IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cloud Security: Impact, Challenges, Vulnerability And Practices To Mitigate Vulnerability

Pratyush Aatray

Research Scholar

University Department of Computer Application

Sona Devi University, Ghatsila, India

Abstract: Cloud security attacks are activities carried out by attackers using cloud computing architecture to get access to sensitive data or resources. These attacks use unauthorized access to cloud resources and data. Cloud security attacks are intentional and exploit common flaws or misconfigurations in cloud infrastructure. Cyber security ensures the security, integrity, and secrecy of communication, life, integration, real or intangible assets, and data in an electronic environment created by institutions, companies, and individuals in information systems. In conclusion, cyber security guarantees the safety of virtual existence on cyber networks. Cyber security protects the infrastructure of information systems, including data integrity and confidentiality. The basic goal of cyber security is to protect the data of individuals and institutions on the internet. These days, cyberattacks are more than just straightforward computer attacks; they also target large corporations and state governments. A strong cyber security policy is the only way to stop each example of a cyberattack. Strong security measures are now crucial due to the growing use of cloud services for vital processes.

Index Terms - Cloud security, cyber security, cyberattack, multi cloud environment, IAM complexity, TCP/IP vulnerability.

I. INTRODUCTION

Cloud security is a must-have for any organization that chooses to expand its operations in the cloud. Cloud security protects all cloud-related data, apps, and infrastructure. To strengthen cloud security, organizations must be completely informed of current attacks. Cloud security attacks are activities carried out by attackers using cloud computing architecture to get access to sensitive data or resources. These attacks use unauthorized access to cloud resources and data. Cloud security attacks are intentional and exploit common flaws or misconfigurations in cloud infrastructure. The term "cyber" refers to networks with infrastructure information systems, often known as "virtual reality". Cyber security ensures the security, integrity, and secrecy of communication, life, integration, real or intangible assets, and data in an electronic environment created by institutions, companies, and individuals in information systems. In conclusion, cyber security guarantees the safety of virtual existence on cyber networks. Cyber security protects the infrastructure of information systems, including data integrity and confidentiality. The basic goal of cyber security is to protect the data of individuals and institutions on the internet. Ignorance of this critical problem can have major risks. For example, a person with bad intents could exploit a network to access devices and take control of the data or steal user credentials like credit card numbers or user ID passwords. Individuals, organizations, large corporations, and even state governments may suffer financial losses as a result of such attacks. Recent research indicates that cyberattacks cost the global economy billions of dollars. These days, cyberattacks are more than just straightforward computer attacks; they also target large corporations and state governments. A strong cyber security policy is the only way to stop each example of a cyberattack. Strong security measures

are now crucial due to the growing use of cloud services for vital processes. Significant monetary losses, legal ramifications, and reputational harm can result from breaches. Furthermore, the evolving nature of threats in the cloud necessitates ongoing awareness and adaptation of security strategies. Efficient cloud security requires not only the identification, but also the prioritizing of vulnerabilities based on their likelihood and possible impact. Risk scoring models provide organizations with a methodical way to optimally distribute resources by ranking threats such as misconfigurations, data breaches, insider attacks, and insecure APIs based on severity.

II. Impact of Attacks on Cloud Security to businesses/ organizations:

• Financial losses:

Cloud security breaches can cause significant financial damage to businesses. The immediate costs to an organization often involve crisis response, system recovery, and possibly ransom payments. However, the financial impact does not end there. Businesses may suffer significant costs as a result of operational disruption, reduced production, and theft of intellectual property or financial data.

• Reputation Damage:

A cloud security assault can have extremely detrimental and long-lasting effects on one's reputation. Customer trust may decline if the public learns about the breach, which might lead to a loss of business and difficulties attracting new clients. Partners and other stakeholders are also put at risk of a damaged reputation.

