Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.730 – 734

RESEARCH ARTICLE

An Efficient Secure Multi Owner Data Sharing for Dynamic Groups in Cloud Computing

I. VARUN[1], VAMSEE MOHAN. B[2]

[1]M.Tech 2nd year, Dept of CSE, PBR VITS, Kavali, Nellore, A.P, India

[2]Associate Professor, Dept of CSE, PBR VITS, Kavali, Nellore, A.P, India

[1] varunvinny1251@gmail.com; [2] vamsi.imq@gmail.com

Abstract— In this paper, we present a secure multi owner data sharing scheme for dynamic groups in the cloud computing. By leveraging on group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. In this propose a new model for Sharing Secure Data in the Cloud computing for the Multiuser Groups. In this one of the biggest concern with cloud data storage is that of data integrity verification at untreated servers. To preserve data privacy, the basic solution is to encrypt data files, and then upload the encrypted data into the cloud. To resolve this problem recently the best efficient method MONA presented for secured multi owner data sharing in however we identified some limitations in that same approach in terms of reliability and scalability. Hence in this paper we are further extending the basic MONA by adding the reliability and as well as improving the scalability by increasing the number of group managers dynamically.

Keywords — Cloud Computing, Data Sharing, Group Signature, Dynamic Groups, User Revocation, Access Control

I. INTRODUCTION

Cloud computing is one of the greatest platforms which provide storage of data in very lesser cost and available for all time over the internet Cloud computing is Internet-based computing, whereby shared resources, software and information are provided to computers and devices on demand. In this several trends are opening up the era of Cloud Computing, which are an Internet-based development and use of computer technology. Cloud Computing means more than simply saving on Information Technology implementation costs. Cloud Computing offers enormous opportunity for new innovation, and even disruption of entire industries. So Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources.

Cloud Computing is recognized as an alternative to traditional Information Technology (IT) due to its intrinsic resource-sharing and low-maintenance characteristics. In this cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud computing users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures, and one of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypting data files, and then uploads the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues.

Many privacy techniques for data sharing on remote storage machines have been recommended [4], [5], [6]. In these models, the data owners store the encrypted data on untreated remote storage. After that they will share the respective decryption keys with the authorized users. This prevent the cloud service providers and intruders to access the encrypted data, as they don't have the decrypting keys. However the new data owner registration in the above said models reveals the identity of the new data owner to the others in the group. The new data owner has to take permission from other data owners in the group before generating a decrypting key [3], [7], [8]. The proposed system identified the problems during multi owner data sharing and proposed an efficient protocols and cryptographic techniques for solving drawbacks in the traditional approach. In this it proposed an efficient and novel secure key protocol for group key generation and using these key data owners can encrypt the all files. Suppose new user register into group the user need not to contact the data owner during the downloading of files and data can be encrypted with AES before uploading the data in to the cloud.

II. RELATED WORK

Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, [1], the authors specified a secure data sharing model, Mona, for dynamic groups in a remote storage. In MONA, a data owner can share data with others in the group without announcing their identity. Moreover, Mona supports effective user repudiation and new user registration. More specially, efficient user repudiation can be attained by a public revocation list without ideating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their presence.

E. Goh, H. Shacham, N. Modadugu, and D. Boneh [5], the contents of files placed on remote server are metadata and file data. The file metadata contains the access control data that encompass collection of encrypted keys. These metadata files are encrypted with public key of authorized users. As the file metadata should be refurbished, the user abrogation in the scheme is an uncompromising issue particularly for large-scale sharing. Nonetheless, the private key should be regenerated for each user for every new user addition into the group. This limits the application to support dynamic groups. Another issue is the encryption load enhances with the sharing scale. .

The proxy reencryption model given by Ateniese et al. [6] strengthens the distributed storage. The data encryption done by the data owners is a two-step procedure. First, encryption is done using exclusive and symmetric content keys. Second, the data is encrypted with a master public key. Proxy cryptography is used by the server to reencrypt the particular content key(s) from the master public key. On the other hand, the remote storage server can be attacked by any malicious user to find the decryption keys of all encrypted blocks.

M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia [2], [9], the data centers hardware and software is what we will call a cloud. When a cloud is made available in a pay-as-you-go manner to the general public, they call it a public cloud; the service being sold is utility computing. They use the term private cloud to refer to internal data centers of a business or other organization, not made available to the general public, when they are large enough to benefit from the advantages of cloud computing that we discuss here. Thus, cloud computing is the sum of SaaS and utility computing, but does not include small or medium-sized data centers, even if these rely on virtualization for management. People can be users or providers of SaaS, or users or providers of utility computing. They focus on SaaS providers (cloud users) and cloud providers, which have received less attention than SaaS users.

D. Pointcheval and J. Stern [10] As Explained in the Introduction, there w ere several proposals for pro v ably secure Signature schemes. However, in all cases, the security was at the cost of a considerable loss in terms of efficiency. Concerning blind signatures, Damgard, Ptzmann and Waidner and more recently at D. Pointcheval and J. Stern [10] As Explained in the Introduction, there w ere several proposals for pro v ably secure Signature schemes. However, in all cases, the security was at the cost of a considerable loss in terms of efficiency. Concerning blind signatures, Damgard, Ptzmann and Waidner and more recently at Crypto '97, Juels et al. Have presented some blind signature schemes with a complexity-based of security. Again, the security y is at the cost of inefficiency. In the weaker setting by the random oracle model, we have provided security arguments for practical and even efficient digital signature schemes and blind signature schemes. On the ground of our reductions, one can justify realistic parameters, even if they are not optimal. Further improvements are expected particularly in the case of blind signatures where it should be possible to obtain a reduction polynomial in the size of the keys and in the number of interactions with the signer.

