International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Threats and Vulnerabilities in Cloud Computing: A Comprehensive Security Analysis

Dr. D. V. Bhavsagar

Associate Professor, Seth Kesarimal Porwal College, Kamptee, Nagapur (MS)

Abstract
Cloud computing remains a cornerstone of modern IT infrastructure in 2025, yet it is plagued by persistent and evolving security issues. This review synthesizes recent data from sources like the Cloud Security Alliance (CSA) Top Threats 2025 report, IBM's Cost of a Data Breach 2025, and various industry analyses, highlighting threats such as misconfigurations, data breaches, API vulnerabilities, and AI-driven attacks. Key statistics reveal that 82% of breaches involve cloud data, with human error accounting for 82% of misconfigurations, leading to an average global breach cost of $4.45 million. Through data analysis, including growth rates and sector-specific impacts, this paper examines vulnerabilities, real-world incidents, mitigation strategies, and future trends. Visual aids, tables, and charts illustrate the escalating threat landscape, emphasizing the need for proactive, AI-enhanced defenses.

Keywords: *Cloud* computing, security, vulnerabilities, threats, Business Computing, Future Trends.

I. INTRODUCTION

The Internet service industry, particularly cloud computing, has emerged as a transformative paradigm for large-scale infrastructure. By leveraging resource sharing, storage virtualization, and a pay-as-you-go provisioning model, cloud computing significantly reduces operational costs while enhancing scalability. Leading cloud platforms, such as Amazon's Elastic Compute Cloud (EC2), Simple Storage Service (S3), and Google App Engine, have become integral to the software industry, offering on-demand computational and storage capabilities. Despite their widespread adoption and efficiency, these cloud services face persistent security and privacy concerns, particularly regarding data processing and storage. Vulnerabilities in cloud computing platforms stem from diverse technological frameworks, including web-based outsourcing, mobile cloud computing, and service-oriented architectures (SOA). To foster user trust and ensure widespread adoption, cloud implementations require adaptive security mechanisms capable of mitigating risks. Without robust safeguards guaranteeing data confidentiality, integrity, and availability, concerns over privacy breaches and sensitive data leakage will remain critical barriers to the full-scale adoption of cloud services.

Privacy, recognized as a fundamental human right, entails both the right to be free from intrusion and the assurance that personal data is used and protected appropriately. However, the adoption of cloud computing introduces significant privacy risks, including the misappropriation of confidential data, uncontrolled service usage, unauthorized data propagation, potential secondary exploitation, cross-border data transfers, and dynamic provisioning complexities. Additional concerns arise from inadequate data retention policies, insufficient mechanisms for secure data deletion, and breaches stemming from low privacy awareness among users.

Currently, privacy agreements in cloud environments are often mediated through third-party services or generic terms and conditions governing personal data processing. These measures, however, fail to address critical vulnerabilities particularly in systems with limited or no user interfaces, where ambiguous consent mechanisms and poorly designed data handling practices exacerbate unauthorized access and misuse. Furthermore, the absence of transparency in cloud security policies raises pressing questions: (1) What specific commitments do Cloud Service Providers (CSPs) undertake to ensure data security? (2) Which security policies are publicly disclosed to users? The lack of clear accountability in these areas has contributed to recurring privacy violations, undermining trust in cloud ecosystems.

2. BACKGROUND

"The evolution of cloud computing has revolutionized the way organizations manage and deploy their IT resources. However, with the increasing reliance on cloud services, there has been a parallel surge in security challenges. This literature review delves into various dimensions of security challenges in cloud computing, aiming to provide a comprehensive understanding of the current state of research in this field" [1].

"Researchers emphasize the need for strong IAM regulations to strike a balance between security and usability. Resilience and efficient incident response are crucial for reducing security issues, with proactive monitoring, quick detection, and clearly defined event response plans. International standards and regulatory compliance are also important aspects of cloud security, with the two most important parts being negotiating different regulatory frameworks and harmonizing international standards" [2].

2.1: The Importance of Cloud Security

"With the increasing adoption of cloud services for critical operations, the importance of robust security measures has become paramount" [3]. "Breaches can lead to significant financial losses, legal repercussions, and damage to reputation. Moreover, the evolving nature of threats in the cloud environment demands continuous vigilance and adaptation of security strategies".

2.2: Data Security and Privacy

"Data security and privacy are paramount concerns in cloud computing, given the nature of the cloud as a shared and remotely accessible infrastructure. Ensuring the confidentiality, integrity, and availability of data is crucial for both service providers and users" [4][5].

2.3: Data Encryption

"One major challenge is protecting data while it is being sent and stored, which calls for the use of strong encryption techniques. Although these algorithms are essential for protecting sensitive data, putting them into practice adds operational complexity and could affect system performance" [6]. "Adopting robust encryption solutions for data in transit and at rest is essential to properly addressing this situation. Furthermore, strengthening the entire data protection plan depends on guaranteeing the safe administration of encryption keys" [7].

