World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Cloud data security: An empirical study of user awareness, perceived risks and protective measures

Omoshalewa Anike Adeosun *

Applied Cybersecurity, Faculty of Computing, Engineering and Science, University of South Wales, Newport, UK.

World Journal of Advanced Research and Reviews, 2025, 25(02), 1185-1192

Publication history: Received on 26 December 2024; revised on 08 February 2025; accepted on 11 February 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.2.0399

Abstract

Cloud-based storage services have grown exponentially, offering many advantages, such as scalability, affordability, and instantaneous data access. However, the increased reliance on servers owned and operated by third-party providers for cloud storage raises concerns regarding data security and vulnerability efficiency. Therefore, this study investigated the vulnerability of cloud-based storage services following a quantitative approach and using a random sampling methodology and online surveys to gather data from professionals. The survey data was analyzed descriptively to summarize the responses and to provide an overview of the responses. Statistical techniques such as frequency distributions, means, and percentages were measured using SPSS. Results revealed that cloud service users were familiar with the prevailing threats such as ransomware, zero-day vulnerabilities, data sabotage, encryption, misconfiguration, insider threats, and overconfidence resonating from the usage. A substantial portion, representing 40.9%, emphasized the implementation of two or more security measures as critical steps for enhancing cloud storage security, 22.7% recommended Multi-Factor Authentication (MFA), 13.6% each mentioned Access Control and management, Employer Training and Awareness, and Regular Audit and Monitoring. 9.2% each, advocated for Data Encryption, Misconfiguration leading to data loss, and Manual Backup, while 4.5% each proposed measures like Regular patch Update, Integration of AI for threat detection like Quantum Resistance Encryption, and Implementing Zero Trust Principles. Recommendations and proposed measures crafted from participant insights were validated by industry professionals with expertise in cloud-based services.

Keywords: Cloud-based storage services; Data security; Vulnerability efficiency; Multi-Factor Authentication (MFA)

1. Introduction

Cloud-based storage services have emerged as a popular solution for individuals and organizations seeking scalable and convenient data storage options (1). With the advent of cloud computing technology, the storage landscape has shifted from traditional on-premises solutions to cloud-based models that offer numerous advantages in terms of flexibility, accessibility, and cost-efficiency (2). This distributed storage infrastructure allows for easy scalability, as additional storage capacity can be allocated on demand, eliminating the need for physical infrastructure expansion (3).

Data management has experienced a massive shift in the evolution of cloud-based storage services, which has brought along scalability, affordability, and easy access (4). Meanwhile, relying on third-party providers leads to a security vulnerability and less data protection (2). Cloud storage systems are vulnerable to cyber threat attacks including data breach, unauthorized access, and data loss, which consequently attack sensitive information (5). With the increase of private data stored in the cloud, security becomes a big issue (6). Therefore, an analysis of cloud storage risk is necessary to safeguard data integrity, confidentiality, and accessibility (7). Understanding the vulnerabilities and potential threats is the first step toward implementing effective security measures and mitigating the risks (8). The adoption of cloud-

* Corresponding author: Omoshalewa Anike Adeosun

based storage services has revolutionized data management for individuals and organizations, but it has also raised concerns about data security and vulnerability (9). Data protection and data accessibility must be ensured by examining thoroughly the risks in cloud storage (10). However, existing studies do not deal with the emerging threats of cloud services. This study fills these gaps by examining cloud storage security, identifying vulnerabilities, and proposing countermeasures to risk. It looks at topics such as data breaches and unauthorized access to more effectively fortify data protection stratagems for organizations and individuals. The study seeks to understand the cloud data security challenges and the mitigation techniques by exploring the security challenges and the mitigation techniques. The findings are critical to building better security measures and adapting to the challenges of cloud storage threats that are evolving.

2. Materials and methods

The research design used is a quantitative methodology, to examine the vulnerability of cloud-based storage services and provide security assessments and suggestions.

2.1. Sampling Technique and Sample Size

Sampling is the process of choosing an appropriate subset of the population, for research purposes (11). Random and purposive sampling was used in this study to investigate cloud storage vulnerabilities. Random sampling ensured the representation of individual users, corporations, and organizations, all of which with an unbiased view. Cloud security specialists, service providers, and organizations with recent breaches were the targeted group for purposive sampling and the resulting expert insights. Twenty-two (22) participants were selected from cloud service providers, cybersecurity organizations, academic researchers, and individual users of cloud storage services. Such strategies were necessary to handle the complexity of cloud storage vulnerabilities and to form proper security recommendations, which are thorough.

