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 1, August 2025
Impact Factor: 7.67

Study on: Strategies for Data Protection in Cloud Environment

Dr. B. Anuja Beatrice[1], Anagha M Krishna[2], Kamalesh N[3]
Head and Associate Professor[1], BCA Students[2,3]
Sri Krishna Arts and Science College Coimbatore
anujabeatriceb@skasc.ac.in[1],anaghamkrishna23bca008@skas.in[2],
kamaleshn23bca025@skasc.ac.in3

Abstract: *Cloud computing has emerged as a transformative technology, enabling organizations to store, process, and manage data with scalability and flexibility. However, the migration of critical information to cloud platforms has raised significant concerns regarding data security, privacy, and compliance. This journal explores key strategies for protecting data in cloud environments, emphasizing encryption techniques, identity and access management, backup and disaster recovery planning, and adherence to legal and regulatory frameworks. The study highlights the importance of adopting a multi-layered security approach that combines technical measures, organizational policies, and compliance mechanisms to ensure confidentiality, integrity, and availability of data. It also examines industry best practices and provides insights into how organizations can align their cloud security strategies with evolving regulatory demands such as GDPR and HIPAA. Through this academic exploration, the journal underscores that effective cloud data protection requires not only advanced technological safeguards but also continuous monitoring, user awareness, and a proactive approach to risk management. The findings stress that as cloud adoption continues to grow, integrating robust security measures is essential for building trust and maintaining resilience in digital infrastructures*.

Keywords: Cloud Computing, Data Protection, Data Security, Encryption, Decryption, Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Backup Strategies, Disaster Recovery, Compliance, GDPR, HIPAA, Cloud Storage, Information Privacy, Cloud Architecture, Security Policies, Shared Responsibility Model, Data Integrity, Data Confidentiality, Cloud Risk Management

DOI: 10.48175/568