Privacy-Preserving Authentication on Shared Authority in Cloud Computing : A Survey

* Ayesha Alveera Sheikh[1]and Dr. Tripti Arjariya[2]

[1, 2] *Department of Computer Science and Engineering*

Bhabha Engineering Research Institute

Bhopal, India

e-mail: ayeshaalveerasheikh@gmail.com and tripti.beri@gmail.com

Abstract

Facilities of distributed computer and data processing contribute to the computers and alternative devices on demand by cloud computing. Three key trusted third party entities are employed to develop system environment, data owner and user. The conception of a shared authority based privacy preserving authentication protocol is employed to produce a system to perform shared access by multiple users. By employing an access request matching mechanism to work out the Security and privacy issue of shared access authority like user authentication and user privacy. Multiple users need to share data, for that, re-encryption is employed to produce significant security for user private data. The Universal Composability model is employed to verify the model of SAPA correctness. It is employed to produce a system with high security and attack free by analyzing different attacks related to the system. For multi-user collaborative cloud applications, privacy preserving data access authority sharing is attractive.

Keywords: *authentication, security, shared access and cloud computing.*

1. Introduction

Data sharing capabilities using Cloud structure plays a significant role in any organization and this can contribute several aids to the user's organization when the data shared in the cloud. Many users from diverse groups devote their data to the cloud and thus the time and cost are required less as compared to alternative forms of data sharing. Google Docs also provides us Data sharing capabilities for group of students or a team working on a project where they can share documents and can team up with each other successfully. It provides the impressive amount of productivity as related to previously existing methods of periodically sending updated versions of a document to representatives of the group via email attachments. The user or any person expects data sharing capability of our computers, phones and laptop, etc. should be effective and time saving. People prefer to share their information with others, such as the family, friends, classmates or the world in day to day life. Working on group projects is still useful for

scholars, as they can team up with representatives and have done the job effectively. All the importance of sharing data using electronic devices, emphasizing on security aspect of data sharing along with the effectiveness of the capabilities.

Following are the security specifications for data sharing in the cloud computing system

- Data security: The provider must assure that their data outsourced to the cloud must secure and the provider has to take security controls to safeguard their information in the cloud [13].
- Privacy: The provider must make clear that all significant data must be enciphered and should still make clear that merely approved users have access to data in its entirety. The diplomas and digital identities should be protected as a data that the provider collects about customer activity in the cloud. [13].
- Data confidentiality: The cloud users need to do their data contents available or revealed to unauthorized users. Only authorized users can access the conscious data while others should not access any information on the data in the cloud. [14][15].
- Fine-grained access control: Data owner can restrain the illegal users to access the data outsourced to the cloud. The data owner grants different access rights to a set of user to access the data, while others not granted to access without licenses. The access permission should be regulated by the owner alone in entrusting cloud environments.
- User revocation: When a user goes back the entry rights to the data, it will not support any new user to access the data at the permissive time. The other legitimate users in the group should not get involved by the abrogation.
- Scalability and Productivity: The sum of Cloud users can be quite large and the users can enter and leave unpredictably, it is fundamental to the system to provide productivity and should still be scalable. The security specifications are massively reliant on sufficient data sharing

2. Literature Survey

In this section, research review on methods of carrying out data sharing in the Cloud is presented that are secure and profitable.

Xenia Huang et.al [10] (2015) have proposed an Identity-based (ID-based) ring signature, which disposes of the refining of certificate verification. The security level of ring signature can be multiplied by adding forward secure ID-based ring signature. Here In this manner, even if the secret key of any user has been compromised, previous generated signatures of all is carried and the user still remains valid. It is useless to suggest all the data owners to re authenticate their data even if a secret key of a private user is endangered. It is especially necessary for a broad scale data sharing scheme and

as strongly as it is eminently efficient and not involve any pairing process. This strategy is suitable exclusively for those who require verification and user privacy.

Huang Qianlong et al. [6] have proposed an attribute-based secure data sharing scheme in the year 2015 with Efficiency and revocation (EARBUDS) in cloud computing. This strategy assures the data confidentiality and also achieve Fine-grained access control. This suggested scheme encrypts data with a Data encryption key using symmetric encryption mechanisms and then encrypted DEK based on Ciphertext policy attribute-based encryption (CP-ABE). The escrow problem can deal with using homophobic encryption techniques to set up the Attribute secret keys of the users by limiting the attribute authority in support with key server. This homophobic encryption technique is also employed to rule out the attribute authority and also stop it from getting the data by setting up the attribute secret keys only. Immediate attribute revocation can accomplish by EARBUDS scheme which assures us the forward and backward security protocol and also less computation cost to users. Security and efficiency are the advantages of this approach.