2.2. Population of the Study

The study's target audience consists of experts in the field of cloud storage security, and individual users utilizing cloud storage services. This study's emphasis on the diverse study group is critical in the pursuit of understanding and improving cloud storage security. It aims to strengthen these people, companies, organizations, institutions, and entities' digital spaces through its analysis and subsequent recommendations, thereby enhancing the security of cloud-based storage services.

2.3. Data Collection Methods

A quantitative approach was used for data collection. The quantitative method employed in collecting data involved constructing an online survey which was administered to gather data from organizations and individual users utilizing cloud storage services. These included professionals from cloud service providers, cybersecurity organizations, and academic researchers. Their perceived vulnerabilities, experiences with security incidents, and satisfaction with the security measures put in place by cloud service providers were the main subjects of the online surveys. The survey was designed using established survey methodologies, ensuring validity and reliability.

2.4. Data Analysis

The survey data was analyzed descriptively to summarize the responses and provide an overview of the perceived vulnerabilities, security incidents, and satisfaction with security measures. Statistical techniques such as frequency distributions, means, and percentages were utilized. The quantitative analysis served as a critical avenue for assessing vulnerabilities on a quantitative scale, deriving statistical insights, and offering a data-driven foundation for the formulation of recommendations.

3. Results and discussion

In the quantitative analysis of this research on cloud-based storage services, multifaceted insights, and critical observations were uncovered through a comprehensive examination of respondents' perceptions and experiences.

3.1. Demographic Characteristics.

Results from the demographic characteristics of respondents are revealed in Table 1. A majority (59.1%) of participants identified as an IT/Security Professional; this is a strong representation of the people who are directly responsible for cloud storage security. In addition, 22.7% held managerial/executive roles, 18.2% were individual users (MOE ± 0.35),

and 18.2% were senior managers. The most common cloud service was Microsoft OneDrive (40.9%) and Google Drive at 27.3%. MOE ± 0.87: Amazon and iCloud also had smaller shares. With regards to usage time 40.9% used cloud storage for more than 5 years, 36.4% for 1 – 3 years, 13.6% for 3 – 5 years, and 9.1% less than 1 year (MOE ±0.48). Other sectors also included finance/banking (18.2%), education (9.1%), healthcare/medical (4.5%), manufacturing (4.5%), and other sectors (MOE ±0.53) each had a smaller share at 63.6%. These findings, however, demonstrate the strength of IT professionals, the popularity of OneDrive and Google Drive, and the wide variety in usage duration and industry representation.

Table 1 Respondents' Work-demographic Characteristics N=22

Demographic characteristics	Frequency	Percentage (%)	Margin of Error at 95% Confidence Interval
What is your role or position within your organization, or are you an individual user of cloud storage services?			
IT/Security Professional	13	59.1	0.35
Manager/Executive	5	22.7	
User/Individual	4	18.2	
Which cloud storage software or service do you or your organization primarily use?			
Google Drive	6	27.3	0.87
Microsoft OneDrive	9	40.9	
Amazon S3	1	4.5	
iCloud	1	4.5	
two or more	5	22.7	
How long have you been using cloud storage services?			
Less than 1 year	2	9.1	0.48
1-3 years	8	36.4	
3-5 years	3	13.6	
Over 5 years	9	40.9	
Which industry sector best describes your organization (if applicable)?			
Technology/IT	14	63.6	0.53
Finance/Banking	4	18.2	
Healthcare/Medical	1	4.5	
Education	2	9.1	
Manufacturing	1	4.5	

3.2. Perceived Vulnerabilities

Table 2 presents the examination of respondents' perceptions of perceived vulnerabilities in cloud-based storage systems. Of the participants, a greater proportion (54.5%) indicated that they were extremely concerned about the security of data saved in cloud-based storage systems. Furthermore, 9.1% of respondents expressed greater concern, compared to 22.7% who expressed ordinary concern. Just 4.5% of respondents said they were less anxious, and 9.1% said they were not at all concerned. This wide range of concerns indicates that a sizable percentage of respondents have serious concerns regarding the security of their data when using cloud storage services (MOE ±0.60). Of the participants, 31.8% acknowledged that they had experienced security incidents relating to cloud storage services in the previous year, while 68.2% reported no events of this kind. The kinds of incidents differed for people who were subjected to security issues. Notably, 18.2% of events reported involved Data Leakage/Breach, 13.6% involved S3 bucket/Access Restriction problems, and 4.5% each included SQL Injection and Privilege Escalation. The vast majority, or 59.1%, said that these specific instances had nothing to do with their experiences (MOE ± 0.21) (Table 2). These results demonstrate that respondents had serious concerns about the security of data stored in cloud-based storage systems. Many of them

have also reported experiencing a variety of security issues, most notably those involving data breaches and access restrictions. These issues have raised concerns about the vulnerability of sensitive information and the effectiveness of security measures in place (12). This realization emphasizes how crucial it is to fix and mitigate these found vulnerabilities in cloud storage services to improve data security (13).

