A Review: A Survey on Privacy Preserving for Secure Cloud Storage

Areeba Kazim
Computer Science
Amity University, Noida

Ritika Varshney
Computer Science
Amity University, Noida

ABSTRACT
Cloud computing technology provides millions of on demand services to its users on internet ranging from infrastructure, software to storage as a service on cloud.

Storage service allows its users to outsource large amount of data without directly controlling it and cloud running on the principle of virtually shared servers do not provide users with the storage location. Therefore, various measures can be adopted for maintaining data integrity, security while entering data in cloud. So here, we are having open audit-ability for distributed storage that shoppers will rely on an outsider examiner (TPA) to test the trait of knowledge. This paper offers the problems known with security whereas golf shot away the client's data to the distributed storage amid the examining. During this paper we'll examine totally different systems to fathom these problems to present protection and security of cloud data. There's lots of analysis being created to identify problems associated CSPs and security.

General Terms
Cloud computing, encryption algorithms

Keywords
Access Control, Data Architecture, Outsourcing, Privacy, Security, Integrity

1. INTRODUCTION
Cloud computing has played a vital role in evolvement of Information technology enterprise. From providing infrastructure, platform and software as a service to resource pooling, network access , rapid elasticity and storage for extensively large files and databases, you name it cloud has it.

Despite of so many advantages, issues related to data integrity and security comes hand in hand such as:

Data once saved on cloud has no guarantee of getting deleted permanently.

CSPs may hide data loss information from users.

CSP might delete data which user do not use frequently without user's permission

Server becomes vulnerable to security threats and security breach attack

Security threats associated to cloud, and where major contemplations of attacks and Counter measures [1].

These issues (in fig 1) have to be considered and proper measures have to be taken in order to provide data integrity and security to data saved on cloud or outsourced to cloud.

Fig 1: Security threats in cloud

2. PRIVACY IN CLOUD STORAGE
Preserving Data security is need of the hour especially when cloud storage is used by various organizations of different fields ranging from educational institutions and huge MNCs relying on services like google drive to individual users like Dropbox, Box, AmazonDrive, Microsoft OneDrive etc.

Such users trust these services and want to maintain their data's privacy by not letting it getting corrupted or not losing it by any means. And if this trust continues millions of other users might want to store data on cloud.

Stored cloud data need to be decrypted before a 3rd party could breech information since it is stored in an encrypted form. Adding to this. These are various methods by which users can inculcate their own security measures in addition to what is provided by system. All things considered, there are still holes among practices and proposed arrangements, irreconcilable circumstances, and difference on prerequisites and ideas.

2.1 Privacy and its basis:
Privacy can be simply put into words by saying: "it is a state of being entirely free from any unauthorized access"

or

"Right of an individual or an organization to keep one's information related to its identity or any other personal information guarded from any unauthorized access"

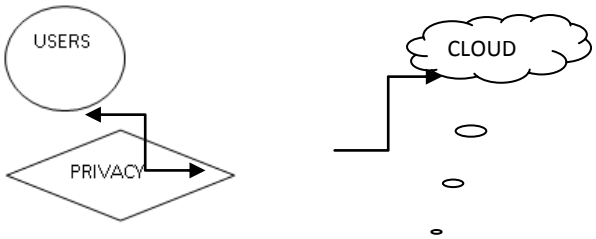

Fig 2: Privacy in cloud storage

Cloud provides privacy by providing various cloud models and each model provides different access levels as shown in the table 1.

Table 1

Models	Accessibility	Secure
PUBLIC	General public	Not secure because of its openness
PRIVATE	Organization	Secure because of its private nature
COMMUNITY	Group of organization	Secure

3. POSSIBLE SOLUTIONS

Figure 3 shows possible solutions to the concerning privacy issues:

