D. Sumithra *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 1, January- 2014, pg. 1-8 **ISSN: 2321-8363**

Public Auditing & Automatic Protocol Blocking with 3-D Password Authentication for Secure Cloud Storage

P. Selvigrija, Assistant Professor, Department of Computer Science & Engineering, Christ College of Engineering &Tech., Pondicherry

D. Sumithra, M.Tech, II Year, Department of Computer Science & Engineering, Christ College of Engineering &Tech., Pondicherry

E-Mail Id: sumithra.deva@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. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. User level security is provided using the 3-D Password by combining textual, graphical and Biometric Finger print. For data level security symmetric key based encryption/decryption using Galois Counter Mode (GCM).

Keywords: 3-D password; Automatic protocol blocker; third party auditing; Audit

Full Text: www.ijcsma.com/publications/january2014/V2I101.pdf