Table 2 Respondents' Opinion on Perceived Vulnerabilities N=22

Statement	Frequency	Percentage (%)	The margin of Error at 95% Confidence Interval
On a scale of 1 to 5, how concerned are you about the security of data stored in cloud-based storage services?			
Not concerned at all	2	9.1	0.60
Less concerned	1	4.5	
Averagely concerned	5	22.7	
More concerned	2	9.1	
Extremely concerned	12	54.5	
Have you or your organization experienced security incidents related to cloud storage services in the past year?			
Yes	7	31.8	0.21
No	15	68.2	
Please specify the type of security incidents you or your organization experienced			
Data Leakage/Breach	4	18.2	
SQL Injection	1	4.5	
S3 bucket/Access Restriction	3	13.6	
Privilege Escalation	1	4.5	
Not applicable	13	59.1	

3.3. Satisfactory Level with Security Measures and Practices

Data from Table 3 shows that 54.5% were satisfied or extremely satisfied, 22.7 (MOE ± 0.31) had no opinion and the rest were dissatisfied with the security protocols of cloud storage providers. For data encryption before storage, respondents were split almost equally, 45.5 percent encrypt their data and 54.5 percent do not (MOE ± 0.23), suggesting a range of security practices. Surprisingly, though, respondents confirmed using multi-factor authentication (MFA) for accessing their cloud storage accounts — 100% of respondents demonstrate a strong desire to tighten access security. The findings indicate mixed opinions of cloud security measures with a substantial portion satisfied and others tuning out. This aligns with the findings of studies that explained that while encryption practices are near equal distribution, the use of MFA is universal, indicating a security focus on improving access security (14,15).

Table 3 Respondents' Satisfactory Level with Security Measures & Practices N=22

Statement	Frequency	Percentage (%)	Margin of Error at 95% Confidence Interval
How satisfied are you with the security measures put in place by cloud service providers?			
Very Satisfied	5	22.7	0.31
Satisfied	12	54.5	
Neutral	5	22.7	
Do you or your organization encrypt data before storing it in the cloud? Answer Options			
Yes	10	45.5	0.23
No	12	54.5	
Are multi-factor authentication (MFA) mechanisms used for accessing cloud storage accounts?			
Yes	22	100	

3.4. Compliance and Regulations

A large majority of participants (86.4%) were aware of and followed compliance requirements for cloud data (MOE ±0.16) while 13.6% were unaware (Table 4). All respondents (100%) reported that their organization or themselves actively enforce cloud storage security rules (Table 4). A robust commitment to regulations was indicated by 72.7 percent of those following compliance measures who did so consistently. For compliance measures (MOE ±0.36) (Table 4), smaller proportions were reported rarely (18.2%) or seldomly (9.1%). The respondents are very aware of and adhere to cloud storage compliance standards, as most of these respondents have been consistently trying to meet legal requirements. Therefore, organizations need to have a comprehensive enterprise-wide compliance strategy, which includes security procedures, regular monitoring, and working with compliance professionals and services (16).

Table 4 Respondents' Compliance and Regulations N=22

Statement	Frequency	Percentage (%)	Margin of Error at 95% Confidence Interval
Are you aware of the compliance regulations governing data stored in the cloud?			
Yes	19	86.4	0.16
No	3	13.6	
Does your organization or do you take specific steps to ensure compliance with cloud storage security regulations?			
Yes	22	100	
If yes, how often?			
Always	16	72.7	0.36
Seldomly	2	9.1	
Rarely	4	18.2	

