International Journal of Information Security and Privacy
Volume 14 • Issue 1 • January-March 2020

Secured Sharing of Data in Cloud via Dual Authentication, Dynamic Unidirectional PRE, and CPABE

Neha Agarwal, Amity University, Uttar Pradesh, India
Ajay Rana, Amity University, Uttar Pradesh, India
J.P. Pandey, KNIT, Delhi, India
Amit Agarwal, University of Petroleum and Energy Studies, Dehradun, India
https://orcid.org/0000-0002-3933-5014

ABSTRACT

Cloud computing is an emergent computing paradigm; however, data security is a significant issue in recent time while outsourcing the data to the cloud preventing users to upload their data on cloud. The data forwarded to cloud can be protected using some cryptographic techniques based on identity, attributes, and prediction. But these algorithms lack their performance when a revoked user collude with cloud; therefore, it becomes essential to develop a secure data sharing framework with some enhanced cryptographic techniques. The proposed methodology presented a secure privacy preserving data sharing with encryption technique called dynamic unidirectional proxy re-encryption (PRE) with cipher text policy attribute-based encryption. The technique ensures the privacy, integrity, and security of the data while retrieving through the cloud. The framework is implemented in the cloud sim with java language. Experimental results proved that proposed frame work attains reasonable results compared to traditional methods.

KEYWORDS

CipherText Policy ABE, Digital Rights Management (DRM), Efficient Elliptic Curve Public Key Encryption (EECPKE), Proxy Re-encryption, Twofold authentication protocol

1. INTRODUCTION

Cloud computing is an emerging paradigm in which resources are outsourced on rent to the customers by the cloud service providers through internet. It is now acknowledged as utility service after electrical, water and gas services(Ali et al. 2015). It not only saves the capital expenditure of the customer but he can scale out or scale in the request for services provided and pay accordingly. It is not limited for storing and sharing data but is also for managing, monitoring and exploring data in space ground data system (Kaddouri et al., 2018). The four main deployment models are public, private, community and hybrid cloud having variations in cost and security. In cloud stack the services are arranged as layers from the most reduced layer to highest layer where each layer symbolizes one service model. IaaS is the most reduced layer, where the cloud supplier maintains a suite of management resources and services to cope a substantial cloud system (Zhu et al., 2013; Sun et al., 2014) and the user utilizes the infrastructure and resources such as network, storage, computational capacity etc without worrying

DOI: 10.4018/IJISP.2020010104

about the complexity and management (Wang et al., 2012; Wei et al. 2014). The central layer PaaS, offers platform and software to develop applications. SaaS located at top layer, where completely developed software applications are provided as a service (Saouli et al., 2015).

For sharing the data, the cloud model comprises of three entities cloud service supplier, client, owner (Boyang Wang et al. 2015). Cloud service supplier regulates Cloud Storage Server (CSS) which has bigger storage space to shield the clients data and in addition high computation control (Manvi and Shyam 2014). Cloud servers gives a novel service approach where information is stored and its replica is maintained so that information can be acquired by clients anytime and from anyplace over the network (Sood 2012). Owner has colossal information documents for sharing and for this he uploads his data in cloud. The client are authorised by the data owner who can access the shared data. It can be a cloud proprietor itself too (Patel et al. 2013; Rong et al. 2013).

Although Cloud can confirm the client's information security through the thought of firewalls, fundamental private networks and by executing other security policies with in its own particular limits (Bera et al. 2015) yet Security is the most important key concern not only for data at transit but also for data at storage (Yang and Jia, 2012)

While outsourcing the sensitive data to be shared on cloud the owner losses his physical control. The data can be stored anywhere in the cloud as a result it becomes difficult to confirm exact location of storage (Li et al. 2015). The data not only have traditional security risks like (Ahmed et al.,2017), DDOS Attack (Li et al.,2015; Jeyanthi et al., 2013), man in middle attack and several intruder attacks (Boukhlouf et al.,2016) etc but even the third party service provider are semi trustful. As a result the owner needs to ensure the confidentiality, security from intruders, privacy, data availability and accessibility to users according to their access rights (AlZain et al. 2012;Zissis et al. 2012; Jakimoski, 2016).

The most common way to maintain confidentiality and security of the data stored in cloud against semi trusted cloud service provider is to send encrypted data. However there may be several other issues such as preventing the user to access the data for which he is not authorized, preventing the collusion between the revoked user and the semi trustful cloud, revoking away the given access right of the authorized user without re-encrypting the content and redistributing the new keys to the authorized users.

The main features needed while outsourcing data in cloud are privacy, Integrity, confidentiality, fine grained access control, Successful revoking privileges from users without in need of regeneration and distribution of re-encryption key, preventing collusion between third party service provider and revoked clients, Successful joining of new users and rejoining of revoked ones.

To ensure the afore mentioned features, In this paper we have proposed a framework based on DRM mechanism to ensure data security, dynamic authorization, license creation and proxy re-encryption. The proposed DRM scheme involves Ciphertext Policy attribute based encryption to ensure confidentiality of user and proxy re-encryption for preventing revoked user to collude along with One time password and license and other security mechanism. Finally we have compared the encryption and decryption time of proposed scheme with RSA and proved that the proposed scheme take less time in comparison to RSA

The outline of this paper is summarized as follows. In section 2 we have review the existing literature, In section 3 we have presented our framework entitle "Dual Authentication Based Security Framework for Cloud Based Data Sharing Applications" and presented the algorithmic description of proposed approach. Thereafter section 4 represents the experimental result and analysis of our approach and its comparison with the existing approach. Finally in section 5 we have drawn conclusion and presented the future scope.