IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

A Survey on Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud

S. Sahaya Nirmala Daisy[1], Dr. D. Ravindran[2]

MPhil Scholar, St. Joseph's College, Truchirapalli, Tamil Nadu, India[1]

Dean, School of Computer Science, St. Joseph's College, Truchirapalli, Tamil Nadu, India[2]

Abstract: Cloud computing is the delivery of computing services over the Internet. The present time cloud computing provides us a efficient way to share data amoung cloud users with low maintenance. In this paper we see the secure multiowner data sharing scheme for dynamic groups in cloud computing. And also a secure multiowner data sharing schema by leveraging group signature and using dynamic broadcast encryption techniques any members can share and data with other users. MONA presented for secured multi owner data sharing to resolve the many problem in the cloud computing.Whenever the existing system is revocation of member form group.manager has to generate a new key and then distribute to other members able to upload or download files. So that we need for generating new key each time whenever therisa revocation of members.

Keywords: Cloud computing,Data sharing, Group Signature,Dynamic group

I. INTRODUCTION

Cloud computing is one of the greatest platform services. That provides the storge of data in very low cost and available for all time.Cloud computing is shared resources, software and informaion through computer devices on demand. Cloud computing means more than simply saving on Information Technology implementation costs. To preserve data privacy and basic solution is to encrypting data files and upload encrypted data into the cloud. As we know sharing data only by manager in a single owned manner is not flexible so we use multi-owner manner in the cloud computing.

Basic concept of MONA

Data storage is the one of the major services provided by the cloud providers. Now consider a practical application. one organization allow all its staff members to store and share data files in the cloud .By using the cloud, the staff become free from the maintenance of data in a local system. But it may create a problem for the data confidentiality. Particularly, the cloud servers that are managed by the cloud providers are not trusted by the users while the data files stored in the cloud are may be sensitive and confidential, that are may be business plans. To maintain the data privacy, one of the solution is to encrypt the data files and then the encrypted files are uploaded into the cloud. Unfortunately, it is not an easy task to design an efficient and secure data sharing method for the groups in the cloud. In the cloud computing the identity privacy is one of the major obstacle. Without giving guarantees to the users, the users are not interested to participate in the cloud computing system. Because whenever the dispute occurs the real identities are disclosed to cloud providers. On the other hand, unconditional identity privacy may create the problem to privacy.

In single owner manner the group manage can only store and change update the data present in the cloud but the multiple –owner manner is more flexible for the practical applications additionally the each and every user in the group not only permitted for reading the data but they was shared by the company.[1].

II. RELATED WOR

B. Waters et al.,[1]

In this paper shows that new methodology for using realizing Ciphertext-Policy Attribute Encryption (CP-ABE) in existing file. To classify the access control in terms of any access formula over the attributes in the system. So that the efficient system, ciphertext size, encryption, and decryption time scales are used in this section. In this paper shows that three method of framework. There are used Parallel Bilinear Diffie-Hellman Exponent (PBDHE) statement which can be viewed as a simplification of the BDHE report. The anther mothod provides the concert tradeoffs to achieve verifiable security in that decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions.

Ming Li et al.,[2]

In this paper recommend the novel framework of access control to PHRs within cloud computing. They used power attribute based encryption (ABE) techniques to encrypt each patient's PHR data. To decrease the key for sharing density, to divided the system for keen on multiple security domains, each area manages only a subset of the users. Through is way each patient has full organize there key, so that key administration complexity are compact to totally. They used the storage as a service software as a

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

service. They are used public key service in two ways that Google Health and Microsoft Health vault.

M. Kallahalla et al., [3]
Plutus is a one of the cryptographic storage system. That secure file sharing system without insertion much trust on the file servers. It makes use of cryptographic primitives to protect the file sharing. Plutus is the wonderful features key management to allowing the human being to users and retain the direct control who gets access to their file. They given the details the mechanisms in Plutus to reduce the number of cryptographic keys exchanged between users by using file groups. To make a feature file read and write access, touch user revocation powerfully. And also is not allow the another userto write fileor read. It's built a model of Open AFS and also its shows that achieve the strong security to compare the systems that encrypt all network interchange.

E. Goh et al .,[4]
This paper presents SiRiUS as a protected fiyle system.And also P2P file system is calledself belief network, like FS,CIFS. SiRiUS was help the network storage to untrusted file to share the cryptographic contact control to read-write user. The Key organization was revocation a simple with least out-of-band significance. SiRiUS has using confusion tree constructions file system to make user to get the advance guarantees for using without block server. SiRiUS introduced the huge file size group to sharing with help of NNL key revocation manufacture. It wished-for the SiRiUS performs well relation to the fundamental file system in malice of using cryptographic operations.

G. Ateniese et al. [5]
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 move up and down without seeing the original plaintext. That the fast and secure re-encryption will become progressively more popular as a method for managing encrypted file systems. In that the wide-spread implementation of BBS re-encryption has been held up by substantial safety risks. In this paper showed the new re-encryption schemes that realize a stronger notion of security and 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.

K.Guruprasad et al., [6]
They are proposed a secure multiowner data sharing theme, named Mona, for dynamic team within the cloud. By investing cluster signature and dynamic broadcast encryption techniques, any cloud user will in secret share information with others. In the meantime, the storage overhead and brainwashing totalling price of our theme are self-employed with the amount of revoked users. They are used high-quality services and save significant investments on their native infrastructures.

R. Lu et al., [7]
In this paper undertake this unfamiliar area in cloud computing for the new secure origin scheme based on the bilinear pairing techniques. The necessary bread and butter of data forensics and post study in cloud computing. Through the plan is characterized by given that the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access, and provenance tracking on disputed documents.

