International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 04 | April - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity Based Encryption Methodology

Ms. Vinaya Reddy S
School of Computer Science and IT, Jain University (Deemed-to-be University), Bangalore Karnataka, India
vinayareddy14@gmail.com

Prof. Dr. J. Bhuvana
School of Computer Science and IT, Jain University (Deemed-to-be University), Bangalore Karnataka, India
J.bhuvana@jainuniversity.ac.in

ABSTRACT- Cloud computing is one of the best ways to store, retrieve and share data which is easy, convenient and also beneficial for both the organization and individuals. But there are many of disadvantages because of which users hesitate to share data to the cloud as they contain important and valuable information. Therefore it is necessary to apply encryption on your user's shared data, for this Identity-based encryption is one of common and promising approach to secure shared data. However access control is not static.

That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data.

To overcome this problem Revocable-storage identity-based encryption (RS-IBE) is introduced, which can provide the forward/backward security of cipher text with functionalities like user revocation and cipher text update that takes place simultaneously. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data sharing system.

Keywords - Cloud computing, data sharing, revocation, Identity-based encryption, cipher text update, decryption key

1. INTRODUCTION

CLOUD computing is a platforms provides huge computing capacity and memory space at a low cost. It helps users to get expected services irrespective of time and location across multiple platforms such as mobile devices, personal computers, etc. and thus brings great convenience to the users. Among various services provided by cloud computing, cloud storage service, such as Drop box, Microsoft's Azure, and Amazon's S3, etc. can provide easy and flexible way to share data over the Internet, which provides various benefits for Cloud users.

However, it also has to face a lot of security threats, which are the primary concerns of cloud users. First and foremost, outsourcing data to a cloud server means that data is out of the control of users. This is why users hesitate because the outsourced data usually contain valuable and sensitive information. Secondly, data sharing is often implemented in an open and maleficent environment, and cloud servers can become a target of any malicious attacks. Even worse, the cloud server itself may reveal users' data for illegal profit. Lastly, data sharing is dynamic. That is, when a user's authorization gets expired, he or she should no longer have the right to access the old and subsequently shared data. Therefore, while outsourcing data to cloud servers, users also want to control access to these data such that only current authorized users can share the outsourced file or data. One of the solutions to overcome this problem is to use cryptographically enforced access control such as

identity-based encryption (IBE). Additionally to overcome the above security threats, identity-based access control placed on the shared data should fulfill the following security goals:

Data Secrecy: Unauthorized users must be prevented from accessing the plaintext of the shared data stored in the cloud. In addition, the cloud server should also be discouraged from knowing the plaintext of shared data.

Backward secrecy: When a user's authorization is expired, or when a user's secret key is compromised, he or she should be prevented from accessing the plaintext of the upcoming shared data that is still encrypted under his or her identity.

Forward secrecy: When a user's authority is expired, or when a user's secret key is compromised, he or she must be prevented from accessing the plaintext of the shared data that was previously accessed by him or her. The important and main problem addressed in this paper is how to build a fundamental identity-based crypto-graphical tool to achieve full security. We also found that there are other security issues that are equally important for a realistic system of data sharing, such as the availability and authenticity of the shared data

2. Problem Statement

Cloud computing provides cryptography in order to perceive flexible, scalable and secure access control of outsourced data. Encryption is the process of converting data into a structure called a cipher text that cannot be understood by unauthorized users and decryption is the process of converting encrypted data into its original form. Use of encryption or decryption is a process helps to keep the unauthorized users from attaining the contents of your shared data. The specific problem addressed in this paper is how to construct a fundamental identity-based cryptographically tool to achieve the above security goals. We also note that there exist other security issues that are equally important for a practical system of data sharing, such as the authenticity and availability of the shared data. To recover the contents of an encrypted file or data, correct decryption key is required to view the plaintext. Sometimes encryption is applied accidently on something that was not meant to be encrypted and the user who was meant to receive the message may not be able to view the message sent to them, encryption may not be strong enough and therefore others can easily interpret information.

