International Journal of Emerging Research in Computer Science
Volume 2 | Issue 4 | April 2026 | ISSN: 3139-101X (Online)
Available online at: https://ijercs.com/
DOI: https://doi.org/10.59828/ijercs.v2i4.31

A Review on Cloud Security Risks and Security Awareness

Ishwari Nandlal Naik[1]✉, Rushikesh Rajendra Pund[2]✉, Sanket Manaji Kadam[3]✉
Department of Computer Science, PVG's College of Science and Commerce, Pune

Received: 07 April 2026 | **Accepted:** 18 April 2026 | **Published:** 29 April 2026

Abstract

Cloud computing has emerged as a transformative paradigm, providing on-demand access to computing resources such as storage, servers, networks, and applications over the internet.
It offers scalable, flexible, and cost-effective solutions through three primary service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Despite its widespread adoption across industries, cloud computing introduces significant security challenges that organizations and individual users must address proactively. This study explores cloud security risks, user awareness levels, and cloud adoption patterns among a sample of 50 respondents collected via a structured Google Form survey. Data was analyzed using Microsoft Excel and Power BI. The findings reveal that while users demonstrate a general awareness of cloud security risks, they frequently fail to implement adequate security practices. The paper concludes with actionable recommendations for bridging the gap between awareness and practice.
Keywords: *Cloud Computing, IaaS, PaaS, SaaS, Cloud Security, Data Privacy, Scalability, Security Awareness, Cyber Threats.*

1. INTRODUCTION

Cloud computing has revolutionized the way individuals and organizations store, process, and share data. By enabling users to access computing resources over the internet without maintaining physical infrastructure, it has drastically reduced operational costs while improving scalability and accessibility. According to Gartner, global spending on cloud services has grown exponentially over the past decade, underscoring its pivotal role in modern IT strategy. However, this rapid adoption has not been without risk.

Moving sensitive data and critical applications to the cloud exposes organizations to a range of security threats, including unauthorized access, data breaches, misconfigured cloud environments, and compliance violations. The shared responsibility model—where cloud providers secure the underlying infrastructure while customers are responsible for securing their data and applications—creates confusion and gaps in protection when not properly understood.

This paper investigates the current state of cloud security awareness among users, identifies common vulnerabilities and risks, and proposes measures to improve security posture.

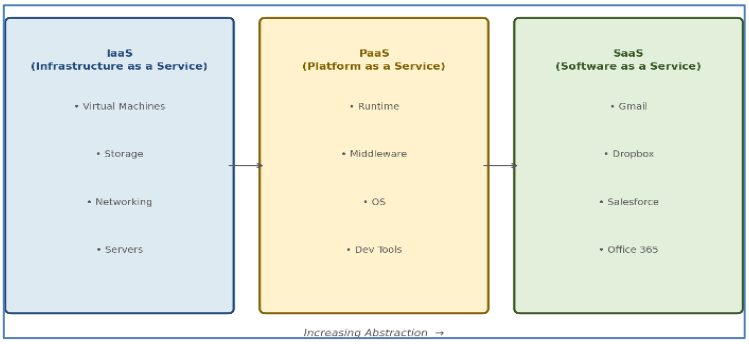

Figure A: Cloud Computing Service Models (IaaS, PaaS, SaaS)

2. OBJECTIVES

The key objectives of this research paper are:

- To study cloud adoption patterns among the surveyed population and identify the most commonly used cloud services.
- To assess the level of security awareness among cloud users regarding risks such as data breaches, unauthorized access, and misconfiguration.
- To identify the principal challenges users face in implementing cloud security best practices.
- To propose practical improvements and recommendations to bridge the gap between awareness and actual security behavior.

3. LITERATURE REVIEW

Cloud computing security has been an active area of research since the early 2010s.

Subashini and Kavitha (2011) identified data security and privacy as the top concerns in SaaS deployments, emphasizing the importance of robust encryption and access control mechanisms.

