IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 8, October 2014.
www.ijiset.com

ISSN 2348 – 7968

Data Sharing in Cloud Using Hybrid Approach

Mr.B.Gunalan M.sc, Mphil, J.Savarimuthu Mphil Computer Science,

Director School of computer science, CMS college of science and commerce, Chinnavedampatti,coimbatore.

CMS college of science and commerce, Chinnavedampatti,coimbatore.

Abstract:

The main objective of this paper is data sharing in cloud using the hybrid approach(MONA and 2-level security system). First this paper develop a secure data sharing scheme Data sharing in a multiple owner way the main issue is to provide privacy and preserve the data from the un trusted cloud To solve this problem this paper uses multi owner data sharing scheme. Secure environments protect their resources against unauthorized access by enforcing access control mechanisms, so increasing security using text based authentication. Using the instant messaging service available in internet, user will obtain the One Time Password (OTP) after text authentication. This OTP used by user to access their personal accounts. The 2-Level Security system is a time consuming and it will provide strong security where the need to store and maintain crucial and confidential data secure.

I INTRODUCTION

Cloud computing security is more simply. Cloud security is an evolving sub-domain of computer , network , and information security. cloud security refers to a broad set of policies, technologies, and controls . There are a many number of security issues associated with cloud computing. The security issues fall into two broad categories:

1.security issues faced by cloud providers

2. security issues faced by their customers.

Cloud computing is recognized as an alternative to Traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. The cloud service providers (CSPs) such as Amazon and it is able to deliver various services to cloud users with the help of powerful data centers. The local data management systems into cloud servers the users can enjoy high-quality services and save significant investments on their local infrastructures one of the most fundamental services offered by cloud providers is data storage. Consider a practical data application. The company allows its staffs in the same group or department to store and share files in the cloud.To utilized the cloud the staffs can be completely released from the troublesome local data storage and maintenance. It also poses a significant risk to the confidentiality of those stored files. The cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and Confidential like the business plans. To preserve data Privacy, a basic solution is to encrypt data files and then upload the encrypted data into the cloud. To design an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues. An efficient cloud security architecture should recognize the issues that will arise with security management. The security management identify these issues with security controls. These controls are put in place of safeguard.Any weaknesses in the system it reduce the effect of an attack.

ISSN 2348 – 7968

Deterrent controls are set in place to prevent any purposeful attack on a cloud system. These controls do not reduce the actual vulnerability of a system. Preventative controls upgrade the strength of the system by managing the vulnerabilities.

In [1], Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the KP-ABE techniques. In this method the Data owner use a random key to encrypt a file where the random key is further encrypted with a set of attributes. In [2], Kallahalla et al. proposed a cryptographic storage system that enables secure file sharing on untrusted servers called as Plutus. By dividing files into file groups and encrypting each file group with a unique file-block key the data owner can share the file groups with others through delivering the corresponding lock box key where the lockbox key is used to encrypt the file-block keys. The files are stored on the untrusted [3] server include two parts: file metadata and file data. The file metadata used to access control information including a series of encrypted key blocks and each of which is encrypted under the public key of authorized users. Ateniese et al. [4] leveraged proxy reencryptions to secure distributed storage. The data owner encrypts blocks of content with unique and symmetric content keys are further encrypted under a master public key. Lu et al. [5] proposed a secure provenance scheme. it is is built upon group signatures and cipher text-policy attribute-based encryption techniques Yu et al. [1] presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique [6]. The NNL construction is a exyended version [7] is used for efficient key revocation. A new user joins the group the private key of each user in an NNL system needs to be recomputed. This may limit the application for dynamic groups.

The limitations of the existing MONA system are overcome using the proposed hybrid system. The proposed hybrid system uses MONA and 2-level security system. Any user in the group can store and share data files with others by the cloud. A new user can directly decrypt the files stored in the cloud before his participation. The advantage of the proposed system are the computational cost and storage costs are very low. In additional security this paper proposed the text based authentication and OTP.

In the remainder of this thesis a module is described in Section II. Simulation results are presented to demonstrate the effectiveness of the proposed method Section III. Finally, a conclusion with some suggestions for future work is included in Section IV.

