

Cloud Computing Security Challenges and Emerging Solutions

Abdul Jaleel Khan Anas¹, Abdul Rahman Syed², Mohammed Adil Tanveer³,
Mohammed Asim Chaudhry⁴, Smt. Sudha V. Paraddy⁵

¹Student, Department of Computer Science, PDA College of Engineering, Kalaburagi, India.
abduljaleelkhananas2@gmail.com

²Student, Department of Computer Science, PDA College of Engineering, Kalaburagi, India.
arsyed80089@gmail.com

³Student, Department of Computer Science, PDA College of Engineering, Kalaburagi, India.
adiltanveero007@gmail.com

⁴Student, Department of Computer Science, PDA College of Engineering, Kalaburagi, India.
mdasim4627@gmail.com

⁵Professor, Department of Computer Science, PDA College of Engineering, Kalaburagi, India.
sudhapareddy@pdaengg.com

ABSTRACT

Cloud computing faces growing security challenges due to its distributed nature and rapid adoption, including data breaches, account hijacking, and misconfigurations. This paper examines key threats exploiting shared infrastructure vulnerabilities and explores emerging solutions such as Zero Trust architecture and AI-driven threat detection. This paper examines four major security challenges, along with three innovative countermeasures, supported by real-world case studies from education, disaster recovery, and enterprise environments. The results show that integrating Zero Trust principles with machine learning enables strong and reliable defense mechanisms for organizations deploying cloud services at scale.

Keywords: Cloud Computing, Zero Trust Architecture, Security Challenges, AI-Based Threat Detection, Cloud-Native Security.

1.INTRODUCTION

Cloud computing has transformed modern IT infrastructure by offering scalable, on-demand resources over the internet. This shift helps organizations reduce capital costs while enabling easy access to services from anywhere in the world. However, moving to the cloud also brings new and complex security challenges. Recent incidents in 2025, such as the Snowflake data breach, highlight the ongoing vulnerabilities in cloud environments. The distributed nature of cloud systems, along with shared infrastructure and increasingly complex configurations, expands the attack surface beyond what traditional data center models were designed to handle. This paper addresses critical security threats in cloud environments and evaluates emerging defence mechanisms. We focus on four primary challenges: data breaches through misconfigurations (affecting 32% of cloud resources), account hijacking, insecure APIs, and insider threats. We then analyse 3 solution categories: Zero Trust architecture, AI-powered anomaly detection, and cloud-native security tools. The remainder of this paper is organized as follows: Section II examines key security challenges, Section III discusses emerging solutions with technical details, Section IV presents real-world use cases, and Section V concludes with recommendations for practitioners.

2.LITERATURE SURVEY

[1] Cloud Security Alliance (2025): The Cloud Security Alliance (CSA) presented the report “Top Threats to Cloud Computing 2025,” which outlines the most significant security risks affecting cloud environments. The report identifies misconfigurations, weak identity and access management, insecure APIs, account hijacking, and shared technology vulnerabilities as major contributors to cloud security incidents. It emphasizes that the distributed and dynamic nature of cloud infrastructure increases the attack surface compared to traditional on-premise systems. The study highlights the limitations of perimeter-based security and recommends adopting Zero Trust Architecture, continuous verification, and automated monitoring as effective mitigation strategies. This report provides a strong foundation for understanding modern cloud security challenges.

[2] Orca Security (2025): Orca Security's "2025 State of Cloud Security Report" presents a data-driven analysis of cloud security risks based on large-scale cloud environment assessments. The report reveals that a significant percentage of cloud workloads are exposed due to misconfigurations, excessive permissions, and unpatched vulnerabilities. It also highlights the growing complexity of multi-cloud environments, which makes centralized security management more challenging. The study stresses the importance of continuous visibility, risk prioritization, and automated remediation. These findings reinforce the need for intelligent and proactive cloud security solutions.

[3] Cast AI (2025): Cast AI discussed "7 Cloud Security Challenges and How to Solve Them," focusing on practical issues faced by organizations adopting cloud services. The article identifies challenges such as lack of visibility, insecure APIs, poor access controls, and inadequate monitoring. It emphasizes that security must be integrated into cloud operations rather than treated as an afterthought. The authors propose cloud-native security practices, automation, and policy-based controls as effective countermeasures. This work highlights the importance of operational security awareness in cloud deployments.

[4] Gigamon (2025): Gigamon's report on "The Future of Cloud Security" explores emerging trends shaping cloud security practices. The study discusses the increasing role of deep observability, AI-driven threat detection, and Zero Trust frameworks in modern cloud environments. It highlights how encrypted traffic, hybrid cloud models, and remote work have changed threat landscapes. The report concludes that future cloud security solutions must be adaptive, intelligent, and capable of real-time threat detection.

