ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

Survey on A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud

Bhagyashri Harel, Prof. Nilesh Sable

Department of Computer Science, JSPM College Wagholi, Pune India.

ABSTRACT*:* In cloud providing security, guarantees for the sharing data file. In Data Sharing privacy-preserving is still a challenging issue, untrusted cloud and trusted Cloud due to the collusion attack that why we proposed the a secure data sharing scheme for dynamic members Firstly, we propose a secure way for key distribution and change the private key when user revoke the any group then other member of that group private key will changes with revoked user. Secondly, our scheme can achieve fine-grained access control with two factor one is user password and seconds is one time Password. Thirdly, we can protect the scheme from collusion attack, which means that revoked users cannot get the original data file even if they conspire with the untrusted cloud

KEYWORDS*:* Access control, privacy-preserving, key distribution, cloud computing

I. INTRODUCTION

Cloud computing is an Internet-based computing type that provides computer-shared computer processing resources and data and other devices on demand. It is a computing style where dynamically scalable and often virtualized resources are provided as an Internet service. One of the most basic services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its employees in the same group or department to archive and share files in the cloud. However, it also represents a significant risk for the confidentiality of stored files. A company allows its staff to be in the same group or department to file and share files in the cloud. However, it also represents a significant risk for the confidentiality of stored files. In particular, cloud-managed cloud servers are not trusted by users, and data files stored in the cloud can be sensitive and sensitive, such as business plans. To safeguard data privacy, a basic solution is to encrypt data files and upload encrypted data to the cloud. Identity privacy is one of the most significant obstacles to the widespread implementation of cloud computing. Without the guarantee of identity privacy, users may not be willing to join cloud computing systems because their real identities could easily be revealed to cloud providers andAttackers.On the other hand, unconditional privacy of identity may result in privacy abuse. For example, the wrong staff can trick others into the company by sharing fake files without being traced. Therefore, traceability, which allows the group manager to reveal the actual identity of a user, is also highly desirable. It is recommended that all members of a group can enjoy full cloud storage and sharing services, defined as multi-owner mode. Compared to the unique owner mode, where only the group manager can store and edit data in the cloud, owner multiple mode is more flexible in practical applications. Specifically, each user in the group can not only read the data, but also modify their part of the data across the entire data file shared by the company.Finally, groups are usually dynamic in practice, for example, a new employee involvement and the current employee revocation in a company.Changing affiliates makes it very difficult to exchange data. On the one hand, the anonymous system challenges new users to know the contents of the stored data files before they participate, as it is impossible for new users to contact anonymous data owners and get their decryption keys.On the other hand, you also need an effective member revocation mechanism without updating the secret keys of remaining users to minimize the complexity of key

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

management. Several security schemes have been proposed for data sharing and falsity servers. In these approaches, data owners store the encrypted data files in a trusted archive and distribute the corresponding decryption.

II. RELATED WORK

1. *This paper "Cryptographic cloud storage,"* The cloud provider one of the best services is data storage the security and privacy issue have major concern for organization for utilizing such service. Cloud data storage has provided significant benefits by allowing users to store massive amount of data on demandin a cost-effective manner. To protect the privacy of data stored in the cloud, cryptographic role-based access control (RBAC) schemes have been developed to ensure that data can only be accessed by those who are allowed by access policies. However these cryptographic approaches do not address the issues of trust. In this paper, we propose trust models to reason aboutand improve the security for stored data in cloud storage systems that use cryptographic RBAC schemes. The trust models provide an approach for the owners and roles to determine the trustworthiness of individual roles and users respectively in the RBAC system. The proposed trust models take into account role inheritance and hierarchy in the evaluation of trustworthiness of roles. We present a design of a trust-based cloud storage system which shows how the trust models can be integrated into a system that uses cryptographic RBAC schemes. We have also considered practical application scenarios and illustrated how thetrust evaluations can be used to reduce the risks and enhance the quality of decision making by data owners and roles of cloudstorage service.

2. *This paper "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,"* It is a greatest platform that provides data storage in very lesser cost and all time it should be available over the internet. The security must be important in the cloud computing. The encryption technique is commonly adopted by the cloud computing that means the encrypted data should be stored on the storage of cloud to protect the data. Encryption is no sufficient as organization obtain have to enforce fine-grained access control on data. Such control is based on the attribute that system is known as the attribute based system. For the data privacy it is important to encrypt the data and upload the encrypted data on the cloud. In cloud it is not easy to design efficient and secure data sharing scheme in multiowner system due to the following challenging issues. Identity, revocation and new member participation i.e. the changes of membership make securely data sharing extremely difficult. On the other hand an efficient member revocation without updating the secret key of remaining user to minimize the complexity of key management. Signed receipt is caused after every member revocation in group that minimizes multiple copy of encrypted file it can help to minimize computation cost.

