International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||

A Self-Secure Anti Collusion Data Sharings in Dynamic Group in Cloud Computing A Survey

Ms. Yogita Dhole[1], Dr. Soumitra Das[2]

Department of Computer Engineering, DYPSOE, Pune, India[1]

Department of Computer Engineering, Indira College of Engineering and Management, Pune, India[2]

ABSTRACT: Cloud Computing users can achieve an effective and economical approach for data sharing among group members in cloud. Meanwhile provided security guarantees for sharing data file since they are outsourced. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. Moreover, for existing schemes, the security of key distribution is based on the secure Key distributed Mail Authentication and data are secure where, unknown user or group Member. In this paper, we propose a secure data sharing scheme for dynamic members. First, we propose a secure way for key distribution without any secure communication channels, and the users can securely obtain their private keys from group manager. Second, our scheme can achieve fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. Third, 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. In our approach, by leveraging polynomial function, we can achieve a secure user revocation scheme. Finally, our scheme can achieve fine efficiency, which means previous users Compulsory to update their private keys for the situation a user is revoked from the group via self-revocation and by group admin.

KEYWORDS: Access Control, Cloud Computing, Key Distribution, Privacy-Preserving.

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 and Attackers. 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 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.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||

I.I. BACKGROUND

The cloud provider provides one of the best services is data storage the security and privacy issue have major concern for organization for utilizing such service. 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 theencrypted data on the cloud. In cloud it is not easy to design efficient and secure data sharing scheme in multiword 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.

I. II. RELATED WORK

1.1 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 demand in 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 about and 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 consider 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 the trust evaluations can be used to reduce the risks and enhance the quality of decision making by data owners and roles of cloud storage service.

1.2 This Paper ”View of Cloud Computing ” Cloud Computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under provisioning for one that becomes wildly popular, thus missing potential customers and revenue. Cloud computing refers to the use of Internet ("cloud") based computer technology for a variety of services. It is a computing model in which virtualized resources are provided as a service over the Internet. The concept incorporates infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) that have the common theme for satisfying the computing needs of the users. Cloud computing services usually provide common business applications online that are accessed from a web browser. This paper pays much attention to the Grid paradigm, as it is often confused with Cloud technologies. We also de- scribe the relationships and distinctions between the Grid and Cloud approaches.

1.3 This Paper “Plutus: Scalable secure file sharing on untrusted storage” We consider the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. We describe, at a high level, several architectures that combine recent and non-standard cryptographic primitives in order to achieve our goal. We survey the benefits such an architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage.

1.4 “SiRiUS: Securing Remote Untrusted Storage” This paper presents SiRiUS, a secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, OceanStore, and Yahoo! Briefcase. SiRiUS assumes the network storage is untrusted and provides its own read-write cryptographic access control for file level sharing. Key management and revocation is simple with minimal out-of-band communication. File system freshness guarantees are supported by SiRiUS using hash tree constructions. SiRiUS contains a novel

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||

method of performing file random access in a cryptographic file system without the use of a block server. Extensions to SiRiUS include large scale group sharing using the NNL key revocation construction. Our implementation of SiRiUS performs well relative to the underlying file system despite using cryptographic operations.

1.5 This Paper "Improved proxy re-encryption schemes with applications to secure distributed storage" In 1998, Blaze, Bleumer, and Strauss (BBS) proposed an application called atomic proxy re-encryption, in which a semi-trusted proxy converts a ciphertext for Alice into a ciphertext for Bob without seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. Following recent work of Dodis and Ivan, we present new re-encryption schemes that realize a stronger notion of security, and we demonstrate the usefulness of proxy re-encryption as a method of adding access control to a secure file system. Performance measurements of our experimental file system demonstrate that proxy re-encryption can work effectively in practice.

1.6 This Paper "Fully collusion secure dynamic broadcast encryption with constant-size Ci-phertexts or decryption keys" This paper puts forward new efficient constructions for public-key broadcast encryption that simultaneously enjoy the following properties: receivers are stateless; encryption is collusion-secure for arbitrarily large collusions of users and security is tight in the standard model; new users can join dynamically i.e. without modification of user decryption keys nor ciphertext size and little or no alteration of the encryption key. We also show how to permanently revoke any subgroup of users. Most importantly, our constructions achieve the optimal bound of O(1)-size either for ciphertexts or decryption keys, where the hidden constant relates to a couple of elements of a pairing-friendly group. Our broadcast-KEM trapdoor technique, which has independent interest, also provides a dynamic broadcast encryption system improving all previous efficiency measures (for both execution time and sizes) in the private-key setting.

