An Inspection On Privacy Preserving Methods In Cloud Computing

R.Rogini[#1], PG scholar of M.E Computer and Communication, Anna university, P.B College of Engineering, Chennai, India.
N.Arun Balaji*[2], Asst Professor, Dept of Electronics and Communication Engineering, Anna university, P.B College of Engineering, Chennai, India.

Abstract— **In the field of computing, cloud computing visualize consistent growth and evolving spontaneously . Still the threats and security problems deal with it. The main focus of this paper is surveying on various privacy preserving concept in cloud computing. This paper is go to handle and examine different steps such as cryptographic step processing, segregation or fragmentation of data, deals with writing access rights and policies. These sort of approaches would preserves the end user data privacy and during public auditing of cloud data privacy preserving is achieved. The inspected approaches are demonstrated and distinguished with one another by stating their merits and demerits. Finally, the concentrated issues to be drawn out in future and centralized results are produced. Earlier outsourcing of encrypted sensitive data, Data access notification to the data owner, providing complete permission of control to user over his/her data. All this function has a capacity to nullify the issues in privacy. In the process of enhancing the privacy preserving approaches in cloud this would serve as a note.**

***Index Terms*—Privacy preserving, Cloud computing, Surveying.**

I. INTRODUCTION

The structure of cloud and its data storing capacity has enormous benefits. Cloud allows to access tremendous resource by the authorized and authenticated cloud users where the resources are shared and outsourced in cloud. The cloud user can gain access (13)from cloud whenever required in a simple way with low cost. By using cloud user no need to own any hardware or install software cloud will be incharge of cost of installing and maintaining both hardware and software. Even with all these advantages, cloud has facing many threats which block the implementation of the cloud services. Both traditional and cloud security challenges are included in this criteria [12].Particularly in cloud computing the problems are many some of them are Cloud users identity management, support for multi-tendency, acquiring the security applications, cloud users privacy preserving, accomplishing the authority over the life cycle of deployed data, etc. Between this, the privacy preserving concept is taken to looked at this inspection. It is very necessary to preserving the cloud users data, identity and users privacy. The growth of cloud computing is getting increased rapidly at the same time, the responsibility of privacy preserving task is getting increased[11,14].Supporting and assuring secure data access in cloud is still in progress for reaching the peak. The problems in privacy preserving task which serves as a obstacle are specified in various format.By considering all these problem and creating a functionality which could not be agreed by the attackers or intruders would lead to efficient preserving of cloud data.

II. PRIVACY PRESERVING METHODS

A. Anonymity based approach

To achieve and preserve privacy in cloud jiang wang et al. make use of Anonymity based method [1].Before releasing the data in cloud , The anonymity algorithm involves in processing the data and anonymises entire data or few information. To mine the required knowledge cloud service provider utilize its background information and associate the specifics with the anonymous data. For preserving users privacy this methodology distinguish from the classic form of cryptography technique, The anonymity algorithm get rid of key managing process because of this reason it showcase as simple and flexible. The anonymising is quiet simple because ,anonymous varies according to the attributes and it is based on cloud service provider. Only limited number of services supported for this approach .This approach would be better if it is based on automating the automisation.

B. Architecture of Privacy Preserving

To achieve and preserve privacy in cloud jiang wang et al. make use of Anonymity based method [1].Before releasing the data in cloud , The anonymity algorithm involves in processing the data and anonymises entire data or few information. To mine the required knowledge cloud service provider utilize its background information and associate the specifics with the anonymous data. For preserving users privacy this methodology distinguish from the classic form of cryptography technique, The anonymity algorithm get rid of key managing process because of this reason it showcase as simple and flexible. The anonymising is quiet simple because ,anonymous varies according to the attributes and it is based on cloud service provider. Only limited number of services supported for this approach .This approach would be better if it is based on automating the automisation.

