International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 5, May - 2014

A Novel Methodology for Secure Multi Owner Data Sharing for Dynamic Group in Cloud

Aswathy V
PG ScholarHead of the Department
Department of Computer Science
KarpagaVinayaga College of Engineering
and Technology, Chennai

J. M Gnanasekar
Department of Computer Science
KarpagaVinayaga College of Engineering
and Technology, Chennai

Abstract - Cloud computing provides an economical and efficient solution for group resource sharing among cloud users due to the character of low maintenance. A challenging issue is sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud due to the dynamic nature of the membership. This paper proposes a secure multi owner data sharing scheme, for dynamic groups in the cloud. RSA scheme provides secure and privacy-preserving access control to users, guaranteeing any member in a group to anonymously utilize the cloud resource. AES-256 algorithm provides effective encryption for the data stored in the cloud. It also provides public revocation mechanism to support efficient revocation.

I. INTRODUCTION

Cloud computing is a subscription-based service where one can obtain networked storage space and computer resources. Cloud computing is recognized as an alternative to traditional information technology [1] due to its intrinsic resource-sharing and low-maintenance characteristics. Data Storage is one of the most fundamental services offered by cloud providers. The cloud provider can both own and house the hardware and software necessary to run a home or business applications. Cloud users face security threats both from outside and inside the cloud. Cloud poses a significant risk to the confidentiality of the stored files since the cloud servers managed by cloud providers are untrusted.

Security mechanism for a single owner manner is much easier compared to security mechanism for a group. However, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues:

1) Identity privacy.
2) Multi Owner Mannerism: Multi owner manner implies that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud.
3) Dynamic Nature of Groups.

Several security schemes for data sharing on untrusted servers have been proposed [4], [5], [6]. These approaches have data owners storing the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, both unauthorized users and storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys. However in these schemes the complexities of user participation and revocation are directly proportional to the number of data owners and the number of revoked users, respectively. Also the single owner manner hinders the adoption of their scheme into the case where any user is granted to store and share data.The scheme proposed in this paper helps to solve the challenges presented above.

II. SYSTEM MODEL AND DESIGN GOAL

The three different entities in the system model are: the cloud, a group manager, and a large number of group members as illustrated in fig 1.

Cloud is operated by CSPs and provides priced abundant storage services. However, the cloud is not fully trustworthy since the CSPs are very likely to be outside of the cloud users' trusted domain. The cloud server is assumed to be honest but curious that is, the cloud server cannot maliciously delete or modify user data due to the protection of data auditing schemes, but will attempt to learn the content of the stored data and the identities of cloud users.

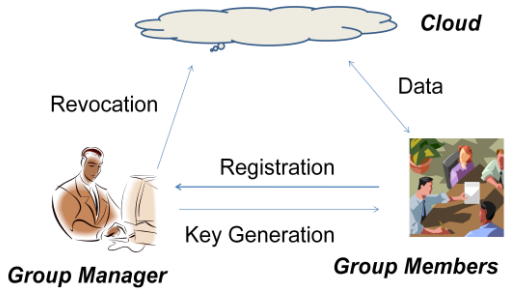

Fig 1 System model.

Group manager is responsible for system parameters generation,registration and revocation of users, and revelation the real identity of a dispute data owner.

Therefore, we assume that the group manager is fully trusted by the other parties.

A set of registered users who can store their private data into the cloud server and share them with others in the group are referred to as Group members.