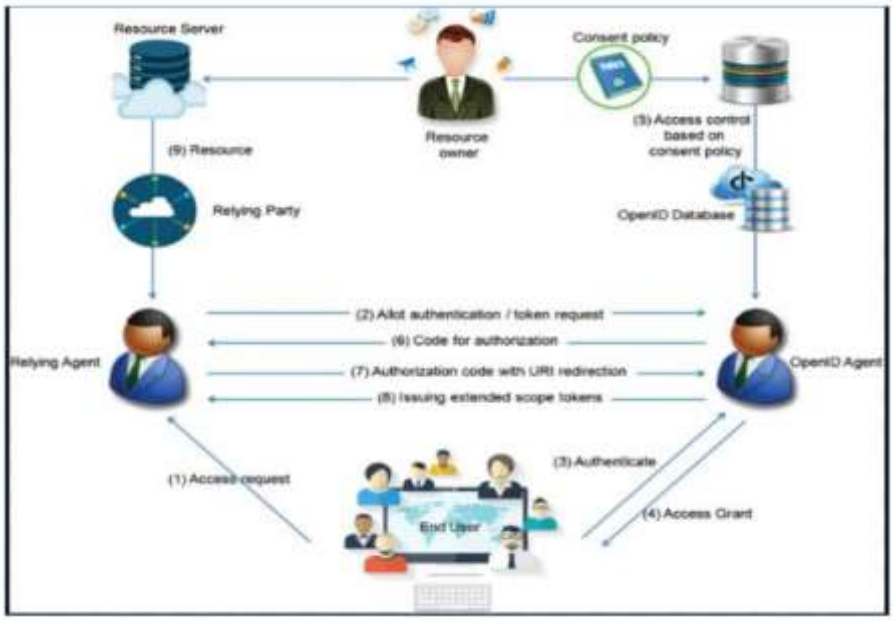

Fig. 1: Access control and authentication in the cloud

2.4: Identity and Access Management

"One of the main challenges in the field of Identity and Access Management (IAM) is managing user identities. This is managing and arranging user profiles and credentials in a system, which is a complex task. Proper authorization and authentication procedures must be guaranteed; this calls for strong protocols to confirm user identities and assign suitable access rights" [8].

A critical challenge in cloud security lies in identity federation—the complex task of managing and synchronizing user identities across disparate systems and security domains. Effective identity and access management (IAM) is fundamental to preserving system integrity, requiring not only robust authentication and authorization mechanisms but also interoperable identity federation solutions.

The implementation of such frameworks faces significant hurdles, including:

1. Maintaining consistent security policies across hybrid environments
2. Ensuring seamless interoperability between heterogeneous systems
3. Preventing privilege creep during cross-domain access provisioning
4. Mitigating risks associated with decentralized identity management

These challenges underscore the necessity for adaptive IAM architectures that can balance security requirements with operational flexibility in distributed cloud ecosystems.

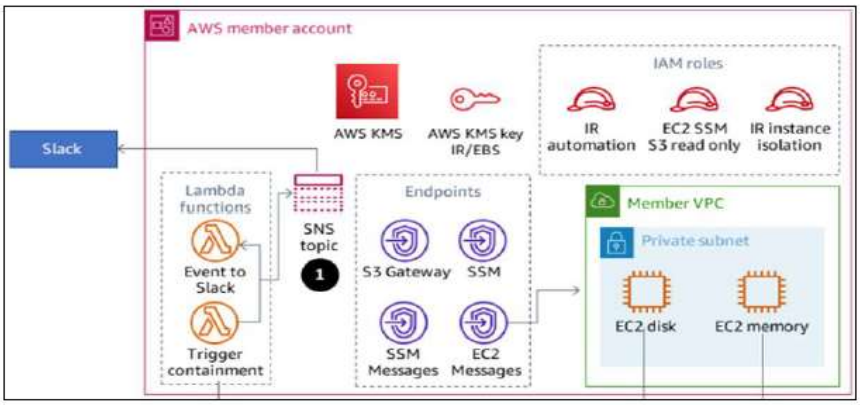

Fig. 2: Cloud incident response and forensics

3: Threats in cloud computing

3.1.1: Authentications

Organizations often struggle with identity and access management (IAM), particularly in assigning role-appropriate permissions to users. A critical failure occurs when user access privileges are not promptly revoked following role changes or employee departures, leaving systems vulnerable to exploitation. The 2019 SingHealth data breach, which exposed over 1.5 million patient records, exemplifies this risk attackers leveraged stolen credentials, and the absence of multi-factor authentication (MFA) allowed unfettered access. Further exacerbating IAM vulnerabilities, developers frequently hardcode credentials and cryptographic keys into source code, inadvertently exposing them in public repositories. Such lapses undermine even robust security architectures, transforming minor oversights into systemic threats.

