An In-Depth Analysis of Trust, Security, and Privacy Concerns in Cloud Storage

Anjaney Shukla[1] and Dr. Narender Kumar[2]
Research Scholar, Department of Computer Science[1]
Research Guide, Department of Computer Science[2]
NIILM University, Kaithal, Haryana, India

Abstract*: Although cloud computing is controversial, many companies are transferring everything to the cloud. Most IT firms need cloud computing. Many users may utilize an integrated cloud computing infrastructure for storage, processing, and most significantly, scalability. Cloud computing offers scalable infrastructure for many services. Cloud computing problems include data security, access control, and privacy. Therefore, we must first identify cloud computing security threats, vulnerabilities, and issues. After assessing these issues, we must propose a cloud computing solution architecture that protects data, access, and privacy. Distribution of reused data needs data security.*

Based on well-known vulnerabilities and concerns, this paper examines major distributed computing security and protection difficulties. This article discusses security, privacy, and trust in current cloud computing settings and helps users recognize their risks, including cloud computing's. Assess distributed computing's core security, trust, and protection issues. (b) Assess approaches to reduce privacy, security, and confidence challenges to build cloud computing trustworthiness, security, and reliability. We will soon quantify cloud computing privacy, protection, and trust issues. A full cloud computing security, privacy, and trust management system will be created and deployed.

Keywords: Virtualization, Security Threats, and Vulnerabilities.