Secure Data Sharing Among Multiple users in Cloud Computing

Aishwarya Shetty
Engineering Student
Department of ISE
AMC Engineering College, Bangalore.

Archana
Engineering Student
Department of ISE
AMC Engineering College, Bangalore.

Bhavya Y.P
Engineering Student
Department of ISE
AMC Engineering College, Bangalore.

Varun Rao
Engineering Student
Department of ISE
AMC Engineering College, Bangalore.

Vidya Rao
Assistant Professor
Department of ISE
AMC Engineering College, Bangalore.

***Abstract*—Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Cloud services offers an on-demand data outsourcing service which reduces burden for storage management. This new technique of data hosting service also brings new security threats towards user's data. During the data accessing, multiple users maybe working in a group to achieve productive benefits. But data sharing is not safe in cloud because the outsourced data can be exposed to risk when accessed by multiple users. Here the privacy criteria of the user is at risk as access request tends to expose all the information. In this paper, we have studied the privacy-preserving authentication protocol to address the mentioned privacy issue for cloud storing. Here we propose a solution to solve the problem of data integrity. Also the privacy of the data owner is achieved.by anonymous access request matching mechanism, proxy-reencryption at cloud server and ring signature.**

Keywords-Cloud computing, authentication protocol, data integrity, ring signature.

I. INTRODUCTION

Cloud computing is the practice of using a network of remote servers which will be hosted on the internet. This is used to process, manage and store the data. This is used as an alternative to local servers or personal computers. The popularity of cloud computing is increasing because it provides on-demand storage, infrastructure management, backup solutions, web based email services, data processing, technical support, virtual infrastructure etc.,[1]. However security and privacy are becoming the main concern with increasing popularity of cloud. The main focus of conventional security approaches is to provide authentication. But as the requirements increases for each application, users may want to access and share each other's data to achieve productive benefits. The sharing of data by users will bring new security and privacy challenges in cloud storage.

Security issues: Most companies use to store their data in their own data centers but nowadays they are prompting to cloud to store their data because this can decrease their operational cost radically, enjoy the services provided by cloud, reduce the burden of storage. But major drawback for storing in cloud is security in terms of data integrity, data leak and data confidentiality especially in shared groups. Few issues are malicious hacker, connection spooping, denial of service, faulty APIs. Insufficient understanding of cloud technology and compatibility between different cloud services is also an issue [10].

In cloud environment, the security protocol should achieve the following requirements.

1. Authentication: It confirms the identity of a person. The credentials provided will be compared with the database. If the credentials match then the user is granted is granted authorization for access.
2. Data anonymity: It is the process of encrypting the data, so that it cannot be accessed by unauthorized user.
3. Access control: The users access desires should not be known to any unknown entity.
4. Forward security: If the password or secret key is compromised, the past sessions must still be protected.

This paper mainly deals with providing the security tools for the four properties described above.

An efficient solution to address the above issues is using "identity based ring signature". Using Ring signature there is no need to verify the validity of public key certificates. Since there is no need for certificate validation,the verification process is very efficient. Ring signature can be performed by any member in a group. One of the main security properties of ring signature is that it is almost impossible to determine the group members key which was used to produce the signature.

Organization: The remainder of this paper is organized as follows. In Section II, we describe the related work. Section III gives an overview of System Model and Problem Formulation. Section IV concludes the paper.

II. RELATED WORK

L. A. Dunning *et al.,* [1] proposed an algorithm for anonymous sharing of private data. The technique iteratively assigned node ID numbers ranging from 1 to N. Here identities received are unknown to the other members of the group. The algorithms are designed on top of a secure sum data mining operation .

M. Nabeel *et al.,* [2] proposed an approach to encrypt documents with different keys using a public key cryptosystem. Here users are grouped based on the policies. Based on this idea, we formalize a new key management scheme, called broadcast group key management (BGKM).

C. Wang *et al.,* [3] proposed cloud storage that helps users to remotely store their data and enjoy the access to high quality cloud applications. Though there are benefits, they are timed.. The proposed design allows users to check the cloud storage for lightweight communication and computation cost.

S. Sundareswaran *et al.,* [4] proposed cloud computing that enabled highly scalable services to be easily accessed over the Internet. The major feature this service is that users' data is processed remotely in machines that users do not own or operate in. Users fear of losing the data problem is addressed by a novel high decentralized information framework to keep track users actual data.

Y. Tang *et al.,* [5] proposed that data backups can be outsourced to third-party cloud storage services to reduce cost. But, security guaranteesshould be provided for outsourced data. A secure overlay cloud storage system that achieves fine-grained, policy-based access control is implemented and key managers that are independent of third-party clouds.

