A Survey on Privacy Preservation and sharing Data Securely in Cloud Storage

Manoj. S. Tore[1], **S. K. Sonkar**[2]

[1, 2]Savitribai Phule Pune University, AVCOE Sangamner

Abstract: ***Cloud computing provides a way to store and share users data over cloud storage. But it is very unsecure to share data over an untrusted cloud. It can expose user privacy to other cloud users and also there is issue of integrity of users shared data. Various people worked on these issues and proposed various approaches to preserve users' privacy and data integrity. A secure multi-owner data sharing technique is proposed which is used for dynamic groups in the cloud. Group signature and dynamic broadcast encryption techniques are proposed so that any cloud user can share data with others anonymously. In this paper we will review various techniques which used for preserving privacy and share data securely in cloud storage.***

Keywords: cloud computing, privacy preservation, security, cloud storage, data sharing

1. Introduction

"Cloud" is a pay per use model used for a simulated collection of computing means. A broad range of benefits are accessible to consumers using cloud computing: availability of a large collection of software applications, large data storage, faster access power and the ability to easily share data across the world. A user can access all of these facilities through his or her browser any time once he/she has access to the Internet. In the early 1990s, a huge ATM network started being called to as "cloud" [1]. The term once again comes into play about twelve years before with the introduction of Amazon's web-based services. Cloud computing agrees consumers and corporate structures to custom all the applications offered by the cloud deprived of the extra effort of installation and also offers access to their personal files from any computer with Internet access.

Cloud computing is a complicated in terms of software, hardware and storage, all of which are available as a provision. Basically it consists of applications running remotely which is made available to all its users. Cloud computing offers access to a large number of sophisticated supercomputers with their resultant processing power, connected at different locations around the world, thus offering lightning speed of computations [2].

Cloud provides noticeable cost savings and speed to users. Using cloud computing, a company can speedily deploy applications where expansion and contraction of the essential technology components can be accomplished with the high and low of the business life cycle. The previous work and research shows that it can be achieved with the help of cloud enablers, such as virtualization, grid computing, that allow applications at runtime to be dynamically deployed onto the most suitable infrastructure [2]. There remain issues of reliability, privacy, security and portability even though the work may have addressed authentication.

However, most researchers focused on the authentication to make sure that a user who is legally allowed to use or share, can upload its data and the main problem is ignored that different users may tend to access and share each other's data fields. A user realizes that the cloud server is requesting for other users for data sharing and access request itself may disclose the user's privacy. The access to the data is may not be achieved though. Many people worked on this issue of privacy while sharing data over cloud, in this paper we are discussing various techniques for privacy preservation and secure data sharing in cloud computing.

2. Related Work

There have been number of surveys on security and privacy in the Cloud computing. Xiao and Xiao [3] identified the five issues related with Cloud; privacy, faithfulness, accessibility, responsibility, and protection and completely surveys the dangers to each of the issue and also remedies for that. Chen and Zhao [4] plot the necessities for accomplishing security. Wang *et al*. [5] researched the elements that affect overseeing data security in Cloud processing. It clarifies the necessary security requirements for ventures to understand the motion of data security in the Cloud. Oza *et al*. [6] studied on different clients to focus the client knowledge of Cloud processing and found that the basic problem of all clients is trust and how to choose between different Cloud Service Providers.

The criticalness of data communication and the need to guarantee security is examined in various existing articles. Sarathy and Muralidhar [7] have done survey for the effect of the Internet on data communication crosswise over numerous diverse associations, for example, government organizations. They arrange data communication into information dissimilar country, question confinement, and record matching. They additionally gave a structure to secure and helpful imparting of information on the web. Mitchley [8] depicts the profits of data communication from a saving money point of view and emphasized the protection issues as of now influencing it. Feldman *et al*. [9] talk about the imperative advantage of information offering regarding general wellbeing, specifically for instruction and expert advancement. Geoghegan [10] inspect a rundown of associations that satisfactorily and securely offer data by means of the Cloud. Nonetheless, it does not speak about the philosophies, the use of association to secure information or the disadvantages of these associations. They also concentrated on other part of security and information imparting; access control. Access control can be used to approve a subset of clients to view private information given that they have the rights of authorization. Sahafizadeh and Parsa [11] reviewed the different sets to control models and assessed its adequacy. On the other hand it is restricted to just programming frameworks and does not think seriously about Cloud frameworks. In next section we will see recent works done for privacy preservation and secure data sharing in cloud.

3. Recent Approaches

In this section we will see the recent work done for empowering the data sharing over cloud storage.

