IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 3, March 2015.
www.ijiset.com
ISSN 2348 – 7968

Secure Information Sharing for Dynamic Groups in Cloud Computing: A Survey

Javed Shaikh
javedgsmcoe@gmail.com

Ajay Kalaskar
ajaykalaskar2010@gmail.com

Deepak Kanhaiye
deepakkanhaiye@gmail.com

Dattatray Waghole
dattawaghole10@gmail.com

***Abstract*—Cloud computing is nothing other than "internet computing". It provides platform for data storage, networks, servers etc. Cloud is easily scalable, flexible but lacks data integrity and data confidentiality. Web-based email services like Gmail and Hotmail deliver a cloud computing service: users can access their email "in the cloud" from any computer with a browser and Internet connection, regardless of what kind of hardware is on that particular computer. Reliability, scalability, flexibility, low maintenance and cost efficiency are the some parameters of the cloud computing. In this paper, we propose a secure multiowner data sharing schema by leveraging group signature and using dynamic broadcast encryption techniques and any members can share and data with other users. The encryption computation cost depends upon the number of revoked user. The main goal in this paper is to achieve the high security to store the data for which an asymmetric algorithm is used.**

***Keywords*— Cloud computing, security analysis, dynamic groups, privacy preserving, access control multiowner data sharing.**

I. INRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers. The cloud computing uses networks of large groups of servers. Typically, running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. Often, virtualization techniques are used to maximize the power of cloud computing. One good example of cloud computing is, 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. However, it also poses a significant risk to the confidentiality of those stored files [1]. 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 encrypt data files, and then upload the encrypted data into the cloud.

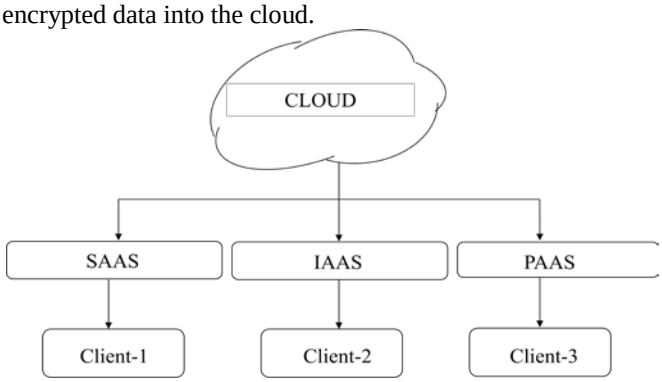

Figure 1. Architecture of Cloud Computing

Refer Figure 1, Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. If a cloud user accesses services on the infrastructure layer [13], for instance, user can run his own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If user accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful data centres. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. 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. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Cloud servers are untrusted by users as the data stored on the cloud may be sensitive and confidential such as business plan. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud storage [3]. 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. First, identity privacy is one of

ISSN 2348 – 7968

the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems. The reason is that their real identities could be easily disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable. Second, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner [4], where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. Thirdly, in case the group manager fails the whole system get collapsed. For which a basic solution is given by providing admin facility. Last but not least, groups are normally dynamic in practice, e.g., new staff participation and current employee revocation in a company. The changes of membership make secure data sharing extremely difficult. On one hand, the anonymous system challenges new granted users to learn the content of data files stored before their participation, because it is impossible for new granted users to contact with anonymous data owners, and obtain the corresponding decryption keys. On the other hand, an efficient membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management. Several security schemes for data sharing on untrusted servers have been proposed. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys [5].

Table 1. Different Techniques in cloud computing

Paper No.	Algorithm/Techniques	Parameters Achieved
1	Group Signature and dynamic broadcast encryption	Data sharing, Increase security, Performance Improvement.
2	Plutus	Key management, Sharing over untrusted server.
3	Atomic proxy re-encryption	Security, Performance.
4	Sirius	P2P file sharing, access control.
5	Bilinear pairing technique	Authentication, confidentiality, security.
6	CP-ABE (cipher policy attribute based encryption)	Access control, size and time complexity.
7	Attribute Broadcast encryption	Revocation, efficient cipher policy.
8	Identity Based encryption	Revocation, email authentication.
10	Fuzzy Identity Based encryption	Revocation, email authentication.
11	ECC (Elliptic curve Algorithm)	Data integrity, authentication, security.

For Different techniques in Cloud computing refer Table 1. Above given table gives list of different types of algorithm used in cloud computing.