Similarly, Ziegeldorf and Lekkas (2012) proposed a trust-based security architecture to address multi-tenancy risks inherent in shared cloud environments. More recent studies highlight the human element as a critical vulnerability. Acar et al. (2019) found that a majority of cloud configuration errors stem from user negligence rather than technical flaws in cloud platforms. The Cloud Security Alliance (CSA) consistently ranks misconfiguration as one of the top threats to cloud security in its annual reports. Research on security awareness training indicates that structured programs significantly improve user behavior.

However, uptake remains inconsistent, particularly among non-enterprise users. This study contributes to this body of work by providing survey data on awareness and practice gaps.

4. RESEARCH METHODOLOGY

4.1. Research Design

This study employs a descriptive-analytical research design. A structured questionnaire was used to collect primary data from a sample of cloud users. Both quantitative and qualitative approaches were applied to analyze patterns in cloud usage, security awareness, and security behavior.

4.2 Data Collection

Data was collected via a Google Form survey distributed through online channels. The survey comprised 20 questions covering three domains: cloud adoption and usage patterns, knowledge of security risks, and actual security practices adopted.

4.3 Sampling

Convenience sampling was employed, yielding 50 valid responses. Respondents included students, IT professionals, and small business owners.

4.4 Data Analysis Tools

Collected data was analyzed using Microsoft Excel for descriptive statistics and Microsoft Power BI for data visualization, including pie charts, bar graphs, and heat maps.

5. FINDINGS AND DISCUSSION

5.1 Cloud Adoption Patterns

The survey revealed high usage of cloud services across all respondent categories.

Approximately 82% of respondents reported using at least one cloud service daily. Cost and scalability were the primary drivers of cloud adoption, cited by 68% of respondents.

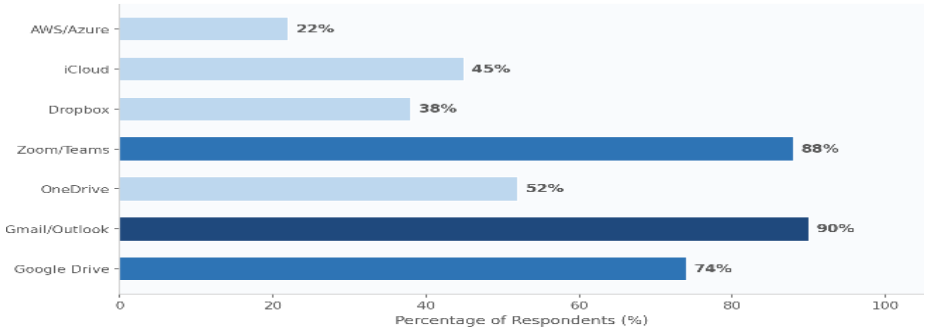

Figure 2: Cloud Services Usage Among Respondents (n=50)

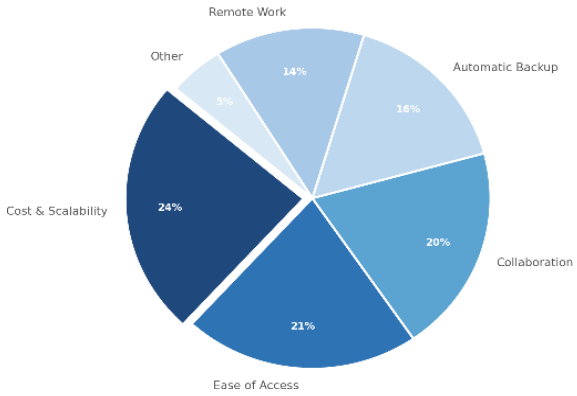

Figure 3: Primary Reasons for Cloud Adoption

5.2 Security Awareness

While 76% of respondents acknowledged awareness of cloud security risks in general, their knowledge of specific threats was considerably lower.

Only 44% could correctly identify phishing attacks as a primary method for account compromise, and just 32% were aware of the shared responsibility model used by major cloud providers.

