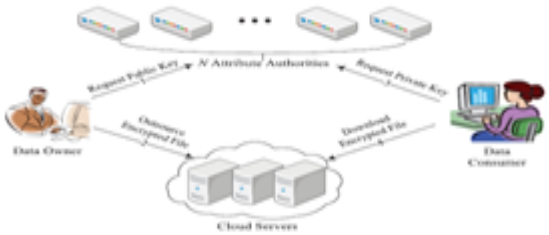

Fig1: General Flow of access control

With the continuous development of large distributed systems, Attribute Based Access Control (ABAC) mechanism has become increasingly important. Figure 1 illustrates the general flow of access control.

II. RELATED WORK

Waters [3] introduced a new methodology for realizing Cipher text-Policy ABE systems from a general set of access structures in the standard model under concrete and non-interactive assumptions. They may be implemented both decisional-Bilinear Diffie-Hellman Exponent (d-BDHE) and decisional-Bilinear Diffie-Hellman assumptions and presented the first cipher text-policy attribute-based encryption systems that are efficient, expressive, and provably secure under concrete assumptions.

Lewko et al. [4] analyze the semi-functional keys and cipher texts are not used in the real system, only in the proof of security. Over a sequence of security games a hybrid argument is employed by the proof. Normal keys and cipher text are used in the initial real security game. In the second game, the cipher text is semi-functional and the keys retain normal. In subsequent games, the keys requested by the attacker are modified to be semi-functional one by one. By the final game, no keys given out are actually useful for decrypting a semi-functional cipher text, and proving security becomes relevantly easy.

Chase and chow [5] is able to prove the capability to do something in an examination and then receive the corresponding credential, without presenting any identifying information. Otherwise, a person may interact with a service by a pseudonym (e.g. a login name) and wish to get attributes relevant to this interaction without revealing the person's full identity.

Goyal et al. [6] presents the first construction of a cipher text-policy attribute based encryption scheme having a security proof based on a number theoretic assumption and supporting advanced access structures. Earlier CP-ABE systems should either support only very limited access structures or had a proof of security only in the generic group model. Our construction may support access structures which may be represented by a bounded size access tree with threshold gates as its nodes.

III. PRIVACY-PRESERVING AUTHENTICATION PROTOCOL

In cloud computing, the major issues are security and privacy. In nature, the existing system has the centralized access control in clouds. The authentication is not supported by this scheme but it uses a symmetric key approach. For the process of both encryption and decryption, the symmetric key algorithm is used. The proposers use a centralized approach where the user receives the secret keys and attributes which are distributed by a single Key Distribution Center (KDC). In existing system [7], for the cloud data storage, a Shared Authority based Privacy preserving Authentication protocol (SAPA) is proposed to address the already mentioned privacy issue.

Figure 2 shows that the SAPA realizes authentication and authorization that does not compromising private information of the user. In cloud storage, new privacy challenge is identified by this system and address a noticeable privacy issue for data sharing while a user challenging the cloud server, in which the challenged request itself should not expose the user's privacy does not matter whether or not it may acquire the access authority. Based on Li et al. [8], authentication protocol is proposed to improve a user's access request related privacy and using the anonymous access request matching mechanism, the shared access authority is achieved. Cipher text-policy attribute based access control is applied to realize that a user may reliably access its own data fields, and adopt the proxy re-encryption to provide authorized data sharing among multiple users. The existing process can implement new approach that is shared authority approach to supports anonymous authentication. The user is authenticated using multifactor approach includes biometric authentication.

The proposed scheme is resilient to replay attacks. In this scheme using Elliptic Curve Diffie Hellman (ECDH) for authentication purpose; ECDH is the one of several cryptographic algorithms adapted from Lewko and Waters [9], most often used to verify that a file has been unaltered. It is also used to implement attribute based access control whereby access rights are permitted to users through the use of policies which accumulate attributes together. The policies can use any kind of attributes (user attributes, resource attributes, environment attribute etc.). In real time cloud environments, this process can be implemented to improve accuracy of the system.

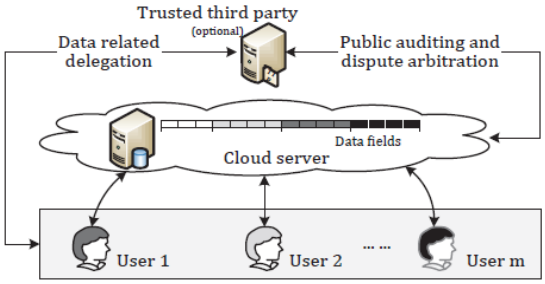

Fig 2: Shared Authority based privacy preserving

IV. PROPOSED METHODOLOGY

4.1 Access control mechanism for user revocation problem:

The cloud storage is a significant service of cloud computing. The cloud storage offers services for data owners to host their data into the cloud. Data security and access control is one of the most challenging ongoing research work in cloud computing, because of users outsourcing their conscious data to cloud providers. Figure 3 illustrates, Access Control can also identify users trying to access a system unauthorized. This is a mechanism which plays a vital role of protection in computer security. Moreover, while updating the cipher texts, all the users require to retain only the latest secret key, rather than to maintain records on all the prior secret keys.

