International Journal on Advanced Computer Theory and Engineering
ISSN: 2319 - 2526
Volume 15 Issue 2s (2026) | Pages: 266-272

Cyber Threats in Cloud Computing

Ruksar Zakir Ansari[1], Devyani Bhondele[2], Munmun Puranik[3]

[1,2,3] MCA, Genba Sopanrao Moze College of Engineering

Peer Review Information

Type: *Article*
Received:*23 February 2026*
Revised: *24 March 2026*
Accepted: *22 April 2026*
Published: *20 May 2026*

Abstract

Cloud computing has become a fundamental component of modern IT infrastructure, offering scalability, flexibility, and cost efficiency. However, the rapid growth of cloud adoption has significantly increased exposure to cyber threats such as data breaches, ransomware, insecure APIs, misconfigurations, insider threats, and DDoS attacks. This study presents a comprehensive analysis of these threats using both secondary research and a primary survey conducted among IT students and professionals in Pune. The findings reveal that data breaches, ransomware, and misconfigurations are the most critical threats. The study also identifies key gaps such as low user awareness, weak identity management, and lack of monitoring. Practical solutions including Zero Trust Architecture, IAM, MFA, encryption, and continuous monitoring are proposed to enhance cloud security.
Cloud computing has become a fundamental component of modern IT infrastructure, offering scalability, flexibility, and cost efficiency. However, the rapid growth of cloud adoption has significantly increased exposure to cyber threats such as data breaches, ransomware, insecure APIs, misconfigurations, insider threats, and DDoS attacks. This study presents a comprehensive analysis of these threats using both secondary research and a primary survey conducted among IT students and professionals in Pune. The findings reveal that data breaches, ransomware, and misconfigurations are the most critical threats. The study also identifies key gaps such as low user awareness, weak identity management, and lack of monitoring. Practical solutions including Zero Trust Architecture, IAM, MFA, encryption, and continuous monitoring are proposed to enhance cloud security.

Keywords: Cloud Computing; Cyber Security; Data Breaches; Ransomware; Identity and Access Management (IAM); Zero Trust; Cloud Security

How to Cite This Article

Ansari, R. Z., Bhondele, D., & Puranik, M. (2026). *Cyber Threats in Cloud Computing*. *International Journal on Advanced Computer Theory and Engineering, 15*(2s), 266–272.

Introduction

Cloud computing enables on-demand access to computing resources over the internet. It is widely used across industries such as banking, healthcare, education, and e-commerce. Despite its benefits, cloud computing introduces several security challenges due to shared resources and remote accessibility. Protecting data confidentiality, integrity, and availability has become a major concern for organizations migrating to the cloud.

Cloud computing enables on-demand access to computing resources over the internet. It is widely used across industries such as banking, healthcare, education, and e-commerce. Despite its benefits, cloud computing introduces several security challenges due to shared resources and remote accessibility. Protecting data confidentiality, integrity, and availability has become a major concern for organizations migrating to the cloud.

Cloud computing enables on-demand access to computing resources over the internet. It is widely used across industries such as banking, healthcare, education, and e-commerce. Despite its benefits, cloud computing introduces several security challenges due to shared resources and remote accessibility. Protecting data confidentiality, integrity, and availability has become a major concern for organizations migrating to the cloud.

Cloud computing enables on-demand access to computing resources over the internet. It is widely used across industries such as banking, healthcare, education, and e-commerce. Despite its benefits, cloud computing introduces several security challenges due to shared resources and remote accessibility. Protecting data confidentiality, integrity, and availability has become a major concern for organizations migrating to the cloud.

Background

Major cloud providers such as AWS, Microsoft Azure, and Google Cloud offer services like IaaS, PaaS, and SaaS. Although these platforms provide security features, improper configurations and human errors often lead to vulnerabilities. Research indicates that cyber-attacks are increasing due to poor awareness and weak security practices.

Major cloud providers such as AWS, Microsoft Azure, and Google Cloud offer services like IaaS, PaaS, and SaaS. Although these platforms provide security features, improper configurations and human errors often lead to vulnerabilities. Research indicates that cyber-attacks are increasing due to poor awareness and weak security practices.