Deepa Noorandevarmath et al., [8]
They imply that any user in the group can securely share data with others by the untrusted cloud. This scheme was able to support dynamic groups. The new settled users can openly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be simply achieved through a novel revocation list without updating the secret Keys of the remaining users. The size and computation overhead of encryption are constant and Independent with the number of revoked users. They are supports efficient user revocation and new user joining. The 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. The main goal was to provide the security for the data and demonstrate the efficiency of our schema in experiment.

C.Suchithra et al., [9]
The person response to express the group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. And also they implement the Load Balancing to process the user requested job, by allocate to the sub servers which will process the job by evaluating the CPU performance level. It was highly suggested that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which was defined as the multiple-owner manner. They are anticipated a cryptographic storage system that enables secure file sharing from an untrusted server, named Plutus. They are reined the two parts of files to be stored those: file metadata and file data. The file meta-data implies the access control information that includes a series of encrypted key blocks, each of which was encrypted under the symmetric key of authorized users. They introduced the scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique.

T.Vijayalakshmi et al., [10]
They are proposed the privacy preserved multi owner data sharing scheme, named Suody. We can used maximum advantage of group signature to build homomorphism authenticators, signed receipts and dynamic broadcast

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

encryption techniques, the user can share the data with others using withheld authorship in the cloud. At the same time overhead in the storage and computation cost for encryption of our scheme for the number of users revoked are independent.

Smt. R. Anitha et al., [11]
In this paper they are used in signature and encryption techniques. It's shows that group manager has to generate a new key and then distribute to other members through this existing group signature revoked member is not able to upload or download files. They are used cryptography techniques to secure data and user private identity for authencation. With RSA algorithm they designed the data sharing scheme, mona for dynamic group in a an untrusted group. The user can share data with other in the group and the group without revealing identity privacy to the cloud.

Renu S1 et al., [12]
In this paper propose a new approach based on biometric encryption for to improve the security of data sharing in public cloud. We combine the digital key with the biometric image to create bioscrypt. These digital keys can be used as the cryptographic key. During the verification the biometric image are combining with bioscrypt to recover the key for the encryption and decryption of the data. Then the cipher text was uploading to the public cloud. And an authorized user can retrieve data by his digital key. This approached was ensures the data integrity and confidentiality.

Mr.K.Janardhan et al., [13]
This paper proposed the group signature and dynamic broadcast encryption techniques in any cloud user can anonymously share data with others. And also the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. And also they analyze the security of scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments

Dr. Santosh Lomte [14]
In this paper authentication model was proposed to using Kerberos technique and threshold cryptography. They used for Kerberos Authentication Model to get the ticket granting server (TGS). With the Kerberos instead of only single ticket generating and generate multiple ticket by TGS (n TGS) out of that some of them (k) are used to decrypt the master key where (k<n). And also they proposed minimizes the problem to exchange of key that are generally occurs in symmetric and asymmetric key cryptography.

III.COCLUSION

To summarize this survey paper presents on mona secure multi-owner data sharing for dynamic group in the cloud. And also advantage &disadvantage of existing system. By separating files into file groups and encrypting every file group with other. That owner will share the file groups with others through delivering the corresponding deposit in the cloud server. However it brings a couple of significant key distribution overhead for large-scale file sharing the file key has to be updated and distributed once more for a user revocation.

REFERENCE

[1] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008."

[2] Ming Li, Shucheng Yu, Kui Ren, And Wenjing Lou" Scalable And Secure Sharing Of Personal Health Records In Cloud Computing Using Attribute-Based Encryption", IEEE transactions On Parallel And Distributed Systems Vol. Xx, No. Xx, Xx 2012.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[4] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[6] K.Guruprasad, K.Tulasi "Data Sharing with Multi-Owners in Cloud" IJESC, ISSN-2321 - 3361 ,July 2014 .

[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[8] Deepa Noorandevarmath, Rameshkumar H .K, C M Parameshwarappa" Sharing Of Multi Owner Data in Dynamic Groups Securely In Cloud Environment", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 6,June-2014

[9] C.Suchithra, G.Appasami" A Secure Multi-Owner Data Sharing and Load Balancing for Dynamic Groupsin the Cloud", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 3, March 2014.

[10] T.Vijayalakshmi, Balika J Chelliah and R. Jegadeesan" SUODY-Preserving Privacy in Sharing Data with Multi-Vendor for Dynamic Groups", Global journal of Engineering, Design & Technology,Vol.3(1):43-47 (January-February, 2014).

[11] Smt. R. Anitha, Roushan Kumar, Abhishek Kumar, Shivam, Abhishek Kumar" Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169,Volume: 3 Issue: 5. May 2015.

[12] Renu S, Hasna Parveen O H" Biometric Based Approach for Data Sharing inPublic Cloud", International Journal of Advanced Research in Computer and Communication Engineering,Vol. 4, Issue 2, February 2015.

[13] Mr.K.Janardhan,Mr.M. Narendra" Mona: Secure Multi-Owner Data Sharing for Dynamic Groups inthe Cloud", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 ,NATIONAL CONFERENCE on Developments, Advances & Trends in Engineering Sciences(NCDATES- 09th & 10th January 2015).

[14] Dr. Santosh Lomte , Shraddha DUdhani (2015) " Secure Key for Authentication & Secret Sharing In Cloud Computing " , International Journal of Advance Research in Computer science and Software engineering, (vol.5, June 2015) ISSN NO: 2277428X.