II. LITERATURE SURVEY

Author Xuefeng Liu proposed the technique of group signature and dynamic broadcast encryption technique through which data is been encrypted for secure data sharing. Here the author is also giving the benefit that if any member is misbehaved his real identity is been revealed by manager. If the misbehaved user is revoked than his unique identity is been updated. This updated key is provided to new user rather than updating remaining user's keys [1]. Author Kallahalla proposed a cryptographic storage system that enables secure file sharing on untrusted servers, named Plutus. 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 file groups, 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 [2]. Atomic proxy re-encryption is an approach proposed by Blaze, Bleumer, and Strauss (BBS). In which a semi trusted proxy converts a cipher text for Alice into a cipher text 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 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 [3].

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 method of performing file random access in a cryptographic file system without the use of a block server. Extensions to SiRiUS

ISSN 2348 – 7968

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 [4]. Secure provenance that records ownership and process history of data objects is vital to the success of data forensics in cloud computing, yet it 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]. We present a new methodology for realizing Ciphertext-Policy Attribute Encryption (CP-ABE) under concrete and no interactive cryptographic assumptions in the standard model. Our solutions allow any encrypt or to specify access control in terms of any access formula over the attributes in the system. In our most efficient system, ciphertext size, encryption, and decryption time scales linearly with the complexity of the access formula. The only previous work to achieve these parameters was limited to a proof in the generic group model. Our next two constructions provide performance tradeoffs to achieve provable security respectively under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions[6]. It provides the paper on the Fine Grained Access Control with the help of the Attribute Based Encryption. So this provides the detailed view about the scalable of users as well as confidentiality of the data. The technique used is Attribute based broadcast encryption technique which is used for efficient revocation of the user. It helps in removing the access of the user without his permission using the cipher key policy and key policy efficiently [7]. Identity Based Encryption [8][9] is better technology for protecting the secure access on the PHR. Because it does not requires the public key cryptosystem. So it's not depends any public key infrastructure. It based on E-mail or IP address for encryption. Efficient Revocation is possible in the Identity Based Encryption. The technique of Fuzzy identity based encryption technique for accessing the data of PHR system over cloud where the public key cryptography is not used. Based on email or IP address the authentication is been provided which is strong.Fuzzy Identity Based Encryption is method for like threshold value matching. In this scheme like set of attributes should be satisfied in matching. For example 10 out of 12 attributes have to satisfy. So the identity based encryption provides the strong authentication as well as confidentiality [10]. Technique of ECC(Elliptic curve algorithm) which provides data integrity and authentication to secure the data in form encryption. This technique provides just the file encryption and data decryption. Elliptic Curve Cryptography is a public key cryptography algorithm. Elliptic curve cryptography provides efficient and secure solutions for the cloud storage servers. It requires fewer bits than the conventional encryption technologies for provides the similar amount of security. It provides data integrity data confidentiality and data origin authentication. Compare with existing cryptosystem it have a smaller key size, it leads to fast computation time, reducing in processing power, saves the storage and bandwidth. The ECC signature algorithm mainly consists of three phases. These are key generation, signature generation and signature verification. The signature generation algorithm use the user's private key to generate the signature. The signature verification algorithm use the user's public key to verify the signature at server [11][12]. Merkle hash tree (MHT), It is constructed as a binary tree. The MHT divides the parent node up to eight blocks. The hash value is associated with every non leaf node. It is an authenticated structure it is proved that the set of elements are unaltered and not damaged. The MHT is used in the proposed Scheme to divides the user's file in to blocks. When the user stores the file in to cloud storage server, it is divided in to eight blocks by using MHT and the hash value will be allocated to each block. The blocks are read from the left to right sequence. The storage server stores the block number, the content associated with that block, and its calculated hash value. It contains the file name, owner of the file, its associated block number, block size and the data associated with that block [13].

II. EXISTING SYSTEM

Refer figure 2, Group Members register to manager and he provides the key using which the user is able to store and modify the data over cloud. In case the member is misbehaved the manager revokes the member via cloud without consulting to the member.

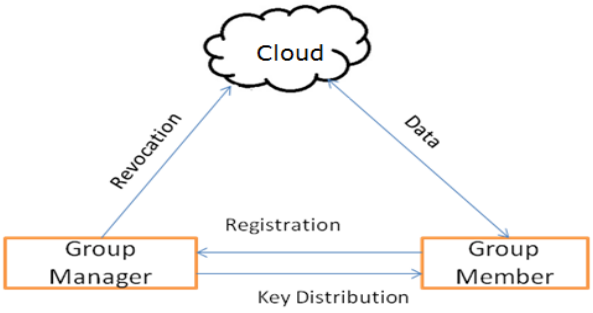

Figure 2. Existing Model of Mona [1]

To preserve data privacy, a basic solution is to encrypt data files, and then upload 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. In the existing System data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively.