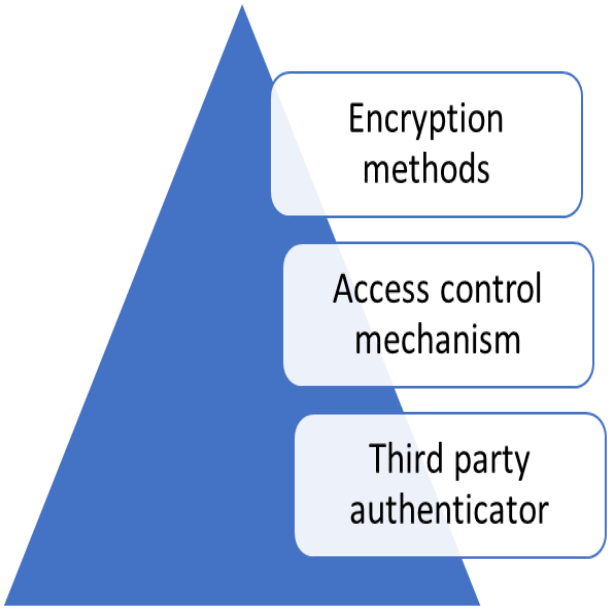

Fig 3: Solutions

3.1 Encryption methods

In order to maintain and preserve privacy various methodologies can be adopted which make use encryption techniques. RuWei et.al [2] 's work showcased the layout of privacy-securing storage (cloud) framework for resolving issues regarding privacy securing and contains layout of model of data organization, key generation and management, communication amongst participants and managing not so constant nature belonging to users right to access and also the dynamic behavior of data. Extirpation based key derivation algorithm and protocols are used in this process, thus maintaining data integrity and confidentiality, solving shortcomings of key derivation, lowering down encryption – decryption overhead, being a pro in managing various keys, thereby saving space, and fastens the system by reducing running overheads, provides remarkable privacy applicable to multiple clients, CSPs and those owning data.What it lacks is to have ways to lower burden of encryption and work on cipher text from owner's part. Although this idea would work but it does increase the encryption responsibility of client. Therefore focus has to be made on cipher text. Another paper proposed a system named YI cloudwhich asks users to encrypt before saving data in cloud secret sharing algorithm comes into play when users' encryption key which can be easily recovered when lost is sharedamongst trusted and authorized parties. The proposed model makes use of algorithm in such a way that privacy is preserved and at the same time lowers down the risk of loss of data if encryption key is lost. Based on symmetric predicate encryption this Theory consists of searches like: unencryptable delegated search and revocable delegated search. But burdens and constraints on data usage comes along with this method which is irradiated by Access control mechanism explained here:

3.2 Access control mechanism

A privacy protecting authenticated gain access to control scheme can be used for security of end user data in cloud storage space. This concept is employed to recognize the authenticity of an individual without knowing the user's id before saving information [3]. Only valid users have the ability to decrypt the stored data. It preserves the level of privacy of data; keep up with the security and retains secrete the personal information of user.

3.3 Third party authenticator

For outsourcing data on cloud, completely relying on cloud service providers may make your data vulnerable to attacks, data corruption and other security threats. Even CSPs cannot be trusted because even they may tamper, modify or delete data or may hide details of data corruption. In such cases THIRD PARTY AUTHENTICATION (figure 4) comes into play. User can keep a check on his data integrity in time to time intervals by appointing a TPA whose job is to verify data integrity, thereafter communicates it with client. STEPS:

1. Using STS protocol which user and auditor are aware of, a secret key is produced.in this way mutual authentication is performed.
2. Cipher text is produced by applying XOR operation between data and key and thereafter stored in cloud
3. User retrieves a hash value by passing his data from hash function.
4. Auditor produces plain text wherein XOR operation be performed on secret key and cipher text which he retrieved from the cloud.
5. Again a hash value is obtained by passing the pain text this time from the hash function.
6. Computed values are compared, if similar then integrity is said to be preserved securely

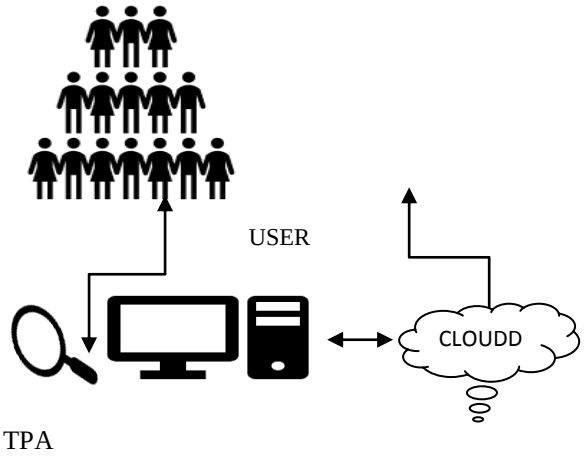

Fig 4: Third party authenticator

4. FUTURE WORK

The future scope of cloud computing will have a combination of cloud based software products and on premises compute to create a hybrid IT solution in attempt to maintain balance of the scalability and flexibility associated with cloud and the security and control of a private data center. In the proposed scheme, cryptography is used to ensure the confidentiality of data, the privacy of the access control rules, and the credentials required for access control

