IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

Google Cloud Platform Threat Detection and Incident Response

Parool Priya[1] and Bipanshi Sharma[2]
Department of Computer Science & Applications[1,2]
Sharda School of Computing Science & Engineering, Sharda University, Greater Noida, India

Abstract: *Cloud computing is revolutionizing the way organizations store, process, and deal with data through greater scalability, cost-efficiency, and responsiveness than ever before. With this surge of momentum to the cloud, though, also comes the most virulent security threats that have to be addressed seriously in order to safeguard critical data as well as ensure regulatory compliance. This study discusses the shared responsibility model of cloud computing and describes how CSPs and customers share security responsibilities. Important issues like data privacy, integrity, and availability are discussed, as well as typical vulnerabilities such as misconfigurations and unauthorized access. The importance of data protection regulations such as GDPR, HIPAA, and PCI-DSS compliance is also emphasized. The research indicates that organizations need to assess their security roles explicitly in the cloud and have strong controls and policies to minimize risk and guarantee compliance.*

Keywords: Cloud Computing, Cloud Security, IAM, Shared Responsibility Model, Zero Trust Architecture, Blockchain, Data Privacy, Access Control, Compliance

DOI: 10.48175/568