III. SYSTEM IMPLEMENTATION

Modules

The Modules used in this project to implement the scheme are:

- User Repository Creation
- Data repository initiation
- Secure Cloud Storage
- Secure data sharing

User Repository Creation

1. Each user or group member subscribes the group key transfer service by registering with Group manager and establishes a group key with GM thus needing a secure channel
2. Group manager sends the group key and interacts with all group members in a broadcast channel
3. User repository is created with group key communication among data users

Data repository initiation

1. Data is stored in encrypted form in the cloud.
2. Hash code template of data is created based on User ID
3. Data is stored in the cloud along with its metadata in secure cloud storage
4. Data authentication done using Digital Signature Algorithm(DSA)
5. Before uploading to or retrieving a data file from cloud server the Group Manager perform Revocation Verification by checking the Revocation List and Signature Verification by using RSA algorithm

Secure Cloud Storage

1. The cloud server is configure using VMware tool
2. Cloud server is honest but curious thus is untrusted
3. Cloud server can't modify data resources present in cloud
4. Files are stored in the cloud servers in encrypted form

Secure Data Sharing

1. Data authentication done before data retrieval from the cloud server and eventual decryption using respected private keys
2. Public Revocation Mechanism used to generate Revocation List
3. Data or keys revocated in the cloud frequently depending upon the kind of data owner's identity and the data to be stored on the cloud
4. RSA algorithm for signature generation and verification procedure
5. For data security we use Advanced Encryption Standard-256(AES-256) scheme.

Enhancement

Initiator Functions

The initiator sends a key generation request to Group manager with a list of group members.Key confidentiality is provided by INITIATOR due to the security feature of a data sharing scheme

Advantages: Initiator provides Advanced Authentication techniques for group members rather than traditional authentication such as username and password. Secure key sharing is achieved.More data confidentiality is achieved.

Process Flow

The Process Flow of the protocol is described here in Fig 2.RSA algorithm for signature generation and verification procedure is implemented for enhanced data integrity mechanism for the data being shared in the cloud storage.

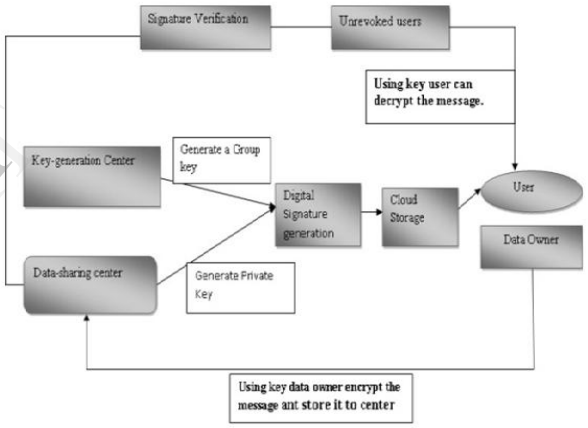

Fig 2 Process Flow of the Scheme

Here a public Revocation Mechanism is used for efficient revocation. For encryption this scheme uses Advanced Encryption Standard(AES-256) algorithm.

Algorithm

RSA Digital Signature Scheme

The private key of the originator is used as input to the algorithm which transforms the data being signed (or its hash value).

Only with the use of originator's public key that is provided to recipient by the originator can the transformation be reversed, and the data decrypted and accessed.

Creation of digital signature with a private key

In this scheme a secure cryptographic hash function (such as SHA-1) is used that takes large objects of varying size and produces a unique fixed-size message digest or

hash value. Once the message digest is calculated this can be encrypted using the private key of the originator to produce the digital signature, as shown in the figure below:

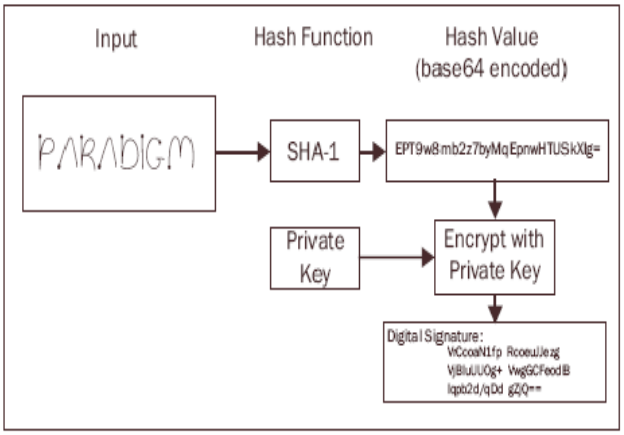

Fig 3 Creating a Digital Signature

Verification of a created digital signature

Using the public key of the originator, the recipient must decrypt the digital signature and recalculate the hash value of the corresponding digital object. If the result of the decrypted signature and the calculated hash value does not match it is concluded that either the object has been altered since it was signed, or the signature was not generated with the corresponding private key of the originator.