5. CONCLUSIONS

Cloud computing introduces area of computing to its various uses and will increase advantages of utility by giving access through any reasonably web association. Though with this easy access to cloud storage here comes the disadvantage and various drawbacks. Need of the hour is to understand that security of privacy is one of the leading concerns which has to be given a thought upon. To resolve risk associated with privacy a variety of techniques are generated in order to ensure privacy. This paper has addressed some approaches dealing with privacy issues in storing data on cloud and also about the audit schemes. Despite the fact that these techniques can handle privacy issues to some extent yet none of them is fully capable of removing privacy threat completely. So taking care of privacy considerations, we'd like to initiate privacy ensuring framework that deals with trouble associated with privacy and its security along with encouraging users to use cloud services with at most trust and confidence

6. REFERENCES

[1] Mohammed, A., AlSudiari, T., &Vasista, T. G. K. 2012. Cloud Computing And Privacy Regulations: An Exploratory Study On Issues And Implications.AdvancedComputing:AnInternationalJournal (ACIJ), 3 (2), 159-169.

[2] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. 2007, October. Provabledata possession at untreated stores. In Proceedings of the 14th ACM conference on Computer and communications security (pp. 598-609). ACM.

[3] Ruj, S., Stojmenovic, M., & Nayak, A. 2012, May. Privacy Preserving Access Control with Authentication for Securing Data in Clouds. In Cluster, Cloud and Grid Computing (CCGrid), 12th IEEE/ACM International Symposium on(pp. 556-563),IEEE

[4] P. Mel and T. Grace, "Draft NIST Working Definition of cloud computing,"http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html, June 2009

[5] M. Armrest, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Kaminski, G. Lee, D.A. Patterson, A. Rabin, Stoical, and M. v nZaharias, "Above the Clouds: A Berkeley View of Cloud Compute- in," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.

[6] Pearson, S. 2012. Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing,pp.3-42.

[7] Cloud Security Alliance, "Top Threats to Cloud Computing," http://www.cloudsecurityalliance.org, 2010

[8] A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm.Security (CCS '07), pp. 584-597, Oct. 2007.

[9] H. Shacham and B. Waters, "Compact Proofs of retrievability,"Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107, Dec. 2008

[10] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.

[11] Huang, Z., Li, Q., Zheng, D., Chen, K., & Li, X. 2011, December. YI Cloud: Improving user privacy with secret key recovery in cloud storage. In Service Oriented System engineering (SOSE), 2011 IEEE 6th International Symposium on (pp. 268-272),IEEE.

[12] Huang, R., Gui, X., Yu, S., & Zhuang, W. 2011. Research on privacy-preserving cloud storage framework supporting ciphertext retrieval. In Network Computing and Information Security (NCIS), 2011 International Conference on (Vol. 1, pp. 93-97),IEEE

[13] .Fan, C. I., & Huang, S. Y. 2012. Controllable privacy preserving search based on symmetric predicate encryption in cloud storage. Future Generation Computer Systems.

[14] Wang, C., Chow, S., Wang, Q., Ren, K., & Lou, W. 2010. Privacy-preserving public auditing for secure cloud storage.

[15] Ruj, S., Stojmenovic, M., & Nayak, A. 2012, May. Privacy Preserving Access Control with Authentication for Securing Data in Clouds. In Cluster, Cloud and Grid Computing (CCGrid),12th IEEE/ACM International Symposium on(pp. 556-563),IEEE.

[16] Yang, K., & Jia, X. 2012. Data storage auditing service in cloud computing: challenges, methods and opportunities. World Wide Web, 15(4), 409-428

[17] Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. 2011. Enabling public auditability and data dynamics for storage security in cloud computing. Parallel and Distributed Systems, IEEE Trans. on, 22(5), 847-859.