Attacks on Cloud Systems and Their Prevention

S. Aynur Uysal
Dogus University, Istanbul, Turkey

Mitat Uysal
Dogus University, Istanbul, Turkey

Abstract

Cloud computing has become the dominant paradigm for delivering computing, storage, networking, and software services because of its elasticity, scalability, and cost efficiency ,. However, these same advantages also enlarge the attack surface by exposing virtualized resources, management APIs, remote identities, and multi-tenant infrastructures to adversaries . Among the most common threats in cloud environments are misconfiguration, identity compromise, insecure APIs, distributed denial-of-service (DDoS), data exfiltration, insider threats, and third-party integration risks . This article examines these attack classes and presents a layered prevention framework based on identity hardening, zero trust, secure API mediation, encryption, monitoring, anomaly detection, and incident recovery . In addition, a mathematical residual-risk model and a Python-based simulation are introduced to illustrate how preventive controls reduce cloud risk in a measurable way. The study aims to provide both a scientific overview and a practical defense perspective for modern cloud systems.

Keywords

Cloud security, cloud attacks, DDoS, insecure APIs, data exfiltration, zero trust, anomaly detection, cybersecurity, cloud defense.