International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-2, Issue-12 E-ISSN: 2347-2693

Survey on Preserving Data Privacy in Cloud

Bincy Paul[1*] and M. Azath[2]

[1]PG Scholar, Mets School of engineering, Calicut university, Kerala, India
[2]Head of Department, Department of computer Science, Calicut University

www.ijcaonline.org

Received: Nov /28 /2014 Revised: Dec/05/2014 Accepted: Dec/18/2014 Published: Dec/31/ 2014

***Abstract*—** Cloud computing is the future of information technology. It demonstrates all the big trends in the design and use of computer architectures. With cloud computing, it is necessary for data to be not only stored in the cloud but also shared across multiple users, when the data are sharing privacy breach of the data can occur. In cloud computing preserving data privacy is an important task because the data itself contains sensitive information. A basic solution for preserving data privacy is to encrypt the data, and then upload the encrypted data into the cloud. As next give a data access notification to the data owner, providing complete permission of control to the user over the data. Designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task. Oruta is the first privacy-preserving mechanism for shared data stored in the cloud. By using homomorphic authenticable ring structures, it gives privacy preserving public auditing for secure clouds to storage system. This survey analyzes various techniques for preserving shared data privacy in the cloud.

***Keywords*—** Cloud computing, Data sharing, Privacy Preserving

I. INTRODUCTION

A. *Cloud Computing*

Cloud computing is emerging technology which consists of existing techniques combined with new technology paradigms. In this technology, different resources like software's, hardware's are shared and information is provided to its users and other peoples on internet whenever demanded [1]. Cloud computing moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This work studies the problem of ensuring the integrity of data storage in Cloud Computing.

The cloud computing is more environment-friendly and energy efficient. The construction of cloud and storing data in it has tremendous benefits. It facilitates the authenticated and authorized cloud users to access enormous resources that are outsourced and shared in the cloud. The locality of physical resources and devices being accessed are in general not known to the end user. Cloud computing takes away the expenses spent on installing all hardware and software, by allowing users to rent the resources based on their needs. Despite all these benefits, cloud computing still faces many challenges which forbid the successful implementation of the cloud. These include both the traditional as well as cloud security challenges [2]. Specific to cloud computing, the issues are many, of which some are: identity management of cloud users, multi-tenancy support, securing the security of applications, preserving privacy of the users, attaining control over the life cycle of outsourced data, etc. Among which, the issues related to privacy preserving are alone looked at in this survey.

B. *Privacy Preserving and Data sharing in Cloud*

Privacy means that the person to be free from all interference and allows the person to maintain a degree of intimacy. Preserving the privacy of user, his identity and data in the cloud is very mandatory. Privacy is the protection for the truthful use of personal information of cloud user, so privacy breaches may create a lot of troubles to cloud users. In the cloud computing environment there are many of the issues are present. The important issue is privacy preservation for the users. The most confidential information of users is stored in the cloud; the users do not want to share their information with others where their data are shared publicly among the cloud. Some of the issues, leads cloud service providers to attain privacy is insufficient user control, Information disclosure, unauthorized second storage, uncontrolled data proliferation, and Dynamic provision.

The importance of data sharing is to ensure privacy and security. The cloud providers enable authenticated and authorized users to access the shared data in the cloud and it allows user to store their data in the public cloud. The user can access or process the data whenever they require it, without consideration of the data location. Some of major requirements of secure data sharing in the Cloud are as follows. Firstly the data owner should be able to specify a group of users that are allowed to view user data. Any member within the group should be able to gain access to the data anytime, anywhere without the data owner's intervention. No-one, other than the data owner and the members of the group, should gain access to the data, including the Cloud Service Provider. The data owner should be able to add new users to the group. The data owner should also be able to revoke access rights against any member of the group over his or her shared

data. No member of the group should be allowed to revoke rights or join new users to the group [3].

This survey analyses and discusses various methods for preserve the privacy of user and data and while performing public auditing on the cloud data like adopting cryptographic methods, writing access rights and policies, anonymising data, segregating or fragmenting and then reconstructing the data, etc.

