Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 12, December 2014, pg.202 – 205

RESEARCH ARTICLE

Privacy Preserving Repository for Social Networking Application across Cloud

[1]Miss. Pritam V. Kilor, [2]Prof. V. B. Bhagat

[1]Student, Computer science and Engineering, P. R. Patil COET, Amravati, Maharashtra, India

[2]AssistantProfessor, Computer science and Engineering, P. R. Patil COET, Amravati, Maharashtra, India

Email id- [1] pritamkilor@gmail.com

ABSTRACT: Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance.Cloud computing has been envisioned as the de-facto solution to the rising storage costs of IT Enterprises.With cloud computing, it is necessary for data to be not only stored in the cloud, but also shared across multiple users. For this purpose many different data sharing techniques are developed in cloud environment.Privacy Preserving Repository for Securing Data across the Cloud is one of them. Cloud is offering different services to its users. Data sharing between two organizations is common in many application areas.

The primary issue to be dealt with when talking about security in a cloud is protection of the data. The main purpose is to build up a privacy preserving repository where data sharing services can update and control the access and limit the usage of their shared data, instead of submitting data to central authorities, and, hence, the shared-disk database architecture will promote data sharing and privacy of data.

Keywords: Cloud computing, Data sharing, Privacy Preserving repository, central authorities, shared-disk database.

I. INTRODUCTION

In recent years, cloud computing is gaining much momentum in the IT industry. Especially, we have seen the dramatic growth of public clouds, in which the computing resources can be accessed by the general public.There are many service provider in the internet, we can call each service as a cloud, each cloud service will exchange data with other cloud, so when the data is exchanged between the clouds, there exist the problem of disclosure of privacy. So the privacy disclosure problem about individual or company is inevitably exposed when releasing or sharing data in the cloud service.One of the biggest advantages of a public cloud is its virtually unlimited data storage capabilities and elastic resource provisioning. As cloud computing comes in service there are some drawbacks such as privacy of user's data, security of user data is very important aspects. Cloud computing is

demand on shared computing resources. With the continuous development of cloud computing technology, its appliance is more and more widely. Now a days, cloud computing is often used with different synonymous like grid computing, cluster computing, distributed computing, autonomic computing.a privacy preserving repository is being presented for acceptance of integration requirements from clients to share data in the cloud and maintain their privacy,collect and integrate the appropriate data from data sharing services, and return the integration results to users. Our repository basically concentrates on the harmonizing operations and is beneficial in the following ways:

- The data sharing services in the cloud possess the ability to update and control the access and usages of their shared data. That is, data can be updated when required and it can be inferred who is using the data and in what way.
- The sharing of data in the cloud is done based on the need-to-share principle, which states that the dispatched information of the data is adequate to support client's integration requirements, but carries no extra information of the data.
- The repository is limited to gathering data from data sharing services and combining the data to satisfy users' requirements. The repository will contain noother information apart from that required to deliver theresults to the user and it cannot use this data for other purposes.

Our goal is to build up a repository to facilitate the data integration and sharing across cloud along with preservation of data confidentiality. For this we will be using an encryption technique to provide data security on data storage [3].

II. RESEARCH METHODOLOGY

Since this paper is concerned about managing the privacy of data which is sent to a database in the cloud, in this section, general approaches to privacy management for data repositories have been placed, for which various techniques have been developed to ensure that stored data is accessed in a privacy compliant way. Some mechanisms and solutions have been built to encrypt confidential data when it is stored in data repositories, Bertino and Ferrari [3], describe access control policy-based encryption mechanisms for Extensible Markup Language (XML) documents. Bertino and Ferrari describe mechanisms for fine-grained encryption of parts of XML documents, in which decryption keys can either be granted to data receivers or collected from LDAP servers, based on data receivers' credentials. Hippocratic databases include mechanisms for preserving the privacy of the data they manage. Their proposed architecture is based on the concept of associating privacy metadata (i.e. privacy policies) to data stored in data repositories, along with mechanisms to enforce privacy.