2. Methodology:

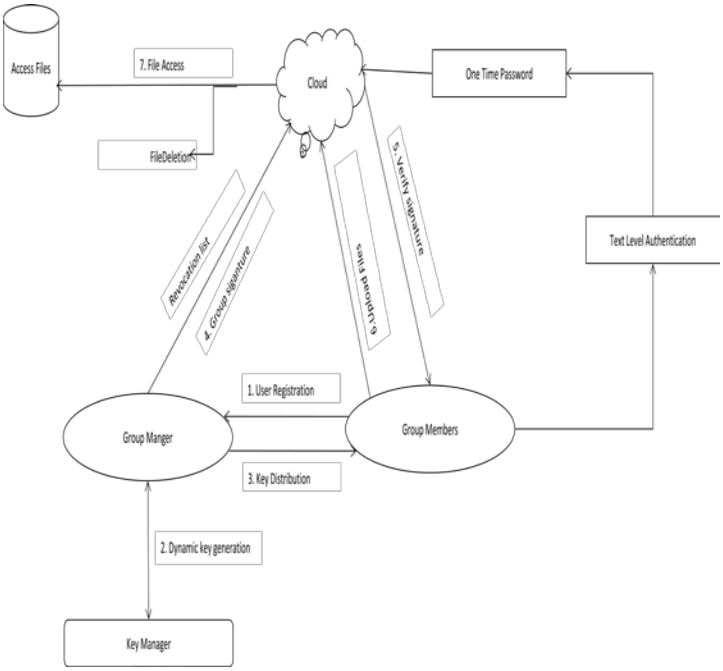

Fig:1 Overall Block Diagram

ISSN 2348 – 7968

2.1 User registration:

The user who has to join the group has to register with the group whose identity is kept secret
and traceable only to the group manager. For the registration of user i with identity ID_i the group manager randomly select a number $x_i \in Z_q^*$ q and computes $A_i : B_i$as the following equation:

$$\begin{cases} A_i = \frac{1}{\gamma + x_i}.P \in G_1 \\ B_i = \frac{1}{\gamma + x_i}.G \in G_1 \end{cases}$$

2.2 Group Manager:

A group manager is responsible for employing group strategy to validate the user within the group for communication. The group manager is used to create the group and the group manager will maintain the lists of users. The group manager also has the responsibility to maintain the revocation when a user moves from a group.

2.3 Key Manager:

A key manager is responsible for employing public and private key pairs to validate your identity. Here the keys are assigned and accessed among the primary users .Session is maintained along with the revocation list to provide effective communication among the system. The key manager is generate the dynamic key and send to the user through the group manger.

2.4 Group Signature:

After the group creation, the group signature has to be done to provide security. All the users in the group sign the messages without revealing the identity of the user. The user wants to revocate from the group his/her identity is selectively disabled from the group without affecting the membership of the unrevoked users. Thus the system is protected from the access of third party members. After group signature the cloud to verify the signature and send to user. Then the user to upload files.

2.5 User revocation

User revocation is done by the group manager through a public available revocation list (RL). It is based on which group Members can encrypt their data files and ensure the confidentiality against the revoked users.

File Storage:

Every user has to provide their file to store in the cloud which has to be updated periodically. With the multi-ownership policy this can be achieved efficiently.

2.6 File Deletion

File stored in the cloud can be deleted by either the group manager or the data owner (i.e., the member who uploaded the file into the server). To delete a file$\mathrm{ID}_{\mathrm{data}}$, the group manager computes a signature $\gamma \mathrm{f1}(\mathrm{ID}_{\mathrm{data}})$and sends the signature along with $\mathrm{ID}_{\mathrm{data}}$to the cloud. The cloud will delete the file if the equation $\mathrm{e}(\gamma \mathrm{f1}(\mathrm{ID}_{\mathrm{data}}), \mathrm{p}) = \mathrm{e}(\mathrm{w}, \mathrm{f1}(\mathrm{ID}_{\mathrm{data}})$ holds.

2.7 File Access:

Each member follow the below rules:

1. Getting the data file and the revocation list from the cloud server. The user first adopts its private key (A; x) to compute a signature u on the message ID_Group,ID_data by using Algorithm 1, where t denote the current time, and the ID_data can be obtained from the local shared file list maintained by the

ISSN 2348 – 7968

manager.The user sends a data request containing ID_Group,ID_data,t,σ_μ to the cloud server. To receive the request the cloud server employs Algorithm 2 to check the validity of the signature and performs a revocation verification with Algorithm 3 if necessary according to the revocation list. After a successful verification the cloud server is respond the corresponding data file and the revocation list to the user.