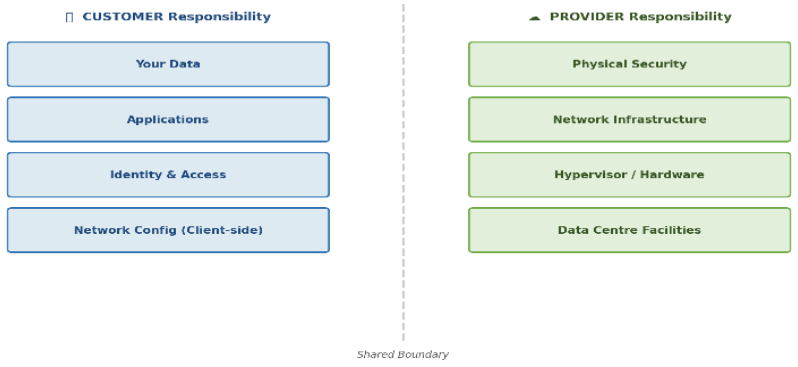

Figure 4: Cloud Shared Responsibility Model

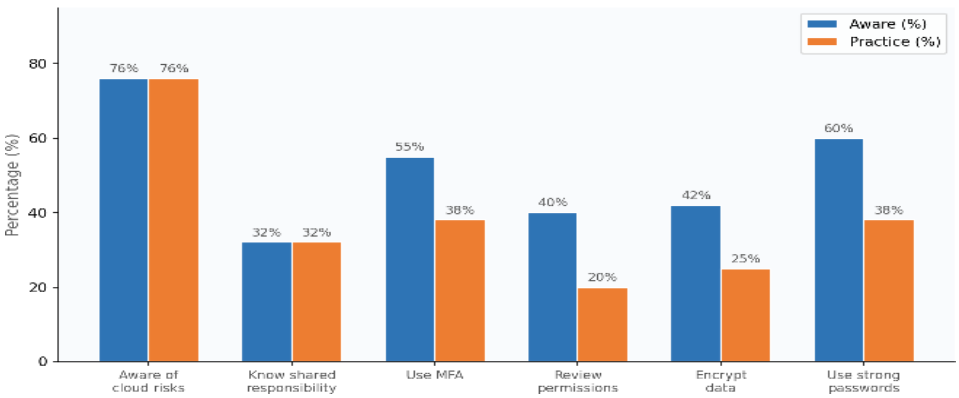

Figure 5: Security Awareness vs. Actual Security Practice

5.3 Security Practice Gaps

Despite their stated awareness, respondents showed significant gaps in actual security practices:

- Only 38% of respondents reported using multi-factor authentication (MFA) consistently.
- 62% had never reviewed access permissions granted to third-party applications.
- 54% relied on default configuration settings when setting up cloud storage.
- Only 28% regularly reviewed their cloud provider's security documentation.
- Password reuse across cloud services was reported by 46% of respondents.

5.4 Key Security Risks Identified

- Based on survey data and supporting literature, the following risks were identified as the most prevalent:
- Misconfigured cloud storage buckets and default permissions.
- Weak or reused passwords lacking complexity requirements. Inefficient use of encryption for data in transit and at rest.
- Lack of regular security audits and access control reviews.
- Limited awareness of regulatory compliance requirements (GDPR, IT Act 2000).