3. *In this paper* "Plutus: Scalable Secure File Sharing on Untrusted Storage," Presented cryptographic storage system that enable secure data sharing. In this technique dividing file into the file group and encrypt each file group with a file block key. In this scheme at the time of user revocation the file block key need to be updated and distributed to the user therefore the system had a heavy key distribution overhead.Plutus is a cryptographic storage system that enables secure file sharing without placing much trust on the file servers. In particular, it makes novel use of cryptographic primitives to protect and share files. Plutus features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. We explain the mechanisms in Plutus to reduce the number of cryptographic keys exchanged between users by using filegroups, distinguish file read and write access, handle user revocation efficiently, and allow an untrusted server to authorize file writes. We have built a prototype of Plutus on OpenAFS. Measurements of this prototype show that Plutus achieves strong security with overhead comparable to systems that encrypt all network traffic.

4. This paper Improved proxy re-encryption schemes with applications to secure distributed storagethat records ownership and process history of data objects is vital to the success of data forensics in cloud computing, yet it

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

is still a challenging issue today. In this paper, to tackle this unexplored area in cloud computing, we proposed a new secure provenance scheme based on the bilinear pairing techniques. As the essential bread and butter of data forensics and post investigation in cloud computing, the proposed scheme is characterized by providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access, and provenance tracking on disputed documents. With the provable security techniques, we formally demonstrate the proposed scheme is secure in the standard model.

5. In this paper Fine Grained Two Factor Access Control for web based cloud computing Services. In this paper, we introduce a new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device. As a user cannot access the system if they do not hold both, the Mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user. Finally, we also carry out a simulation to demonstrate the practicability of our proposed 2FA system.
6. In this paper"Sirius: Securing remote entrusted storage" Optimal Coding and Allocation for perfect Secrecy in multiple cloud. For user to store data in the cloud, using services provided by multiple cloud storage providers (CSPs) is a promising approach to increase the level of data availability and confidentiality, as it is unlikely that different CSPs are out of service at the same time or collude with each other to extract information of a user. This paper investigates the problem of storing data reliably and securely in multiple CSPs constrained by given budgets with minimum cost. Previous works, with variation in problem formulation typically trickle the problem by decoupling it into sub problem and solve them separately.

7. In this paper "Circuit Cipher text- policy Attribute based Hybrid encryption with verifiable Delegation in cloud computing" In the cloud, for achieving access control and keeping data confidential, the data owners could adopt attribute-based encryption to encrypt the stored data. Users with limited computing power are however more likely to delegate the mask of the decryption task to the cloud servers to reduce the computing cost. As a result, attribute-based encryption with delegation emerges. Still, there are caveats and questions remaining in the previous relevant works. For instance, during the delegation, the cloud servers could tamper or replace the delegated ciphertext and respond a forged computing result with malicious intent. They may also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving. Furthermore, during the encryption, the access policies may not be flexible enough as well. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation has been considered in our work. In such a system, combined with verifiable computation and encrypt-then-mac mechanism, the data confidentiality, the fine-grained access control and the correctness of the delegated computing results are well guaranteed at the same time. Besides, our scheme achieves security against chosen-plaintext attacks under the k-multilinear Decisional Diffie-Hellman assumption. Moreover, an extensive simulation campaign confirms the feasibility and efficiency of the proposed solution

8. In this paper "Secure Data Sharing in Cloud Computing using Revocable Storage identity based encryption"Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data. Identity-based encryption is a promising cryptographical primitive to build a practical data sharing system. 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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

system. Consequently, the revoked user cannot access both the previously and subsequently shared data. To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of ciphertext by introducing the functionalities of user revocation and ciphertext update simultaneously. Furthermore, we present a concrete construction of RS-IBE, and prove its security in the defined security model. 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. Finally, we provide implementation results of the proposed scheme to demonstrate its practicability.

III. PROPOSED SYSTEM

1. In this system propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group.
2. The system provides a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.
3. The system can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.
4. Secure data sharing scheme which can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untruth cloud. Our scheme can achieve secure user revocation with the help of polynomial function.
5. System is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated.
6. System will provide security analysis to prove the security of our scheme.