Y. Zhu *et al.,* [6] proposed a access control mechanisms in cloud computing. Attribute-based access control provides a flexible approach that integrates data access of data owner policies within the encrypted data. But, it is difficult to explore temporal attributes in specifying and enforcing the data owner's policy. Here an efficient temporal access control encryption scheme for cloud services is implemented.

R. S´anchez *et al.,* [6] proposed a consumer cloud computing system that has emerged as a key system in several areas including distributed computing, service oriented architecture and consumer electronics. This ecosystem manages security and identity. A architecture based on privacy and reputation extensions is presented.

J. Yu *et al.,* [7] proposed a cloud computing system with a promising pattern for data outsourcing. But, concerns of sensitive information which causes privacy problems are present.The system focuses on addressing data privacy issues and inevitably leaked data using (TRSE) scheme.

Boyang Wang *et al.,*[8] proposed a ring signatures to compute the verification information needed to audit the integrity of shared data, the identity of signer on each block in shared data is kept private from a third party auditor, who is still able to publicly verify the integrity of shared data without retrieving the entire file.

Xinyi Huang *et al.,*[9] Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be putinto the cloud for storage or analysis purpose.Identity-based (ID-based) ring signature, which eliminates the processof certificate verification, can be used instead.

III. BACKGROUND

A. RING-SIGNATURE:**-** It is a type of digital signature that can be performed by any member of a group of users that each have keys. Therefore, a message signed with a ring signature is endorsed by someone in a particular group of people. One of the security properties of a ring signature is that it should be computationally infeasible to determine which of the group members' keys was used to produce the signature. Ring signatures are similar to group signatures but differ in two key ways: first, there is no way to revoke the anonymity of an individual signature, and second, any group of users can be used as a group without additional setup.

B. AES ALGORITHM:**-** AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text.

C.*ELLIPTICAL CURVE CRYPTOGRAPHY (ECC) ALGORITHM:*

Elliptical curve cryptography (ECC) is a public key encryption technique based on the algebraic *elliptic curve over finite fields .ECC requires smaller keys compared to non-ECC cryptography to provide equivalent* *security. ECC theory* that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation insteadof the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helpsto establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. ECC was developed by Certicom, a mobile e-business security provider, and was recently licensed by Hifn, a manufacturer of integrated circuitry (IC) and network security products. RSA has been developing its own version of ECC. Many manufacturers, including 3COM, Cylink, Motorola, Pitney Bowes, Siemens, TRW, and VeriFone have included support for ECC in their products.

IV.EXISTING SYSTEM

previous focus was on the authentication to check that only the valid users can access its authorized data, which neglects the case that different users in a group should share data among them to give productive benefits and in some cases to get specific users data that is sharing of their own data to another in a collaborative relationship. To achieve this they have used attribute based encryption and access control mechanism. In the previous system the group sharing was done using attribute based encryption in which only two users at a time can share their data and Revocation is even more challenging in attribute-based systems, given that each attribute possibly belongs to multiple different users, whereas in traditional PKI systems public/private key pairs are uniquely associated with a single user. In principle, in an ABE system, attributes, not users or keys, are revoked. Now discuss how the revocation feature can be incorporated.When a user challenges the cloud server to request other users for data sharing, the access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this work, we aim to address a user's sensitive access desire related privacy during data sharing in the cloud environments, and it is significant to design a humanistic security scheme to simultaneously achieve data access control, access authority sharing, and privacy preservation. We enhance the system using Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, enhance the security of ID-based ring signature by providingforward security: If a secret key of any user has been compromised, all previous generated signatures that include this user still remainvalid.

V. SYSTEM ARCITECTURE

The system model for the cloud storage architecture is shown. It includes three main network entities namely users, a cloud server, and a trusted third party.

• User is an individual who uses cloud for data storage and to perform other computations in cloud. There can be multiple users in cloud and different users may belong to a common organization and independent authority will be given to them on certain data fields.

• Cloud server is an entity which is managed by cloud service provider. The cloud server is mainly used to store the data of users in a remote server. It is also said to be an entity which will provide unlimited storage and provide lots of services.

• Trusted third party is considered as an optional entity which is used to provide advanced capabilities. The perform actions on behalf of the users. They are also used to perform the auditing of data of the user and help in dispute arbitration.