• Regulatory Compliance Issues:

Attacks on cloud security may potentially negatively impact an organization's ability to comply with regulations. A number of data protection laws, including GDPR, HIPAA, and PCI DSS, have already been adopted by industries that deal with sensitive data, including the government, healthcare, and financial sectors. Strict security requirements and prompt notification of data breaches are required under these regulations.

III. Cloud Security Challenges

3.1 IAM Complexity & Lack of Visibility

Cloud security relies on Identity and Access Management (IAM) to restrict access to critical resources to authorized users. However, IAM can be complex and lack visibility. IAM management in hybrid and distributed cloud settings increases complexity. Misconfigurations in roles and permissions often lead to privilege escalation or unwanted access. According to papers, while the installation of Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) helps with principle-of-least-privilege enforcement in theory, firms continue to struggle with scalability and administration of dynamic user roles in large businesses. This adds operational overhead, making IAM one of the most commonly reported cloud adoption pain issues. Cloud customers have less visibility into data flows, setups, and monitoring since they do not always have direct access to the underlying infrastructure. This "blind spot" makes it more difficult to identify malicious activity, illegal changes, or simply noncompliance. Because logs and data are dispersed across multiple services in multi-tenant systems, monitoring becomes more challenging. Security Information and Event Management (SIEM) products and sophisticated logging tools are recommended; however, research shows they require significant adaptation to function in quickly evolving cloud systems.

3.2 Multi-Cloud Environments and Compliance Challenges:

The increased adoption of multi-cloud methods, in which enterprises distribute workloads across AWS, Azure, Google Cloud, and on-premises infrastructures, provides flexibility but fragments security controls. Each supplier has unique security capabilities, making conventional monitoring and enforcement difficult. Many articles note that this fragmentation leads to configuration discrepancies and redundant security efforts, increasing the risk of misconfigurations and breaches. Researchers believe that centralized policy orchestration and cloud-agnostic security frameworks are crucial for mitigating these concerns. Cloud usage involves adherence to global regulatory frameworks such as GDPR, HIPAA, and ISO standards. One major issue is that cloud hosts can host data internationally, creating legal uncertainty for purchasers. A lot of publications talk about how difficult it is to audit cloud process, especially when hosts don't give much

information about their internal controls. Organizations frequently rely on third-party certificates, but research warns that relying too much on them could produce a false sense of security. As a long-term approach, continuous compliance monitoring using cloud-native solutions is suggested.

3.3 Cloud Computing Security Issues and Solutions:

The Industrial Revolution has accelerated the growth of cloud computing, which has resulted in a number of complex security challenges. According to studies, common vulnerabilities include insider threats, cloud misconfigurations, and data exposure. The financial impact of data breaches in cloud computing is rather substantial. A crucial but typically complex aspect of cloud platforms is the shared responsibility model of security, which requires exact specifications between cloud providers and consumers. Artificial intelligence (AI) and machine learning (ML), which offer a way to process massive amounts of data and produce high-accuracy predictions with little human interaction, are being used more and more in response to such problems in order to enhance threat detection, automate response, and make systems more cyber resilient.

3.4 Data Residency Challenges:
Given the tendency of firms operating in multiple regions, residency and data sovereignty are major challenges. For redundancy, cloud providers duplicate and move data, often across borders without the user's knowledge. According to research, this poses a risk of breaking data protection laws, especially in delicate sectors like finance and health. In order to maintain control, researchers advise clients to use encryption with locally controlled keys and secure explicit data locality terms in Service-Level Agreements (SLAs).

IV. VULNERABILITY OF CLOUD SECURITY

4.1 Software vulnerabilities:

Errors or problems in applications give attackers the chance to take advantage of these flaws and compromise the system. Attacks brought on by software security flaws include buffer overflow and race situations.

4.2 Firewall vulnerabilities:

Firewalls protect networks from intrusions by acting as hardware and software barriers. An error, flaw, or incorrect assumption made during the firewall's design, implementation, or configuration that can be used to launch attacks on the trusted network the firewall is meant to protect is referred to as a firewall vulnerability.

