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 5, November 2025
Impact Factor: 7.67

Secure Data Sharing using Cloud Computing

Afza Kulsum[1] and Dr Soumyasri S M[2]
Student, Department of MCA[1]
Associate Professor, Department of MCA[2]
Vidya Vikas Institute of Engineering and Technology, Mysuru

Abstract: *Cloud-based file sharing is now ubiquitous across education, healthcare, finance, and government, yet widely used platforms still suffer from misconfigured links, provider-side key custody, and coarse, user- managed permissions. This paper presents Secure File Sharing Using Cloud, a production-oriented web system that unifies client-side AES encryption with an admin- controlled authorization workflow to deliver end-to-end confidentiality, accountable access, and practical scalability. The system adopts a three-tier architecture— React frontend, PHP/AJAX application layer, and MySQL data layer—deployed on AWS EC2 for elasticity and high availability. Files are encrypted prior to upload and remain ciphertext at rest; cross-user retrieval is possible only after explicit administrative approval, with all actions captured in immutable audit logs. We formalize a threat model covering eavesdroppers, credential guessing, SQL injection, and honest-but-curious cloud providers, and map each risk to concrete controls: HTTPS transport, authenticated encryption (AES-GCM), salted password hashing, strict session handling, least-privilege queries, and centralized authorization. A prototype implementation demonstrates that secure operation need not compromise usability: uploads and downloads of files up to 50 MB complete within 3–5 seconds, and the system remains stable with 100 concurrent users while preventing unauthorized access by design. Compared with prior work that emphasizes cryptographic strength, big-data throughput, or system-level mechanisms in isolation, our approach integrates cryptography, governance, and cloud deployment into a cohesive platform suitable for small-to-medium organizations and academic institutions. We discuss extendability to role- based access control, multi-factor authentication, hybrid key distribution (AES + RSA), and verifiable, tamper-evident logging. We release implementation artifacts, schema templates, and threat-model checklists to support replication, audits, and classroom adoption and practitioner use*

Keywords: Secure file sharing; Cloud computing; AES; Access control; AWS; Admin authorization; Web security

DOI: 10.48175/IJARSCT-30027