INTERNATIONAL CONFERENCE ON RESEARCHES IN ENGINEERING, SCIENCE, TECHNOLOGY, MANAGEMENT AND HUMANITIES (ICRESTMH – 2024)

25TH AUGUST, 2024

CERTIFICATE NO : ICRESTMH /2024/C0824815

Impact of Security Framework in Cloud Computing

Moram Sunil Kumar Reddy

Research Scholar, Ph. D. in Computer Science and Engineering
Dr. A.P.J. Abdul Kalam University, Indore, M.P., India.

ABSTRACT

The rapid adoption of cloud computing has transformed digital infrastructures, offering scalable and cost-effective solutions for businesses and individuals. However, the increasing reliance on cloud environments has also introduced significant security challenges, including data breaches, unauthorized access, and cyberattacks. This paper examines the impact of security frameworks in cloud computing, focusing on their role in mitigating risks and ensuring data confidentiality, integrity, and availability. Effective security frameworks integrate encryption techniques, identity and access management (IAM), intrusion detection systems (IDS), and artificial intelligence (AI)-based threat monitoring to enhance cloud resilience. The study highlights how compliance with industry standards such as ISO 27001, NIST, and GDPR strengthens cloud security by enforcing best practices. Additionally, the adoption of zero-trust architectures and blockchain technology further reinforces authentication mechanisms and secure data transactions. Findings suggest that a well-structured security framework not only prevents cyber threats but also improves trust among cloud service users by ensuring regulatory compliance and data protection. The research underscores the importance of continuous monitoring, automated threat detection, and real-time incident response in securing cloud environments. Future advancements in AI-driven security and quantum encryption are expected to further enhance the robustness of cloud security frameworks.