To overcome these problems RIBE concept is introduced to ensure forward or backward secrecy by using User revocation and ciphertext update methods.

3. LITERATURE REVIEW

1) Towards Cloud definition- A break in cloud

AUTHORS: L. M.Vaquero, L.Rodero-Merino, J.Caceres and M. Lindner

This paper discusses the conception of Cloud Computing to get full description of what a Cloud is, using the important characteristics generally related to this paradigm within the literature. About 20 definitions are studied with the extraction of a consensus definition yet as a minimum definition containing the essential characteristics. This paper pays more attention to the Grid paradigm, because it is usually confused with Cloud technologies. It also explains the relationships and distinctions between the Grid and Cloud approaches.

2) A vision for socially motivated resource sharing - Social Cloud Computing

AUTHORS: K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana

Online connections in social networks frequently supports real world connections or relationships, thus used to infer league of trust between users. This model leverages these connections to make a dynamic "Social Cloud," thereby enabling users to share heterogeneous resources within the environment of a social network. Additionally, the essential social corrective mechanisms (incentives, disincentives) is oriented to enable a cloud-based framework for long run sharing with lower privacy concerns and security overheads than are present in traditional cloud environments. Because of the distinctive complexion of the Social Cloud, a social market place is suggested as a way of regulating sharing. The social market is novel, because it uses both social and profitable protocols to facilitate trading. This paper defines Social Cloud computing, outlining various aspects of Social Clouds, and

demonstrates the approach employing a social storage cloud implementation in Facebook.

3) Privacy preserving public auditing for secure cloud storage

AUTHORS: C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou,

Using cloud storage, users can casually store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the load of local data storage and maintenance. But the fact that users don't have physical ownership of the assigned data makes the information integrity protection in cloud computing an alarming task, mainly for users with restriction computing resources. However, users should be able to only use the cloud storage as if it is local, without concern about the necessity to verify its honesty. Consequently, authorizing public survey for cloud storage is of crucial significance so that users can resort to a third-party auditor (TPA) to find the honesty of outsourced data and be worry free. To safely launch a good TPA, the auditing process should not have new vulnerabilities toward user data privacy and establish no additional online load to user. A secure cloud storage system supporting privacy-preserving public auditing is proposed in this paper. Additionally results extend to enable the TPA to perform checkups for multiple users at the same time and efficiently. Expensive security and performance analysis show the proposed schemes are provably secure and largely effective. Primary experiment performed on Amazon EC2 instance demonstrates the fast performance of the design.

4) Secure and efficient dynamic auditing protocol for data storage in cloud computing

AUTHORS: K. Yang and X. Jia

In cloud computing, data providers or owners host or upload their data on cloud servers and users access the data or information from cloud servers. On account of information or data outsourcing, this new paradigm of information or data hosting service introduces new security challenges, which needs an independent auditing service to test the data honesty within the cloud. Some existing remote integrity checking methods can only be used for static archive data hence, can't be applied to the auditing service as the info within the cloud can be dynamically updated. Like this efficient and secure dynamic auditing protocol is apt to assure data owners that the data is correctly stored within the cloud. In this paper, first design of auditing framework for cloud storage systems is introduced and efficient and privacy-preserving auditing protocol is proposed. Next, auditing protocol is continued to support the info or data dynamic operations, which is capable and provably secure within the random oracle model. And also to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer. The analysis and simulation results show that the proposed auditing protocols are immune and adequate, especially to reduce the computing cost of the auditor.