C. Access control for privacy preserving

Miao Zhou et al. [3] proposed a flexible approach of access control and deal with the user privacy in the environment of

ISSN: 2278 – 7798

cloud. Certain kind of attributes linked with every cloud user that determines their access rights. Two tier encryption model is introduced in this paper where the base phase and surface phase builds up the two tiers of the model. In the first 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 encrypted data in the cloud is dynamically re-encrypted by the SRM during the data owner request. Either a new user has to be created or an existing cloud user has to be repealed when the request for SRM given. The access policies remains hidden to the cloud server so the privacy of user data is not agreed because however the re-encryption going to take place in cloud server. In this manner privacy of data is preserved by giving complete access control to the data owner and by not allowing the cloud provider to learn information about the stored data .

D. Authorization system for privacy preserving task

David W. Chadwick et al. proposed a policy for the intention of privacy preserving of users data that is based on authorization infrastructure for the cloud [4].Access policies can be define by user itself and users data also be attached with it. By accomplishing this process guarantee the controlled access of data in cloud .For making authorization decision and enforcing the decision, Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs) are used. Launched master PDP is used to figure out and solves the issues among different decision of PDPs. Obligation service act as a piece of authorization infrastructure, because of this process the data owner is indicated regarding the access of authorized and unauthorized data access. Cloud provider is trusted by the authorization infrastructure and deal with the issues that enter by means of outsider. If the encryption of outsourced data has not done properly even after trusting the cloud provider.

E. A Privacy Preserving data outsourcing

It is specified in [5], For preserving the confidentiality of users data another method is constructed. By using graph privacy constraints are illustrated. In the graph given links and nodes specifies the confidentiality and attributes between the corresponding nodes. Among the entire group of attributes sensitive attributes are the subset of the group. The knowledge of the attribute should not be reveal to external party. By considering this sort of attributes a relation to be drawn and that is vertically fragmented. A part of fragment is given to owner while the rest of fragment is placed in external server. The fragmented relation can be reconstructed by using common id. To perform fragmentation and locating the fragmentation at appropriate place a graph coloring algorithm is used. During fragmentation it is important to verify that the confidentiality constraints not been breached by the server fragment and also it is to be checked that the workload is kept minimized at the source. Metrics such as Min-Attr, Min-Query and Min-Cond are used to carry out the fragmentation. These metrics ensures that outsourced data will always be protected from third party attacks by combining with the respective fragmentation guarantees. Thus this process make use of fragmentation alone to achieve privacy efficiently and effectively without considering the cryptographic techniques. By constructing a hyper graph rather than two dimensional graph its effectiveness can be improved.

F. PccP Model in cloud

An another approach to achieve privacy a model is introduced and named as Preserving cloud computing Privacy is given in [6]. The basement of the model in this approach is consumer layer where the cloud user request for request for accessing the cloud services is given. Network interface or address mapping act as second layer. The purpose of this layer is to change the real IP address depends on access request. By doing this it ensures the privacy of users IP address. The next layer is the topmost layer of the model it is privacy preserved layer it is associated with Unique user cloud identity generator. Some sensitive information can be preserved by this layer by using Privacy check mechanism. By using this mechanism the amount of data transparency can be determined in the cloud also enables the user to specify the access control. Transparency purpose in cloud (TPC) is used when some Personal Data Attribute (PDA) of a user has to be specified within the transparency level where Boolean function of the attribute is carried out. Thus both access control and data content prevented by PccP.

G. Dynamic Metadata reconstruction

In cloud overall possibility of metadata exploitation is focused by Adeela Waqar et al. [7].There is chances to compromise users privacy by attacker by means of retrieving knowledge of the metadata. To preserve data privacy a framework is proposed. For this reason first step is the metadata in cloud has to be separated then the separated data are grouped into a private form. Based on the sensitivity of data, Groups are separated into partially private and non private form. The next phase is table splitting , here there are two section that is the database table has horizontal and vertical splitting. Database normalization is assured by the splitting of the table database. The next phase is called ephemeral referential consonance where metadata reconstruction can be take place when required by the cloud. This phase assures there is no data leakage before and after splitting of database table. Thus this method proves to be efficient.