3.1.2: Data sections

Cloud environments face many of the same security threats as traditional corporate networks, but the concentration of sensitive data on cloud servers has made service providers particularly attractive targets for cyber attacks. The severity of potential damage depends largely on the nature of the compromised data. While breaches involving personal financial information often dominate headlines, incidents exposing government data or intellectual property can have far more devastating consequences. In addition to reputational harm, organizations suffering cloud data breaches may face significant legal liabilities. Regulatory penalties, lawsuits, and compliance violations frequently follow such security incidents, particularly when they involve protected or classified information. The shared responsibility model of cloud computing further complicates liability attribution, leaving both providers and clients vulnerable to legal action.

3.1.3: Application APIs

Modern cloud services universally employ application programming interfaces (APIs) as fundamental components for system interaction and management. IT teams extensively utilize these interfaces for critical operations including cloud provisioning, administration, and performance monitoring. However, the security and reliability of cloud services are inherently dependent on API integrity, creating significant vulnerabilities when these interfaces are compromised.

The risk profile escalates when third-party integrations leverage these APIs, as organizations must often expose sensitive services and authentication credentials to facilitate interoperability. Poorly secured APIs represent particularly vulnerable attack surfaces due to their public internet accessibility, potentially leading to severe security breaches. These vulnerabilities primarily manifest in three core security

domains: confidentiality violations (unauthorized data access), accountability failures (inadequate logging and traceability), and availability disruptions (service outages).

4: Security challenges of cloud computing

4.1: Malicious attacking

"Security dangers can happen from both outside of and inside associations. In a cloud situation, an insider can annihilate entire foundations or control or take information. Frameworks that rely exclusively upon the cloud specialist co-op for security are at most serious danger" [9]

4.2: Database backup

"The cloud merchant ought to guarantee that standard backup of information is executed that even guarantee security with all measures. However, the backup information is commonly found in decoded structure which can prompt abuse of the information by unapproved individuals. In this way information backups lead to different security dangers. More the worker virtualization builds, a very troublesome issue with backup and capacity is made. Information reduplication is one of the answers for diminish backup and disconnected stockpiling volumes" [10].

4.3: Unencrypted data

Data encryption serves as a fundamental security mechanism that mitigates various external and malicious threats to cloud systems. Unencrypted data remains particularly vulnerable as it lacks essential protection mechanisms, enabling unauthorized access to sensitive information. When cloud servers store data in plaintext format, they risk exposing critical user information to malicious actors through system breaches or improper access controls.

A notable case demonstrating these risks involved Dropbox, which faced significant criticism for employing a single encryption key across all user data. This implementation flaw created a system-wide vulnerability where compromise of one key could potentially expose all stored data. Unencrypted or improperly secured data significantly increases the risk of malicious exploitation, as attackers can readily access and misuse sensitive information without needing to bypass encryption barriers.

5. Conclusion

Cloud computing presents immense potential, yet its inherent security risks grow proportionally with its benefits. This dual-edged nature makes cloud environments equally valuable to organizations and malicious actors each group stands to gain distinct advantages from cloud adoption. While security concerns remain significant, they should not overshadow cloud computing's transformative capabilities. Instead, ongoing research into robust, trustworthy, and adaptive security frameworks is essential to sustain its growth and adoption.

Security in cloud computing is non-negotiable. Despite existing challenges, cloud platforms are poised to become the dominant paradigm for business computing. However, addressing critical security vulnerabilities—alongside other operational and compliance issues is imperative to ensure long-term viability and trust in cloud-based solutions.

References

1. Rana NP, Slade EL, Sahu GP, Kizgin H, Singh N, Dey B, Gutierrez A, Dwivedi YK. Digital and social media marketing. Springer, 2020.
2. Kim D, Kim KS. Privacy-preserving public auditing for shared cloud data with secure group

management. IEEE Access. 2022 Apr 22, 10:44212-23.
3. Abdel-Rahman M. Advanced Cybersecurity Measures in IT Service Operations and Their Crucial Role in Safeguarding Enterprise Data in a Connected World. Eigenpub Review of Science and Technology. 2023 Jul 15, 7(1):138-58.
4. Kansal M, Singh P, Singh MK, Varshney S. A Systematic Study of Services and Security Model in Cloud Computing: A Brief Overview. Convergence of Cloud Computing, AI, and Agricultural Science. 2023:1-6.
5. Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31, 47(6).
6. Gupta I, Singh AK. A holistic view on data protection for sharing, communicating, and computing environments: Taxonomy and future directions. arXiv preprint arXiv:2202.11965. 2022 Feb 24.
7. Banasode PS, Padmannavar S. Protecting and Securing Sensitive Data in a Big Data Using Encryption. EAI Endorsed Transactions on Smart Cities. 2020 Apr 17, 4(11):e5-.
8. Mihailescu MI, Nita SL. A searchable encryption scheme with biometric authentication and authorization for cloud environments. Cryptography. 2022 Feb 14, 6(1):8.
9. A. K. Pandey et al., “Trends in Malware Attacks: Identification and Mitigation Strategies,” in Critical Concepts, Standards, and Techniques in Cyber Forensics, IGI Global, 2020, pp. 47–60.
10. R. Hackworth, “Data encryption,” Itnow, vol. 37, no. 5, pp. 12–13, 1995, doi: 10.1093/combul/37.5.12.