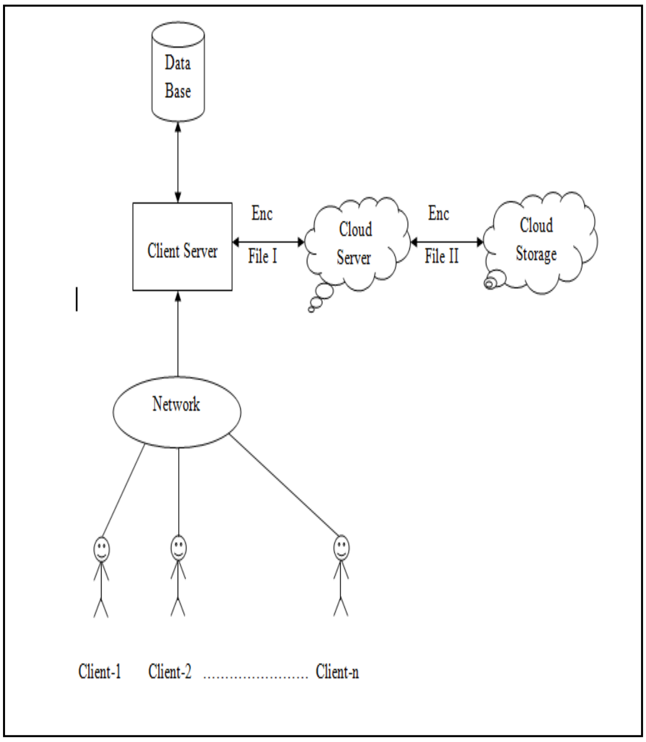

Fig1. System Architecture

While storing the data in cloud server the user will upload the file to cloud and this file will be stored in a remote server. The user will upload the data to the cloud so as to access the different services provided by the cloud. The cloud services are operated in distributed, parallel and also in cooperative modes. During the process of accessing the data in cloud, the user will interact with the cloud server autonomously without outside disruption. The user is designated with complete and discrete authority on its own data fields. The cloud must give an assurance that the data which is deployed cannot be accessed by unauthorized users.

In some situations, there are multiple users in a system and the users could have different affiliation attributes from different interest groups. We know that data sharing is very important for productive benefits. One of the users may wish to access other associate users' data fields to achieve bi-directional data sharing. This has mainly two aspects: firstly if the aimed user would like to share its data fields, secondly how the user will have its access request hidden if the aimed user declines or ignores its challenge. In the paper, we give specific importance on the process of access control to be provided for data and access authority sharing other than the transmission and management of data in cloud.

In our paper, the admin will create the various groups in cloud. Each user will be added to the group by the admin. Only the admin will be able to add the user's to the group. The members of the group can access the files uploaded in the group. For security of the file, each file will undergo double encryption before being uploaded to the cloud.

First the file will be encrypted in the local server and later it will be encrypted again in the cloud server. The two encryption algorithms used here are RNS and AES. The RNS algorithm will be used for encryption in the local server and the AES algorithm is used to encrypt the data in the cloud server. Each member of the group will be able to access the file securely using the concept of ring signature.

Ring signature is a type of digital signature which can be used to provide security to various users who are in a group. By using ring signature the member's key was used to produce the signature cannot be determined. The name is kept ring signature because the signature will form a circle during the verification process. Here the verifier will know that the signature is generated by one of the members of the group but will be unable to tell which member actually produced the signature. This is useful in achieving additional security. Also to verify the integrity of the file we are using cryptographic hash functions.

The hash function used in our paper is MD5 which will produce the hash value for the data. Once the receiver will receive the data, the hash value is generated again. This hash value will be compared with the previous hash value to check the integrity of the file. If the hash value is same then the user will download the file.

VI.EXPERIMENTAL RESULTS

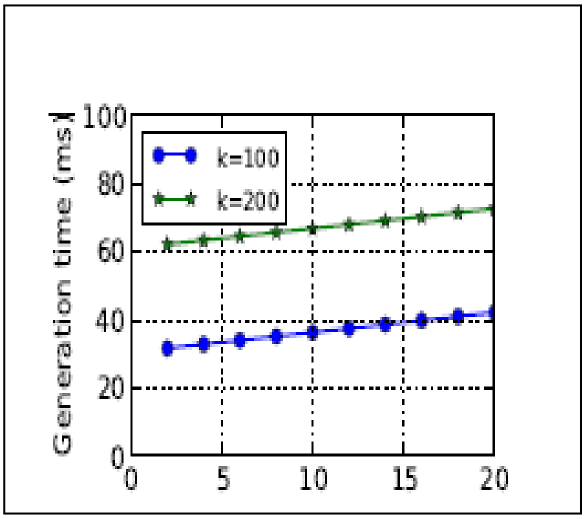

Fig 2. Impact of d on signature generation time (ms).

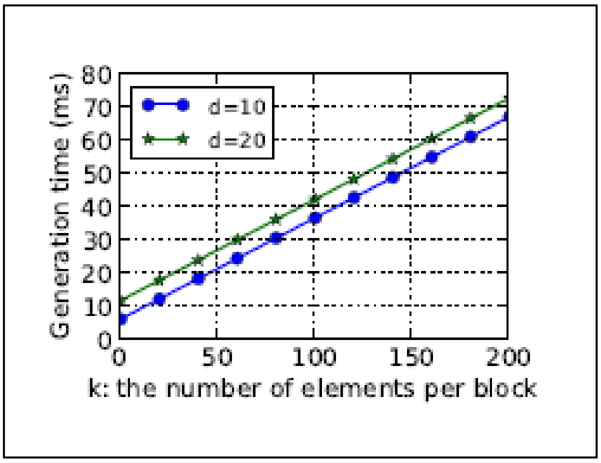

Fig 3. Impact of k on signature generation time (ms).