ISSN 2348 – 7968

Disadvantages:

a) In the existing Systems, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing.
b) Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers.
c) On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable.
d) Only the group manager can store and modify data in the cloud.
e)The changes of membership make secure data sharing extremely difficult the issue of user revocation is not addressed.

IV. PROPOSED SYSTEM

From Figure 3, we propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud.
a) Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. b) User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users.
c) The size and computation overhead of encryption are constant and independent with the number of revoked users.
d) We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.
e) Moreover, the real identities of data owners can be revealed by the group manager and cloud admin when disputes occur.
f) We provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

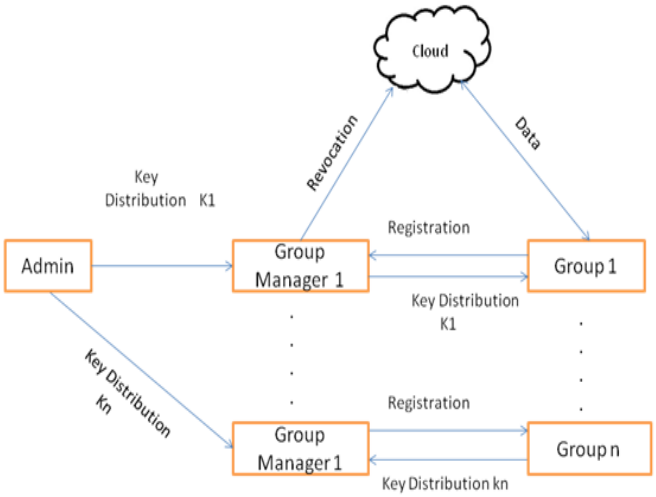

Figure 3. Proposed System Model

Advantages:

a) Any user in the group can store and share data files with others by the cloud.
b) The encryption complexity and size of cipher texts are independent with the number of revoked users in the system.
c) User revocation can be achieved without updating the private keys of the remaining users.
d) A new user can directly decrypt the files stored in the cloud before his participation.
e) In case manager fails admin take over him and provide efficient data sharing in multiowner.

V. CONCLUSION

Cloud computing is one of the best environment for data storage. It is widely used in today's world with very low cost characteristic and enhancing, the security and privacy will attract more towards cloud computing. In this paper, author achieves secure data sharing in multiowner without revealing the real identity to the cloud. Further author provides all the user of the cloud to share the data over cloud, new user joining and revocation is done efficiently. New user can directly decrypt the file without contacting with data owners. Moreover, the storage overhead and the encryption computation cost are constant. We achieved a well performed system by providing admin facility in case the manager fails to provide efficient data sharing in multiowner and preventing the system from failure. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well. In future research on this area several techniques can be applied. One of the best techniques can be applied to increase the security as well as performance of the system. It will increase the efficiency of the time.

ISSN 2348 – 7968

REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and JingboYan, "Mon Secure Multi -Owner Data Sharing for Dynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL & DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013.

[2] 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.

[3] 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.

[4] M.R.Kalai Selvi,"Secure Data Sharing for Dynamic and Large Groups in the Cloud" Vol.2, Issue 1, March 2014

[5] 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

[6] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization" , Proceeding International Conference Practice and Theory in Public Key Cryptography Conference Public Key Cryptography,http://eprint.iacr.org/2008/290.pdf, 2008.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,"Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06),pp. 89-98, 2006.

[8] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation", Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.

[9] R.Shreelakshmi, "Secure Personal Health Records access in Cloud Computing" ,Vol. 16, Issue 2, Apr 2014

[10] E. Kamalakannan1,"Investigation on Improving the Security of Public Health Record System in Cloud Computing", Vol. 1, Issue 8, October 2013

[11] Aqeel Khalique ,Kuldip Singh,Sandeep Sood "Implementation of Elliptic Curve Digital Signature Algorithm" International Journal of Computer Applications (0975 – 8887) Vol 2 – No.2, May 2010

[12] K.HariPriya "An Efficient Cloud Storage with Secure Dynamic Data Modification", vol.4, Issue 5,May 2013

[13] Deepa Noorandevarmat ," Sharing Of Multi Owner Data in Dynamic Groups Securely In Cloud Environment", vol. 2, Issue 6, June 2014