To resolve the issue of privacy on shared data, an OPOR framework is introduced for Secure Data Sharing in Public Clouds introduced Merkle hash tree. This algorithm gives a feasible replacement for traditional public key cryptosystem that needs trusted third party to provide key to band user to their public keys. In this system the overall key management is too expensive and complicate because TTP produces its own signature on each user public keys and manage user keys. Access control mechanism is used in the newly introduced system. To ignore the key escrow problem encrypt each data by employing the access control policy.

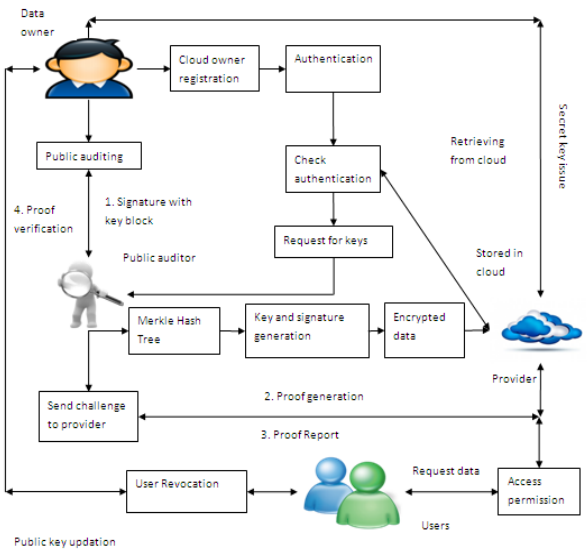

Fig 3: User Revocation Framework

Revocation of users and keys is a well studied, but a nontrivial problem. In our scheme, when a user V is revoked, it is imperative to update public keys of attributes in SV, user attribute secret keys for remaining users who possess at least one attribute in SV, and re-encrypt data whose access structure specifies at least one attribute in SV, where set SV contains all attributes associated with V. If all these tasks are performed by the DMs, it would introduce a heavy computing overhead. Therefore, we propose a scalable revocation scheme, which takes advantage of abundant resources in a cloud by delegating most of the computing tasks in revocation to the CSP. To enable this revocation scheme to work well, we require each attribute a with ID to be bound to a version number, which increases by one whenever a user associated with a is revoked. Correspondingly, each attribute public key is changed into this form: We simply present the scalable revocation scheme by describing the following algorithm:

1. Update Attribute: DMi updates PKta to PKtþ1 a by adding each version number to 1, and outputs a PRE key
2. CreateUpdateKey: To generate an update key for updating PKt 0 a to the latest public key PKt a, the CSP sets Update Key

In this algorithm user initially provide its ID to the cloud which returns private key to the user in interim also item of plain text's owner then encrypt the data using the public key and transmit the encrypted data along the public keys to the cloud and the user downloads and decrypt the data. Based on Yu et al [10] the public key is changed for entire groups, if the user revoked from the group.

V. EXPERIMENTAL RESULTS

In this section, the performance of the system is evaluated using the performance metrics such as storage overhead, communication cost and computation efficiency. In cloud storage systems the storage overhead is one of the most important issues of the access control scheme. In our scheme, besides the attributes storage, each shared authority id also requires to store a public key and a secret key for each user in the system.

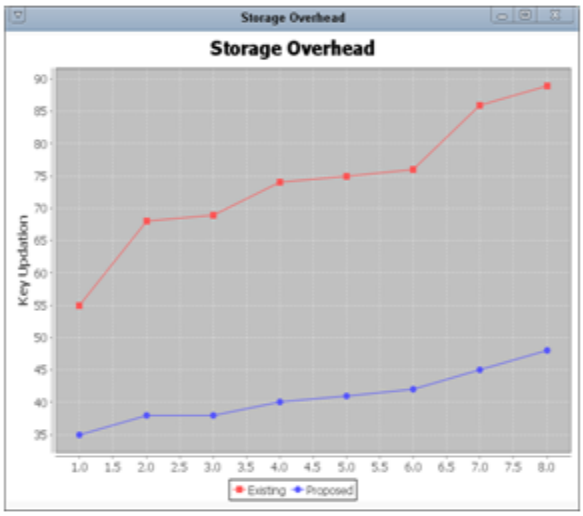

Fig 4: Storage Overhead performance

Figure 4 depicts the storage overhead on each shared authority in proposed scheme is also linear. The same communication cost is produced for the normal access control. The communication cost of attribute revocation is linear to the number of decrypted data which contain the revoked attribute. Figure 5 shows the computation efficiency of both encryption and decryption is compared in two criteria: the number of authorities and the number of attributes per authority.