3.5. Respondent's Recommendations

Recommendations for making clouds safer were given by respondents. Nearly 40.9% emphasized that multiple security measures should be implemented. Multi-factor authentication (MFA) was specifically suggested by 22.7%, Access Control, Employer training and awareness, and Regular audits and monitoring (13.6% each). To improve cloud security, it takes a layered approach, with multiple measures such as multi-factor authentication, access control, regular audits, and employer-led training to mitigate vulnerabilities (17,18). Advocating smaller percentages (9.2%) for Data Encryption, Misconfiguration, and Manual Backup, 4.5% proposed Regular Patch Updates, AI-Based Threat Detection, and Zero Trust Principles (Table 5). Organizations are ready for evolving threats with advanced strategies including AI-based threat detection, zero trust principles, data encryption, and misconfiguration management (18,19). About 45.5 percent were satisfied and 36.4 percent were very satisfied while 18.2 percent were neutral (MOE ± 0.32). Of note, 13.6% were worried about training, audits, misconfigurations, and backup, and half said that did not apply to their experience (Table 5). The identified challenges were User Awareness/Technical Knowhow (22.7%), Data Privacy (13.6%) and Access Control (9.2%), 54.5% of these being not relevant (Table 5). Respondents also identified areas for improvement, including flexibility and accessibility (40.9%), scalability and cost savings (13.6%), or which did not apply (27.3%). Of those, 72.7 percent thought cloud storage could be as secure as on-premises alternatives, while 27.3 percent disagreed (Table 5). However, they pointed to cloud breaches like Capital One, Verizon, Uber, and Microsoft showing just how complicated cloud security can be. These insights call for additional security methods, user awareness, and improvement in areas like scalability and accessibility (20). Key areas of focus include data privacy, integrity, access control, performance optimization strategies, resource allocation mechanisms, scalability solutions, and emerging technologies such as edge computing, serverless architectures, and containerization (21). This makes it clear that cloud storage vulnerabilities require further research.

Table 5 Respondents' Recommendations N=22

Statement	Frequency	Percentage (%)	Margin of Error at 95% Confidence Interval
In your opinion, what are the most critical security measures organizations should implement to enhance cloud storage security?			
MFA	5	22.7	
Regular Patches Update	1	4.5	
Data Encryption	2	9.2	
Integration of AI for threat detection like Quantum Resistance Encryption	1	4.5	
Access Control & and management	3	13.6	
Implement Zero Trust Principles	1	4.5	
Two or more measures	9	40.9	
How satisfied are you with the security of your organization or your data stored in the cloud?			
Very Satisfied	8	36.4	0.32
Satisfied	10	45.5	
Neutral	4	18.2	
Please share any additional thoughts, concerns, or experiences related to cloud storage security.			
Employer Training and Awareness	3	13.6	
Regular Audit and Monitoring	3	13.6	
Misconfiguration leading to data loss	3	13.6	
Manual Backup	2	9.2	
Not applicable	11	50	
What challenges do you face in balancing the convenience of cloud storage with security?			
Data privacy	3	13.6	
Access control	2	9.2	
User awareness/Technical Know-how	5	22.7	
Not applicable	12	54.5	
What do you believe are the key areas of improvement for cloud storage security?			
Flexibility / Accessibility	9	40.9	
Storage Scalability	3	13.6	
Cost Saving	3	13.6	
Disaster Recovery	1	4.5	
Not applicable	6	27.3	
Do you believe that cloud storage services can be as secure as on-premises solutions?			
Yes	16	72.7	
No	6	27.3	
Are there any specific security incidents or breaches in the cloud that you believe should be highlighted for further research?			

Capital One Data Breach
Verizon Data Exposure
Human Errors & Misconfiguration
Uber Data Breach
Social Media Network Breach (Facebook, LinkedIn)
Toyota Motor Company Breach
Microsoft Security Breach
Sheer Volume of Data per Leak (Obscene Data Volume)

4. Conclusion

The research employs a quantitative approach of integrating participant insights with established frameworks to understand current practices, vulnerabilities, and emerging trends. Participants flagged significant security risks such as ransomware, misconfigurations, zero-day vulnerabilities, and over reliance on cloud service providers. These challenges demonstrate the fluidity of cybersecurity, one where defenses must evolve to meet the ever more complex threat. The findings validate the need for strong measures like access control, multi-factor authentication, encryption, and constant monitoring. The study also emphasizes the necessity for organizations to adopt forward-thinking strategies, including "zero trust architecture," "quantum-safe encryption," and "AI-driven security." These approaches align with evolving cybersecurity paradigms and are pivotal in addressing emerging threats. Education and awareness remain central to these efforts, as they empower users to make informed decisions and mitigate risks effectively. From a wider perspective, the integration of the LESPI framework ensures that the study does not ignore legal, ethical, social, and professional implications, thereby underlining the necessity of privacy, transparency, and following the standard. This study contributes to improving collective resilience to cybersecurity challenges by examining the societal and professional implications of cloud storage security.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest is to be disclosed

Statement of ethical approval

The research ethics board of the University of South Wales gave the ethical approval for this study.

Statement of informed consent

Informed consent was obtained from all participants, outlining the study's objective, procedures, potential dangers, and advantages. Data collection delays, participant privacy concerns, and legal compliance issues were the potential challenges. To prevent misuse, data disclosure, and ethical breaches during the study, the researcher secured data and followed informed consent protocols.