II. PRIVACY PRESERVING METHODS

The privacy has to be preserved anytime and anywhere. For preserving privacy there are several methods have been used and it's done in both ways preserving the privacy of the data as well as preserving the privacy while preferring some third party auditing to assure the data correctness.

A. *Preserving Privacy without Auditing Mechanism*

1) Anonymity-based system: To preserve privacy in cloud jiang wang et al. generate Anonymity based system [4].in Anonymity based system use anonymity algorithm for preserving data privacy. The anonymity algorithm handles the data and anonymises all or some information before discharging it in the cloud surroundings. To mine the required knowledge cloud service provider utilizes its background information and associate the specifics with the unspecified information. The approach differs from the classic cryptography technology for preserving user's privacy as it gets rid of key management and thus it stands simple and flexible. The compliance status of the cloud service provider for each privacy issues to various laws and regulations and the level of control which is being provided by the cloud service provider to the customer on the data. While anonymising is easier, the attributes that has to be made anonymous varies and it depend on the cloud service provider. This approach will be suitable only for limited number of services. Thus, the method has to be bettered by automating the anonymisation.

2) Architecture for Privacy preserving: In general a user cannot access all the data stored on the cloud, there exits at least one privileged role with unlimited administrative accesses. This cloud database storage [5] architecture provides data privacy without the need to trust corporate administrators as well as external cloud administrators. The system consists of a Data Management, Encryption Proxy and a User Interface. Through user interface, the request for accessing database is obtained, which is sent as an XML/RPC request to the user engine, rule engine and finally to the cloud database. By means of encrypting and assigning secured identities for each request and response at each stage, together with the maintenance of machine readable usage /access rights, privacy is preserved. While it is simpler to do the encryption plans, there exists a trouble in giving machine discernable access rights.

3) Privacy-Preserved By Access Control: Miao Zhou et al. [6] deal with the user privacy in the environment of cloud and proposed a flexible approach of access control. Each user in cloud is linked with certain characteristics, which determines their access rights. The paper proposed a two-tier encryption model in which the base phase and surface phase builds up the two tiers of the model respectively. In the base phase local attribute-based encryption takes place on the outsourced data by the data owner. On the other hand surface phase process involves where operation done by cloud servers, afterwards the initialization completed by the data owner. Server re-encryption mechanism (SRM) implements by the surface phase. The SRM dynamically re-encrypts the encrypted data in the cloud, when the holder of that data demands. The request for SRM arises either when a new user has to be created or an existing user has to be repealed. Though the re-encryption takes place in cloud server, the privacy of users data is not compromised as the access policies remains hidden to the cloud servers. Thus, in this paper privacy of data is preserved by providing full access control to the owner of the data and by disallowing the cloud provider to gain knowledge about the data.

4) Authorization System for Privacy Preserving: David W. Chadwick et al. [7] intended a policy based authorization infrastructure that a cloud provider can run as an infrastructure service for its users. And it will protect the privacy of users' data by allowing the users to set their own privacy policies, and then enforcing them so that no unauthorized access is allowed to their data. This assures the controlled access of data in the cloud. Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs) are used for making authorization decisions and enforcing these decisions respectively. Master PDP is launched which figures out and solves the conflicts among various decisions of different PDPs. As the cloud provider is trusted, encryption of outsourced data is not done. The enhancement of this approach could be done by focusing on security threats from cloud providers and also by partitioning the infrastructure into separate services, each running in a distinct virtual machine.

5) A Privacy preserving data outsourcing: For preserving the confidentiality of users' data a method is constructed, by using graph privacy constraints. Here, privacy is expressed in terms of a set of confidentiality constraints [8]. And represent the confidentiality constraints as a graph where the nodes are the attributes and links represent paired confidentiality. Sensitive attributes are the subset of the entire group of attributes. These attributes should not be leaked out to the external party. A relation is drawn over such attributes, which is then vertically fragmented. A graph coloring algorithm is used to perform fragmentation and placing the fragments at the appropriate location, as well. While fragmenting, it is necessary to check that the workload is kept minimized at the source and also the confidentiality constraints not been

breached by the server fragment. The fragmentation is carried out based on certain metrics like Min-Attr, Min-Query and Min-Cond. Apply the graph coloring problem with two colors for the cyclic portion of the graph use some heuristic to eliminate the cycles, and complete the coloring of all nodes. By constructing a hyper graph rather than two dimensional graphs its effectiveness can be improved.

