OPEN ACCESS

Int. Res. J. of Science & Engineering, 2015; Vol. 3 (6): 231-236 ISSN: 2322-0015

RESEARCH ARTICLE

Privacy Preservation and Secure Data Sharing in Cloud Storage

Chavhan Bhaurao* and Deshmukh Swati

Department of computer science & engineering, G. H. Raisoni College of Engineering & Management, Amravati
*Corresponding Author Email : chavhanbhaurao@gmail.com

Manuscript Details

Received : 23.11.2015
Revised :28.12.2015
Revised received : 04.12.2015
Accepted: 10.12.2015
Published: 15.12. 2015

ISSN: 2322-0015

Editor: Dr. Chavhan Arvind

Cite this article as:
Chavhan Bhaurao and Deshmukh Swati. Privacy Preservation and Secure Data Sharing in Cloud Storage, *Int. Res. J. of Science & Engineering,* 2015, 3(6):231-236.

ABSTRACT

Cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Privacy preservation and secure sharing of the data over un-trusted cloud is still a challenging issue, due to the frequent change of the membership. A secure multi owner data sharing technique is proposed for dynamic groups in the cloud. By us group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. The storage overhead and encryption computation cost of our technique are independent with the number of users. In addition, to this the security of proposed technique with rigorous proofs, and demonstrate the efficiency of proposed system.

Keywords: Cloud computing, data sharing, privacy-preserving, access control, dynamic groups.

1. INTRODUCTION

Cloud computing is recognized as an alternative to traditional information technology (Armbrust *et al*., 2010) due to its intrinsic resource sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful data centers. By migrating the local data management systems into cloud servers, users can enjoy high quality services and save significant investments on their local infrastructures. But as per review completed by Chavhan and Wadhe (2014) on cloud services in which data sharing is done has various security problem and to overcome we have to implement some technique for secure data sharing.

One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs

can be completely released from the troublesome local data storage and maintenance. However, it also has a significant risk to the confidentiality of those stored files. Specifically, 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, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud (Kamara and Lauter , 2010).

Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues.

- Identity privacy is one of the most significant obstacles for the wide deployment of cloud computing.
- Any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner.
- Groups are normally dynamic in practice.

Our contributions: To solve the challenges presented above and propose a secure multi-owner data sharing scheme for dynamic groups in the cloud.
The main contributions include:

- Propose technique assured secure multi-owner data sharing. It implies that any user in the group can securely share data with others by the un-trusted cloud.
- Proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners.

Proposed technique provides secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.

2. LITERATURE REVIEW

Kallahalla *et al*. (2003) proposed a cryptographic storage system that enables secure file sharing on untrusted servers, named 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 lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation.

Goh *et al*. (2003) files stored on the untrusted server include two parts: file metadata and file data. The file metadata implies the access control information including a series of encrypted key blocks, each of which is encrypted under the public key of authorized users. Thus, the size of the file metadata is proportional to the number of authorized users. The user revocation in the scheme is an intractable issue especially for large-scale sharing, since the file metadata needs to be updated.

Ateniese *et al*. (2005) leveraged proxy reencryptions to secure distributed storage. Specifically, the data owner encrypts blocks of content with unique and symmetric content keys, which are further encrypted under a master public key. For access control, the server uses proxy cryptography to directly re-encrypt the appropriate content key(s) from the master public key to a granted user's public key. Unfortunately, a collusion attack between the untrusted server and any revoked malicious user can be launched, which enables them to learn the decryption keys of all the encrypted blocks.

Lu *et al*. (2010) proposed a secure provenance scheme, which is built upon group signatures and cipher text-policy attribute-based encryption techniques. Particularly, the system in their scheme is set with a single attribute. Each user obtains two keys after the registration: a group signature key and an attribute key. Thus, any user is able to encrypt a data file using attribute-based encryption and others in the group can decrypt the encrypted data using their attribute keys. Meanwhile, the user signs encrypted data with her

group signature key for privacy preserving and traceability. However, user revocation is not supported in their scheme.

Yu *et al*. (2010) presented a scalable and fine-grained data access control scheme in cloud computing based on the KPABE technique. The data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KP-ABE. Then, the group manager assigns an access structure and the corresponding secret key to authorized users, such that a user can only decrypt a cipher text if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegates tasks of data file reencryption and user secret key update to cloud servers. However, the single owner manner may hinder the implementation of applications with the scenario, where any member in a group should be allowed to store and share data files with others.

Chavhan and Kamble (2014) in there review compare the various techniques used for data security and privacy of user data. This survey conclude that implementation of strong security algorithm is necessary for secure data sharing and maintaining privacy of user.

