IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, May 2024

A Reliable and Equitable Attribute-Based Proxy Re-encryption System for Cloud Data Sharing

Rishi N[1] and S Anu Priya[2]
PG Student, Department of Computer Applications[1]
Assistant Professor, Department of Computer Applications[2]
Vels Institute of Science Technology and Advanced Studies, Pallavaram, Chennai, India
22304347@vistas.ac.in and anupriya.scs@velsuniv.ac.in

Abstract: *The widespread acceptance and quick growth of cloud computing have made data sharing easier than ever before. What is preventing widespread adoption of cloud computing, however, is how to guarantee the security of the user's data in the cloud. Safe data sharing in cloud computing can be achieved through the use of proxy re-encryption. With the use of a semi trusted cloud server, a data owner can encrypt shared data in the cloud using their own public key, converting it into an encryption meant only for authorized recipients to control access. To help us grasp this fundamental better, this paper provides a thorough and motivating overview of re-encryption of proxy servers from a variety of angles. For granular access control of shared data, Ciphertext-Policy Attribute based Aes (CP-ABE) is a possible cryptographic primitive. Each user in CP-ABE has a set of attributes, and access structures based on attributes are used to encrypt data. If and only if a user's characteristics meet the requirements of the ciphertext access structure, the user can decrypt a ciphertext. Practical applications typically call for additional requirements in addition to this fundamental one. Our research centers on the significant problem of attribute revocation, which poses a challenge for CP-ABE methods*

Keywords: Proxy Re-Encryption, Data Sharing, Security, Cloud Computing