Major cloud providers such as AWS, Microsoft Azure, and Google Cloud offer services like IaaS, PaaS, and SaaS. Although these platforms provide security features, improper configurations and human errors often lead to vulnerabilities. Research indicates that cyber-attacks are increasing due to poor awareness and weak security practices.

Problem Statement

Organizations face increasing cyber threats that compromise cloud security. Existing research often focuses on specific threats, lacking a holistic approach. There is a need to analyze major threats, identify gaps, and propose effective solutions for real-world cloud environments.

Organizations face increasing cyber threats that compromise cloud security. Existing research often focuses on specific threats, lacking a holistic approach. There is a need to analyze major threats, identify gaps, and propose effective solutions for real-world cloud environments.

Organizations face increasing cyber threats that compromise cloud security. Existing research often focuses on specific threats, lacking a holistic approach. There is a need to analyze major threats, identify gaps, and propose effective solutions for real-world cloud environments.

Objectives

- Identify major cyber threats in cloud computing.
- Analyze user awareness levels.
- Evaluate impact on confidentiality, integrity, and availability.
- Identify gaps in security practices.
- Propose effective solutions.
- Identify major cyber threats in cloud computing.
- Analyze user awareness levels.

- Evaluate impact on confidentiality, integrity, and availability.
- Identify gaps in security practices.
- Propose effective solutions.

Hypotheses

To match academic research standards, both **null** and **alternate** hypotheses are.

Null Hypotheses (H_0)

$H_0$1: Cyber threats do not significantly affect the security and reliability of cloud computing. **$H_0$2:** User awareness does not have any significant relationship with cloud security vulnerabilities.

$H_0$3: Cyber threats do not negatively impact confidentiality, integrity, and availability of cloud systems.

$H_0$4: Security measures such as IAM, MFA, Zero Trust, and encryption do not significantly reduce cyber threats.

Alternate Hypotheses (H_1)

$H_1$1: Cyber threats significantly affect the security and reliability of cloud computing.

$H_1$2: Lower user awareness increases cloud security vulnerabilities.

$H_1$3: Cyber threats negatively impact confidentiality, integrity, and availability of cloud systems. **$H_1$4:** Practical solutions such as IAM, MFA, Zero Trust, and encryption significantly enhance cloud security.

Scope Of Study

Technical Scope

- Cyber Threats such as data breaches, ransomware, insecure APIs, DDoS attacks, insider threats, misconfigurations, and account hijacking.
- Cloud service models (IaaS, PaaS, SaaS).
- Cloud providers: AWS, Azure, Google Cloud.
- Security mechanisms including IAM, MFA, Zero Trust, encryption, continuous monitoring and API gateways & API security.

Geographical Scope

Survey participants (IT students and professionals) from Pune region.

Research Scope

Mixed-method study including secondary research and primary survey. Focus on identifying patterns, gaps, impacts, and solutions. Analysis includes qualitative and quantitative insights.

Literature Review

Existing literature on cloud computing security highlights a wide range of threats and vulnerabilities that arise due to the dynamic and shared nature of cloud environments. Early studies by Bhadauria and Sanyal (2011) and Jensen et al. (2011) identified fundamental security concerns such as data leakage, insecure interfaces, and lack of user control in cloud infrastructures. These foundational works emphasize that cloud systems are highly susceptible to security risks due to multi-tenancy and virtualization.

Several researchers have identified weak Identity and Access Management (IAM) as a major contributor to cloud security breaches. Poor authentication mechanisms and improper authorization controls often lead to unauthorized access and data exposure (Zissis & Lekkas, 2013; Hashizume et al., 2014). In addition, insecure APIs and interfaces are considered critical vulnerabilities, as they act as entry points for attackers to exploit cloud services (Subashini & Kavitha, 2016).