[5] Exabeam (2025): Exabeam published "61 Cloud Security Statistics You Must Know in 2025," providing statistical insights into cloud security incidents and trends. The report indicates a steady rise in identity-based attacks, data breaches caused by misconfigurations, and delayed threat detection. These statistics underline the need for stronger identity controls, behavioral analytics, and automated incident response mechanisms. The data supports the argument that traditional security approaches are insufficient for modern cloud ecosystems.

[6] Darktrace (2021): Darktrace's study "The 10 Most Common Cloud Security Threats" identifies prevalent attack vectors such as insider threats, credential theft, malware, and denial-of-service attacks. The work emphasizes the importance of AI-based behavioral analysis to detect previously unknown threats. Although published earlier, the study remains relevant as many of the identified threats continue to evolve and impact cloud infrastructures.

[7] Google Cloud (2025): Google Cloud's documentation on "What is Zero Trust?" explains the principles and implementation of Zero Trust Architecture. The model eliminates implicit trust by continuously verifying users, devices, and applications before granting access. The study highlights least-privilege access, micro-segmentation, and continuous authentication as core principles. This work provides a conceptual framework for designing secure cloud systems.

[8] Wiz (2024): Wiz presented "Cloud Security Best Practices: 22 Steps for 2025," outlining practical guidelines for securing cloud environments. The study emphasizes identity management, vulnerability scanning, continuous monitoring, and DevSecOps integration. It highlights the importance of embedding security into the cloud development lifecycle. These best practices align closely with modern cloud-native security strategies.

[9] AccuKnox (2025): AccuKnox's article "Zero Trust: The Absolute Solution to Cloud Security" discusses the effectiveness of Zero Trust models in mitigating cloud threats. The study explains how continuous authentication, policy enforcement, and micro-segmentation reduce attack impact. It also highlights the role of automation and AI in enforcing Zero Trust policies at scale. This work supports the adoption of Zero Trust as a core cloud security strategy.

3.METHODOLOGY

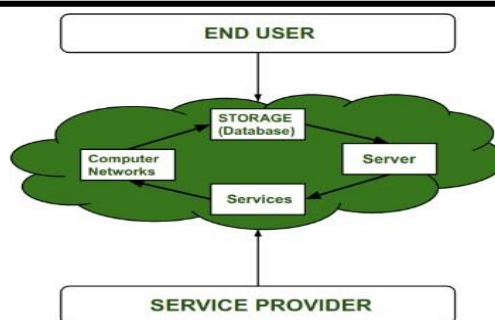


Fig. 1. Cloud Security Architecture Integrating Zero Trust and AI-Based Threat Detection

Figure 1 illustrates a cloud security architecture that combines Zero Trust principles with AI-driven threat detection. All users and devices must undergo continuous identity verification before accessing cloud resources, eliminating implicit trust. The Zero Trust layer enforces least-privilege access and micro-segmentation to reduce lateral movement during breaches. Cloud services such as applications, databases, and APIs are continuously monitored by machine learning models that analyze behavioral patterns to detect anomalies in real time. This integrated approach effectively mitigates common cloud security threats such as misconfigurations, account hijacking, insecure APIs, and insider attacks, making it suitable for large-scale cloud deployments.

3.1 CLOUD SECURITY CHALLENGES

A. Data Breaches and Misconfigurations: Cloud infrastructure complexity creates misconfiguration vulnerabilities. The 2024 Snowflake incident exemplifies this threat, where attackers accessed customer accounts through improperly configured authentication settings. Compromised credentials remained undiscovered for extended periods, highlighting gaps in continuous monitoring practices. Misconfiguration stems from: inadequate access control policies, improper API permissions, and insufficient audit logging. Organizations struggle to maintain consistent security postures across multiple cloud providers and services.

B. Account Hijacking and Credential Theft: Attackers exploit weak password practices and credential reuse across platforms. Once compromised, account credentials enable unauthorized data access, malware deployment, and lateral movement within cloud infrastructure. The threat persists because users frequently employ identical passwords across personal and professional accounts.

C. Insecure APIs and Denial-of-Service Attacks: Cloud services expose APIs for integration and automation. Weak API security allows attackers to: (1) bypass authentication mechanisms, access sensitive data, and manipulate service functionality. Distributed denial-of-service (DDoS) attacks overwhelm cloud services with traffic floods, causing service unavailability.

D. Insider Threats and Skills Shortage

Internal security incidents from disgruntled employees or negligent administrators pose significant risks. Additionally, shortage of cloud security expertise results in: inconsistent security implementations, delayed incident response, and inadequate monitoring across multi-cloud environments.

Challenge	Impact	Example
Misconfigurations	Data exposure	Snowflake 2024 breach
Account Hijacking	Resource control loss	Credential theft
Insecure APIs	Unauthorized access	Hacker interference

DoS Attacks	Service downtime	Traffic overload
-------------	------------------	------------------

Table 1: Primary Security Challenges in Cloud Environments.