III. MONA Model

In the literature analysis we have seen many methods for secure data sharing in cloud computing, however most methods failed to achieve the efficient and as well as secure method for data sharing for groups. To provide the best solutions for the problems imposed by existing methods, recently the new method was presented called as MONA [1]. This approach presents the design of secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud. In MONA, a user is able to share data with others in the group without revealing the identity privacy to the cloud. Then additionally, MONA supports efficient user revocation and new user joining methods. 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. Moreover, the storage overhead and the encryption computation cost are constant. Therefore practically in all cases MONA outperforms the existing methods.

Fig 3.1 Existing MONA Model

Access control*:*

The requirement of access control is twofold. First, group members are able to use the cloud resource for data operations. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked.

Data confidentiality*:*

Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. Specifically, new users should decrypt the data stored in the cloud before their participation, and revoked users are unable to decrypt the data moved into the cloud after the revocation.

Anonymity and traceability:

Anonymity guarantees that group members can access the cloud without revealing the real identity. Although anonymity represents an effective protection for user identity, it also poses a potential inside attack risk to the system.

Efficiency:

The efficiency is defined as follows: Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the remaining users. That means, the remaining users do not need to update their private keys or re-encryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

The main disadvantage of MONA Model is However as per reliability and scalability concern this method needs to be workout further as if the group manager stop working due to large number of requests coming from different groups of owners, then entire security system of MONA failed down.

Thus to achieve the reliable and scalable MONA approach, in this paper we are presenting the new framework for MONA called as MONA with Reliability and Scalability. In this method we are further presenting how we are managing the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers. This method claims required efficiency, scalability and most importantly reliability.

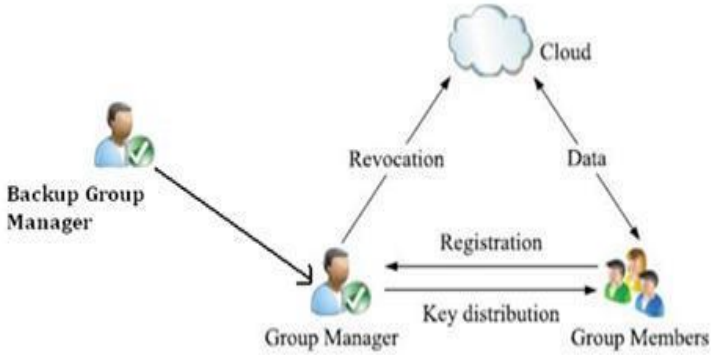

Fig 3.2 Proposed MONA Model

To overcome the disadvantage of existing system MONA, the proposed MONA is if the group manager stop working due to large number of requests are coming from different groups of owners, then backup group manager will remains available. That will take the all responsibilities of group manager and work same as existing group manager.

Performance

The performance of proposed system is more compare to existing one, because in proposed system if new user enters into the cloud he does not depend on other users. The new user directly communicates with the group key manager and getting secret key. So the performance of the proposed system is high.

Security:

The security of proposed system is high compare to existing one. Since the group members only know the secret key. Suppose an unknown person enter into group he does not find the secret key i.e. the user enters into group confirm that he must be a group member.

Complexity: The complexity of proposed system is low compare to existing one. Because the new user does not worry about getting the secret key i.e. the new user does not depend on the remaining group members. The new user directly communicates with group key manager and gets the secret key. The encryption and decryption of file also take less time.

IV. CONCLUSION

In this paper, we propose a secure data sharing scheme, for dynamic groups in an untreated cloud. A user is able to share data with others in the group without revealing identity privacy to the cloud. and additionally, Its 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. However, assuring and enhancing security and privacy practices will attract more enterprises to world of the cloud computing In Thus to achieve the reliable and scalable MONA approach; in this paper we are presenting the new framework for MONA called as Reliable and Scalable MONA. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as fine.

REFERENCES

[1].Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan, Ieee transactions on parallel and distributed systems, vol. 24, no. 6, june 2013.

[2].M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3].S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing,"Proc. IEEE INFOCOM, pp. 534-542, 2010.

[4].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.

[5].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.

[6].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.

[7]. Boneh, D., Boyen, X., Shacham, H.: Short Group Signatures. In: Proc. CRYPTO. pp. 41–55. Springer-Verlag (2004).

[8]. Boneh, D., Freeman, D.M.: Homomorphic Signatures for Polynomial Functions. In: Proc. EUROCRYPT. pp. 149–168. Springer-Verlag (2011)

[9]. Boneh, D., Gentry, C., Lynn, B., Shacham, H.: Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In: Proc. EUROCRYPT. pp. 416–432. SpringerVerlag (2003)

[10]. D. Pointcheval and J.Stern, Security, Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000.

SHORT BIOGRAPHY

Mr. I. Varun received the **B.Tech** Degree in Computer Science and Engineering from Jawaharlal Nehru Technological University, Anantapur, in **2012.**He currently pursing **M.Tech (CSE) in Dept of Computer Science and Engineering** in PBR VITS Engg college, kavali, Nellore**,** under JNTUA University, Anantapur**.**

Mr. Vamsee Mohan. B received the B.Tech degree from P.B.R Visvodaya Institute of Technology & Science, Nellore, A.P., and India in 2005. He completed M.Tech in Computer Science from Scholl of Information Technology, JNTUniversity, Hyderabad, India in 2009.He is having nearly 8 years of teaching experience. He is currently working asAssoc.Professor, Dept of C.S.E, PBRVITS College, Nellore, A.P, India. He is a member of DR Reddy Research Forum (DRRF), PBR Visvodaya Institute of Technology & Science (PBRVITS), Kavali. He published 9 papers in various conferences and journals.