3.1 Attribute Based Encryption

Attribute Based Encryption (ABE) is one of the feasible and guaranteed strategy that is used to give fine-grained access control to the information in the Cloud. At first, access to data in the Cloud was given through Access Control List, this was not versatile and just gave coarse-grained access to data. Goyal et al. [12] initially proposed Characteristic Based encryption that gives a more adaptable and fine-grained access control to data in correlation to Access control list. Trait Based Encryption is a right to gain entrance control instrument where a client or a bit of data has characteristics connected with it. A right to gain access control strategy is characterized and if the properties fulfill the right to gain access control arrangement the client ought to have the capacity to get access to the bit of data. There are two types of ABE, which are given as follows.

3.1.1 Key-Policy ABE (KP ABE)

The right to gain access control is put away with the client's private key and the scrambled information with some properties associated with it. A client can just unscramble the information and if the characteristics of the information accomplish the right to gain access control in the client's key. The right to gain access control approach is normally characterized as a right to gain access tree with inside hubs speaking to edge entryways and leaf hubs speaking to characteristics.

3.1.2 Cipertext Policy ABE

It is opposite to the KP-ABE. The right to gain access control strategy is put away with the data and the qualities are put away in the client's key.

3.1.3 ABE for data sharing

ABE is used for data sharing and joint efforts meets expectations. Tu *et al*. [13] made use of CP-ABE in the setting of large business applications furthermore created a renouncement system that at the same time grants high versatility and fine-grained access control. The authority allots clients with a set of properties inside their secret key and distributes the secret key to the separate clients. Any client that fulfills the right to gain access control strategy characterized by the information associate can get access to the information. At the point when a client is discarded the access a right, the information is re-scrambled in the Cloud rendering the renounced client's key futile. The plan is semantically secure against chosen ciphertext assaults against the CP-ABE model. After access rights are discarded it further calculates the ciphertext so it cause overhead to the system. Li *et al*. [14] affected ABE in the setting of the offering of individual records (PHR) in the Cloud. Their system consists of an open area comprising of clients who make access to an expert records, for example, specialists, medical attendants and medicinal analysts, furthermore individual space, which consists of clients who are generally connected with the data holder, for example, family and close companions. Part ascribes are relegated to the clients in general society area that speaks to their proficient part and they recover their secret keys from a characteristic power. This is feasible as the data manager requires not be online at all times. As far as access control, data managers define part based fine-grained access control approaches for their PHR documents. Using part based access strategies extraordinarily reduces key administration overhead for managers and clients as the manager does not need to oversee keys for every individual client.

3.2 Proxy Re-Encryption

Midway Re-encryption is an alternate strategy that is quick getting to be received for empowering secure and secret data communication and joint effort in the Cloud. Midway Re-encryption [15] grants a semi-trusted intermediary with a re-encryption key to interpret a cipher text under the data manager's open key into an alternate cipher text that can be decoded by an alternate client's secret key. Intermediary doesn’t have the capacity to get to the plaintext in any way. Specialists have utilized intermediary re-encryption in connection to the Cloud and specifically for secure and secret data sharing in the Cloud.

3.2.1 Proxy Re-Encryption for sharing data

Different works in writing have presented proxy re-encryption for empowering secure and private data sharing in the Cloud. Tran *et al*. [16] used the thought of Proxy Re-encryption scheme where the data manager's private key is separated into two sections. One half is kept away in the data manager's machine while the other is kept away in the Cloud server. The data manager encodes the data with a large portion of his private key, which then gets encoded again by the cloud server by using his other 50% of the key. An alternate client who has been allowed access rights will then have the same key isolated with different parts. One half will be kept at client's machine and the other half kept away on the Cloud server. The client who has access rights can then recover the data as the cloud server will unscramble the cipher text with a large portion of the client's private key enter in the cloud server and afterward decode again on the client's side to recover the full plaintext. At the point when the information holder wishes to deny a client from getting to the information, he basically informs the Cloud server to evacuate the client's key piece. The primary quality with this scheme is that it doesn't oblige re-encryption if a client's rights are denied and henceforth reduces calculation costs, particularly when considering the large number of clients in gatherings. The model additionally expects that the data holder has officially offered authorization to various clients to get to the data.

3.3 Hybrid ABE and PRE

ABE and Proxy Re-encryption have additionally been used as a part of mixture with one another to give more security and protection to data sharing in the Cloud. Different works in writing are exploiting integrating the abilities of the two plans to give a more security and ensure further trust in the data holder for the protected sharing of data in the Cloud.

