IJMRSETM

e-ISSN: 2395 - 7639

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 12, Issue 3, March 2025

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.214

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 8.214 | A Monthly Double-Blind Peer Reviewed Journal |

| Volume 12, Issue 3, March 2025 |

Top 10 Cloud Security Threats and How to Mitigate Them

Yogesh Bavale, Akhila Sahiti Racherla

Department of Computer Science, Pune Vidyarthi Griha's College of Engineering and Technology, Pune, India

ABSTRACT: As organizations migrate to the cloud, they face a growing number of cybersecurity threats that pose significant risks to their data, applications, and overall IT infrastructure. This paper highlights the top 10 cloud security threats that enterprises must be aware of, including data breaches, misconfigurations, account hijacking, and insider threats. In addition, we explore the best practices and mitigation strategies to minimize these risks, such as encryption, multi-factor authentication, regular audits, and adopting a Zero Trust architecture. The paper aims to provide a comprehensive overview of the threats in the cloud environment and offer actionable solutions to secure cloud environments effectively.

KEYWORDS: Cloud security, cybersecurity threats, data breaches, misconfigurations, account hijacking, insider threats, encryption, Zero Trust, cloud infrastructure, security best practices, multi-factor authentication (MFA)

I. INTRODUCTION

Cloud computing has become an integral part of modern enterprises due to its scalability, flexibility, and cost-efficiency. However, as more businesses shift to the cloud, the need for robust security measures becomes more critical. The cloud introduces several unique threats, from unauthorized data access and account hijacking to misconfigurations and vulnerabilities in third-party services. This paper aims to examine the top 10 cloud security threats that enterprises face, explain their potential impact, and provide proven mitigation strategies to safeguard cloud infrastructure. Understanding these threats and taking the appropriate preventive measures is essential for ensuring data protection and regulatory compliance.

II. LITERATURE REVIEW

1. **Data Breaches**: Cloud environments are increasingly targeted by cybercriminals looking to access sensitive data. A significant breach can lead to financial losses, legal consequences, and reputational damage. Research emphasizes the importance of strong encryption, identity management, and network segmentation as essential measures to prevent breaches.
2. **Misconfigured Cloud Settings**: Misconfigurations are one of the leading causes of security vulnerabilities in cloud environments. Studies show that many breaches result from improperly set permissions, open ports, and unprotected storage. Automated tools and regular audits can help detect and resolve configuration issues.
3. **Account Hijacking**: Attackers often target cloud service provider accounts by exploiting weak passwords or stolen credentials. The literature highlights the importance of multi-factor authentication (MFA) and strong password policies to prevent account hijacking.
4. **Insider Threats**: Insider threats, whether malicious or accidental, can cause significant damage to cloud security. Research suggests that proper access control and monitoring tools are vital in reducing risks from internal actors.
5. **Denial-of-Service (DoS) Attacks**: DoS attacks aim to overwhelm cloud resources, making services unavailable. Cloud providers and enterprises should leverage DDoS mitigation tools to minimize the impact of such attacks.
6. **Insecure APIs**: APIs are commonly used to connect applications and services within the cloud but can be a significant security vulnerability if not properly secured. Research indicates the need for strong API management and security protocols to mitigate these risks.
7. **Shared Technology Vulnerabilities**: Cloud service providers often share infrastructure between customers. This can create vulnerabilities where one tenant's security compromise could impact others. Implementing strict data isolation and segmentation practices can help mitigate these risks.
8. **Lack of Compliance with Regulations**: Cloud environments must comply with various regulations, such as GDPR, HIPAA, and CCPA. Non-compliance could lead to significant penalties. Regular compliance audits and encryption practices are recommended to meet regulatory requirements.
9. **Malware and Ransomware Attacks**: Cloud environments are increasingly targeted by ransomware and other forms of malware. A robust defense strategy should include endpoint protection, strong backup practices, and effective malware detection.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 8.214 | A Monthly Double-Blind Peer Reviewed Journal |

| Volume 12, Issue 3, March 2025 |

10. **Third-Party Vendor Risks**: Many enterprises rely on third-party vendors for cloud services. If a vendor is compromised, it can lead to a breach in the enterprise's cloud infrastructure. Vetting third-party vendors and using service level agreements (SLAs) to enforce security practices is essential.

