International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Trends and Challenges in Cloud Computing Security — Literature-Based Study

Pavan wavhal, Kunal Sawant, Kartik Tambolkar

Abstract

Cloud computing continues to reshape the digital world by offering scalability, flexibility, and cost efficiency to organizations of all sizes. However, this growing dependence on cloud platforms has created new, complex security concerns for organizations. This research paper discusses the latest trends and challenges in cloud computing security based on recent published research papers, surveys, and industry reports from 2023 to 2025.

It also highlights key developments including the emergence of Zero Trust Architecture, the introduction of DevSecOps in the software development pipeline, and the use of AI and ML to spot threats ahead of time. However, comprehensive deployment of advanced security tools will be required for better. management of hybrid and multi-cloud environments, which is expected to involve Cloud *Native Application Protection Platforms.*

Keywords

Cloud Security, Zero Trust, CNAPP, AI in Security, Multi-Cloud, DevSecOps, Data Protection, Misconfiguration

Objectives

1. To examine the evolution of cloud computing security and understand how it differs from traditional IT security.
2. identify recent trends and technological advancements in cloud protection
3. To explore key challenges such as data breaches, misconfigurations, lack of expertise.
4. To analyze findings from academic studies and industry reports.
5. To propose strategies and recommendations for enhancing cloud security through automation, monitoring, and governance.

INTRODUCTION

Cloud computing has fast become the cornerstone of modern information technology. It permits organizations to store, process, and manage data on remote servers hosted by providers such as AWS, Microsoft Azure, and Google Cloud Platform. This model supports scalability, innovation, and global collaboration while reducing infrastructure costs.

However, as more services and data have moved to the cloud, security has become a pressing issue. Cloud environments are dynamic in nature, interconnected, and shared by multiple tenants. This increases the risk of unauthorized access, data breaches, and configuration errors. Classic perimeter-based security models that protect on-premise systems are no longer sufficient in this distributed environment.

Modern security strategies such as Zero Trust, DevSecOps, and AI-driven threat monitoring are changing the way that cloud infrastructure is defended. Yet, new challenges that include regulatory compliance, human error, and multi-cloud complexity demand constant attention.

The study aims to analyze these emerging trends and challenges in the security of cloud computing using a literature-based approach. It provides insights into current practices, identifies recurring threats, and

suggests practical recommendations to improve the security posture for the evolving cloud ecosystem.

Literature Review

1. Zero Trust and Access Control

Kumar and Mehta (2024) in *"Zero Trust Architecture in Cloud Computing"* emphasized that the Zero Trust model replaces traditional perimeter-based security with continuous verification of users and devices**. [1]**

2. AI and Machine Learning in Cloud Security

Patil et al. (2024) discussed how AI and ML techniques improve intrusion detection and anomaly detection systems in their work *"Machine Learning for Cloud Security: A Systematic Review."* **[2]**

3. Misconfiguration as a Major Threat

Mitchell (2024) highlighted in *"Automatic Identification of Misconfiguration Errors in Cloud Environments"* that more than half of cloud breaches result from simple setup errors like open ports or public storage buckets. **[3]**

4. Multi-Cloud Complexity

The *Thales Global Cloud Security Study (2024)* revealed that over 70% of enterprises operate across multiple cloud providers. This approach improves flexibility but introduces visibility and management problems. **[4]**

5. DevSecOps and Automation

Sharma and Gupta (2025) in *"Integrating DevSecOps for Cloud-Native Security"* demonstrated that embedding security tools in the development process reduces vulnerabilities and speeds up issue detection. **[5]**

Paper Title	Authors	Summary of the Paper	Area Discusse
Zero Trust Architecture for Cloud Computing	Kumar & Mehta	Provides Zero-Trust security model fo cloud systems and explains continuou verification approach.	
AI-Driven Intrusion Detection for Cloud Security	Ahmed, Ali & Khan	Studies Machine Learning based intrusion detection systems for cloud security and identifies future threats.	AI / ML Threa Detection
A Review on Cloud Misconfiguration Vulnerabilities	Mitchell	Analysis of major cloud misconfigurations, their role in breaches, and automated tools to prevent them.	Cloud Misconfigurat & CSPM
DevSecOps Security Integration in Cloud	Sharma & Gupta	Discusses integration of DevSecOps practices, Shift-Left security, and automated CI/CD scanning.	DevSecOps & CI/CD Securit
Cloud-Native Application Protection Platforms (CNAPP): A Survey	Wang & Li	Reviews cloud-native security platforms combining CSPM, CWPP, identity security into CNAPP solutions.	Cloud-Native Security Tools (CNAPP)
Multi-Cloud Security Challenges and Solutions	Hawlader & Hossain	Identifies multi-cloud risks, lack of common policy framework, and suggests unified security orchestration.	Multi-Cloud Security

FINDINGS & SUGGESTIONS

FINDINGS

- Cloud adoption increasing rapidly
- SASE + Zero-Trust becoming standard
- Insider threats and human error remain major risks

- Cloud security skills gap widening

SUGGESTIONS

- Conduct regular cloud security audits
- Provide employee security training
- Use strong identity access controls (IAM, MFA)
- Adopt automated compliance tools
- Implement Zero-Trust & DevSecOps pipeline

METHODOLOGY

1. Research Design

The study uses a descriptive approach to summarize key ideas, trends, and solutions identified in existing literature without performing new experiments.