2. Checking the validity of the revocation list. This operation is same as the file generation phase.

3. Verifying the validity of the file and decrypting it.

2.8 Traceability

When a data dispute occurs, the tracing operation is performed by the group manager to identify the real identity of the data owner. Given a signature $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2}$ the group manager employs his private $(\xi_1, \xi_2)$to compute $A_i = T_3 - (\xi_1 . T_1 + \xi_2 . T_2)$.

2.9 2-level Security:

Additional security this paper includes the 2 level security system.

Level 1: Security at level 1 has been imposed by simple text -based password.

Level 3 Security System will then generate a one-time numeric password that would be valid just for that login session. The authentic user will be informed of this one time password on his email id.

3. Experimental Results:

In this chapter discuss about the results of proposed system. To compare the existing and proposed with the security metrics. The proposed model increases the security of dynamic groups in the cloud. This system increases the security since the group members are not directly given access to their group managers and the users can create the new group dynamically in this system that increases the flexibility. The graph shows that the proposed has a better performance than the previous methods.

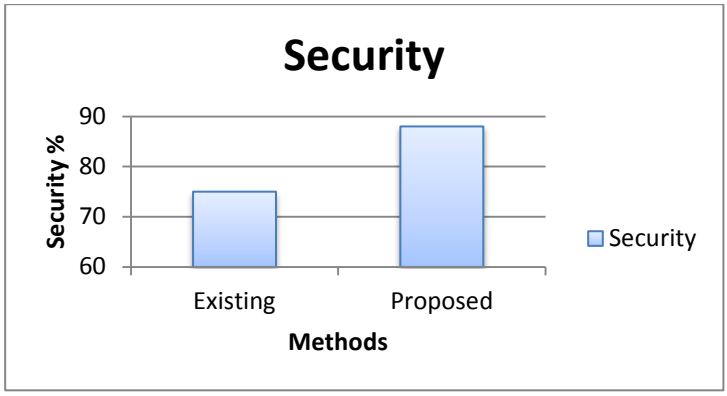

Fig:2 Compare the security of the system

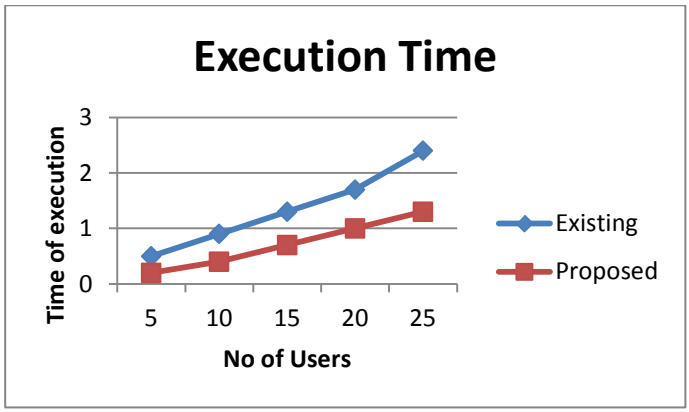

Fig:2 Compare the time.

The above results shows proposed system provides better results. The number of user's increases then the time also increases. The proposed system takes less execution time compare to the existing system.

Conclusion:

This paper develops the dynamic groups for data sharing in cloud is very efficient. This system supports dynamic users and

ISSN 2348 – 7968

dynamic groups efficiently. User invocation and revocation is updated by the group manager so that any changes in the system is reflected to all the users thus the system works more efficiently. For additional security this project used two level security system. This system provides the more security. A new type authentication system was highly secure and efficient. This system is also more users friendly. The experimental results shows the proposed system is secure and time consuming. This system provides the better results.

Reference:

[1] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,"Proc. IEEE INFOCOM, pp. 534-542, 2010.

[2] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[3] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[4] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[5] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[7] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[8] The GNU Multiple Precision Arithmetic Library (GMP), http:// gmplib.org/, 2013.

[9] Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL), http://certivox.com/, 2013.

[10] The Pairing-Based Cryptography Library (PBC), http://crypto. stanford.edu/pbc/howto.html, 2013.

[11] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[12] V.Sathana1, J.Shanthini "Three Level security System for Dynamic Groups in Cloud"
International Journal of Computer Science Trends and Technology (IJCST) – Volume1 Issue2, Nov-Dec 2013

[13] M. TamilSelvan , M. Newlin Rajkumar "Improved Authentication Scheme for Dynamic
Groups" in the Cloud International Journal of Computer Trends and Technology (IJCTT) – volume 11 number 3 – May 2014