H. Public auditing for protected data storage

In cloud overall possibility of metadata exploitation is focused by Adeela Waqar et al. [7].There is chances to compromise users privacy by attacker by means of retrieving knowledge of the metadata. To preserve data privacy a framework is proposed. For this reason first step is the metadata in cloud has to be separated then the separated data are grouped into a private form. Based on the sensitivity of data, Groups are separated into partially private and non private form. The next phase is table splitting , here there are two section that is the database table has horizontal and vertical splitting. Database normalization is assured by the splitting of the table database. The next phase is called ephemeral referential consonance where metadata reconstruction can be take place when required by the cloud. This phase assures there is no data leakage before and after

ISSN: 2278 – 7798

splitting of database table. Thus this method proves to be efficient.

By improving the security strength of data storage C. Wang et al. in [9] enhanced their previous proposal. For this purpose a new custom for privacy-preserving public auditing is designed. Due to this intention Public auditing with zero-knowledge leakage is achieved. Enhanced the batch auditing process with the improvement in main auditing scheme. As an extension to the previous work support for data dynamics and generalization of the auditing scheme considered to be improvise in this paper. The better performance of the proposed design is demonstrated by conducting an experiment on an instance of Amazon EC2 .

I. Oruta concept

Another type of public auditing mechanism is propounded by Boyang Wang et al. [10] base on analysis of the work of Wang et al. Oruta support privacy of data, identity privacy. During the public auditing process also it assures correctness and unforgeability. the identity privacy is not achieved in [8],[9]. In this approach there are three main sector cloud server, TPA and the cloud users. Users are consider to be in two category original user and group of user, the original users are owner of the outsourced data. Original user has the capability to control the data and its transaction also. To carry out auditing for verifying the rightness of data all users send their request to TPA. Homomorphic Authenticable Ring Structures (HARS) scheme consist of three algorithms: KeyGen, RingSign and RingVerify are built here for achieving the privacy-preserving auditing. To focusing on an efficient auditing process the approach can be empowered mainly to make sure integrity of shared data in grouped users' environment.

III. CONCLUSION

The concept of cloud computing is drastically improving day by day. But there is some sort of threats are arising to acquire or learn data information in cloud. In this paper some of issues about privacy are discussed and the technique to solve the threats are surveyed. It is shown that different types of techniques used some methods are based on traditional cryptographic while other follows new type of methodologies to focusing on privacy task. Thus to conclude that every users data in cloud is stored in secure manner and also accessing, processing and auditing done in authenticated way. At the same time the user should have complete action of control towards their own data. Hence considering all this fact there is a possibility to secure the cloud computing in future.

REFERENCES

[1]. Wang J, Zhao Y et al. (2009). Providing Privacy Preserving in cloud computing, International Conference on Test and Measurement, vol 2, 213–216.

[2]. 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.

[3]. 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.

[4]. Chadwick D W, and Fatema K (2012). A privacy preserving authorisation system for the cloud, Journal of Computer and System Sciences, vol 78(5), 1359–1373.

[5]. 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.

[6]. Rahaman S M, and Farhatullah M (2012). PccP: A Model for Preserving Cloud Computing Privacy, International Conference on Data Science & Engineering (ICDSE), 166–170.

[7]. Waqar A, Raza A et al. (2013). A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata, Journal of Network and Computer Applications, vol 36(1), 235–248.

[8]. Wang C, Wang Q et al. (2010). Privacy-Preserving Public Auditing for Storage Security in Cloud Computing, Proceedings IEEE INFOCOM'10.

[9]. 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.

[10]. 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.

[11]. Gellman R (2009). WPF REPORT: Privacy in the clouds: Risks to privacy and confidentiality from cloud computing.

[12]. 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.

[13]. Takabi H (2010). Security and Privacy Challenges in Cloud Computing Environments, IEEE Security & Privacy, vol 8(6), 24–31.

[14]. Xiao Z, and Xiao Y. Security and Privacy in Cloud Computing, IEEE Communications Surveys & Tutorials, vol PP(99), 1–17.

ISSN: 2278 – 7798