References

[1] Vurukonda N, Rao BT. A study on data storage security issues in cloud computing. *Procedia Computer Science*. 2016;92:128-135. doi:10.1016/j.procs.2016.07.335

[2] Selvamani K, Jayanthi S. A review on cloud data security and its mitigation techniques. *Procedia Computer Science*. 2015;48:347-352.

[3] Alouffi B, Hasnain M, Alharbi A, Alosaimi W, Alyami H, Ayaz M. A systematic literature review on cloud computing security: Threats and mitigation strategies. IEEE Access. 2021;9:58414-58427. doi:10.1109/ACCESS.2021.3073203

[4] Suby M. Cloud data protection and security for 2021: Strategies, statistics, and predictions. 2021. Available from: https://www.securitymagazine.com/articles/95143-cloud-data-protection-and-security-for-2021-strategies-statistics-and-predictions

[5] Ali M, Khan SU, Vasilakos AV. Security in cloud computing: Opportunities and challenges. Information Sciences. 2020;478:145-154.

[6] Hashizume K, Rosado DG, Fernández-Medina E. An analysis of security issues for cloud computing. Journal of Internet Services and Applications. 2013;4(1):5.

[7] Kumar R, Goyal R. On cloud security requirements, threats, vulnerabilities, and countermeasures: A survey. Computer Science Review. 2019;33:1-48.

[8] Riggs H, Tufail S, Parvez I, Tariq M, Khan MA, Amir A, Vuda KV, Sarwat AI. Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Sensors. 2023;23(8):4060. doi:10.3390/s23084060

[9] Soveizi N, Turkmen F, Karastoyanova D. Security and privacy concerns in cloud-based scientific and business workflows: A systematic review. *Future Generation Computer Systems*. 2023;148:184-200.

[10] Alquwayzani A, Aldossri R, Frikha M. Prominent security vulnerabilities in cloud computing. *International Journal of Advanced Computer Science and Applications*. 2024;15:10.14569/IJACSA.2024.0150281.

[11] Sharma G. Pros and cons of different sampling techniques. *International Journal of Applied Research*. 2017;3(7):749-752.

[12] Filkins BL, Kim JY, Roberts B, Armstrong W, Miller MA, Hultner ML, Castillo AP, Ducom JC, Topol EJ, Steinhubl SR. Privacy and security in the era of digital health: what should translational researchers know and do about it? *Am J Transl Res*. 2016 Mar 15;8(3):1560-80. PMID: 27186282; PMCID: PMC4859641

[13] Coppolino L, D'Antonio S, Mazzeo G, Romano L. Cloud security: Emerging threats and current solutions. *Computers & Electrical Engineering*. 2017;59:126-140.

[14] Okeke R, Orimadike S. Enhanced cloud computing security using application-based multi-factor authentication (MFA) for communication systems. *European Journal of Electrical Engineering and Computer Science*. 2024;8:1-8. doi:10.24018/ejece.2024.8.2.593.

[15] Suleski T, Ahmed M, Yang W, Wang E. A review of multi-factor authentication in the Internet of Healthcare Things. *Digit Health*. 2023 May 22;9:20552076231177144. doi:10.1177/20552076231177144. PMID: 37252257; PMCID: PMC10214092.

[16] Rohana N, Ranjan P. Compliance and regulatory challenges in cloud computing: A sector-wise analysis. *International Journal of Global Innovations and Solutions*. 2024;3:10.21428/e90189c8.68b5dea5.

[17] Ajiga D. Designing cybersecurity measures for enterprise software applications to protect data integrity. *Computer Science & IT Research Journal*. 2024;5(8):1920–1941. doi:10.51594/csitrj.v5i8.1451.

[18] Samira Z, Weldegeorgise YW, Osundare OS, Ekpobimi HO, Kandekere RC. Comprehensive data security and compliance framework for SMEs. *Magna Scientia Advanced Research and Reviews*. 2024;12(01):043–055

[19] Obi OC, Dawodu SO, Daraojimba AI, Onwusinkwue S, Akagha OV, Ahmad IAI. Review of evolving cloud computing paradigms: security, efficiency, and innovations. *Computer Science & IT Research Journal*. 2024;5(2):270–292.

[20] Rohan R, Pal D, Hautamaki J, Funilkul S, Chutimaskul W, Thapliyal H. A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*. 2023;9:e14234. doi:10.1016/j.heliyon.2023.e14234.

[21] Ige AB, Kupa E, Ilori O. Best practices in cybersecurity for green building management systems: Protecting sustainable infrastructure from cyber threats. *International Journal of Science and Research Archive*. 2024;12(1):2960–2977. doi:10.30574/ijsra.2024.12.1.1185.