4.3 TCP/IP vulnerabilities:

TCP/IP vulnerabilities affect multiple layers of a network. In an insecure network, these protocols may be lacking in desirable features. TCP/IP vulnerabilities can lead to attacks such as ARP and fragmentation.

4.4 Wireless network vulnerabilities:

Wireless networks are vulnerable to protocol-based attacks, just like traditional networks. Insecure wireless access points can also pose a threat since they allow an attacker to obtain unauthorized access to a personal or corporate network.

4.5 Operating system vulnerabilities:

Operating system vulnerabilities affect Windows, macOS, and Unix. The operating system's security determines the security of the apps that run on it. The slightest oversight by the system administrator might render operating systems vulnerable.

V. BEST PRACTICES TO MITIGATE VULNERABILITIES

The following are some of the greatest ways to reduce risks in cloud security:

• To prevent unwanted access to your cloud resources, use identity and access control systems. Encrypt data while it's in transit and at rest at all times.

• Make frequent backups of your data and adhere to the least privilege access principle. Strengthen your network security and create a zero-trust cloud security architecture. Recognize your requirements for compliance, correct policy infractions, and fill up any holes in your current policies.

• Update your firmware and software and stay up to date using patch management. Additionally, you should confirm that the security procedures of your cloud service provider adhere to industry standards. Use a continuous cloud threat monitoring system and safeguard your workloads and containers. Conduct regular patches and assessments of cloud security.

• Improve data governance policies and combine cloud security solutions to reduce silos. You should also develop an incident response strategy and undertake frequent penetration testing.

• Enable MFA and set rate limits for APIs. Check the API configurations and correct any errors. Train your employees on the latest cloud security techniques to ensure that they are never caught off guard by adversaries.

VI. CONCLUSION

Cloud security is at a stage where attackers are increasingly using AI to automate reconnaissance, develop very sophisticated phishing, bypass anomaly detection, and test multi-tenant boundaries at scale. Meanwhile, defenders are deploying AI/ML for behavior analytics, adaptive authentication, and real-time threat hunting—but these systems are also becoming attack targets for data poisoning, model evasion, and API misuse. Existing work in our community has already established AI as a force multiplier for real-time monitoring and response in cloud environments, with a goal toward increasingly autonomous control loops that reduce detection and containment times. Following that arc, the near-term research imperative is sound ML governance and "secure by design" telemetry pipes to prevent biased or spoofed inputs from spilling over into access decisions. The future of near-cloud security is identity and data-centric, continually validated (ZTA/SASE), autonomously instrumented by AI, secured against AI-powered attackers, and based on global standards. In practice, this entails creating crypto-agile architectures today, elevating people's and workloads' identities to first-class protected assets, relocating controls to platform and pipeline code, and ensuring preparedness against evidence that fulfils several frameworks at once. Organizations that view security as an engineered platform capability rather than a bolt-on will adapt the quickest to the changing environment described by your references.

REFERENCES

1. Bhavana B R, Shashank R, Druva H P (2025). Modern Cloud Security Threats and Vulnerabilities: A Comprehensive Review.

2. Robert Dilworth (2025). Cloud Computing and Security: An Overview of Vulnerabilities, Cyber Attacks, and AI-Driven Solutions.

3. Ömer Aslan, Semih Serkant Aktuğ, Merve Ozkan-Okay, Abdullah Asim Yilmaz and Erdal Akin (2023).
4. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions.

5. Milan Chauhan and Stavros Shiaeles (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions

6. Fabian S¨uß, Marco Freimuth, Andreas Aßmuth, George R S Weir and Bob Duncan (2024). Cloud Security and Security Challenges Revisited

7. Aisha A. Abba, Aisha Muhammad, Kashim K. Mohammed (2021). Cloud Security

8. Cloud Security Attacks: Types & Best Practices. SentinelOne.

9. Top 15 Cloud Security Vulnerabilities. SentinelOne.