5) Public auditing for shared data using efficient user revocation

AUTHORS: B. Wang, B. Li, and H. Li

With data storage and sharing services within the cloud, users can easily modify and share data in groups. To make sure shared data honesty can be verified publicly, users in the group need to cipher signatures on all the blocks in shared data. Different blocks in shared data are commonly signed by different users since data modifications are performed by different users. Considering security needs, a revoked user from the group and the blocks which were already signed by the revoked user should be re-signed by current user. This method, which allows an existing user to download the identical- part of shared data and re-sign in during user revocation, is faulty due to massive size of shared data. In this paper, a completely unique public auditing mechanism for the honesty of shared data is proposed with impressive user revocation. By adopting the idea of proxy re-signatures, we allow the cloud to re-sign blocks on account of existing users during user revocation, so the existing users need not download and re-sign blocks on their own. Additionally, a public verifier checks the honesty of shared data without restoring the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. Besides, this structure supports batch auditing by verifying multiple auditing

functions concurrently. Experimental results show that this mechanism can significantly improve the productivity of user revocation.

4. SYSTEM ANALYSIS

EXISTING SYSTEM:

- Boneh and Franklin first proposed a natural revocation way for IBE. They appended the current time period to the ciphertext, and non-revoked users periodically received private keys for each time period from the key authority.
- Boldyreva, Goyal and Kumar introduced a novel approach to achieve efficient revocation. They used a binary tree to manage identity such that their RIBE scheme reduces the complexity of key revocation to logarithmic (instead of linear) in the maximum number of system users.
- Subsequently, by using the aforementioned revocation technique, Libert and Vergnaud proposed an adaptively secure RIBE scheme based on a variant of Water's IBE scheme.
- Chen et al. constructed a RIBE scheme from lattices.

DISADVANTAGES OF EXISTING SYSTEM:

- Unfortunately, existing solution is not scalable, since it requires the key authority to perform linear work in the number of non-revoked users. In addition, a secure channel is essential for the key authority and non-revoked users to transmit new keys.
- However, existing scheme only achieves selective security.
- This kind of revocation method cannot resist the collusion of revoked users and malicious non-revoked users as malicious non-revoked users can share the update key with those revoked users.
- Furthermore, to update the cipher-text, the key authority in their scheme needs to maintain a table for each user to produce the re-encryption key for each time period, which significantly increases the key authority's workload.

PROPOSED SYSTEM:

- It seems that the concept of revocable identity-based encryption (RIBE) might be a promising approach that fulfills the aforementioned security requirements for data sharing.
- RIBE features a mechanism that enables a sender to append the current time period to the ciphertext such that the receiver can decrypt the ciphertext only under the condition that he/she is not revoked at that time period.
- **A RIBE-based data sharing system works as follows:**

  Step 1: The data provider (e.g., Varun) first decides the users (e.g., Alisha and Ram) who can share the data. Then, Varun encrypts the data under the identities Alisha and Ram, and uploads the ciphertext of the shared data to the cloud server.

  Step 2: When either Alisha or Ram wants to get the shared data, she or he can download and decrypt the corresponding ciphertext. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available.

  Step 3: In some cases, e.g., Alisha's authorization gets expired, Varun can download the ciphertext of the shared data, and then decrypt-then-re-encrypt the shared data such that Alisha is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again.

ADVANTAGES OF PROPOSED SYSTEM:

- The proposed scheme can provide confidentiality and backward/forward2 secrecy simultaneously
- We prove the security of the proposed scheme in the standard model, under the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) assumption. In addition, the proposed scheme can withstand decryption key exposure
- The procedure of ciphertext update only needs public information.
- The additional computation and storage complexity is brought in by forward secrecy.

- For Unauthorized user and the cloud server, the plaintext of the shared data is not available

5. IMPLEMENTATION

Public key and private key are used to encryption and decryption respectively in this scheme. Normally forward secrecy or backward secrecy provided for security. In this paper, Forward secrecy is used for advanced security. Revoke user can't access the previous or subsequent data so that revocable identity based encryption technique is used.

Data providers upload the files into storage server using the encryption technique. For the encryption key is used and this key provide by the key authority.

Key authority is responsible for sending the key to data provider. In this paper, random function used for generating the key to encryption as well as decryption. Storage server stores the files which are uploaded by data provider.