3. SYSTEM IMPLEMENTATION

This section describes architecture, functional diagram and algorithm used to implement the proposed system.

3.1 Architecture of Proposed system

A system architecture or systems architecture is the conceptual model that defines the structure, 233 behaviour, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures of the system.

System architecture can comprise system components, the externally visible properties of those components, the relationships (e.g. the behaviour) between them. There have been efforts to formalize languages to describe system architecture; collectively these are called architecture description languages (ADLs)

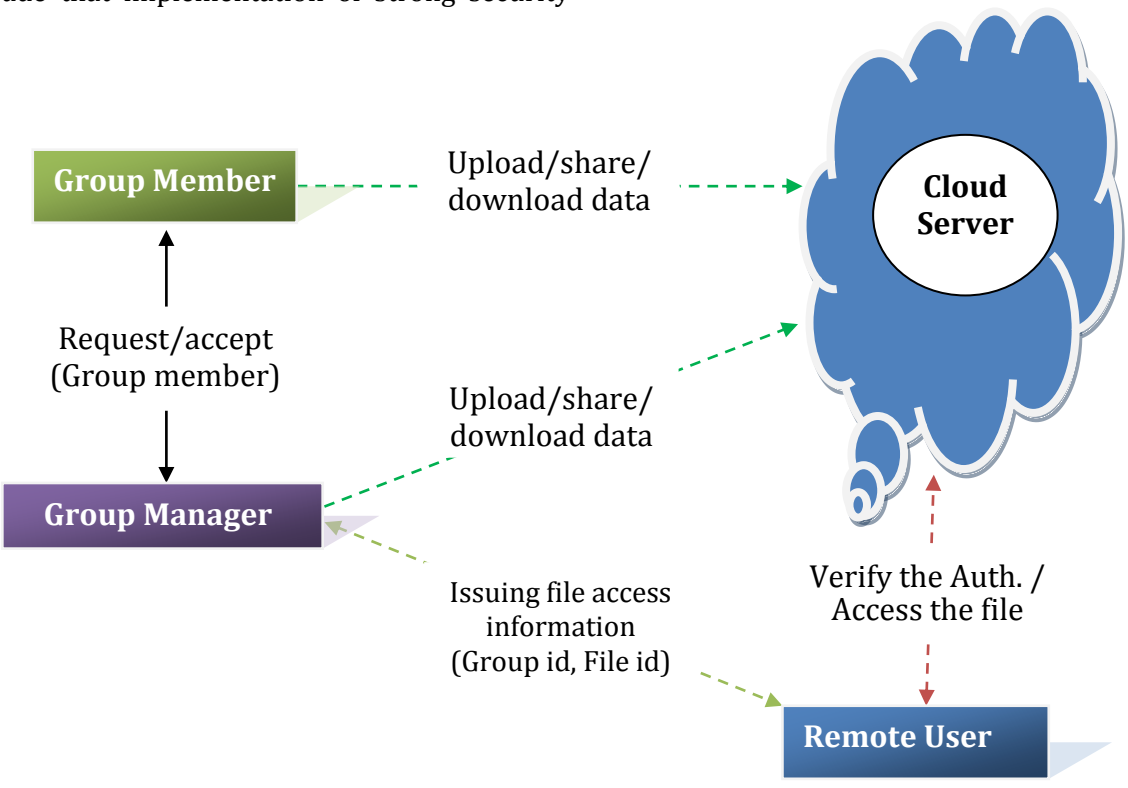

Fig. 1: Architecture diagram of Proposed System

The fig.1 shows the system architecture of the privacy preservation and secure data sharing in cloud storage. The application is run on the php based web application that is connect to the network and data is stored on the cloud server that helps to retrieve and stored that data in the database. The privacy preservation and secure data sharing in cloud storage application consists of php application for login purpose and use the secure data sharing services.

3.2 Data Flow Diagram

A data-flow diagram (DFD) is a graphical representation of the "flow" of data through an information system. DFDs can also be used for the visualization of data processing (structured design). On a DFD, data items flow from an external data source or an internal data store to an internal data store or an external data sink, via an internal process. In the above DFD, it shows that firstly user has to Log in on to our application, then System will checks the details of the user with the details available in the database. After valid login user can securely shared the data in group and also access data shared with it.

