Data Storage Security Model for Cloud Computing

Hiren B. Patel[1], Dhiren R. Patel[2], Bhavesh Borisaniya[2], and Avi Patel[3]

[1] S.P. College of Engineering, Visnagar, India
[2] S.V. National Institute of Technology, Surat, India
[3] City University, London, UK
{hbpatel1976,dhiren29p,borisaniyabhavesh,avi2687}@gmail.com

Abstract. Data security is one of the biggest concerns in adopting Cloud computing. In Cloud environment, users remotely store their data and relieve themselves from the hassle of local storage and maintenance. However, in this process, they lose control over their data. Existing approaches do not take all the facets into consideration viz. dynamic nature of Cloud, computation & communication overhead etc. In this paper, we propose a Data Storage Security Model to achieve storage correctness incorporating Cloud's dynamic nature while maintaining low computation and communication cost.

Keywords: Cloud Computing, Data Storage Correctness, Privacy, Security.

1 Introduction

The apparent benefit of having Cloud computing model is to relax the user from the lumber of storing and maintaining data or computing resources locally. This reduces the initial investment of any organization drastically, and provides a pay-as-you-go model. In spite of these noticeable advantages, Cloud computing has not been adopted widely in practice due to security and privacy concerns. Along with these, other traditional IT security issues such as integrity, confidentiality, availability, reliability, non-repudiation, efficient retrieval, data sharing etc. have the same significance in Cloud computing. Among all these, data storage correctness is one of the important security issues in Cloud.

There are various methods being adopted for the data storage correctness. Trusted third party such as cryptographic coprocessors is preferred by many researchers [2] [3] [6] [8] [11]. It adds additional cost on Cloud users' part for extra hardware. One implement the functionalities of cryptographic coprocessor using open source code in form of client application [1] [8]. It can be proved as cost-effective solution with some compromise at performance level.

In this paper, we aim to provide a client application based Data Storage Security Model. Rest of the paper is organized as follows. Section 2 discusses the recent work carried out followed by problem statement in Section 3. Section 4 presents our proposed scheme in detail along with the validation the planned-goals with the design. Section 5 includes some possible techniques to implement the core components of this model. With conclusions in section 6 follows references at the end.

V.V. Das and J. Stephen (Eds.): CNC 2012, LNICST 108, pp. 37–45, 2012.

2 Related Work

This section illustrates recent research in Cloud data storage correctness. There are few approaches which make use of soft client applications without use of extra hardware. Kamara at el. [1] propose a template of complete secure storage structure without mentioning much on implementation of components involved. Pearson et al. [8] describe a privacy manager which protects the data being stolen or misused. Though both of these approaches reduce the burden of extra hardware cost from Cloud user/provider, the performance is compromised to some extent, which can be improved with third party auditor (TPA) and/or additional hardware such as cryptographic coprocessors.

Recently, few researchers have proposed approaches based on third party auditor (TPA). Wang at el. [2] propose an approach which enables public auditability for Cloud data storage security through external TPA, without demanding local copy of data or imposing extra online burden on Cloud. Gowrigolla at el. [12] outline a data protection scheme with public auditing which allows data to be stored in encrypted form on Cloud server without loss of accessibility or functionality for authorized users. Homomorphic token are being utilized by Wang at el. [3] and Tribhuvan at el. [10] to achieve data storage correctness. Wei at el. [4] develop an auditing scheme which seeks data storage security, computation and privacy preservation with the help of probabilistic sampling technique and verifier technique. Chuang at el. [5] design an Effective Privacy Protection Scheme (EPPS) which provides privacy protection according to user's demand and also claim to achieve performance.

Temper-proof cryptographic coprocessors configured by trusted third party are proposed by Itani at el. [6] and Ram at. el. [11] to solve the problem of securely processing confidential data in Cloud infrastructure based on various trust levels. Cheng at el. [7] make use of Trusted Platform Module (TPM) with sealed storage ability. While enjoying the benefits of improved performance through extra hardware, these approaches pose cost burden on Cloud users/providers side. Security issues for cross-Cloud environment are addressed by Li at el. [9]. Xu at el. [13] address the security problem in the direction of securing document service. Yu at el. [14] argue that the Cloud data security problem should be solved from data life cycle perspective.

As every proposal discussed here has its own way of understanding the problem of data storage correctness, they do not handle the problems from all facets. For an instance, ignoring dynamic nature of Cloud or adding unnecessary cost on user part may distract the users from Cloud.

3 Data Storage Security Model

In this section, we propose a data storage security model, which intends to solve the data security problem from multiple facets. The first part outlines the design goals which we aim to achieve and the second part describes the proposed model.