And users download or access the file as per their need. Download the file is done with decryption process. In this paper, time quantum also provided for downloading the data.
Below System architecture show the exact picture of how the system works.

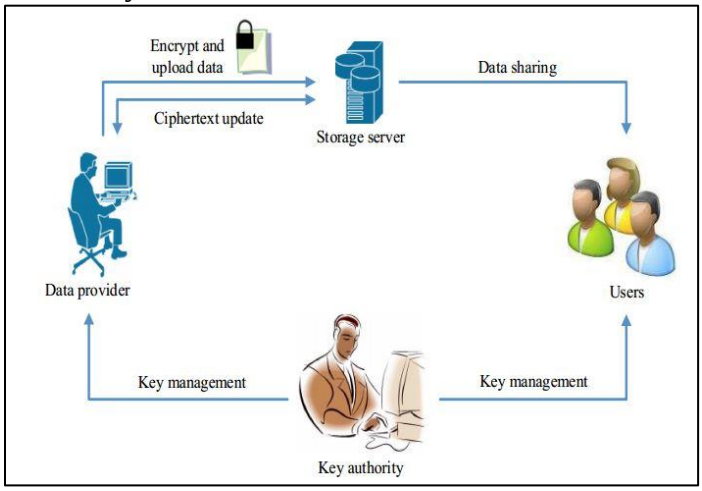

Fig.1- System Architecture

5.1 MODULES

- System Construction Module
- Data Provider
- Cloud User
- Key Authority (Auditor)

5.2 MODULES DESCSRIPTION

- **System Construction Module**

In the first module, we develop the proposed system with the required entities for the evaluation of the proposed model. The data provider first decides the users who can share the data. Then, Data provider encrypts the data under the identities of the user, and uploads the ciphertext of the shared data to the cloud server.

When user wants to get the shared data, she or he can download and decrypt the corresponding ciphertext. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available.

- **Data Provider**

In this module, we develop the Data Provider module. The data provider module is developed such that the new users will Signup initially and then Login for authentication. The data provider module provides the option of uploading the file to the Cloud Server. The process of File Uploading to the cloud Server is undergone with Identity-based encryption format. Data Provider will check the progress status of the file upload by him/her. Data Provider provided with the features of Revocation and Ciphertext update the file. Once after completion of the process, the Data Provider can logout the session.

- **Cloud User**

In this module, we develop the Cloud User module. The Cloud user module is developed such that the new users will Signup initially and then Login for authentication. The Cloud user is provided with the option of file search. Then cloud user feature is added up for send the Request to Auditor for the File access. After getting decrypt key from the Auditor, he/she can access to the File. The cloud user is also enabled to download the File. After completion of the process the user can logout the session.

- **Key Authority (Auditor)**

Auditor Will Login on the Auditor's page. He/she will check the pending requests of any of the above person. After accepting the request from the above person, he/she will generate master key for encrypt and Secret key for decrypt. After the complete process, the Auditor can logout the session.

6. ACTIVITY DIAGRAM

You have 3 Modules that is Data Provider, User and Key Auditor/Authority and these are the following activities of the Modules.

