Chapter 3
Legal Challenges in Cloud Computing

Tushar
https://orcid.org/0000-0001-7190-7687
United College of Engineering and Research, Prayagraj, India

Pooja Jaiswal
https://orcid.org/0009-0007-2507-1525
University of Allahabad, Prayagraj, India

Nandita Pradhan
https://orcid.org/0009-0006-8819-1009
United College of Engineering and Research, Prayagraj, India

Sweta Singh
United University, Prayagraj, India

Prabhat Chandra Shrivastava
https://orcid.org/0000-0003-0766-6422
Faculty of Science, University of Allahabad, Prayagraj, India

Venktesh Mishra
https://orcid.org/0000-0003-4476-4064
United College of Engineering and Research, Prayagraj, India

ABSTRACT

Cloud computing has enabled fast organizational growth and diversified service acceptance. These services accelerate product development and hosting, giving consumers and third parties instant access. Cloud computing problems must be considered and implemented by service providers. This chapter emphasizes cloud computing's legal, contractual, and security issues. Enterprise clients benefit from several cloud computing projects. Despite these benefits, cloud data security and privacy remain problems. The cryptography and data security issues discuss such algorithms, key management, humans, and legal and regulatory issues. Regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) put stringent obligations on enterprises to safeguard user data,

DOI: 10.4018/979-8-3373-3186-7.ch003

as discussed in this chapter. Addressing cloud computing's ubiquitous security vulnerabilities requires a detailed understanding of the selected solution. This chapter also provides a methodology for organizations to analyze virtual dangers and damages.

1. INTRODUCTION

This scheme aims for the digitalization and integration of public data, thereby facilitating broader financial inclusion. Through the utilization of cloud-based infrastructure, beneficiaries are successfully identified and government subsidies are directly transferred (via Direct Benefit Transfer) into citizens' bank accounts, eliminating multiple intermediary layers. “Such Information, Communication, and Technology (ICT) solutions assist policymakers in removing unintended beneficiaries who have been availing subsidies amounting to 3.17 lakh crore (as per the Indian Budget Estimates of 2022-23), while also ensuring the timely transfer of social security benefits. Cloud computing is defined as a large-scale distributed computing paradigm. It is becoming an increasingly important topic for businesses and organizations, with various services being provided over the internet within competitive timeframes. This accelerates business operations, allowing for quicker delivery and scaling within a competitive environment. Cost reduction (through pay-per-use models), maintenance, enhanced productivity, scalability, and elasticity are all offered to businesses through cloud computing (Moghe et al., 2012)”. A comprehensive analysis of cloud computing regulations reveals significant challenges in harmonizing global legal standards. Data protection frameworks, such as the GDPR, which mandate stringent guidelines on data storage, processing, and transfer, have been extensively examined in previous studies. The literature also highlights the challenges posed by jurisdictional conflicts, where contradictory laws on data handling and privacy are imposed by different countries. Data privacy is considered the most critical issue in cloud computing.

Strict requirements for the protection of user data are imposed on organizations by regulations such as GDPR and the California Consumer Privacy Act (CCPA). However, ensuring compliance becomes complex when data is stored in multiple jurisdictions with varying legal requirements. It is revealed in this chapter that organizations often struggle to maintain visibility and control over data flows in the cloud (Avanthi and Naveen, 2024). Clarity on key aspects such as data security, service uptime, and liability is often lacking in Service Level Agreements (SLAs). This chapter found that these details are frequently overlooked by organizations during contract negotiations, which can lead to disputes during service disruptions or security breaches. The strengthening of SLA frameworks is considered essential for ensuring mutual accountability. Anonymized personal data is not considered