Survey on: Secure and Efficient Data sharing scheme for outsourced Cloud Data

Tejal Deshmukh[1], **Mr. S. B. Javheri**[2]
[1, 2] Department of Computer Engineering
[1, 2] Rajashri Shahu College of Engineering,Savitribai Phule Pune University,Pune, India.

Abstract-*Cloud computing allows users to connect with server through web based tools and internet connectivity, instead of direct server connection. Users can store and retrive their data and softwares on cloud server. Users can outsourced their data on cloud and can also share the data trough cloud. This functionality is greatly affected by unauthorized entities. Therefore cloud facing the big challenge in data sharing. These challenges are secure data sharing with maintaining privacy of users. Several advanced schemes for secure data sharing has been developed from last few years. This paper presents the study on recent and advanced privacy and security preserving data sharing schemes in cloud computing. These schemes are basically based on encryption, user revocation, confidentiality etc. This paper also provide the comparative analysis of recent secure data sharing technique based on their advantages and disadvantages.*

Keywords-Cloud computing, data sharing, revocation, Identity-based encryption, ciphertext update, decryption key exposure

I. INTRODUCTION

With the advent of cloud computing technology, sharing data through a third-party service provider has never been more economical as well as convenient than now. However, because of data outsourcing and untrusted storage servers, data access control becomes a challenging problem in cloud storage, where differentiated data access is frequently required in the sense that users with various attributes should be granted different levels of access privileges. Traditional methods depend on access control lists are no longer suitable for cloud computing, because they need a fully trusted cloud server.

Data sharing in cloud must be protected and achieves confidentiality to the data. An efficient method recently used for sharing sensitive data in cloud is mediated certificate less encryption which offers more security. Because of the pairing less operations, this technique enables immediate revocation thereby ensures security and confidentiality to the data which resides in the cloud. Existing issue like as key escrow and certificate revocation problem can be overcome by this approach. Using this method, in the data owner module, overall overhead can be avoided and single encryption is carried out in the whole process.

Some of major requirements of secure data sharing in the Cloud are as follows:

- Firstly the data owner should be able to specify a group of users that are allowed to view his or her data.
- Any member within the group should be able to gain access to the data anytime, anywhere without the data owner's intervention.
- No-one, other than the data owner and the members of the group, should gain access to the data, including the Cloud Service Provider.
- The data owner should be able to add new users to the group.
- The data owner should also be able to revoke access rights against any member of the group over his or her shared data. No member of the group should be allowed to revoke rights or join new users to the group.

Identity-based encryption (IBE) is a new pattern of public-key encryption (PKE) that uses the identity string of a user for the public key of the user. Revocable IBE (RIBE) is an extension of IBE that can handle the dynamic credentials of users by providing an efficient revocation mechanism. An ideal revocation method in IBE is that a sender just creates a ciphertext without worrying about the revocation of a receiver and only the receiver needs to check the revocation of his credential to decrypt the ciphertext

The particular problem addressed in this paper is how to construct a fundamental identity-based cryptographical tool to achieve the above security goals. 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.

II. LITERATURE SURVEY

In this paper [1], to construct a cost-effective and secure data sharing system in cloud computing, it proposed a

concept called RS-IBE, which supports identity revocation and ciphertext update simultaneously such that a revoked user is prevented from accessing previously shared data, and subsequently shared data. Moreover, a concrete construction of RS-IBE is presented. The developed RS-IBE scheme is proved adaptive-secure in the standard model, under the decisional ℓ-DBHE assumption. The comparison results describe that this scheme has advantages in terms of efficiency and functionality, and thus is more feasible for practical applications.

This paper [2] illustrate the concept of FDR-CP-ABE and present a concrete scheme, which is depend on AND-gates policy supporting positive and negative attributes with wildcards. The developed scheme is confirm protected and enjoys desirable properties such as no secret key update, partial ciphertext update, and constant-size ciphertexts. The FDR-CP-ABE construction can be used to realize fine-grained attribute-based access control over encrypted data in cloud computing.

This paper [3], insert the update function for CP-ABE such that data access policy can be dynamically updated after the ciphertext is generated. First of all, present a new linear secret sharing (LSS) matrix update algorithm depend on previous LSS matrix generation algorithm. Then summarize the common structure of some typical CP-ABE schemes and abstract a basic CP-ABE scheme from them. Then, depend on the matrix update algorithm, implement the policy update algorithm with the encryption algorithm of the basic CP-ABE scheme. In this scheme, data access policy can be directly changed without key update.

