IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

Attribute -Based Data Sharing Security in Cloud with Data Integrity

Chetana kanifnath Zole[1], Shruti Abaji Urkude [2] , Diksha Pramod Hiradeve [3], Hemant Ghanshyam Khonde [4] ,Neehal Balkrishna Jiwane [5] , Ashish Baban Deharkar

Students, Shri Sai College of Engineering and Technology, Bhadrawati, India[1-4]

Assistant Professor, Shri Sai College Of Engineering and Technology, Bhadrawati, India [5]

Assistant Professor, Somayya Institute of Technology, Chandrapur, India [6]

Abstract: *Cloud computing offers high performance, availability and low cost for data storage and sharing, offers improved utilization of resources. In cloud computing, cloud providers sacrifice an abstraction of unlimited storage space for clients to bulk data. It can assist clients in reducing their capital expense of data managements by moving the local managements system to cloud servers. But security issues arise as our primary limitation since we now outsource storing data, which may be sensitive, to cloud service providers. For maintaining privacy of data, a common technique is to encrypt data files prior to clients uploading the encrypted data to the cloud. Cloud storage solutions can enable clients to minimize their financial and upkeep overhead of data managements. It is difficult to make a secure data sharing plan, particularly for changing groups in the cloud. In order to resolve the issue, here present a secure data sharing method for often updated groups. In this paper, a scheme based on AES encryption is suggested that integrates the cryptographic methods with Group Data Sharing and also an anonymous control method for tackling the privacy in data and also the user identity privacy in existing access control methods. If the member of the group can be revoked means, automatically replace public keys of current group and no longer need encrypt again original data. Any member of group can access data source in cloud and revoked members does not permit accessing the cloud again after revoked. At last integrate this secure distribution scheme into group data sharing systems..*

Keywords: Cloud computing, Data sharing, Security, Privacy Data confidentiality, Data integrity ,Access control

DOI: 10.48175/568