Chapter 6
Cloud Security and Privacy

Rubi Kadyan
https://orcid.org/0009-0003-4264-8913
Bhagat Phool Singh Mahila Vishwavidyalaya, Sonipat, India

Sunita Rani
https://orcid.org/0000-0002-6833-6737
Bhagat Phool Singh Mahila Vishwavidyalaya, Sonipat, India

Vinod Kr. Saroha
Bhagat Phool Singh Mahila Vishwavidyalaya, Sonipat, India

ABSTRACT

This chapter explores the key security threats and vulnerabilities at different levels, such as SaaS, PaaS and IaaS in cloud computing and provides their solutions. It will comprehensively analyze common security risks such as data breaches, unauthorized access and compliance issues. Discuss all security issues such as application security, data security, network security issues, authentication and authorization issues. It explains various data security techniques such as Cryptography, Steganography, Homomorphic cryptography, Quantum cryptography, DNA cryptography, Machine learning and Deep learning, Multi-factor authentication, and Blockchain to describe which technique is suitable at which stage of data. It explains regulatory bodies such as GDPR (European Union), HIPAA (United States), CCPA (United States), DSL (China), CSL(China), IT Act, and PDPB (India) and case studies related to regulatory role in data privacy. It describes the role of AI and machine learning, zero-trust architecture in threat detection, and the future of cloud computing.

DOI: 10.4018/979-8-3693-9984-2.ch006

1. INTRODUCTION

Today, in the digital world, Cloud computing has transformed the way of businesses and individuals to store, process, and manage data at low cost, anytime, anywhere, with availability and scalability. However, this convenience comes with significant challenges related to security and privacy. In the cloud, more sensitive information is stored, including personal, financial, and proprietary business data; the risks of data loss (breaches), unauthorized access, and privacy violations have increased exponentially. Security and privacy are top priority concerns in the cloud environment. In the cloud environment, services are provided by the service provider, and users have no control over data and other infrastructure. The users are unaware of where data is processed and where data is stored. Users can access the cloud service only when connected to the Internet. This created a security issue in a cloud environment.

Definition

Cloud security means setting policies, procedures, tools, and techniques to protect the cloud's data and infrastructure. It also provides solutions to Cloud-based issues, including data security, Infrastructure security, and resource availability (C. K. V. K. V. L. Reddy, 2024).

1.1. Importance of Cloud Security

A. **Data Protection:** Cloud security protects sensitive information (personal, financial, or business) from unauthorized access. Data encryption, both in transit and at rest, is one of the primary ways to safeguard data confidentiality.
B. **Mitigating Cyber Threats:** Cybercriminals engage in illegal activity in cloud environments, so robust security is needed to protect against illegal activity such as hacking, ransomware, and malware. Cloud security technologies such as firewalls, intrusion detection systems (IDS), and other security techniques (cryptography, steganography and deep learning) ensure that systems remain secure in a cloud environment.
C. **Cost-Efficiency** A robust cloud security framework helps organizations avoid costly consequences like data breaches, legal actions, or regulatory penalties. By leveraging the cloud provider's built-in security services, organizations can avoid the expense of building and maintaining on-premises security infrastructure (Cherbal et al., 2024)

Edge Computing: A Review on Computation Offloading and Light Weight Virtualization for IoT Framework
Minal Parimalbhai Pateland Sanjay Chaudhary (2020). *International Journal of Fog Computing (pp. 64-74).*
www.irma-international.org/article/edge-computing/245710