Hong Liu et al., have introduced a shared authority based privacy preserving authentication protocol to focus on (SAPA) to focus on the privacy issues for cloud storage. In this scheme, shared access authority by anonymous access request matching mechanism can achieve to provide Ciphertext-policy attribute based access control. We can set up users to approach its own data fields also proxy re-encryption refers to provide data sharing among different users using the proposed scheme. It provides the Universal Compos ability model to turn out that the SAPA has some design correctness. When a user demands the cloud server to offer other users to carry out the data sharing, this access request itself may disclose a user's privacy. This strategy is used to focus on user's sensitive access related privacy while sharing the data in a cloud environment to carry out the data access control and give access to the approved user and privacy preservation. Through this protocol called SAPA protocol, it retains the authentication and authorization of the user without compromising user's confidential information.

Xing dong et al., [3] (2014), come up with an efficient, extensible and flexible privacy-protected data management with semantic security. They employed two techniques Ciphertext policy attribute-based encryption (CP-ABE) and Identity based Encryption (IBE) that yielded a dependable and secure cloud data sharing service that provides dynamic data access to users. This strategy also assures the robust data sharing preserves the privacy of cloud users and reinforces the productive and stable dynamic operations, which have file formation, user revocation and alteration of custom attributes. This strategy also reinforces the fine-grained access control and full collusion resistance and backward secrecy. Although cloud computing is economically attractive to customers and enterprises, it does not protect users' privacy and data preservation. The recommended scheme provides semantic security for data sharing in cloud computing through the generic bi-linear group design and imposes backward secrecy and access privilege confidentiality. The behavior analysis of this scheme incurs a small overhead compared to existing schemes.

Qing Tang et al., [9] (2014) have suggested a searchable encryption, namely multi-party searchable encryption (MPSE). It enables users to permit each other to search in their encrypted data. For the worst case and the average-case collusion problem that happens because of the user status dynamics and the security model is considered here. They proposed a new scheme in which they included provable security for the system. A security model in MPSE also provides a stronger security guarantee than that of [11]. In the formulation of MPSE the authorization gives the approval on indexation level, now for each of her indexes, for example, Alice can decide whether or not Bob can search, i.e. if Bob tries all the keywords of which he has an authority of then Alice can support allow Bob to look for a subset of keywords in her indexes i.e. the index of Alice and the cloud server colluded with Bob now can also recover the keyword that are all present in Alice's search queries. This MPSE formulation expects that the Alice can find out a problem of single trap door search for all indexes that have authorized by her, and the disadvantages of this formulation are If Alice have many key pairs in the index and use them with various peers then it leaks some unnecessary information which is not appropriate. In contrast, the inverted index structure may not face these kinds of problems, as shown in [12].

3. Some of Encryption Technique

Some encryption techniques used in the existing system are discussed and summarized as follows:

A. Attribute Based Encryption (ABE)

Attribute-based encryption is one public-key encryption. In this technique, the secret key of a user and the ciphertext depend on attributes. The decryption of a ciphertext is possible only if the set of attributes of the user key matches the cipher text attributes. It provides a secure way that allows data owners to share, outsource data on untrusted servers.

B. Identity-Based Encryption (IBE)

In this encryption technique called Identity-based systems allow any party to create a public key from a known identity value such as to create an ASCII string (e.g. Email id). Figure.1 shows us an example of an Identity based Encryption scenario. Private Key Generator called as a trusted third party generates the corresponding private keys to operate the Private Key Generator which first distributes a master public key and keeps the equivalent master private key. Given the master public key, any party which is the part of the process can compute a public key, should be relate to the identity and can done by merging the master public key with the identity value. To achieve a corresponding private key, the party gives authority to the user to use the identity ID contacts Private Key Generator, which also uses the master private key to create the private key for identity ID. As a result, parties may encrypt messages without prior distribution of keys between individual participants.