In paper *"*Trust-Based Privacy Preservation for Peer-to-Peer Data Sharing*"* suggested technique privacy preserving repository to integrate data from various data sharing services. The performance of decryption depends on these parameter repository only collects the minimum amount of information from data sharing services based on user's integration requests, and data sharing services can restrict our repository to use their shared information

only for users integration requests, but not other purposes. They assume that our repository can access all shared data and focus on how data sharing services shared data for specific data integration requests to prevent our repository from using the shared data for other purposes. In this research they have only focused on matching operations and additive homomorphism encryption schemes there repository could be easily extended to support SUM andAVG aggregate operations.

A privacy-preserving public auditing system for data storage security in Cloud Computing. to utilize the homomorphic non-linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process that not only reduces the burden of cloud user from the tedious and possibly pricey auditing task, but also alleviates the users terror of their out sourced data security.

Cong Wang et al [2] propose a privacy-preserving public auditing system for data storage security in cloud computing. They utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data contentstored on the cloud server during the efficient auditing process that not only removes the burden of cloud user from the tedious and possibly expensive auditing task, although also assuages the user's fear of their out sourced data escape. Taking into consideration TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, they further extend our privacy-preserving public auditing protocol into a multiuser situation, where the TPA can execute numerous auditing tasks in a batch manner for better efficiency [3].

III. DATA ANALYSIS

The social networking applications have become very popular and commonly used by the users in the modern times. The social applications not only provide a platform to connect the users to their friends and colleagues but also give an important facility to share their data amongst the friends. The sharing of the private data to the friends shows a threat that the data may get leaked and may fall into the hands of unauthorized users. The objectives of propose project work to preserve the privacy of the data while it is being shared by the user to the friends. The preserving the data privacy can be done by preventing the data being accessed by unauthorized users in a shared environment, preventing data to be accessed by the friends of the users but not authorized to access the data. The sharing of the data can also be need-based, which means that the important data can be shared for a small amount of time to the friends and after the time is over the sharing features can be removes. The sharing of the data amongst friends can be done by generating a private security key sent to the users who can access the data and a public key to authenticate the data being shared. The user needs to provide the security key to access the data. To implement the proposed idea of privacy-preservation, a social networking site would be creating wherein users can share their data amongst the friends.

IV. CONCLUSION

Our research indicates that that Security and Privacy are the major issues that are needed to be countered, efforts are being made to develop many efficient System That can Provide Security and privacy at the user level and maintain the trust and intellectual property rights of the user. The presented privacy preserving repository to integrate data from various data sharing services and an approach to security policy integration and conflict reconciliation for collaborating organizations in ubiquitous computing environments. The repository only collects the minimum amount of information from data sharing services or from the client across the cloud which is based on user's integration requests, and data sharing services can restrict our repository to use their shared information only for user's integration requests, but not other purposes.

REFERENCES

[1] Ranjita Mishra and Sanjit Kumar Dash ,*A Privacy Preserving Repository for Securing Data across the Cloud* ―IEEE 978-1-4244-8679, 2011

[2] Cong Wang, Sherman S.M. Chow, Qian Wang, KuiRen, and Wenjing Lou ―*Privacy-Preserving Public Auditing for Secure Cloud Storage*‖, IEEE Transactions On Computers, Vol. 62, No. 2, pp. 362 – 375, February 2013.

[3] Bertino E, Ferrari E (2002) Secure and selective dissemination of XML documents. ACM Trans InfSyst Secur5(3):290–331

[4] Yuan, Jiawei, and Shucheng Yu. "*Privacy Preserving Back-Propagation Neural Network Learning Made Practical with Cloud Computing*", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, Issue 1, pp. 212 – 221, 2014.

[5] Wang, Cong, Qian Wang, KuiRen, and Wenjing Lou. "*Privacy-preserving public auditing for data storage security in cloud computing.*" In proceedings of 2010 IEEE INFOCOM, pp. 1-9, 2010U.K.: Cambridge Univ. Press, 2001–2004, vol. 1 and 2.

[6] http://en.wikipedia.org/wiki/Cloud_computing.

[7] Rakshit, A. , et. Al, *"Cloud Security Issues",* 2009, IEEE International Conference on Services Computing

[8] Srinivas, D. "*Privacy-Preserving Public Auditing In Cloud Storage Security*." International Journal of computer science and Information Technologies,ISSN: 0975-9646, vol. 2, no. 6, pp. 2691-2693, 2011

