Assignment 5.1: Cloud Security Risks & Mitigations

Joshua A Wortz

University of San Diego

Course Number: CSOL-500

Dr. Michelle Moore

02/10/2025

Cloud computing has transformed modern IT infrastructure by offering scalable, on-demand access to resources and services. However, cloud environments face significant security risks due to their internet-based nature. Cyber threats such as unauthorized access, malware infections, and denial of service (DoS) attacks can compromise data confidentiality, integrity, and availability. We will examine these three risks by analyzing their manifestations, real-world examples, and mitigation strategies to safeguard cloud environments.

Unauthorized access occurs when an attacker gains entry to cloud resources without proper authorization. Common causes are credential theft, weak authentication, or cloud misconfigurations (Hashizume et al., 2013). Cloud environments' shared infrastructure increases the risk of credential-based attacks (Süß et al., 2024). A notable unauthorized access occurred in 2018 when the marketing firm Exactis exposed 340 million records due to an unprotected database. Attackers could easily access sensitive information, resulting in a massive data breach. The consequences of unauthorized access include the exposure of confidential business and customer data, financial losses due to regulatory fines, and reputational damage leading to loss of customer trust. One solution to reduce the risk of this type of attack is implementing multi-factor authentication, which will significantly reduce the risk of credential-based breaches (Süß et al., 2024). Enforcing least privilege access control ensures users have only the necessary permissions, limiting the potential damage in case of a security breach.

Malware infections in cloud environments include ransomware, trojans, and keyloggers, often introduced through software vulnerabilities or phishing (Takabi et al., 2010). The shared nature of cloud environments allows the malware to spread rapidly if not adequately contained. The Securonix Threat Research Team reported that new cloud-based servers are targeted often within minutes of exposure. Attackers deploy malware for cryptomining or data exfiltration,

demonstrating how quickly cloud environments can be compromised. Malware infections can lead to data loss and encryption through ransomware, unauthorized access to sensitive information, and operational disruptions, resulting in financial losses. Regular software updates and anti-malware tools prevent infections (Süß et al., 2024). Employing isolation techniques such as sandboxing and containerization ensures that malware does not spread across cloud environments, further reducing its impact.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks overwhelm cloud services with excessive traffic, causing downtime and rendering them inaccessible (Mirkovic & Reiher, 2004). These attacks are particularly harmful due to cloud platforms' reliance on web accessibility. In 2018, GitHub faced a massive 1.35 Tbps DDoS attack using memcached reflection, briefly disrupting services before mitigation measures restored operations (Süß et al., 2024). The impact of DoS attacks includes prolonged downtime, financial losses, degradation of customer experience, and the risk of attackers using them as distractions for more sophisticated intrusions. Deploying DDoS mitigation services such as AWS Shield and Azure DDoS Protection helps detect and block abnormal traffic patterns before they affect services. Load balancing and rate limiting distribute traffic across multiple servers and cap request rates, preventing overload and mitigating attack effectiveness.

Cloud security remains a critical concern as organizations increasingly migrate to cloud environments. Unauthorized access, malware infections, and DoS attacks seriously threaten data integrity and availability. Implementing robust authentication mechanisms, proactive malware defenses, and advanced DDoS mitigation strategies can help organizations enhance their cloud security posture. Given the evolving nature of cyber threats, maintaining vigilance and adopting adaptive security measures are essential for safeguarding cloud infrastructure.

References

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013, February 27). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, *4*(5). https://doi.org/10.1186/1869-0238-4-5

Mirkovic, J., & Reiher, P. (2004, April 01). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39-53. https://doi.org/10.1145/997150.997156

Süß, F., Freimuth, M., Aßmuth, A., Weir, G. R. S., & Duncan, B. (2024). *Cloud security and security challenges revisited*. Retrieved from http://arxiv.org/abs/2405.11350v1

Takabi, H., Joshi, J. B. D., & Ahn, G.-J. (2010, December 03). Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security & Privacy*, *8*(6), 24-31. https://doi.org/10.1109/MSP.2010.186