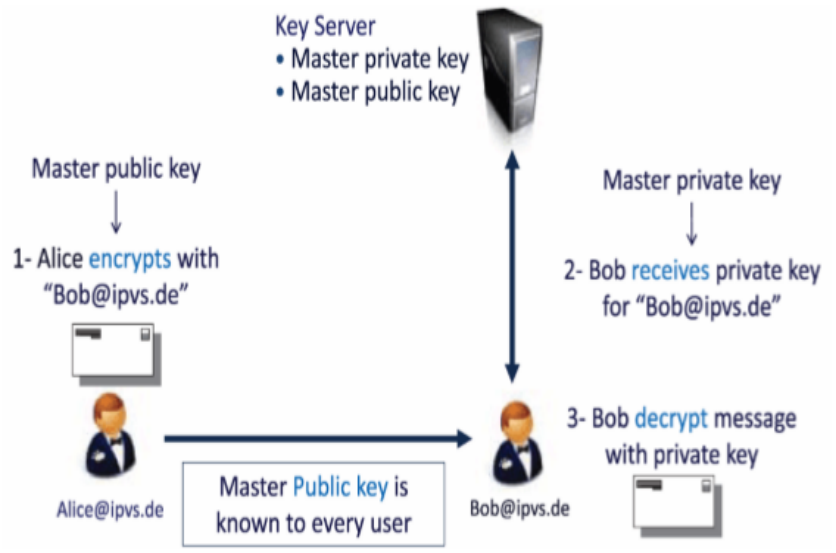

Figure.1. Identity-Based Encryption

C. Proxy Re-encryption

Another important technique which enables secure data sharing and confidential data sharing in the cloud is the Proxy Re-encryption technique. Proxy Re-encryption allows a semi-trusted proxy with a re-encryption key to convert a cipher-text under the data owner's public key into another cipher-text other user's secret key can decrypt.

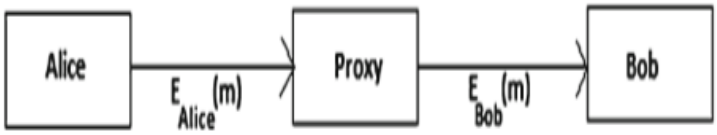

Figure.2. A basic proxy Re-encryption scheme

Figure.2 shows the basic Proxy Re-encryption scheme. A user called Alice can encrypt her data by using her public key. Alice can also send the encrypted data to a proxy when she wants to share her data with another user, say Bob. The proxy converts the data encrypted under Alice's public key into data to encrypt under Bob's public key and sends this to Bob. Bob can use his private key to decrypt the cipher-text and reveal the data.

D. Ciphertext-Policy Attribute Based Encryption

In ciphertext - policy attribute-based encryption (CP-ABE), a user's private-key is related to a set of attributes and a cipher text define an access policy over a set of defined attributes within the system. A user will decrypt a ciphertext only if he attributes suit the policy of the respective cipher text. Policies may determine over attributes using disjunctions, conjunctions and (k, n)-threshold gates, i.e., k out of n attributes have to be

given. For instance, let us assume to define the attributes to be {A, B, C, D} and user 1 receives a key to attributes {A, B} and user 2 receives a key to attribute {D}. If it encrypts a cipher text regarding the policy (A∧C)∨D, user 1 cannot decrypt, while user 2 will decrypt. An advantage of this scheme called CP-ABE is the users can get their private keys only after the data has encrypted regarding policies. So, can encrypt data without knowledge of the actual set of users will decrypt only by specifying the actual policy.