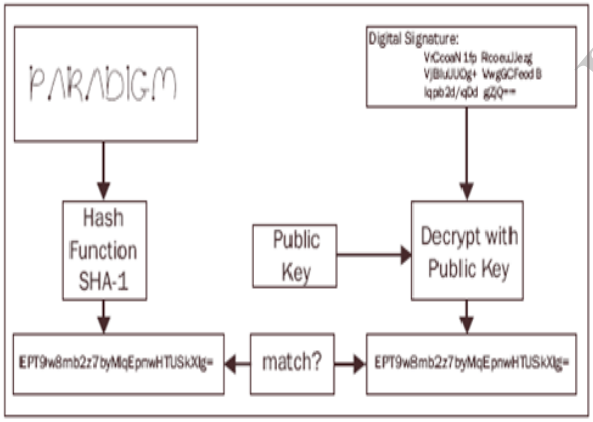

Fig 4 Verifying a Digital Signature

To generate a signature, the RSA digital signature scheme applies the sender's private key to a message. The signature can then be verified by applying the corresponding public key to the message and result of the verification process is either valid or invalid result. Thus the RSA digital signature scheme comprises of two operations — sign and verify. The security of the signature and encryption are partially dependent on the choice of hash function used to compute the signature as RSA does not mandate the use of a particular hash function.

AES Algorithm

Here we use AES-256 for encryption. It is called AES-256 because it uses Plain Text and Cipher Text of 256bits. The design of AES-256 is shown below in Fig 5.

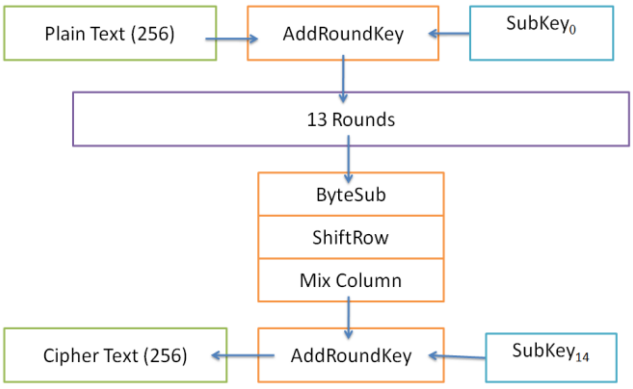

Fig 5 Design of AES-256

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the plaintext, into the ciphertext. The number of cycles of repetition is 14cycles for AES-256.

Each round consists of several processing steps. They are:

1. KeyExpansion—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 256-bit round key block for each round plus one more.
2. InitialRound
    1. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds
    1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
    2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
    3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

4. AddRoundKey

4. Final Round (no MixColumns)

1. SubBytes
2. ShiftRows
3. AddRoundKey.

IV. RESULT

The Project is implemented using Java as programming language. Netbeans IDE is used as IDE for coding. Cloud is simulated using VMware Server 3.0 and wamp server for combining PHP and MySQL for database purposes. Java Swing is used for creating Java Panels. The database stores the list of group members registered and also the revocation list. The revocation is decided based on the cloud subscription date provided to each registered group members. The following are screenshot of scheme