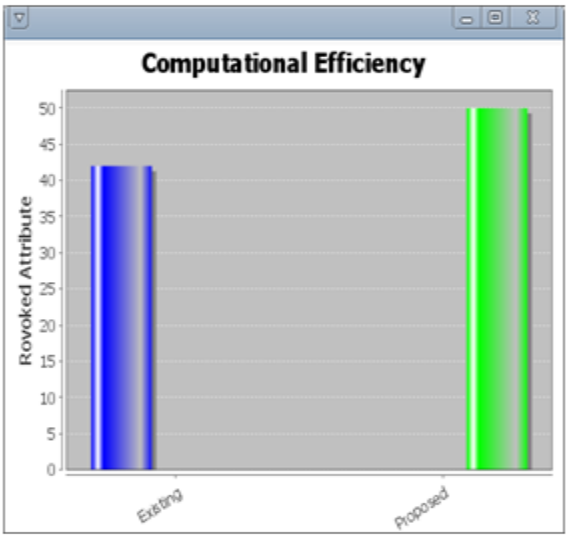

Fig 5 Computational Efficiency

VI. CONCLUSION

Cloud computing is world's best innovation which uses advanced computational power and improves data sharing and data storing capabilities. It increases the ease of usage by providing access through any race of internet connection. As every coin has two sides it also has some drawbacks. Cloud storage has a major issue of privacy security. To ensure that the risks of privacy have been mitigated, a variety of techniques can be used in order to achieve privacy. In this project, among the dynamic groups, the data file is shared securely. Without exposing their identity, members within the group can share the data efficiently. Public key updation is used for entire security. When compared to other algorithm, key size is very small; it is not able to be hacked easily. Revocation list is used for efficient revocation without updating private keys of remaining users. Key management can be focused so as to revoke the private keys from the group members and updated the public key for each groups.

REFERENCES

[1] Ateniese.G, Burns.R.C, Curtmola.R, Herring.J, Kissner.L, PetersonZ.N.J, and Song. ProvabledataD.X possession at untrusted stores. In Proceedings of the2007 ACM Conference on Computer and CommunicationsSecurity, CCS 2007, pages 598–609, 2007.

[2] Boneh.D,. Boyen.X, and Shacham.H. Short groupsignatures. In In proceedings of CRYPTO'04, volume 3152of LNCS, pages 41–55. Springer-Verlag, 2004

[3] Chang E C., Xu J., (2008) "Remote integrity check with dishonest storage server," in Proceedings of ESORICS, volume 5283 of LNCS. Springer-Verlag.

[4] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In Advances in Cryptology (CRYPTO'01),volume 2139 of LNCS, pages 213–229, 2001.

[5] Hsiao.H.C, Lin.Y.H, Studer.A, Studer.C, Wang,H. Kikuch.K.Hi,Perrig.A, Sun.H.M, and Yang. A studyof.B.Y user-friendly hash comparison schemes. In ACSAC,pages 105–114, 2009.

[6] Juels.A and B. S. K. Jr. Pors: proofs of retrievability forlarge files. In Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, pages 584–597, 2007.

[7] Li J., Kim K.,(2010) "Hidden attribute-based signatures without anonymity revocation" Information Sciences, vol. 180.Oprea A., Reiter M.K., Yang K.,(2005) "Space-efficient block storage integrity," in In Proc. of NDSS.

[8] Schwarz T.S.J., Miller E.L.,(2006) "Store, forget, and check: Using algebraic signatures to check remotely administered storage," in ICDCS '06: Proceedings of the 26th IEEE International Conference on Distributed Computing Systems. Washington, DC, USA: IEEE Computer Society.

[9] Shah M.A., Swaminathan R., Baker M.,(2008) "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, http://eprint.iacr.org/.

[10] Wang C., Wang Q., Ren K., Lou W.,(2010) "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM.

[11] Wang Q., Ren K., Yu S., Lou W.,(2011) "Dependable and secure sensor data storage with dynamic integrity assurance," ACM Transactions on Sensor Networks.

[12] Zheng Q., Xu S.,(2011) "Fair and dynamic proofs of retrievability," in CODASPY.

[13] Zhu Y., Hu H., Ahn G.J., Yu M.,(2012) "Cooperative provable data possession for integrity verification in multicloud storage," IEEE Trans.

[14] Zhu Y., Wang H., Hu Z., Ahn G.J., Hu H., Yau S.,(2011) "Dynamic audit services for integrity verification of outsourced storages in clouds," in SAC.