TABLE I
COMPARISON OF PRIVACY PRESERVING IN CLOUD COMPUTING

Without Auditing Mechanism	APPROACHES	DESCRIPTION	LIMITATIONS
	Anonymity-based system[3]	Anonymises the sensitive data before storing in cloud.	→This is only suitable for limited number of services. →It has to be betered by automating the anonymisation
	Architecture for Privacy preserving[4]	Prevents both internal and external attacks.	→It doesn't provide complex machine readable access rights. →The syntax of XML-based rights expressions is complicated
	Privacy-Preserved By Access Control[5]	Determines access rights for users and achieves access control.	Lack of scalability and flexibility
	Authorization System for Privacy Preserving[6]	Puts forth a policy based authorisation infrastructure.	Lack of virtualizing the infrastructure services.
	A Privacy preserving data outsourcing[7]	Guarantees privacy by means of data fragmentation.	Cost of encryption/re encryption technologies is high
	Preserving cloud computing Privacy (PccP) Model for cloud[8]	Preserves both user identification and information.	Inefficiency of user id generation.
With Auditing Mechanism	Public Auditing for Data Storage Security[9]	Third party auditing with Secured batch auditing.	Identity is not preserved
	Public Auditing for Secure Cloud Storage[10]	Enhanced and secured third-party auditing. Public auditing with zero-knowledge leakage.	Identity is not preserved

6) Preserving cloud computing Privacy (PccP) Model for cloud: An another method for privacy is named as Preserving cloud computing Privacy[9] .This model that incorporates a three-level architecture, and it aims to preserve privacy of information pertaining to cloud users. The Consumer Layer deals with all the aspects which relate to enabling the user of the cloud to access the cloud services being provided by the cloud service provider. The Network Interface Layer creates an appropriate mapping between the original IP addresses of the users with a modified IP address, and thereby ensuring the privacy of the IP address of the users. The Privacy Preserved Layer utilizes the functionality of the Unique User Cloud Identity Generator for which an algorithm is proposed in this paper to generate an unique User Service Dependent Identity (USID) with privacy check by establishing mapping among the existing user identity (ID), if any to ID's available in a pool of User ID's to enhance the privacy of sensitive user information. A Privacy check method based on information privacy is being proposed which contributes significantly in maintaining user control over the generated user identities (USID's). Both access control and data content is prevented by PccP.

B. Preserving Privacy with Auditing Mechanism

The auditing mechanism is mainly two types like public audit ability and private audit ability. The private audit ability gives higher efficiency. The public audit ability enables everybody like users, customers to interact with cloud server or cloud storage.Forconsistencyand privacy user may resort to TPA. The auditing protocols are likethird party auditing and data owner auditing.

1) Public auditing for protected data storage: C. Wang et al. proposed a privacy-preserving method to carry out public auditing on the cloud information [10]. In case of cloud computing, it is not sufficient to adopt the traditional cryptographic measures to achieve security. The reason is due to data outsourcing and the ubiquitous nature of the data. So, in this paper they opt the concept of Third Party Auditing (TPA). Homomorphic authenticator and random masking ensures that TPA could not gain any knowledge during the process of auditing. Thus, TPA is trusted and capable of accessing the cloud storage to perform auditing. The audit report brings out the risks, if any is present in the data. The public auditing system is built using four algorithms and two phases. KeyGen and SigGen algorithms make up the first phase called Setup, in which initialization of secret parameters and generation of verification metadata are done. Following this, the Audit phase carries out the auditing process and ascertains the correctness of data in the cloud server. This is done in this second phase using GenProof and VerifyProof algorithms. The approach guarantees the correctness of data in cloud server, preservability of privacy and security for batch auditing [15]

C. Wang et al. in [11] enhanced their previous proposal by improving the security strength of data storage. A new protocol for privacy-preserving public auditing is designed for this purpose. Public auditing with zero-knowledge leakage is also achieved. Batch auditing is also enhanced with the improvement in main auditing scheme.