Hierarchical identity-based encryption (HIBE) can be extended to revocable HIBE (RHIBE) if a private key of a user can be revoked when the private key is revealed or expired. Existing, different selectively secure RHIBE schemes were proposed, but it is still unsolved problem to build an adaptively secure RHIBE scheme. This paper [4], developed two RHIBE framework in composite-order bilinear groups and prove their adaptive security under simple static assumptions. To prove the adaptive security, use the dual system encryption framework, but it is not easy to use the dual system encryption framework in RHIBE since the security model of RHIBE is quite dissimilar with that of HIBE. It display that it is possible to resolve the issue of the RHIBE security proof by carefully designing hybrid games.

In this paper [5], the main objective is resolving the major problem of identity revocation, introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. This scheme offloads most of the key generation related operations during key-issuing as well as key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users to execute locally. This goal is accomplished by exploiting a novel collusion-resistant method: employ a hybrid private key for each user, in which an AND gate is involved to connect and bound the identity component and the time component. Furthermore, we propose another construction which is provable secure under the recently formulized Refereed Delegation of Computation model. At the last, it will give extensive experimental results to describe the efficiency of the proposed construction.

This paper [6], provide an affirmative solution to tackle the efficiency issue incurred by revocation. Implement the first cloud-based revocable identity-based proxy re-encryption (CR-IB-PRE) scheme that supports user revocation but also delegation of decryption rights. No matter whether a user is revoked or not, at the end of a given time period the cloud acting as a proxy will re-encrypt all ciphertexts of the user under the current time period to the next time period. If the user is revoked in the forthcoming time period, he cannot decrypt the ciphertexts by using the expired private key anymore. It state that this primitive is applicable to many practical network applications, such as subscription-based cloud storage services. Comparing to some naive solutions which needs a private key generator (PKG) to communicate with non-revoked users in each time period, the current scheme provides definite advantages in terms of communication and computation efficiency. This scheme only requires the PKG to publish a constant-size public string for each time period and meanwhile, the workload of ciphertexts update is off-loaded to the cloud server. More importantly, the scheme can be proven secure in the standard model.

This paper [7] presented a new system satisfying the concept by leveraging identity-based encryption, asymmetric pairing group conversion, identity-based proxy re-encryption and searchable encryption technologies. It proved the system in the generic bilinear group model. This system is cost effective as well as permit the system users to update keyword field at anytime. The efficiency analysis showed its great potential in the applications of large scale database.

This paper [8], revisit RIBE from the viewpoint of both security models and constructions. Firstly, introduce a realistic threat, which call decryption key exposure, and show that all prior RIBE constructions, except the Boneh-Franklin one, are vulnerable to decryption key exposure. then, implemented the first scalable RIBE scheme with decryption

key exposure resistance by connecting the (adaptively secure) Waters IBE scheme and the (selectively secure) Boneh-Boyen IBE scheme, and show that RIBE scheme is more effective than all existing adaptively secure scalable RIBE schemes. Additionally, introduce a new security definition of revocable identity-based signature (RIBS) with signing key exposure resistance, and propose the first scalable RIBS scheme based on the Paterson-Schuldt IBS. Finally, give implementation results of this schemes to adduce the feasibility of schemes.

Sr.no	Paper Title	Technique Used	Advantages	Disadvantages
1	Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption	proposed a concept called RS-IBE, which supports identity revocation and ciphertext update simultaneously such that a revoked user is prevented from accessing previously shared data, and subsequently shared data	functionality ,efficiency, and it is feasible and cost-effective data-sharing system.	Security, privacy
2	Attribute-Based Data Sharing with Flexible and Direct Revocation in Cloud Computing	It illustrate the concept of FDR-CP-ABE and present a concrete scheme, which is depend on AND-gates policy supporting positive and negative attributes with wildcards	This scheme supports direct attribute and user revocation	It is not flexible
3	Policy Update for Ciphertext-Policy Attribute-Based Encryption	insert the update function for CP-ABE such that data access policy can be dynamically updated after the ciphertext is generated	The communication, computation, and storage costs for an update no longer depend on the number of users,	Not secure
4	Revocable hierarchical identity-based encryption with adaptive security	developed two RHIBE framework in composite-order bilinear groups and prove their adaptive security under simple static assumptions	the first RHIBE schemes that achieve the adaptive security	--------
5	Identity-based encryption with outsourced revocation in cloud computing	introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting	Efficient schema	-------

