Chapter 21
A Generic Privacy Breach Preventing Methodology for Cloud Based Web Service

S. R. Murugaiyan
Manonmaniam Sundaranar University, India

T. Vengattaraman
Pondicherry University, India

D. Chandramohan
Pondicherry University, India

P. Dhavachelvan
Pondicherry University, India

ABSTRACT

The present focuses on the Cloud storage services are having a critical issue in handling the user's private information and its confidentiality. The User data privacy preserving is a vital facet of online storage in cloud computing. The information in cloud data storage is underneath, staid molests of baffling addict endeavor, and it may leads to user clandestine in a roar privacy breach. Moreover, privacy preservation is an indeed research pasture in contemporary information technology development. Preserving User Data in Cloud Service (PUDCS) happens due to the data privacy breach results to a rhythmic way of intruding high confidential digital storage area and barter those information into business by embezzle others information. This paper focuses on preventing (hush-hush) digital data using the proposed privacy preserving framework. It also describes the prevention of stored data and de-identifying unauthorized user attempts, log monitoring and maintaining it in the cloud for promoting allusion to providers and users.

1. INTRODUCTION AND RELATED WORK

This paper focuses on cloud digital data loss and its privacy preserving by proposing a novel framework approach to mitigate the risk and protect the data from attackers. In Cloud, it have high digital data storage center in which user privacy maintenance is a wearisome chore for both end-user and service provider. Unceremonious seclusion, contracted with habitual user's personal information, is the main reason to develop and propose this novel framework for maneuver in data progression and maturity. The current information dispensation conceded slightest relationship and input circumstances.

DOI: 10.4018/978-1-4666-8111-8.ch021

Radical usages of cloud data irrespective of consign and contrivance may direct to violate user's privacy and their needs. Moreover Anmin Fu *et al.* (2012) express the dominant usage of critical data and its preserving techniques are handled in an earlier data protection method. Virtual swarm is ensuing cohesion with provider and user. More informational confidentiality have personage precincts for user acquiescence and admittance to data exodus in storage area. The general privacy issue and its preserving methodologies adopted so for are not meeting the requirement of cloud user. The limitation of data attackers generally overcomes to preserve better utilization of authorized user data. Preserving sensitive information proposed a privacy preserving approach for mitigating the security for user data using encryption and decryption technique. Moreover, the author proposed a Petri-net based framework approach to preserve user information, and an evolutionary model for protecting the digital data.

A cookie based monitoring the user behavior (Wang, 2010, 2013) used an identity based data storage and retrieval and a frame work to establish enough trust among user on providers. To illustrate the scientific structure for normal systems are not adequate more over a perfunctory approach for preserving confidential data. It is noted to be less cost effective process for implementing in many field where-ever privacy is necessity. a general behavior of data analysis (Ye Wang *et al.,* 2012) in his approach he experiments a better data utility option with improved privacy preserving technique. Once all information readily available online one can easily get into others storage without any risk and makes the data into risk and there is no information privacy in cloud storage. A hand over technique was proposed to secure the data in a theoretical analysis of authentication system and providing data privacy through public auditability. Data's can be preserved and an audio representation high lights the cloud users secrecy and maintenance to a secure and efficient data retrieval by using attribute based encryption, theoretical analysis of authentication and an novel architecture to preserve user privacy and authentication (Wang, 2012; Hari & Paul, 2013).

If and only if no one else knows even something regarding your personal data, it may climb to be information privacy. A detailed discussion on social networking provider's and their need of user personal information, literally they are utilizing it for business and making confidential data into profit. Data request oriented service communication for the cloud services and moreover the data stored in distributed environment privacy representation as an assurance to make and mitigate trust on them to provide a better service cloud providers (Dhasarathan, 2012, 2014).

A publicly audit cloud storage may reduce the cloud owners expertise and cloud users privacy threat. It also reduces the cost for data users and develops more trust on cloud providers. (Li *et al., 2010*) the trust on data storage may implicate by data coloring techniques. Trust overlay methods supports for multiple data centers. The high level surveillance of Zhang *et al.* (2010) with the help of user's identity based crypto systems may reduce the misbehavior and certificates are unnecessary to prove the identity of a user. To design a structured search engine (Haodong Wang *et al*., 2010) to protect the sensitive user information in mobile cloud a snoogle information retrieval search engine were developed.

Main focus to prevent the data integrity (Hao *et al*., 2011) public verifiability for remote data integrity checking and verification carried out without the concern of third party auditors. It may reduce the leakage of data to third party auditors. A mutual agreement technique is adopted by Yi Lin *et al.* (2011) for ubiquitous environment a key agreement scheme with user authentication technique to minimize the leakage of secrete information form serves. The systematic and symbolic system (Huang *et al.,* 2010) the combination of lazy revocation, multi-tree structure and symmetric encryption are used to design an efficient privacy preserving framework for the cloud storage.