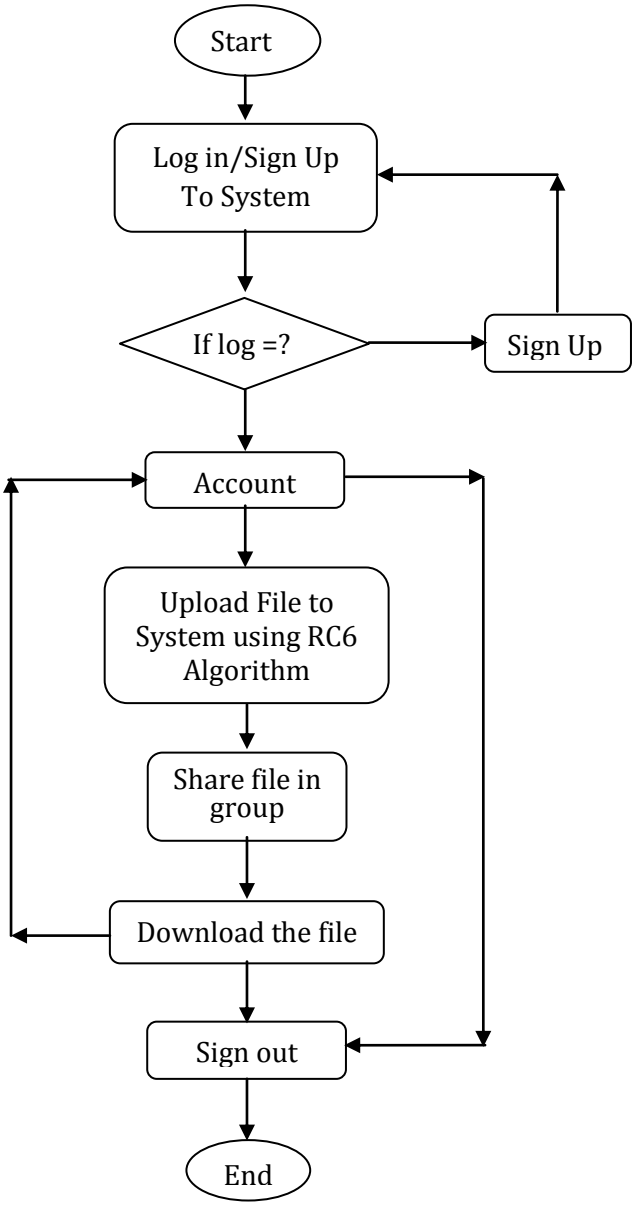

Fig. 2: Data Flow Diagram

3.3 RC6(Rivest Cipher Version 6)

In cryptography, RC6 (Ronald *et al.*, 1998) is symmetric key block cipher derived from RC5. It was designed by Ron Rivest, Matt Robshaw, RaySidney and Yiqun Lisa Yin to meet the requirement of the Advanced Encryption Standard (AES) competition. The algorithm was one of the finalists, and also submitted to NESSIE and CRYPTREC projects. It is a proprietary algorithm, patented by RSA Security. Below fig. 2.3 show RC6 Cipher process.

RC6 proper has a block size of 128 bits and supports key sizes of 128, 192, and 256 bits, but, like RC5, it may be parameterized to support a wide variety of word-lengths, key sizes, and number of rounds. RC6 is very similar to RC5 in structure, using data-dependent rotations, modular addition, and XOR operations; in fact, RC6 could be viewed as interweaving two parallel RC5 encryption processes, however, RC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word, and not just the least significant few bits.

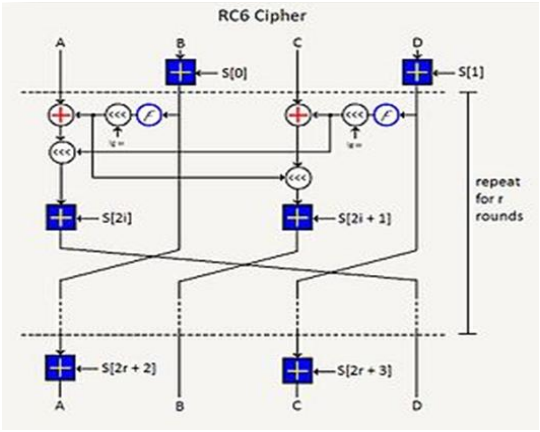

Fig. 3: RC6 Cipher

4. Experimental Result Analysis

The experimental result analysis is performed on cloud computation cost for performing various input and output operation performed by client request. The cloud computation cost is measured in term of CPU time (second) required to serve client request. We take both inputs and outputs request to calculate the cloud computation cost.

We also compare cloud computation cost with following Paper-

- Mona: Secure Multi Owner data sharing for dynamic groups in the cloud (Liu *et al.*, 2013).
- Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Cipher texts or Decryption Keys (Delerablee *et al.*, 2007).