Data breaches remain one of the most common and severe threats in cloud computing. Studies show that these breaches are primarily caused

by weak access controls, improper encryption practices, and insecure storage mechanisms (Gupta & Khandelwal, 2015; Khan, 2018). Furthermore, the rapid adoption of cloud services has increased the risk of ransomware attacks, where attackers encrypt cloud-hosted data and demand ransom for its recovery (Singh & Chatterjee, 2021; Mishra & Tiwari, 2021).

Another significant concern highlighted in the literature is misconfiguration of cloud resources, which is considered a leading cause of security failures. Misconfigured storage buckets, databases, and access permissions often expose sensitive data to the public (Patil & Deshmukh, 2020; Fernandes et al., 2021). Similarly, insider threats arising from malicious or negligent employees can lead to misuse of privileges and unauthorized data access (Rai et al., 2019).

Distributed Denial of Service (DDoS) attacks are also widely discussed as a major threat to cloud availability. These attacks overwhelm cloud servers with excessive traffic, causing service disruptions and downtime (Somani et al., 2015). Additionally, Zhang et al. (2016) highlight privacy concerns and data confidentiality issues as key challenges in cloud adoption.

To address these challenges, researchers have proposed various security mechanisms and frameworks. Common recommendations include the use of strong encryption techniques, multi-factor authentication (MFA), continuous security monitoring, and implementation of Zero Trust Architecture to ensure strict access control (Sharma et al., 2014; Rai et al., 2019; Singh & Chatterjee, 2021). These measures aim to enhance data protection, reduce vulnerabilities, and improve overall cloud security resilience.

Overall, the literature indicates that while cloud computing offers significant benefits, it also introduces complex security challenges that require robust and multi-layered defense strategies.

Methodology

This study adopts a mixed-method approach combining secondary research and primary survey. Data was collected using a structured questionnaire from 32 respondents. The research design is descriptive and analytical. Analysis methods include percentage and comparative analysis. Ethical considerations such as anonymity and voluntary participation were maintained.

Table 1: Demographic Distribution of Respondents (N = 32)

Sr. No.	Category	Number of Respondents	Percentage (%)
1	IT Students	20	62%
2	IT Professionals	12	38%
3	Aware of Cloud	28	88%
4	Not Aware	4	12%

Results And Findings

The survey results indicate that 88% of respondents are aware of cloud computing. Data breaches (72%), ransomware (59%), and misconfigurations (53%) are identified as major threats. 81% of users have medium to low awareness, and 44% do not use strong authentication measures. These findings highlight significant gaps in cloud security awareness and practices.