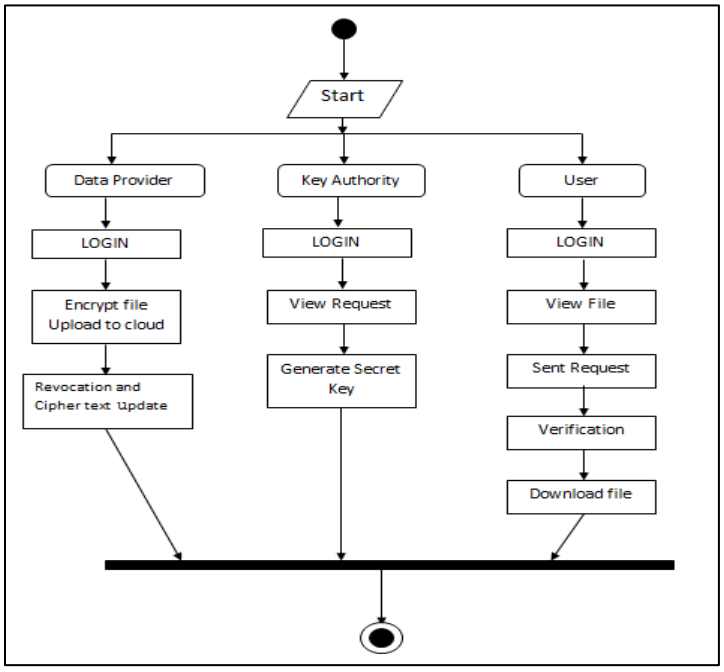

Fig.2 - Activity Diagram

7. Future Scope or Enhancement

In our future work we can add the concept of Data Deduplication. Data Deduplication is a special data compression technique for eliminating duplicate copies of repeated data.
We consider file size, file name and file type for data deduplication and we can achieve storage area and storage cost.

Conclusion

Cloud computing brings great convenience to people. Particularly, it helps in the sharing data over the Internet. In this paper, to build a low-cost and secure data sharing system in cloud computing, a concept called RS-IBE is introduced, which supports identity or user revocation and ciphertext update concurrently so that a revoked user is prevented from accessing previously shared data, as well as future or upcoming shared data. Moreover, a strong construction of RS-IBE is presented. The proposed RS-IBE scheme is proved is a standard model, under the decisional ℓ-DBHE assumption. The demonstration of our scheme has advantages in terms of productivity and performance, and thus is more capable for practical applications.

Reference

1. L.M Vaquero, L.Rodero Merino, J.Caceres and M.Lindner, 'A break in the cloud:towards a cloud definition', ACM SIGCOMM Computer Communication Review, vol.39, no.1, pp-50-55, 2008
2. K.Chard, K.Bubendorfer, S.Caton and O.F Rana, ' Social Cloud Computing- Vision for social motivated resource sharing', Service Computing, IEEE Transaction on vol.5, No-4, pp-551-563, 2012
3. C.Wang, S.S Chow, Q.Wang, K.Ren and W.Lou, 'Privacy-Preserving public auditing for secure cloud-storage', Computers, IEEE Transactions on vol.62, no-2, pp-362-375, 2013
4. G.Anthes, 'Security in Cloud', Communications of ACM, vol.53, no.11, pp-16-18, 2010
5. K.Yang, X.Jia, 'Efficient and secure dynamic auditing protocol for data storage in Cloud Computing', Parallel and distributed systems, IEEE Transaction on vol.24, no.9, pp-1717-1726, 2013
6. B Wang, B Li, H.Li 'Public audit for shared data with efficient user revocation', in INFOCOM, IEEE, pp-2903-2912, 2013
7. S. Ruj, M. Stojmenovic and A.Nayak 'Decentralized access control with anonymous authentication of stored data in cloud', Parallel and Distributed System, IEEE Transaction on vol.25, no.2, pp-384-394, 2014
8. X.Huang, J.Liu, S Tang, Y Xiang, K. Liang, L. Xu and J. Zhou, 'Cost effective authentic and

anonymous data sharing with forward security', IEEE transaction on 2014

9. C –K Chu, S.S Chow, W G Tzeng, J Zhou and R H Deng, 'Key aggregate crypto-system for scalable data sharing in cloud', Parallel and distributed systems, IEEE Transactions on vol.25, no-2, pp-468-477, 2014
10. A Shamir, ' Identity based crypto system and signature scheme', Advances in cryptology, Springer, 1985
11. D. Boneh and M Franklin, 'Identity based encryption from weil pairing', SIAM journal, vol.32, no.3, pp-586-615, 2003
12. S.Micali 'Efficient-certificate-revocation', tech. Rep-1996
13. W Aiello, S Lodha and R Ostrovsky, 'Fast digital identity revocation', in Advance in Cryptology-Crypro 1998, Springer, pp-137-152