Table 1: Comparisons of computation cost of cloud in proposed system and existing system

Request	Cloud Computation cost(second)		
	Proposed System	MONA[12]	ODBE[11]
0	0	1.579	1.6
20	0.795	1.678	1.85
40	1.09	1.746	2.2
60	1.35	1.824	2.44
80	1.75	1.949	2.8
100	2.31	2.10	3.25

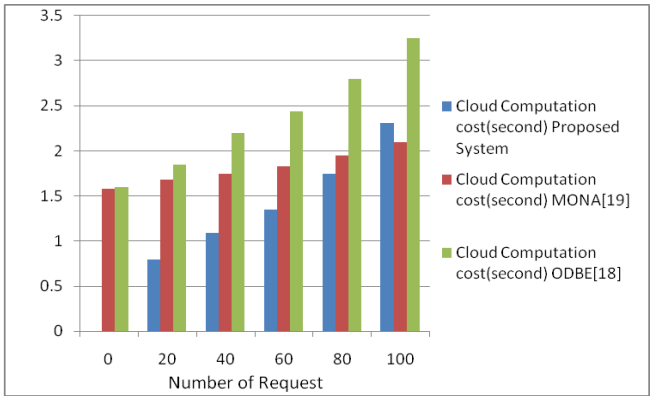

Fig 4: Graphical representation of comparisons of computation cost of cloud.

The above (Fig. 4) shows the graphical representation of comparison of computation cost of cloud in proposed system and existing system. The graph show that the computation cost of our system is better because the input and output operation is only involved file sharing parameter such as group id, user id and symmetric encryption key and is independent of file size.

5. CONCLUSION & FUTURE SCOPE

Proposed system introduced privacy preservation and secure data sharing strategy for cloud storage, which will provide high security to shared data in group. In proposed technique, a user is able to share data with other in group without revealing identity privacy to the cloud. Users efficiently join the group and new user can directly decrypt shared data file stored in cloud after participation. Moreover, the storage overhead and encryption computation cost are constant. Extensive analysis shows that the proposed technique satisfies the desired security requirement and guaranteed efficiency as well.

In future more advance and sophisticated feature for secure data sharing can be implemented. File encryption technique can be used for more secure data sharing. The system with file encryption and path encryption data is secured from unauthorized access of data. Another technique which can be introduced in proposed technique is two factor authentications. Two factor authentication provide more security while authentication process because while login process required username, password and OTP verification

REFERENCES

1. Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G, Patterson DA, Rabkin A, Stoica I and Zaharia M. A View of Cloud Computing, Comm. *ACM*, Apr. 2010; 53(4):50-58.
2. Chavhan BB and Wadhe AP. Review Paper on Security problems in Cloud services, 2014
3. Kamara S and Lauter K. Cryptographic Cloud Storage,‖ *Proc. Int'l Conf. Financial Cryptography and Data Security (FC)*, Jan. 2010; pp. 136- 149.
4. Kallahalla M, Riedel E, Swaminathan R, Wang Q, and Fu K. Plutus: Scalable Secure File Sharing on Untrusted Storage, *Proc. USENIX Conf. File and Storage Technologies*, 2003; pp. 29-42.

5. Goh E, Shacham H, Modadugu N and Boneh D. Sirius: Securing Remote Untrusted Storage," *Proc. Network and Distributed Systems Security Symp. (NDSS)*,2003; pp. 131-145.
6. Ateniese G, Fu K, Green M and Hohenberger S. Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," *Proc. Network and Distributed Systems Security Symp. (NDSS)*, 2005; pp. 29-43.
7. Lu R, Lin X, Liang X and Shen X. Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," *Proc. ACM Symp. Information, Computer and Comm. Security*, 2010; pp. 282-292.
8. Yu S, Wang C, Ren K and Lou W. Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," *Proc. IEEE INFOCOM*,2010; pp. 534-542.
9. Chavhan Bhaurao and Kamble Rutuja. Review on Privacy Preservation and Secure Data Sharing on Cloud Storage, Int. Res. J. of Sci. & Engg., 2014; 2 (6): 226-234.
10. Rivest, Ronald L, *et al*. The RC6TM block cipher." *First Advanced Encryption Standard (AES) Conference*. 1998.
11. Delerablee C, Paillier P and Pointcheval D. Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys, *Proc. First Int'l Conf. Pairing-Based Cryptography*, 2007; pp. 39-59.
12. Liu X, Zhang Y and Yan J. Mona: Secure Multi Owner data sharing for dynamic groups in the cloud" *Proc. IEEE Transactions on parallel and distributed systems*, June, 2013; 24(6).