C. Comparison of Privacy Preserving Methods in Cloud Computing

Table 1 [12-15] show the comparison between privacy preserving mechanism with auditing and without auditing and also mentions the limitations of each method in the related works. The limitations pointed out in the table are overcome by the new powerful security mechanism called Oruta [12].Oruta provides data privacy, identity privacy. Also it ensures correctness and unforgeability While carrying out the public auditing mechanism.

III. CONCLUSION

In Cloud Computing, it is necessary that every cloud user must be guaranteed that his data is stored, processed, accessed and audited in a secured manner at any time. This survey discusses some of the techniques for preserving data privacy in the cloud. The main limitation of above methods is overcome by the powerful security mechanism called Oruta for shared data privacy. Oruta provides data privacy and identity privacy for shared data.

REFERENCES

[1] http://en.wikipedia.org/wiki/Cloud_computing
[2] Rong C, Nguyen S T et al. (2013). “Beyond lightning: A survey on security challenges in cloud computing”, Computers & Electrical Engineering, vol 39(1), 47–54.
[3] DananThilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo “Secure Data Sharing in the Cloud”
[4] Wang J, Zhao Y et al. (2009).” Providing Privacy preserving in cloud computing”, International Conference on Test and Measurement, vol 2, 213–216.
[5] Greveler U, Justus b et al. (2011). “A Privacy Preserving System for Cloud Computing”, 11th IEEE International Conference on Computer and Information Technology, 648–653.
[6] Zhou M, Mu Y et al. (2011).” Privacy-Preserved Access Control for Cloud Computing”, International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, 83–90.

[7] Chadwick D W, and Fatema K (2012). "A privacy preserving authorization system for the cloud", Journal of Computer and System Sciences, vol 78(5), 1359–1373.
[8] Sayi T J V R K M K, Krishna R K N S et al. (2012) "Data Outsourcing in Cloud Environments: A Privacy Preserving Approach", 9th International Conference on Information Technology- New Generations, 361–366
[9] Rahaman S M, and Farhatullah M (2012). "PccP: A Model for Preserving Cloud Computing Privacy", International Conference on Data Science & Engineering (ICDSE), 166–170.
[10] Wang C, Wang Q et al. (2010). "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing", Proceedings IEEE INFOCOM'
[11] Wang C, Chow S S M et al. (2013). "Privacy-Preserving Public Auditing for Secure Cloud Storage" IEEE Transactions on Computers, vol 62(2), 362–375.
[12] Wang B, Li B et al. (2012)."Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", IEEE Fifth International Conference on Cloud Computing, 295-302
[13] Jithin, S., and P. Sujatha. "An Analysis on Privacy Preserving in Cloud Computing."
[14] Onankunju, Bibin K. "Access Control in Cloud Computing."
[15] T. Jothi Neela, and N. Saravanan, Privacy Preserving Approaches in Cloud: A survey, IJST, vol.6.

AUTHORS PROFILE

Bincy Paul. has completed B Tech in CSE from Jawaharlal college of engineering and technology College of Engineering and Technology, Palakkad, Kerala, in 2012. Presently she is pursuing her M Tech in CSE from Mets School of engineering, Thrissur, Kerala. Her research interests include cloud computing and privacy preserving.

Dr. M. Azath is Head of Department of Computer Science and engineering, Mets School of Engineering, Mala. He has received Ph.D. in Computer Science and Engineering from Anna University in 2011. He is a member in Editorial board of various international and national journals and also a member of the Computer society of India, Salem. His research interests include Networking, Wireless networks, Mobile Computing and Network Security.