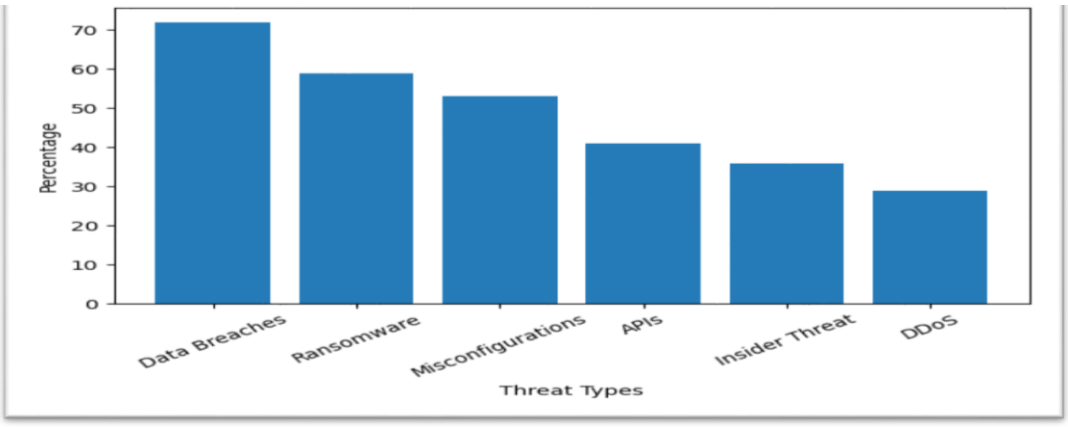

Fig.1. *Distribution of major cyber threats in cloud computing*

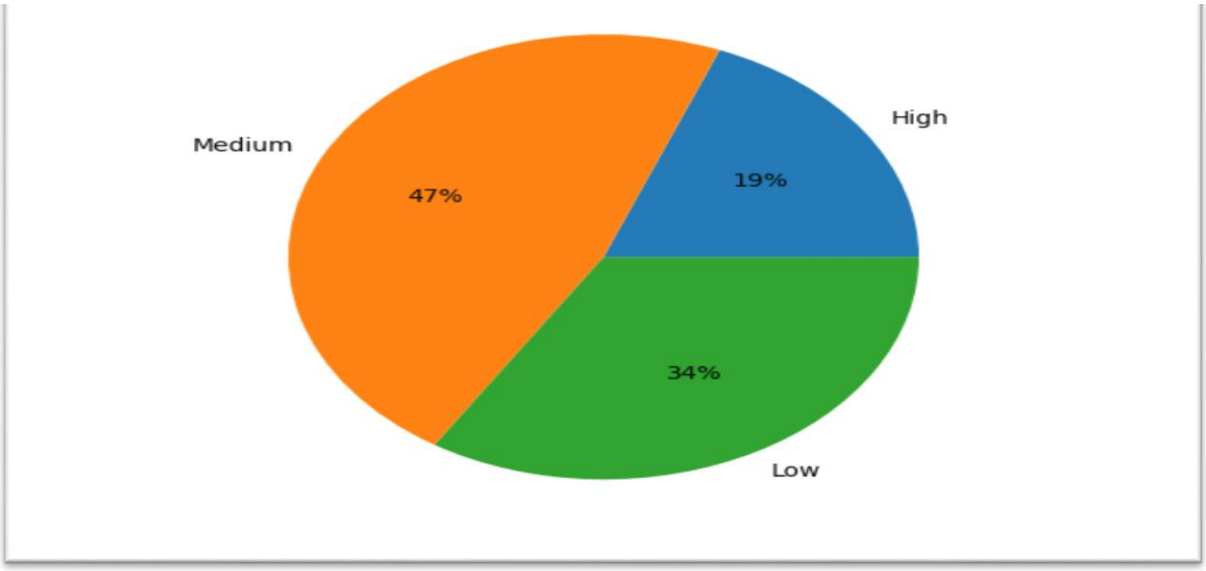

Fig. 2. *User awareness levels regarding cloud security*

Discussion

The findings suggest that while cloud adoption is high, security awareness remains inadequate. Human errors and weak identity management contribute significantly to vulnerabilities. The results align with existing literature, confirming that misconfigurations and lack of monitoring are major concerns. Organizations must focus on improving awareness and implementing strong security frameworks.