1.7 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 cloudit is not easy to design efficient and secure data sharing scheme in multi owner 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.

1.8 In this paper "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud ," 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.

1.9 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 cipher text and respond a forged computing result with malicious intent. They may also cheat the eligible users by responding

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||

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 cipher text-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-multi linear Decisional Diffie-Hellman assumption. Moreover, an extensive simulation campaign confirms the feasibility and efficiency of the proposed solution

1.10In 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.

II. INDENTATIONS AND EQUATIONS

2.1Notation

ID_iThe Identity of user i
ID_{data} The Identity of data
Pk the public key of user that needs to be negotiated with group manager
Sk the corresponding private key to Pk
$KEY=(x_i,A_i,B_i)$ the Private key which is distributed to the user from the group manager and used for data sharing
$Enc_k()$ Symmetric encryption algorithms used the encryption key k
$AENC_k()$ Asymmetric encryption algorithms used the encryption key k
UL group User List
DL Data List

2.2Equations

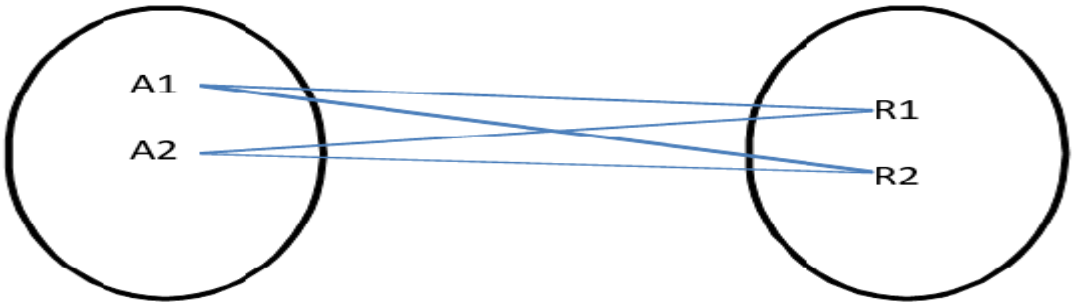
ID_i,pk,ac,v_i (1)
U,R (2)
$R.e(v_1.F(pk||ac||ID_i).P,W)=e(U,P)$ (3)
$ID_i,V_2,AENC_{sk}(ID_i,,V_1,ac)$ (4)
$AENC_{pk}(KEY,V_2)$ (5)
$ENC_{B1}(ID_{data},C1,C2,C,t_{data})$ (6)
$C_1=K.Y€G_1$ (7)
$C_2=K.P €G_1$ (8)
$K=Z^k€G_2$ (9)
$C=ENC_k(M)$ (10)
S={s,e,X,Y,$,GM.GU}
Where,
S=Start of the Applications

1. Group Member (Group User) registration with dynamic Groups.
2. Group Member (Group User) Login with Email & password.
3. Load the Data in Cloud.
4. e=end of Program.
5. Group Manger (GM) login with Name& Password.
6. $AENC_{PK}$=Encryption at content Level
7. Group Manger (GM) {$DF=(ID_{group},ID_{data},CE,EK,t_{data})$, σ_{DF}} To Cloud C.
8. E=end of program.

Functions: Polynomial function are used

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||



A1: A1 is User which are revoke from Group then Private key of all member is updated.
A2: A2 is User which is revoking from Group then Private key of all member is updated.
R1:R1 is user of Same Group
R2:R2 is user of Same Group

III. SYSTEM OVERVIEW

In the new proposed system, a secure data sharing scheme which can be achieved through a secure key distribution and data sharing for dynamic group along with secure way non-secure communication channel. New re-encryption is used for assigning the permission data encryption. The Users can securely obtain their Private key from group Manger with Certificate authorities for verification scheme. The System can achieve the fine grained access control. Hybrid cloud is used for efficient use of cloud. Our System used for data sharing can be protected from collusion attack. The Revoked user not gets the original data access once when they revoked from particular even if they tried with untruth cloud. System supports the dynamic group efficiently when user joins the group or revoked from group their private key is updated and recomputed.