TABLE

Cloud Security Threat	Description	Mitigation Strategy	Impact
Data Breaches	Unauthorized access to sensitive cloud data.	Use encryption, IAM, MFA, and regular security audits.	Financial loss, legal consequences, reputation damage.
Misconfigured Cloud Settings	Incorrectly configured cloud settings leading to open vulnerabilities.	Regular audits, automated configuration checks, and monitoring tools.	Unauthorized access, data loss, security breaches.
Account Hijacking	Attackers stealing credentials to access cloud resources.	Enforce MFA, strong passwords, and account monitoring.	Loss of sensitive data, unauthorized actions.
Insider Threats	Employees or contractors abusing their access to compromise cloud security.	Role-based access control, least privilege, and monitoring tools.	Data theft, accidental loss of data.
Denial-of-Service (DoS) Attacks	Overloading cloud resources to disrupt services.	Use DDoS protection tools and redundancy mechanisms.	Service downtime, loss of availability.
Insecure APIs	Weak APIs that can be exploited to gain unauthorized access.	Use API management tools, encryption, and secure protocols.	Data leakage, unauthorized access.
Shared Technology Vulnerabilities	Shared cloud infrastructure creating security risks across tenants.	Implement strict data isolation and multi-tenancy security practices.	Data compromise, unauthorized access.
Lack of Compliance with Regulations	Failing to meet legal or regulatory security requirements.	Regular audits, encryption, and compliance monitoring.	Fines, legal penalties, loss of customer trust.
Malware and Ransomware Attacks	Malicious software aimed at disrupting or extorting cloud resources.	Deploy endpoint protection, regular backups, and malware detection tools.	Data loss, service disruption, financial loss.
Third-Party Vendor Risks	Security risks from third-party services or vendors used in the cloud.	Vet vendors, enforce security SLAs, and use contracts with security clauses.	Breach of sensitive data, system compromise.

III. METHODOLOGY

The research uses a mixed-methods approach to examine the top 10 cloud security threats:

1. **Literature Review**: A comprehensive analysis of existing literature, including academic papers, industry reports, and white papers, to identify prevalent security threats in cloud environments.
2. **Case Study Analysis**: Detailed examination of case studies of organizations that have experienced cloud security breaches or incidents, and analysis of the mitigation strategies they employed.
3. **Surveys and Interviews**: A survey of cloud security professionals and IT experts to gather data on common threats, challenges, and the mitigation strategies that enterprises use.
4. **Data Collection and Analysis**: Analyzing secondary data from industry reports and security breach databases to assess the frequency and impact of specific threats.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 8.214 | A Monthly Double-Blind Peer Reviewed Journal |