Yu *et al*. [17] was one of the first, which includes ABE, Proxy Re encryption and languid encryption plans for Cloud security. The plan meets expectations by data manager scrambling his data using a symmetric key and after that encoding the symmetric key using a set of credits as shown by KP-ABE plan. Another client joins the framework when the data holder gives a right to gain access and its comparing secret key and circulates this to the new client. To deny a client, the data holder decides the base number of properties, which will never fulfill the denied client's right to gain access and redesign these as absolutely. All the remaining clients' secret keys will likewise be examined and repaired. Because of the overpowering load of the data holder which may oblige him to be online at all times to give key upgrades, proxy re-encryption is acquainted with grant the Cloud to do these errands. Thus the large part of the computational overhead is appointed to the Cloud. The data holder's data is kept secure and confidential at all times as the Cloud is just presented to the encrypted data and not the first data substance.

Yang and Zhang [18] similarly proposed a mixture of the ABE scheme and Proxy Re-encryption scheme to empower secure data sharing in the Cloud. The model includes a data manager, say Alice, scrambling data d with an arbitrary key k_alice then decides an alternate irregular worth k1 and using access control strategy poll, encodes k1 using ABE. Alice then registers k2 using operations on k and k1, ie, k2 = k ∗ k1 and encodes with her open key using proxy re-encryption. The two keys (ABE key and proxy key) and the encoded data are then put away in the Cloud. Using an authorization list, if authorized clients are present, she can then acquire the proxy key which is then scrambled with the client's key. Using this, she unscrambles the ABE key, and then figure out k, i.e, k1 ∗ k2 lastly acquires the decoded record. This procedure guarantees that data is kept classified against the Cloud and from any unauthorized clients. In the situation that a client is renounced access rights, the data holder basically advises the Cloud to empty the client's section in the authorization rundown and subsequently is computationally proficient. In any case, this scheme does not manage the situation where a denied client rejoins the bunch with different access benefits. The disavowed client still possess the decryption keys relating to ABE and therefore in principle can recover access to data he is not permitted.

Liu *et al*. [19] proposed a clock-based proxy re-encryption scheme (C-PRE) and joined CP-ABE to complete fine-grained access control and adjustable client repudiation. In C-PRE, the data holder and the Cloud share a secret key and this key is used to figure out the PRE keys focused around the Cloud's inside clock. The Cloud will re-scramble the encrypted data with the PRE keys. Each client is attached with an associated properties and a qualified time which decide to what extent the client can get to the data. The data itself is connected with a right to gain access control by CP-ABE furthermore has a right to gain access time. At the some point when a client appeals to get record, the Cloud decides the current time using its interior clock and after that using the shared key to figure out PRE keys in time design for all the qualities in the right to gain access. The PRE keys are then used to re-encode the encrypted data. Just clients whose characteristics fulfill the right to gain access control structure and whose qualified time fulfills the right to gain access time can unscramble the data. The basic advantage with this procedure is that the re-encryption of all the data is designated to the Cloud rather than the data holder and subsequently is productive from the data manager's point of view. The client disavowal issue is similarly handled since the data must be gotten to if the client's property fulfills the right to gain access control structure and their qualified time fulfills the right to gain access time. One problem with this strategy however, is that data is re-encoded each time a client makes a right to gain access demand. Despite the fact that the re-encryption is assigned to the Cloud, it is still not an exceptionally effective arrangement particularly when considering large data sizes.

4. Discussion

Table 1: Summary

Method	ABE	PRE	Likelihood of Collision attacks	User Revocation	Data Owner (Online/Offline)
Tu et al.	Yes	No	No	Slow	Offline
Li *et al.*	Yes	No	No	Fast	Offline
Tran *et al.*	No	Yes		Fast	Offline
Yu *et al.*	Yes	Yes	No	Slow	Offline
Yang and Zhang	Yes	Yes	No	Fast	Offline
Liu *et al.*	Yes	Yes	No	Slow	Offline

The Table 1 shows a summary of the present literatures based on secure and confidential data sharing in the Cloud. Many of the works reviewed has a strong attention on preventing collision attacks as well as researching ways for the data holder to be online only when required. In terms of user revocation, some of the reviewed works shows fast procedure of user revocation where revocation includes simply removing a key for instance. Other researches required that the data to be re-encrypted and the keys to be re-distributed in a secure way and this mainly happens with works that uses ABE techniques. Data sharing and collaboration in the Cloud is still currently a strong attention of research today and in specifically many researches are focusing on the user revocation problem as well as methods to manage the sharing and collaboration of large data sizes.

