International Journal of General Engineering
and Technology (IJGET)
ISSN (P): 2278–9928; ISSN (E): 2278–9936
Vol. 10, Issue 1, Jan – Jun 2021; 327–348
© IASET

International Academy of Science,
Engineering and Technology
Connecting Researchers; Nurturing Innovations

RISK MITIGATION IN CLOUD-BASED IDENTITY MANAGEMENT SYSTEMS: BEST PRACTICES

Srinivasulu Harshavardhan Kendyala[1], Balaji Govindarajan[2], Imran Khan[3], Om Goel[4], Prof.(Dr.) Arpit Jain[5] & Dr. Lalit Kumar[6]

[1]Scholar, University of Illinois, Hyderabad, Telangana, India – 500074

[2]Scholar, University of Madras, Chennai, Tamil Nadu, India, 600078

[3]Scholar, Visvesvaraya Technological University, MVJ College of Engineering, Bangalore, India

[4]Independent Researcher, ABES Engineering College Ghaziabad, India

[5]Independent Researcher, Kl University, Vijaywada, Andhra Pradesh, India

[6]Associate Professor, Department of Computer Application IILM University, Greater Noida, India

ABSTRACT

As organizations increasingly adopt cloud-based identity management systems (IdM), the associated risks pose significant challenges to data security, compliance, and operational integrity. This paper explores effective risk mitigation strategies tailored for cloud-based IdM systems, emphasizing the importance of a proactive approach to security. By identifying potential vulnerabilities, including unauthorized access, data breaches, and compliance failures, organizations can implement best practices to fortify their identity management frameworks.

Key strategies include adopting a robust multi-factor authentication (MFA) mechanism, which significantly enhances user verification and reduces the risk of unauthorized access. Regular audits and compliance assessments are essential for ensuring adherence to industry standards and regulatory requirements, helping organizations stay ahead of potential vulnerabilities. Furthermore, organizations should prioritize the use of encryption for data at rest and in transit, safeguarding sensitive information from unauthorized interception.

Additionally, implementing a comprehensive incident response plan is critical for addressing security breaches promptly and effectively. This paper also highlights the role of continuous monitoring and threat intelligence in maintaining the integrity of cloud-based IdM systems. By fostering a culture of security awareness among employees and stakeholders, organizations can enhance their overall risk posture. Ultimately, this research provides a framework for organizations to navigate the complexities of cloud-based identity management while mitigating risks, thereby ensuring secure and compliant operations in an increasingly digital landscape.

KEYWORDS: *Cloud-Based Identity Management, Risk Mitigation, Data Security, Multi-Factor Authentication, Compliance Assessment, Encryption, Incident Response Plan, Continuous Monitoring, Threat Intelligence, Security Awareness.*

Article History

Received: 19 Jun 2021 | Revised: 24 Jun 2021 | Accepted: 29 Jun 2021