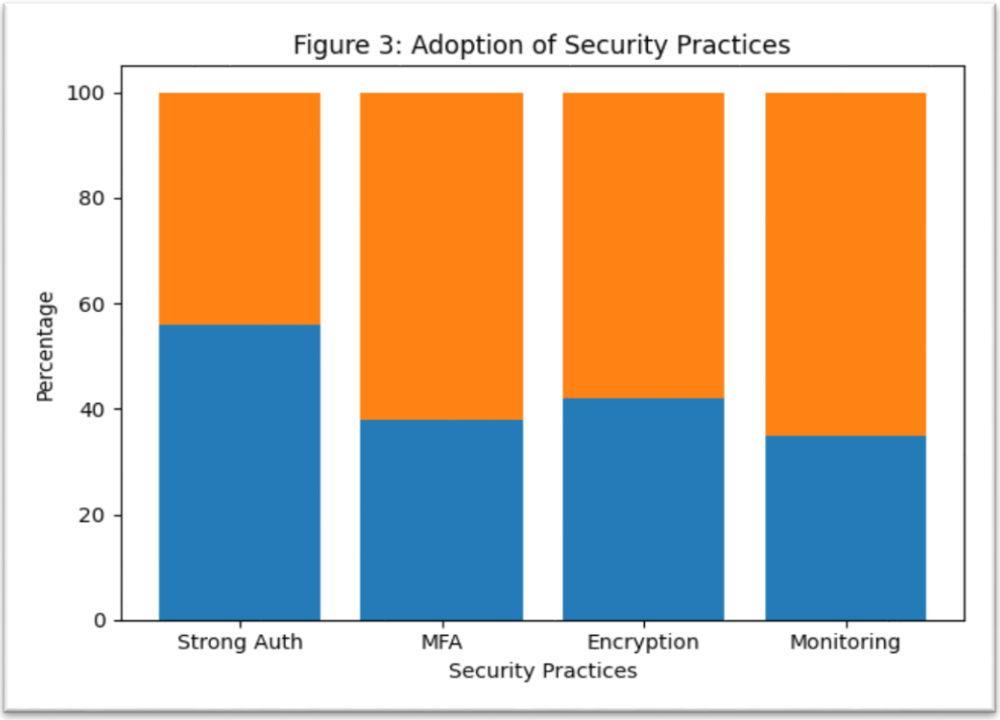

Fig. 3. *Adoption of security practices among users*

Proposed Solutions

Key solutions include implementing Zero Trust Architecture, strengthening IAM and MFA, encrypting data, conducting regular audits, securing APIs, maintaining backups, continuous monitoring, user training, and adopting multi-cloud security strategies.

Key solutions include implementing Zero Trust Architecture, strengthening IAM and MFA, encrypting data, conducting regular audits, securing APIs, maintaining backups, continuous monitoring, user training, and adopting multi-cloud security strategies. These measures

help reduce risks and enhance overall cloud security posture.

Table 2: Mapping of Cyber Threats with Security Solutions

Sr. No.	Threat Type	Recommended Solution
1	Data Breach	Encryption + IAM
2	Ransomware	Backup + Monitoring
3	Misconfiguration	Regular Audits
4	Insecure APIs	API Security + Authentication
5	Insider Threat	Access Control + Monitoring
6	DDoS Attacks	Traffic Filtering & Load Balancer

Key solutions include implementing Zero Trust Architecture, strengthening IAM and MFA, encrypting data, conducting regular audits, securing APIs, maintaining backups, continuous monitoring, user training, and adopting multi-cloud security strategies. These measures help reduce risks and enhance overall cloud security posture.

Limitations

- The study is mainly based on secondary data such as research papers, reports, and published literature.
- Due to time and resource constraints, extensive primary data collection was not conducted.
- The research focuses on commonly observed cyber threats in cloud computing and does not deeply analyse advanced or emerging threats.
- The proposed solutions are general best practices and their effectiveness may vary depending on organizational size and cloud environment.
- Rapid technological changes in cloud computing may affect the long-term relevance of the findings.

Future Scope

- Future research can include primary data collection through surveys, interviews, or case studies of organizations using cloud services.
- Advanced cyber threats such as zero-day attacks, APTs, and AI-driven attacks can be studied in detail.
- The effectiveness of cloud security solutions can be evaluated using real-time attack simulations and practical implementations.
- Comparative studies across different cloud service providers and deployment models can be conducted.
- Integration of emerging technologies like AI, machine learning, and automation for cloud threat detection can be explored further.

Conclusion

Cloud computing continues to reshape how organizations store, process, and manage data. However, the increasing dependence on cloud services has also expanded the threat landscape. This study concludes that cyber threats such as data breaches, ransomware, misconfigurations, insecure APIs, insider threats, and DDoS attacks pose significant risks to cloud environments.

The study concludes that while cloud computing offers numerous advantages in terms of accessibility, scalability, and cost efficiency, it also faces significant cyber threats. Data breaches, ransomware, insecure APIs, and misconfigurations are identified as the most impactful threats. Survey results reveal that user awareness and security practices are still not at a desirable level, contributing to increased vulnerabilities.

The research highlights that effective security in cloud computing requires a combination of advanced technologies such as Zero Trust Architecture, IAM, encryption, and continuous monitoring, along with proper user awareness. Organizations must invest in security tools, enforce strict access controls, and conduct regular training programs to minimize risks.