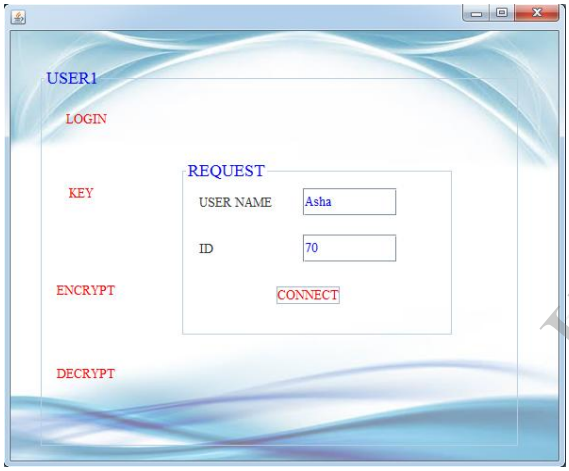

Fig 6 User login

Here the Fig 6 shows that user can login and connect to the Key Generation Centre to obtain the key. The key generation processes are as follows

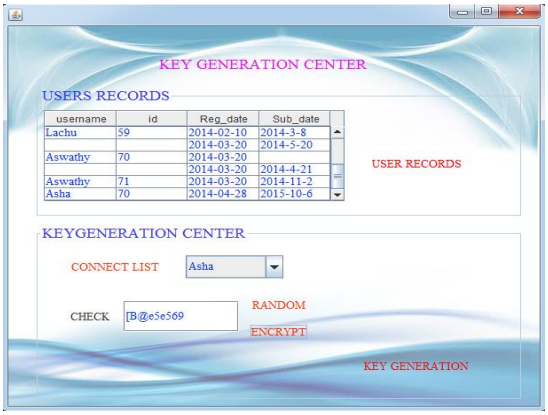

Fig 7 Key Generation Centre

In Fig 7 the key generated is further distributed through a key distribution centre shown in Fig 8

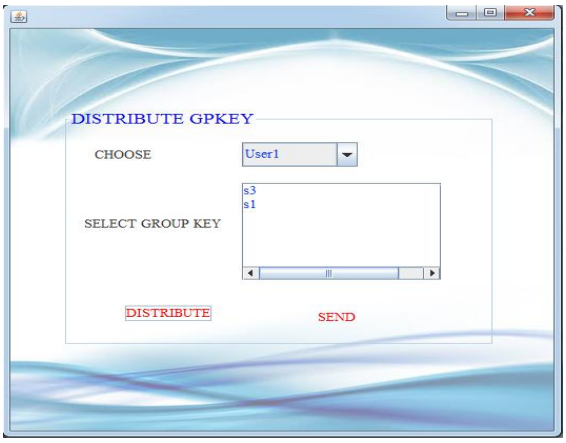

Fig 8 Key Distribution

Fig 9 below shows that the file that needs to be encrypted is first digitally signed and the data is later encrypted.

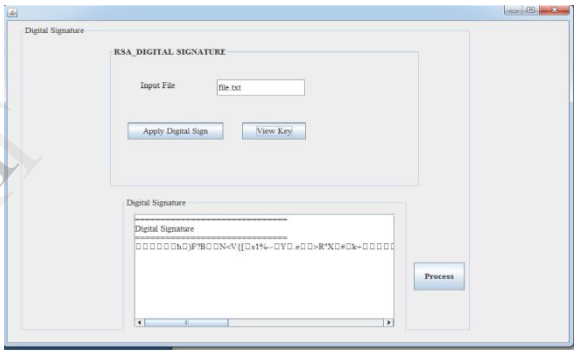

Fig 9 Applying Digital Signature

Fig 10 below shows the encryption of the file that need to be uploaded to the cloud

