

Research on cloud computing models and data security issues in cloud computing

Phoumpaseud Sivongsay

Abstract: This study explores cloud computing models and the critical issue of data security within these environments. Cloud computing offers scalable, on-demand access to shared computing resources, including networks, servers, storage, and applications. However, the migration of data and applications to third-party infrastructure introduces significant security challenges. This research systematically examines the fundamental service models—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—alongside deployment models such as public, private, and hybrid clouds. The core focus is on identifying and analyzing key data security threats, including data breaches, data loss, insecure interfaces, and account hijacking. The study evaluates existing security mechanisms, such as encryption, access control, and identity management, assessing their effectiveness in mitigating risks. Furthermore, it discusses the shared responsibility model between cloud providers and clients. The findings highlight that while cloud computing offers substantial benefits, robust security protocols and a clear understanding of responsibility are essential for protecting sensitive data. The research concludes with recommendations for enhancing data security posture in cloud environments.

Keywords: Cloud computing, data security, cloud security model, data protection