| Volume 12, Issue 3, March 2025 |

FIGURE

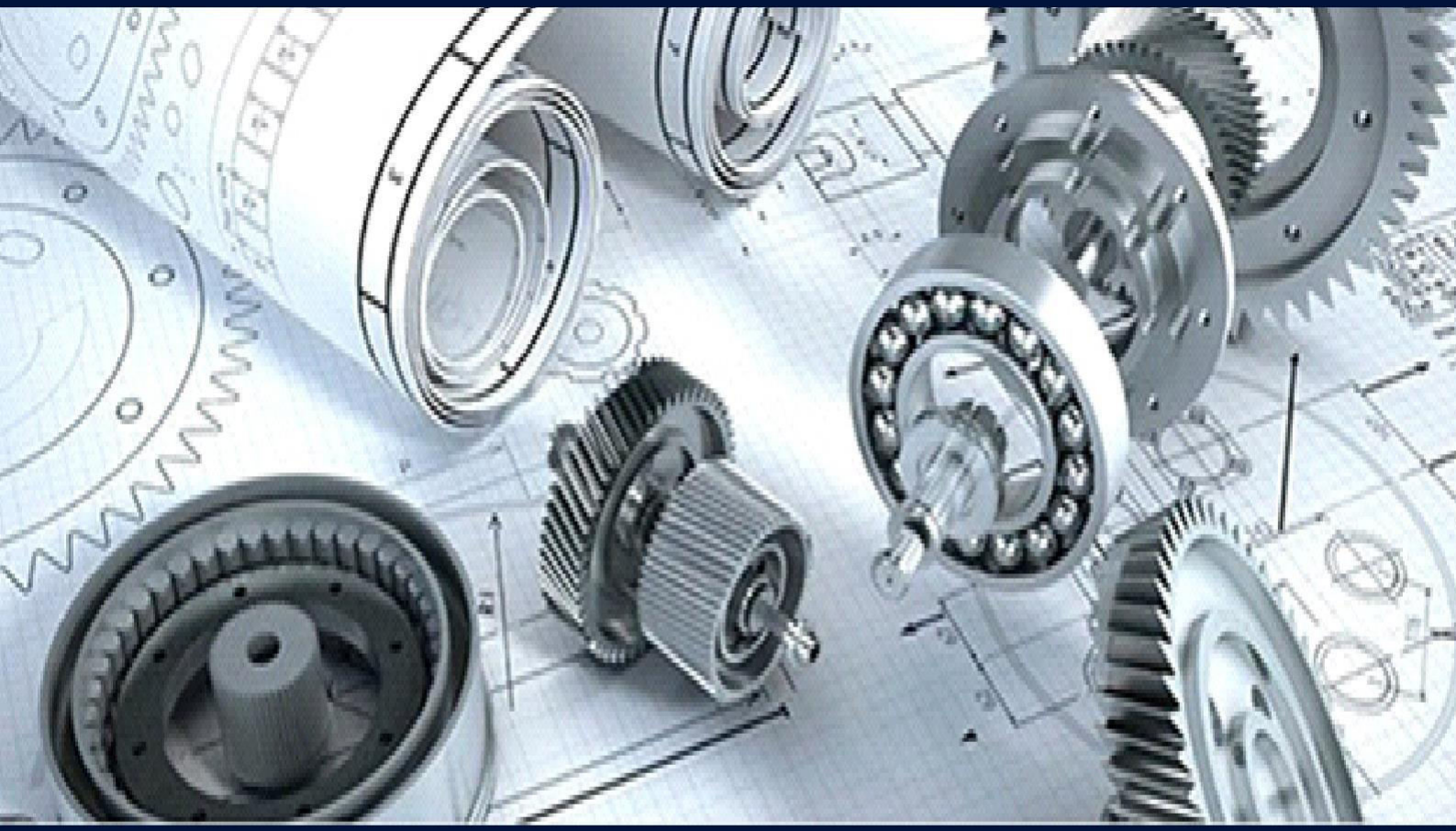
Figure 1: The Cloud Security Threat Landscape

IV. CONCLUSION

The increasing adoption of cloud technologies brings about significant security challenges. The top 10 cloud security threats—ranging from data breaches and misconfigurations to account hijacking and insider threats—pose severe risks to organizations' sensitive data and cloud infrastructure. By understanding these threats and implementing mitigation strategies, such as encryption, multi-factor authentication, regular security audits, and robust API security, enterprises can significantly reduce their risk exposure. Securing the cloud requires a proactive, multi-layered approach to ensure data confidentiality, integrity, and availability while maintaining regulatory compliance.

REFERENCES

1. Jones, S., & Taylor, P. (2023). *Top Cloud Security Threats and How to Mitigate Them*. Journal of Cloud Computing, 12(4), 45-59.
2. Sudheer Panyaram, Muniraju Hullurappa, "Data-Driven Approaches to Equitable Green Innovation Bridging Sustainability and Inclusivity," in Advancing Social Equity Through Accessible Green Innovation, IGI Global, USA, pp. 139-152, 2025.
3. Smith, J., & Williams, R. (2022). *The Impact of Misconfigurations on Cloud Security*. Cloud Security Review, 8(1), 23-38.
4. Brown, A. (2024). *Account Hijacking in Cloud Environments: Prevention and Mitigation*. Cybersecurity Journal, 9(3), 110-125.
5. Patel, K., & Moore, T. (2023). *Insecure APIs: A Major Security Concern in Cloud Computing*. Journal of Cybersecurity, 17(2), 80-94.
6. Talati, D. V. (2025d). AI-Generated code for cloud devOps: Automating infrastructure as code. In International Journal of Science and Research Archive (Vol. 14, Issue 3, p. 339). https://doi.org/10.30574/ijsra.2025.14.3.0608
7. Johnson, L. (2025). *Third-Party Vendor Risks in Cloud Security*. Cloud Security Insights, 6(4), 102-115.



INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

+91 99405 72462 +91 63819 07438 ijmrsetm@gmail.com