3.2 EMERGING SECURITY SOLUTIONS

A. Zero Trust Architecture

Zero Trust eliminates implicit trust assumptions, treating every access request as potentially malicious. This model verifies identity and device posture before granting resource access. Key principles include:

- 1. Continuous Verification:** Every user, device, and request undergoes authentication and authorization checks.
- 2. Least Privilege Access:** Users receive only minimum permissions necessary for their role.
- 3. Micro-Segmentation:** Networks divide into smaller security zones, limiting lateral attacker movement.

Zero Trust reduces breach impact by containing compromised credentials to limited resources. Organizations implementing Zero Trust report 47% reduction in security incidents.

B. AI and Machine Learning for Threat Detection

Machine learning models analyse historical data to identify abnormal behaviour patterns. Real-time anomaly detection enables: (1) early threat identification, (2) automated response triggering, and (3) adaptive threat intelligence. AI systems outperform rule based detection by adapting to novel attack methodologies. Cloud providers including AWS, Azure, and Google Cloud integrate ML-based security services that detect threats 60% faster than traditional methods.

C. Cloud-Native Security Tools and Best Practices

Modern defence requires multi-layered approaches:

- Multi-factor authentication (MFA) enforces identity verification across multiple channels.
- Continuous monitoring and patch management reduce exposure windows.
- API gateways control and inspect all application-to-service communications.
- DevSecOps integration embeds security throughout software development pipelines. Data encryption (at-rest and in-transit) protects information from interception and unauthorized access.

Cloud-Native Application Protection Platforms (CNAPP) provide unified visibility and control across hybrid cloud deployments, simplifying security management.

3.3 REAL-WORLD APPLICATIONS

A. Education Sector: Student Data Protection

Universities deploy Zero Trust architecture to protect sensitive student records in Google Cloud environments. Multi-factor authentication ensures only authorized faculty and students access assignment repositories and grades. This approach successfully prevented unauthorized access during widespread remote learning periods in 2023–2024.

B. Enterprise Disaster Recovery: Ransomware Mitigation

Financial institutions utilize AI-powered anomaly detection in AWS to identify ransomware-like encryption activities. Automated responses trigger immediate backup restoration and incident notifications, reducing recovery time objectives from hours to minutes.

C. Multi-Cloud Management: Policy Consistency

Global enterprises maintain consistent security policies across AWS, Azure, and Google Cloud using centralized management platforms. This approach reduces compliance audit findings by 35% and simplifies policy updates across all cloud providers.

4.CONCLUSION

Cloud security requires proactive, automated defences beyond traditional perimeter-based approaches. Zero Trust architecture and AI-driven threat detection provide effective countermeasures to evolving threats. Organizations must: (1) implement continuous verification mechanisms, (2) deploy machine learning-based anomaly detection, and (3) adopt cloud-native security tools. Future research should address quantum computing threats to current encryption standards and investigate automated incident response coordination across multiple cloud providers. The rapid evolution of cloud computing necessitates continuous security improvement. Practitioners must balance operational efficiency with robust security postures to enable safe cloud adoption.

REFERENCES

- [1] Cloud Security Alliance, "Top Threats to Cloud Computing 2025," Cloud Security Alliance, Sep. 2025. [Online]. Available: <https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2025>. [Accessed: Nov. 30, 2025].
- [2] Orca Security, "2025 State of Cloud Security Report," Orca Security, Jul. 2025. [Online]. Available: <https://orca.security/lp/2025-state-of-cloud-security-report/>. [Accessed: Nov. 30, 2025].
- [3] Cast AI, "7 Cloud Security Challenges and How to Solve Them," Cast AI, Oct. 21, 2025. [Online]. Available: <https://cast.ai/blog/7-cloud-security-challenges-and-how-to-solve-them/>.
- [4] Gigamon, "The Future of Cloud Security: Cloud Security Trends," Gigamon, Aug. 26, 2025. [Online]. Available: <https://blog.gigamon.com/2025/08/26/the-future-of-cloud-security-cloudsecurity-trends/>.
- [5] Exabeam, "61 Cloud Security Statistics You Must Know in 2025," Exabeam, Nov. 5, 2025. [Online]. Available: <https://www.exabeam.com/explainers/cloud-security/61-cloud-securitystatistics-you-must-know-in-2025/>.
- [6] Darktrace, "The 10 Most Common Cloud Security Threats," Darktrace, Dec. 2021. [Online]. Available: <https://www.darktrace.com/cyber-ai-glossary/the-most-common-cloudsecurity-threats>.
- [7] Google Cloud, "What is Zero Trust?" Google Cloud, Nov. 20, 2025. [Online]. Available: <https://www.darktrace.com/cyber-ai-glossary/the-most-common-cloudsecurity-threats>.
- [8] Wiz, "Cloud Security Best Practices: 22 Steps for 2025," Wiz, Dec. 22, 2024. [Online]. Available: <https://www.wiz.io/academy/cloud-security-best-practices>.
- [9] AccuKnox, "Zero Trust: The Absolute Solution to Cloud Security," AccuKnox, Sep. 18, 2025. [Online]. Available: <https://accuknox.com/blog/zero-trust-cloud-security-future>.