Overall, a layered and proactive security approach is essential to protect cloud environments from evolving cyber threats. This study provides

practical recommendations that can help users and organizations strengthen their cloud security posture and ensure safe adoption of cloud technologies.

A multi-layered security strategy incorporating Zero Trust Architecture, IAM and MFA, encryption, secure API management, continuous monitoring, and regular configuration audits is essential for improving cloud security. User awareness and training also play a crucial role in reducing human-error-based vulnerabilities.

Acknowledgement

The authors express their sincere gratitude to the faculty and staff of the Department of Information Technology, Genba Sopanrao Moze College of Engineering, Pune, for providing the necessary infrastructure and academic support for this research work.

We would like to extend our heartfelt thanks to our project guide, Prof. Munmun Puranik, for her valuable guidance, continuous support, and insightful suggestions throughout the development of this research on Cyber Threats in Cloud Computing.

We also acknowledge the contributions of various researchers and authors whose published works and studies have provided a strong foundation for our analysis and understanding of cloud security challenges.

Special appreciation is extended to the cloud computing platforms and cybersecurity communities for providing resources, tools, and knowledge that supported this study.

Finally, we thank our peers and colleagues for their constructive feedback and encouragement during the preparation and completion of this research paper.

References

1. Gupta, P., & Khandelwal, R. (2015). *Cloud computing security threats*. *International Journal of Engineering Research and Technology (IJERT).* https://www.ijert.org/cloud-computing-security-threats
2. Rai, A., Singh, R., & Kumar, P. (2019). *Cloud security threats and frameworks: A survey*. *International Journal of Engineering Research and Technology (IJERT).* https://www.ijert.org/cloud-security-threats-frameworks-a-survey
3. Sharma, P., Gupta, D., & Verma, A. (2014). *A survey on cloud security issues and techniques*. *arXiv.* https://arxiv.org/abs/1403.5627
4. Bhadauria, S. S., & Sanyal, S. (2011). *A survey on security issues in cloud computing*. *arXiv.* https://arxiv.org/abs/1109.5388
5. Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2015). *DDoS attacks in cloud computing: Issues, taxonomy, and future directions*. *arXiv.* https://arxiv.org/abs/1512.08187
6. Singh, A., & Chatterjee, K. (2021). *Cloud security challenges and solutions*. *arXiv.* https://arxiv.org/abs/2105.12581
7. Subashini, S., & Kavitha, V. (2016). *A survey on security issues in service delivery models of cloud computing*. *arXiv.* https://arxiv.org/abs/1601.01498
8. Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2011). *On technical security issues in cloud computing*. *arXiv.* https://arxiv.org/abs/1101.5613
9. Zissis, D., & Lekkas, D. (2013). *Addressing cloud computing security issues*. *arXiv.* https://arxiv.org/abs/1309.2426
10. Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2021). *Security issues in cloud environments: A survey*. *Applied Sciences (MDPI).* https://www.mdpi.com/2076-3417/11/19/9005
11. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2014). *An analysis of security issues for cloud computing*. *Computers (MDPI).* https://www.mdpi.com/2073-431X/3/1/1
12. Khan, M. A. (2018). *Cloud computing security threats and mitigation techniques*. *Management Science Studies Journal.* https://jmss.a2zjournals.com/index.php/mss/article/view/14
13. Patil, S., & Deshmukh, R. (2020). *Study of cloud computing security issues*. *Asian Journal of Computer Science and Technology.* https://ajcst.co/index.php/ajcst/article/view/1946
14. Mishra, P., & Tiwari, S. (2021). *Security challenges in cloud computing*. *International Journal of Recent Innovations in Trends in Computing and Communication.* https://ijritcc.org/index.php/ijritcc/article/view/4249
15. Zhang, Y., Chen, X., & Li, J. (2016). *Security and privacy issues in cloud computing*. *Journal of Electrical and Electronic Engineering.* https://www.sciencepublishinggroup.com/article/10.11648/j.jeee.20160406.11