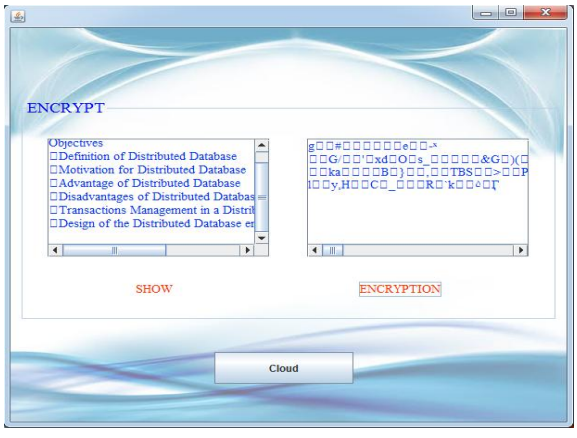

Fig 10 Encryption of File to be uploaded

The encrypted file is then uploaded into the cloud. The uploaded file can be downloaded by either the same user or any other user in the group as the key is distributed to all the members in the group. Once the user logins in before

downloading we need to validate if the user is revoked or not. If the user is a revoked user then he can't proceed and can't continue to download the file. Only a non revoked user can download the file thus preventing the misuse of data by malicious revoked user. The validation of the user is shown in fig 11.

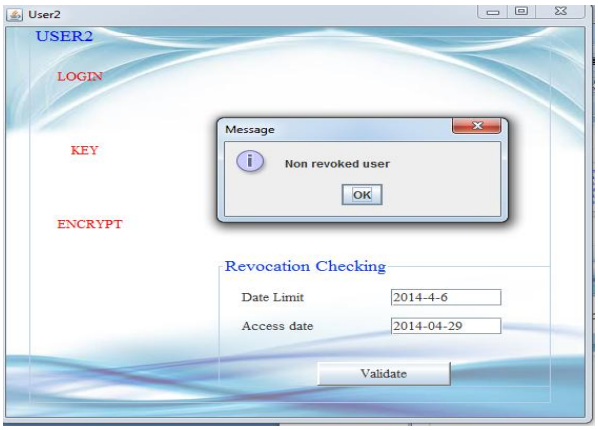

Fig 11 Validation of User

Since the validation is over then the file can be downloaded by the user and then the file is decrypted to obtain the original file that was uploaded.

V. FUTURE ENHANCEMENT

Currently MIT is trying to develop a new encryption standard called Functional Encryption scheme that combines three existing schemes — homomorphic encryption, garbled circuit and attribute-based encryptionwhich will help the data sharing in cloud. The practical implementation has not yet began but in future the Functional encryption scheme will help in computing data from encrypted data without completely decrypting the data. Functional Encryption will also ensure end to end security of the data. It will also help in better implementation of multi-owner mannerism as well as multi tenant cloud if used with a Digital Signatures as in this scheme.

V. CONCLUSION

This project focuses on problem of secure data sharing scheme for dynamic groups in an untrusted cloud. In this scheme, a user is able to share data with others in the group without revealing identity privacy to the cloud. This scheme also supports efficient user revocation and new user joining. Efficient user revocation can be achieved through a public revocation list. We propose the Group manager for reducing the execution time of user for the keys generated at the user or data owner side, also group manger responsible for generating the group keys for the communication between the data owners in the cloud .In addition we validate the authenticity of data by secure digital signature mechanism. Moreover, as a future enhancement we propose Initiator which acts as the middleware between the group manager and the data owners for providing versatile authentication mechanism.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53,no. 4, pp. 50-58, Apr. 2010.

[2] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[3] 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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] Prasanth SP, Gowtham B, "AES and DES Using Secure and Dynamic Data Storage in Cloud", Proc IJCSMC, Vol 3, Issue 1,pp 401-407, January 2014.

[9] AmanpreetKaur, Gaurav Raj, "Secure Broker Computing Paradigm Using AES and Selective AES Algorithm", Proc. IJARCSSE, Vol 3, Issue 3, pp 79-83, March 2013.

[10] RSA Laboratories , How is RSA Algorithm used for Authentication And Digital Signatures In Practice? , http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/authentication-and-digital-signatures-practice.htm

[11] PARADIGM, Metadata for authenticity: hash functions and digital signatures, http://www.paradigm.ac.uk/workbook/metadata/authenticity-signatures.html.

[12] RSA Digital Signature, http://www.drdobbs.com/rsa-digital-signatures/184404605.