

Risk and Challenges in Cloud Computing

Gouri Chiniwalmath, Research Scholar (CSE), Sunrise University, Alwar (Rajasthan)

Abstract

Cloud computing has emerged as a transformative technology that provides on-demand access to computing resources, storage, applications, and services through the internet. It offers significant advantages, including scalability, cost efficiency, flexibility, resource sharing, and improved accessibility. However, the widespread adoption of cloud computing also introduces various risks and challenges that organizations must carefully manage. This study examines the major risks associated with cloud computing, including data security and privacy, unauthorized access, data loss, service outages, cyberattacks, insecure application interfaces, vendor lock-in, compliance issues, and inadequate control over shared infrastructure. Dependence on internet connectivity and third-party cloud service providers can also affect service availability and business continuity. Furthermore, multi-tenancy environments may increase the risk of data exposure if appropriate isolation and security mechanisms are not implemented. Effective risk management requires organizations to adopt strong authentication and authorization mechanisms, encryption, regular security assessments, backup and recovery strategies, continuous monitoring, and appropriate access-control policies. Compliance with relevant legal and regulatory requirements is also essential for protecting sensitive information and maintaining customer trust. The study highlights the importance of developing comprehensive cloud security frameworks that combine technological solutions with organizational policies, employee awareness, and continuous risk assessment. Addressing these challenges effectively can help organizations maximize the benefits of cloud computing while reducing security, operational, and financial risks associated with cloud-based environments.

Keywords: Cloud computing, cybersecurity, data security, privacy, cloud risks, data loss, service availability, vendor lock-in, risk management, compliance.