III. PROPOSED SYSTEM

In proposed system we provide a secure data sharing for cloud storage system with the support of revocable-storage identity-based encryption. Also present the idea of data self destruction is included using which data owner can store the data from specific date to some specified date. After the specified time the data will be removed from the server. Due to this method the chances of data leakage is reduce and system become more secure.

Module Description

1. Key Authority: The function of key authority to generate the keys as well as manage the keys. The key authority provide the key to the data provider to encrypt the data as well as authenticate users to decrypt the data.

2. Data provider: The work of data provider is provides the data to the storage server in encrypted format in a particular time period. The data provider first decides the users who can share the data. Then, encrypts the data under the identities of users, and uploads the ciphertext of the shared data to the cloud server.

3. Storage Server: In this module we use cloud as a storage server where data provider save encrypted data and authenticated users share data in a allocated time period.

4. Users and User Revocation: Here number of users are share the data in a perticular time period. Also this system

efficiently do the user revocation process. Among the users one admin is present who has authority to revocate thee users in a particular time period.

5. Data Self-Distruction:: In this module data self destruction is included using which data owner can store the data from specific date to some specified date. After the specified time the data will be removed from the server.

The proposed system architecture are as follows;

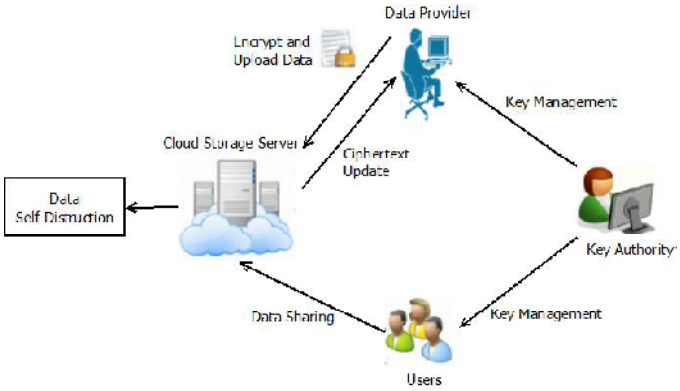

Fig 1. System Architecture

IV. CONCLUSION

Cloud computing is very popular for their functionalities like data storage. From this survey we observe that, this cloud computing functionality is surrounded with multiple issues including secure data outsourcing, secure data sharing, privacy of users, flexibility, scalability, access control, efficient seach etc. This paper focused on the problem of secure data sharing schemes in cloud computing. Also discussed some of the recent technologies developed in recent years to solve the issues mentioned above.

REFERENCES

[1] Wei, Jianghong, Wenfen Liu, and Xuexian Hu. "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption." IEEE Transactions on Cloud Computing (2016).

[2] Zhang, Yinghui, et al. "Attribute-Based Data Sharing with Flexible and Direct Revocation in Cloud Computing." TIIS 8.11 (2014): 4028-4049.

[3] Yuan, Wei. "Dynamic Policy Update for Ciphertext-Policy Attribute-Based Encryption." IACR Cryptology ePrint Archive 2016 (2016): 457.

[4] Lee, Kwangsu. Revocable hierarchical identity-based encryption with adaptive security. Cryptology ePrint Archive, Report 2016/749, 2016.

[5] Li, Jin, et al. "Identity-based encryption with outsourced revocation in cloud computing." Ieee Transactions on computers 64.2 (2015): 425-437.

[6] Liang, Kaitai, et al. "An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing." European Symposium on Research in Computer Security. Springer International Publishing, 2014.

[7] Liang, Kaitai, et al. "Efficient multi-function data sharing and searching mechanism for cloud-based encrypted data." Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016.

[8] Seo, Jae Hong, and Keita Emura. "Revocable identity-based cryptosystem revisited: Security models and constructions." IEEE Transactions on Information Forensics and Security 9.7 (2014): 1193-1205.