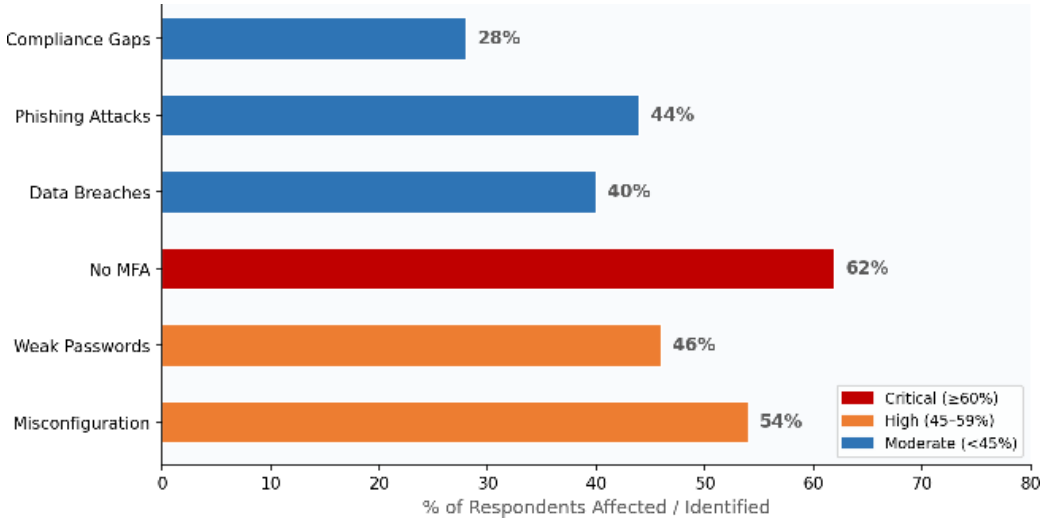

Figure 6: Top Cloud Security Risks Identified

6. Recommendations

Based on the findings, the following recommendations are proposed:

- Mandatory Security Awareness Training: Implement role-specific cloud security training covering the shared responsibility model, common attack vectors, and access management best practices.
- Enable Multi-Factor Authentication: All cloud accounts, especially those holding sensitive data, should enforce MFA as a minimum security requirement.
- Regular Configuration Audits: Periodically review cloud configurations, permissions, and access logs.
- Automated tools such as AWS Trusted Advisor can help identify misconfigurations.
- Strong Password Policies: Enforce password complexity requirements and encourage the use of password managers to reduce password reuse.
- Data Classification and Encryption: Sensitive data should be classified and encrypted before uploading to cloud storage.
- Encryption keys should be managed by the data owner.
- Incident Response Planning: Develop and regularly test cloud-specific incident response plans to minimize the impact of security breaches.

7. Conclusion

Cloud computing is an indispensable component of modern digital infrastructure, offering significant benefits in cost efficiency, scalability, and accessibility.

However, the rapid adoption of cloud services has outpaced the development of an effective security culture among users. This study demonstrates that while a majority of users are broadly aware of cloud security risks, this awareness does not consistently translate into secure behavior.

The most significant gaps identified include low adoption of multi-factor authentication, poor password hygiene, over-reliance on default configurations, and limited familiarity with the shared responsibility model.

Organizations must invest in creating a security-conscious culture where awareness and practice are closely aligned. Future research should expand the sample size and employ longitudinal methods to assess whether targeted interventions improve security behavior over time.

REFERENCES

[1]. Subashini, S., & Kavitha, V. (2011).A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1–11.

[2]. Zissimopoulos, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583–592.

[3]. Acar, Y., et al. (2019). How Internet Resources Might Be Helping You Develop Faster but Less Securely. IEEE Security & Privacy, 15(2), 26–35.

[4]. Cloud Security Alliance. (2024). Top Threats to Cloud Computing: Pandemic 11. CSA Report.

[5]. Mell, P.,&Grance, T. (2011). The NIST Definition of Cloud Computing (Special Publication 800-145). NIST.

[6]. Gartner Inc. (2024). Forecast: Public Cloud Services, Worldwide. Gartner Research Report.

[7]. Amazon Web Services. (2023). AWS Shared Responsibility Model. https://aws.amazon.com/compliance/shared-responsibility-model/

[8]. Microsoft Azure.(2023). Security best practices and patterns. Azure Documentation.

Cite this Article:

Naik, I.N., Pund, R.R., Kadam, S.M. (2026). A Review on Cloud Security Risks and Security Awareness. International Journal of Emerging Research in Computer Science, 2(4), 18–22.

Journal URL: *https://ijercs.com/*

DOI: https://doi.org/10.59828/ijercs.v2i4.31