5. Conclusion

Data sharing in the Cloud is quick getting to be accessible within a short span of time as requests for data sharing keeps on growing quickly. In this paper, we displayed a survey on empowering secure and classified data sharing in Cloud computing. We identified definitions with Cloud registering and protection. We then took a view at protection and security problems affecting the Cloud emulated by what is consistently done to address these problems. We then talked about why data in the Cloud is major and the customary methodology to data sharing in the Cloud. We clarified the different procedures, specifically ABE and PRE that are right now used to power secure data sharing in the Cloud. We similarly audited current situation of-the-craftsmanship writing in connection to secure and private data sharing in the Cloud and gave a full review on the fate of data sharing in the Cloud where the data holder could have more control over the use of their data.

References

[1] Rich Maggiani, 2009 Cloud Computing Is Changing How We Communicate", In IEEE 978-1-4244-4358-1/09.

[2] Midya Azad Ismail, Klinsega Jeberson,"Secure Data Sharing Through Cloud Computing", In International Journal of Computer Engineering & Technology(IJCET), 2014,vol. 5, pp. 41-47.

[3] Xiao Z, Xiao Y (2012) Security and privacy in cloud computing. *IEEE Commun Surveys Tutorials,* 99:1–17.

[4] Chen D, Zhao H. Data security and privacy protection issues in cloud computing. *International conference on computer science and electronics, engineering*, 2012; pp 647–651.

[5] Wang J, Liu C, Lin GTR (2011) How to manage information security in cloud, computing, pp 1405–1410.

[6] Oza N, Karppinen K, Savola R (2010) User experience and security in the cloud-An empirical study in the finnish cloud consortium. *IEEE second International conference on cloud computing technology and science* (CloudCom) 2010:621–628.

[7] Sarathy R, Muralidhar K (2006) Secure and useful data sharing. Decis Support Syst, 204–220.

[8] Mitchley M (2006) Data sharing: progress or not? Credit, Manage, 10–11.

[9] Feldman L, Patel D, Ortmann L, Robinson K, Popovic T. Educating for the future: another important benefit of data sharing. Lancet, 2012; 19; 379 (9829): 1877–1878. doi: 10.1016/S0140-6736(12)60809-5.

[10] Geoghegan S. The latest on data sharing and secure cloud computing. Law, Order, 2012;pp 24–26.

[11] Sahafizadeh E, Parsa S (2010) Survey on access control models. 2nd *International conference future computer and communication* (ICFCC) 2010, pp V1–1-V1-3.

[12] Goyal V, Pandey O, Sahai A, Waters B . Attribute-based encryption for fine-grained access control of encrypted data. 13th ACM conference on computer and communications security (CCS '06) 2006, pp 89–98.

[13] Tu S, Niu S, Li H, Xiao-ming Y, Li M (2012): Fine-grained access control and revocation for sharing data on clouds. IEEE 26th international parallel and distributed processing symposium workshops and PhD forum (IPDPSW) 2012, pp 2146–2155.

[14] Li M, Yu S, Zheng Y, Ren K, Lou W (2013) Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans Parallel Distrib Syst, 131–143.

[15] Wang X, Zhong W (2010) A new identity based proxy re-encryption scheme. *International conference biomedical engineering and computer science (ICBECS)* 2010:145–153.

[16] Tran DH, Nguyen HL, Zha W, Ng WK (2011) Towards security in sharing data on cloudbased social networks. 8th International conference on information, communications and signal processing (ICICS) 2011, pp 1–5.

[17] Yu S,Wang C, Ren K, LouW(2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. In: *INFOCOM, 2010 proceedings IEEE*, pp 1–9.

[18] Yang Y, Zhang Y (2011) A generic scheme for secure ata sharing in cloud. 40th *International conference parallel processing workshops (ICPPW)* 2011, pp 145–153.

[19] Liu Q, Wang G, Wu J (2012) Check-based proxy re-encryption scheme in unreliable clouds. 41st *International conference on parallel processing workshops* (ICPPW) 2012, pp 304–305.

Author Profile

Mr. Manoj S. Tore received the B.E. degree in In Computer Engineering from University of Pune, in 2012. Currently he is pursuing Master's degree in Computer Engineering from Amrutvahini college of Engineering, Sangamner under University of Pune. His areas of interest are network Security and cloud computing. He is currently working in the field of Network security and Cloud computing.

Prof. S. K. Sonkar received the Master degree in Computer science and Engineering from SRTMU Nanded. He is currently pursuing the Ph.D. degree in computer science from University of Pune. He is presently working as Assistant Professor in Dept. of Computer Engineering in Amrutvahini college of Engineering, Sangamner, India. His current research interests include network security and Cloud Computing.