2. Data Collection

Data was collected from:

- Academic journals such as IEEE, Springer, and IJFMR.
- Industry reports including Thales (2024), Fortinet (2025), and KuppingerCole (2025).
- Survey-based studies and case reports on real-world cloud incidents.

3. Selection Criteria

Only publications from 2023–2025 were considered to ensure up-to-date relevance. Sources were selected for their focus on security trends, technical solutions, and measurable results.

4. Data Analysis

Each source was carefully reviewed to identify recurring trends, challenges, and best practices. The findings were grouped under thematic areas such as AI in security, Zero Trust, DevSecOps, and compliance.

RESULTS

1. Cloud security is moving toward Zero Trust and continuous verification models.

2. AI and ML tools are widely used for anomaly detection and automated threat response.

3. DevSecOps integration reduces vulnerabilities during the development stage.

4. CNAPP platforms are simplifying multi-cloud security management.

5. Misconfigurations remain the leading cause of cloud breaches.

6. There is a global shortage of trained cloud security experts.

DISCUSSION

- Zero Trust is becoming a foundation for modern cloud defense because it minimizes insider risks and enforces strict access control.
- AI and ML enhance detection capabilities but require careful supervision to prevent misuse
- DevSecOps promotes early detection and prevention of vulnerabilities, saving time and resources.
- Persistent misconfigurations highlight the need for automated checks and stronger training.

CHALLENGES & LIMITATIONS

Cloud computing security faces several challenges, such as misconfiguring cloud resources, misuse of identities, and a rise in cyber-attacks. Managing security across different cloud platforms like AWS, Azure, and Google Cloud is complex and requires significant expertise.

This study relies on secondary data, and real-time cloud security testing was not conducted. Cloud technology and threats are constantly evolving, so the findings may change over time.

FUTURE TRENDS & OPPORTUNITIES

- **Secure Edge Solutions**: Securing cloud and remote workforce access via Secure Access Service Edge will drive increased demand for network-security professionals.
- **AI-Security Research:** Opportunities in developing AI-powered threat prevention and smart anomaly systems.
- **Security by Design-DevSecOps:** In all cloud projects, security shall be integrated right from the coding phase.
- **Security Awareness Training:** Growing demand for cloud cybersecurity trainers and consultants.

CONCLUSION

Cloud computing has become the foundation of modern digital transformation. While it offers scalability and innovation, it also exposes organizations to evolving threats. This study concludes that achieving effective cloud security requires adopting Zero Trust models, integrating security into DevOps (DevSecOps), and utilizing AI-powered monitoring for continuous protection.

However, challenges like misconfigurations, human error, skill shortages, and regulatory complexities persist. The results confirm that security success in the cloud depends on cooperation between service providers

REFERENCES

1. Kumar, R., & Mehta, A. (2024). *Zero Trust Architecture in Cloud Computing: A Paradigm*. IJFMR.

2. Patil, S., et al. (2024). *Machine Learning for Cloud Security: A Systematic Review*. JISEM.

3. Mitchell, B. S. (2024). *On the Automatic Identification of Misconfiguration Errors in Cloud-Native Environments*. ACM.

4. Thales Group. (2024). *Global Cloud Security Study*.

5. Sharma, P., & Gupta, N. (2025). *Integrating DevSecOps for Cloud-Native Security*. IJICT.

6. Fortinet. (2025). *Cloud Security Skills Gap Report*.

7. KuppingerCole Analysts. (2025). *Leadership Compass: CNAPP Platforms*.

8. Chen, D., & Zhao, H. (2023). *Cloud Computing Security: Policy Based Control and Future Trends.* **Journal of Cloud Computing**.

9. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2021). *An analysis of cloud computing security issues.* **Journal of Software: Evolution and Process**, Wiley.

10. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2020). *A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities.* **Computers & Security**, Elsevier.

11. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2021). *An analysis of cloud computing security issues.* **Journal of Software: Evolution and Process**, Wiley.

12. Mollah, M., Islam, K., & Islam, S. (2021). *A Review on Data Security in Cloud Computing.* **International Journal of Computer Applications**.

13. Singh, J., Sharma, R., & Gupta, A. (2022). *Cloud Security Issues and Solutions: A Review.* **International Journal of Applied Engineering Research**.

14. *Liao, H., Lin, S., & Wang, Y. (2022).* Zero-Trust Architecture: Principles and Practices in Cloud Security. ***IEEE Access***.