Performance of Signature Generation

The generation time of a ringsignature on a block is determined by the number ofusers in the group and the number of elements in each block. As illustrated in Fig. 2 and Fig. 3, when k isfixed, the generation time of a ring signature is linearlyincreasing with the size of the group; when d is fixed, thegeneration time of a ring signature is linearly increasing with the number of elements in each block. Specifically,when d = 10 and k = 100, a user in the group requiresabout 37 milliseconds to compute a ring signature on ablock in shared data.

The existing system focuses on the attribute based access control. Since it has various drawbacks we have choosen ring signature to improve the security in group during data sharing in cloud.In attribute based access control the security is ensured to only the members which have that attribute whereas using ring signature the security is also given to the entire group.Using ring signature better security is achieved since the identity of the user who generated the message will not be revealed.This causes the security to increase.

Another advantage of using ring signature over attribute based access control is that it increases the efficiency. Since in attribute based access control only few users could access the file the efficiency is reduced greatly.It is very important for a group of users to access the file to achieve productive benefit.Using ring signature even this drawback is overcome.

The performance in ring signature is slightly less than attribute based access control. But is considerable since the other to features provide more benefit. Hence using ring signature provides additional security then the existing attribute based access control.

VII.CONCLUSION

Here the new security challenge during accessing the data in the cloud computing to achieve privacy-conserve access authority sharing is identified. Authentication is established to guarantee data confidentiality and data integrity. Data innominate user access is achieved by using the covered values that are exchanged during transmission. Privacy of the users is enhanced by anonymous access requests and ring signature, which will privately inform the cloud server about the users' access desires. Forward security is realized by the session identifiers to prevent the session correlation. It indicates that the proposed scheme can be possibly applied for enhanced privacy preservation in cloud applications.

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," National Institute of Standards and Technology, USA, 2009.

[2] Hong Liu, Huansheng Nimg, Qingxu Xiong "Shared Authority Based Privacy reserving Authentication Protocol in Cloud Computing

[3] L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 402-413, 2013.

[4] M. Nabeel, N. Shang and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," *IEEE Transactions on Knowledge and Data Engineering*, 2012.

[5] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," *IEEE Transactions on Services Computing*, vol. 5, no. 2, pp. 220-232, 2012.

[6] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, pp.556-568, 2012.

[7] Y. Tang, P. C. Lee, J. C. S. Lui, and R. Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE *Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 903-916, 2012.

[8] Y. Zhu, H. Hu, G. Ahn, D. Huang, and S. Wang, "Towards Temporal Access Control in Cloud Computing," in *Proceedings of the 31st Annual IEEE International Conference on Computer Communications (IEEE INFOCOM 2012)*, pp. 2576-2580, March 25-30, 2012.

[9] R. S´anchez, F. Almenares, P. Arias, D. D´ıaz-S´anchez, and A. Mar´ın, "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing," *IEEE Transactions on Consumer Electronics*, vol. 58, no. 1, pp. 95-103, 2012.

[10] Ms.Sonam M. Kamble#1, Prof.A.C.Lomte*2 "Homomorphic Authenticable Ring Signature (HARS) mechanism for Public Auditing on Shared Data in the cloud (Oruta)"International Journal of Engineering Research and General Science Volume 2, Issue 6, October-November, 2014 ISSN 2091-2730

[11] Yu Fang Chung1 Zhen Yu Wu2 Feipei Lai1&3 Tzer Shyong"Anonymous signcryption in ring signature schemeover elliptic curve cryptosystem" ieee.

[12] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, "Security issues for cloud computing" the university of texas at dallas.

[13] Y. Xiao, C. Lin, Y. Jiang, X. Chu, and F. Liu, "An Efficient Privacy-Preserving Publish-Subscribe Service Scheme for Cloud Computing," in *Proceedings of Global Telecommunications Conference(GLOBECOM 2010)*, December 6-10, 2010.

[14] K. Hwang and D. Li, "Trusted Cloud Computing with SecureResources and Data Coloring," *IEEE Internet Computing*, vol. 14,no. 5, pp. 14-22, 2010.

[15] C. Wang, K. Ren, W. Lou, J, Lou,"Toward Publicly AuditableSecure Cloud Data Storage Services," *IEEE Network*, vol. 24, no.4, pp. 19-24, 2010.