Advantages of Proposed System:

1. The computation cost is irrelevant to the number of revoked users in RBAC scheme. The reason is that no matter how many users are revoked, the operations for members to decrypt the data files almost remain the same.
2. The cost is irrelevant to the number of the revoked users. The reason is that the computation cost of the cloud for file upload in our scheme consists of two verifications for signature, which is irrelevant to the number of the revoked users. The reason for the small computation cost of the cloud in the phase of file upload in RBAC scheme is that the verifications between communication entities are not concerned in this scheme.
3. In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, our scheme is able to support dynamic groups efficiently, when a new user

IV. PROPOSED TECHNIQUES

Role-based encryption techniques:

Role-based-access-control (RBAC) is a policy neutral access control mechanism defined around roles and privileges. The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments. A study by NIST has demonstrated that RBAC addresses many needs of commercial and government organizations.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

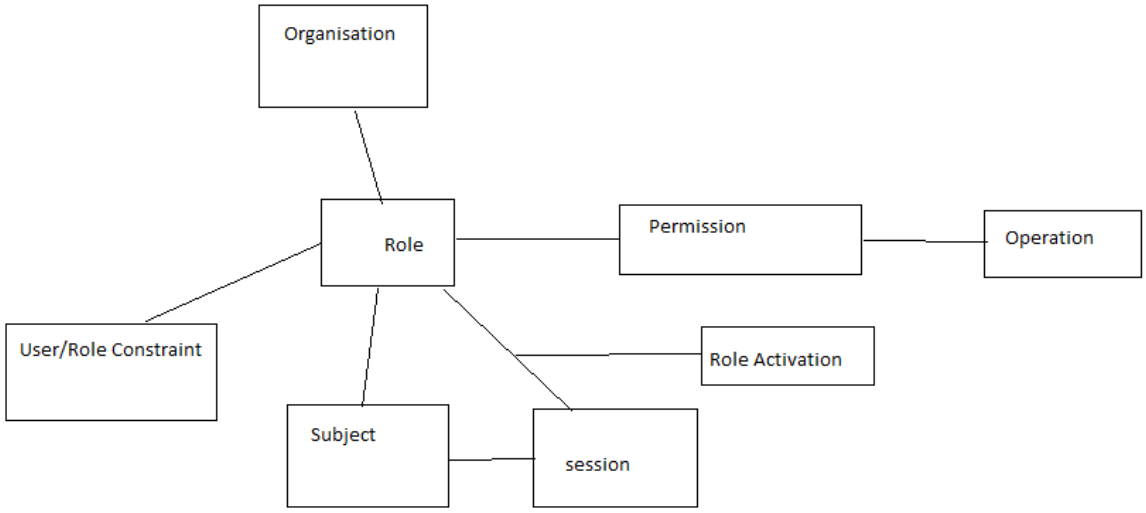

Fig 1.2 Role Attribute- based encryption techniques.

PERFORMANCES ANALYSIS

Number	Factor	AES	Blowfish	Two Fish
1.	Key Length	AES accepts keys of 128, 192 or 256 bits (128 bits is already very unbreakable), uses 128-bit blocks	Blowfish is 64 bits. Blowfish is efficient in software, at least on some software platforms (it uses key-dependent lookup tables, hence performance depends on how the platform handles memory and caches).	Two Fish is 128 bits Relatively complex key Schedule
2.	Cipher Type	Symmetric Block cipher	Symmetric Block Algorithms	Symmetric Block Algorithms and Advanced Encryption Standard content
3.	Round	14	16	Not fixed around 2^{256}

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 7, July 2018

Number	Factor	DES	DiffieHellman	Random Number Generator
1.	Key Length	56 bits	128 bits	128 bits
2.	Block Size	64 Bits	128 Bits	192 bits

V. CONCLUSION

The system is design for secure data sharing scheme, for dynamic groups in an untruth cloud. a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, It supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. A new type authentication system, which is highly secure, has been proposed in this system.

REFERENCES

.[1] S.Kamara and K. Lauter, "Cryptographic cloud storage," in Proc.Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.
[2] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: Theessential of bread and butter of data forensics in cloudcomputing," in Proc. ACM Symp. Inf., Comput.Commun.Security,
2010, pp. 282–292.
[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable secure file sharing on untrusted storage,"in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.
[4] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improvedproxy re-encryption schemes with applications to secure
[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable,and fine-grained data access control in cloud computing," in distributedstorage," in Proc. Netw. Distrib. Syst. Security Symp., 2005,pp. 29–43.
[6] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote entrusted storage," in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131–145.
[7] B. Waters, "Ciphertext-policy attribute-based encryption: Anexpressive, efficient, and provably secure realization," in Proc. Int.Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography,2008, pp. 53–70.
[8] NazatulHaque Sultan Ferdous Ahmed Barbhuiya, A Secure Re-Encryption Scheme for Data Sharing in Unreliable Cloud Environment,978-1-5090-2616-6/16 2016 IEEE DOI 10.1109/SERVICES.2016.16.