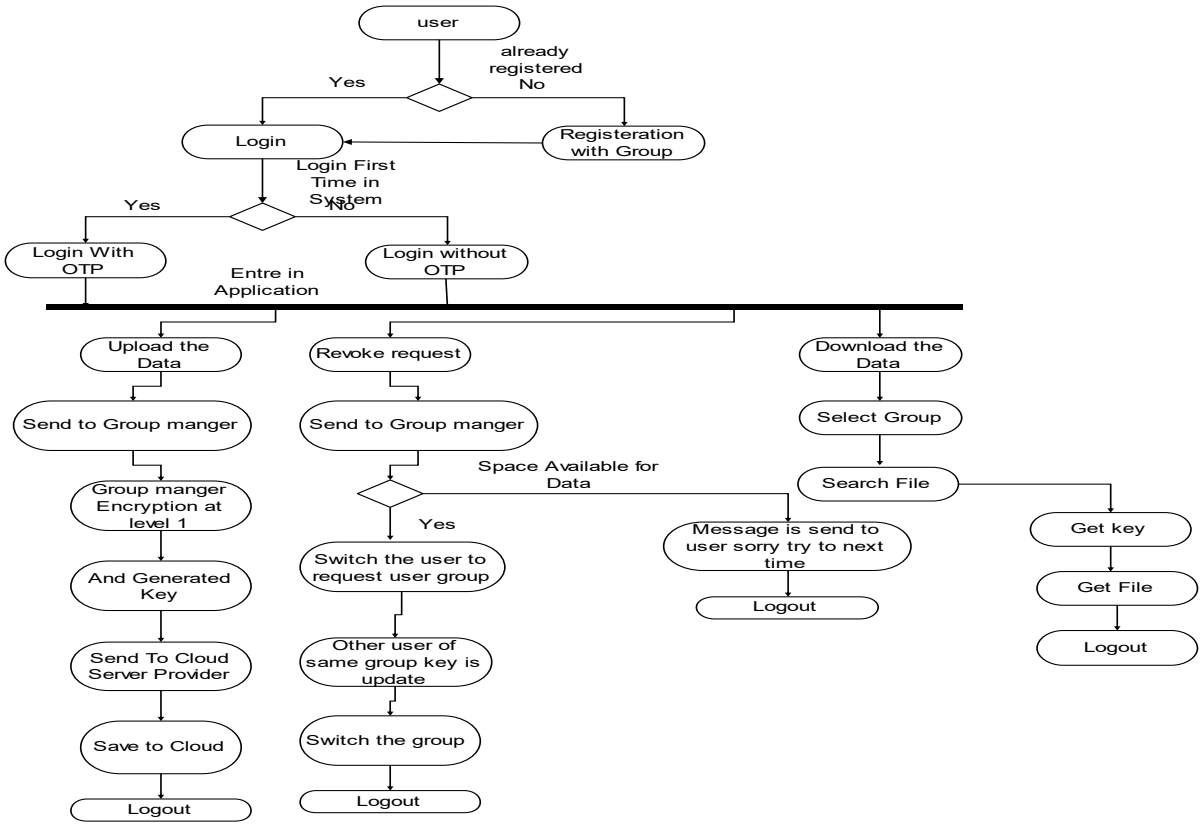


Fig 1: System Overview Diagram

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 5, May 2020||

IV. CONCLUSION

In this paper, we design a secure anti-collusion data sharing scheme for dynamic groups in the cloud. In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities. Also, our scheme can support dynamic groups efficiently, when a user is revoked from the group, then all member's key of same group should be updated and recomputed. Moreover, our scheme can achieve secure user revocation, the revoked users cannot get the original data files of other group members.

REFERENCES

[1] S.Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.
[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.
[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] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131–145.
[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw. Distrib. Syst. Security Symp., 2005, pp. 29–43.
[6] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size Ciphertexts or decryption keys," in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 39–59.
[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun.Security, 2010, pp. 282–292.
[8] "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud "Xuefeng Liu, YuqingZhangBoyang Wang, and Jingbo Yan 2013 IEEE.
[9] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, 2008, pp. 53–70.
[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.