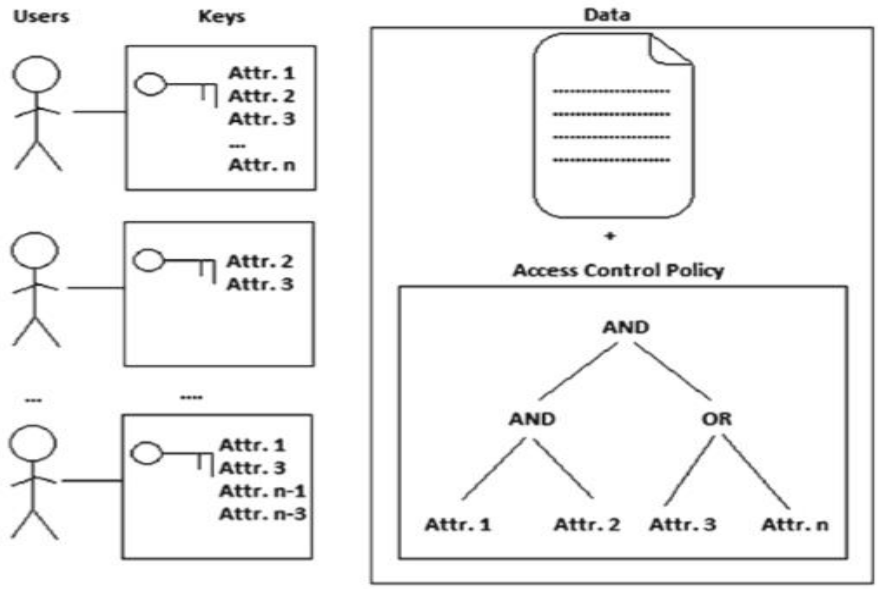

Figure.3. Ciphertext-policy attribute-based encryption

4. Conclusion

Data sharing in the cloud is accessible as requirements for data sharing continues to explode. In this study, we present a discussion of secure data sharing in a cloud computing situation. To cut down the cost data owner outsource the data. It becomes problematic for the data owner to dominate their data because a cloud service provider is a third-party provider. The complication with data sharing in the cloud is the privacy and preservation issues. Various techniques suggested in this report to support privacy and reliable data sharing such as Data sharing with forward security, reliable data sharing for influential groups, Attribute based data sharing, encrypted data sharing, They use Shared Authority Based Privacy-Preserving Authentication Protocol to access the control of outsourced data. The review confirms that secure anti collusion data sharing scheme for influential groups produce more efficiently, supports access control structure and data confidentiality to enforce privacy and preservation in effective group sharing. There is further opportunity for forthcoming research in reliable data sharing for influential groups.

References

[1] *Zhongma Zhu and Rui Jiang, " A Secure AntiCollusion Data Sharing Scheme for Dynamic Groups in the Cloud," IEEE Transactions On Parallel And Distributed Systems, Vol. 27, No. 1, January 2016.*

[2] *Hong Liu, Huansheng Ning, Qingxu Xiong and Laurence T. Yang, "Shared Authority Based Privacy Preserving Authentication Protocol in Cloud Computing," IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 1, January 2015.*

[3] *Xin Dong a, Jiadi Yu a, Yuan Luo , Yingying Chen, Guangtao Xue , Minglu Li, "Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing," Science Direct journal homepage: www.elsevier.com/locate/cose computers & security 42 (2014) 151e164, Elsevier Ltd 2013.*

[4] *Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 6, June 2013.*

[5] *Kaiping Xue and Peilin Hong, "A Dynamic Secure Group Sharing Framework in Public Cloud Computing," . Citation information: DOI 10.1109/TCC.2014.2366152, IEEE Transactions on Cloud Computing.*

[6] *HUANG Qinlong, MA Zhaofeng, YANG Yixian, FU Jingyi and NIU Xinxin, "EABDS: Attribute-Based Secure Data Sharing with Efficient Revocation in Cloud Computing," Chinese Journal of Electronics Vol.24, No.4, Oct. 2015.*

[7] *Junbeom Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing," IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 10, October 2013.*

[8] *Ming Li Member, Shucheng Yu, Yao Zheng, 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 2012.*

[9] *Qiang Tang, "Nothing is for Free: Security in Searching Shared and Encrypted Data," IEEE Transactions on Information Forensics and Security, Vol. 9, No. 11, November 2014.*

[10] *Xinyi Huang, Joseph K. Liu, Shaohua Tang, IEEE, Yang Xiang, Kaitai Liang, Li Xu, and Jianying Zhou, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security," IEEE Transactions On Computers, Vol. 64, No. 4, April 2015.*

[11] *R. A. Popa and N. Zeldovich, " Multi-Key Searchable Encryption," Available: http://eprint.iacr.org/2013/508.*

[12] *R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 79–88.*

[13] *Tim, Mather, SubraKumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise perspective of Risks and Compliance," O'Reilly Media, Inc., 2009.*

[14] *Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE, "HASBE: A Hierarchical Attribute-Base Solution for Flexible and Scalable Access Control in Cloud Computing" in Proc.IEEE Transactions on Information Forensics and Security, vol.7, No.2, April 2012.*

[15] *Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia. A view of cloud computing. Communications of the ACM, Volume 53 Issue 4, pages 50-58. April 2010.*

[16] *S.Yu, C.Wang, K.Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE Infocom 2010, 2010, pp. 534– 542.*