



RESEARCH ARTICLE

A Protected Erasure-Code Based Cloud Repository System

R. Deepika Sagar¹, T. Madhumathi²

PG Scholar, Department Software and Engineering, TKR College of Engineering and Technology, Hyderabad, A.P-500 097, India
Email: ramarapudeepika@gmail.com

Assistant Professor, Department Information Technology and Engineering, TKR College of Engineering and Technology, Hyderabad, A.P-500 097, India

Abstract—A cloud storage system, consisting of a collection of storage servers, provides long term storage services over the Internet. Storing data in a third party's cloud system causes serious concern over data confidentiality. General encryption schemes protect data Privacy, but also limit the functionality of the storage system because a few operations are supported over encrypted data. Constructing a protected storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority. a threshold proxy encryption scheme and integrate it with a decentralized erasure code such that a protected distributed storage system is formulated. The distributed storage system not only supports protected and robust data storage and retrieval, but also lets a user forward his data in the storage servers to another user without retrieving the data back. The Major technical contribution is that the proxy encryption scheme supports encoding operations over encrypted messages as well as forwarding operations over encoded and encrypted messages. This method fully integrates encrypting, encoding, and forwarding. Here Examine and suggests suitable Arguments for the number of copies of a message dispatched to storage servers and the number of storage servers queried by a key server.

Keywords:-Decentralized erasure code, proxy encryption, threshold cryptography, protected storage system.

Full Text: <http://www.ijcsmc.com/docs/papers/November2013/V2I11201365.pdf>