JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURITY OF DATA SHARING IN CLOUD COMPUTING

Ms.Swapnali Sanjay Nayakavade[1], Ms. Vaishali Tanaji Hogale [2],

Prof. Shreyash Sohani [3], Prof. Madhuri Choudhari [4], Prof. Harshada Ahire[5]

12 Students ,Department of Master of Computer Applications, Dr. D. Y. Patil Centre for Management & Research, Chikhali, Pune, India

34 Assistant Professor , Department of Master of Business Administration, Dr. D. Y. Patil Centre for Management & Research, Chikhali, Pune, India

5 Assistant Professor , Department of Master of Computer Application, Dr. D. Y. Patil Centre for Management & Research, Chikhali, Pune, India

Abstract : Cloud computing has become a foundational technology for data storage and sharing, offering scalability,flexibility, and cost-effectiveness. However, this widespread adoption introduces serious concerns regarding data security and privacy, including the risk of data breaches, unauthorized access, and cyber attacks on sensitive information. The shared infrastructure of cloud environments makes it critical to ensure only authorized users access specific information. This project aimed to analyze user awareness and the effectiveness of security measures like encryption and access control in securing shared cloud data. A survey conducted among students and IT professionals revealed that a majority of users are aware of encryption and Multi-Factor Authentication (MFA), and that the use of these practices significantly reduces the risks of data breaches and unauthorized access. The study concludes that the combined role of technology (encryption and Role-Based Access Control - RBAC) and user awareness is vital for achieving secure data sharing in cloud environments.

Keywords **– Cloud Computing, AES(Advanced Encryption Standard) ,RBAC(Role-Based Access Control), MFA(Multi-Factor Authentication.**

I.INTRODUCTION

Cloud computing represents one of the most transformative technological shifts of the 21st century, enabling individuals and large enterprises to store, manage, and share vast amounts of data without reliance on proprietary local infrastructure. Platforms such as AWS, Google Drive, and Dropbox provide unparalleled advantages in terms of cost-efficiency, scalability, and ubiquitous access, rendering them indispensable for modern personal, academic, and professional endovers.

However, the very architecture that grants the cloud its efficiency—the shared infrastructure model—introduces complex and serious concerns regarding data security and confidentiality. When sensitive data, encompassing academic records, corporate intellectual property, or financial details, is entrusted to third-party shared systems, ensuring its integrity and exclusivity becomes paramount. If robust protections are absent or ineffective, the potential for unauthorized access, data breaches, cyber attacks, or insider threats can lead to catastrophic financial, legal, and reputational damage. Consequently, cloud security has escalated into a top strategic priority for both Cloud Service Providers (CSPs) and end-users.

The fundamental defence mechanisms in this environment are technological and centered on data obfuscation and authorization control. Encryption, utilizing standards such as Advanced Encryption Standard (AES) , renders data unreadable to any party lacking the correct decryption key. Access control, particularly Role-Based Access Control (RBAC), meticulously defines and enforces permissions, ensuring that access to specific data sets is granted exclusively to authorized users based on predefined organizational roles. For instance, RBAC prevents a general employee from accessing a comprehensive company database, restricting them only to department-specific files.

II. REVIEW OF THE LITERATURE

The foundational literature on cloud computing identifies inherent challenges tied to its architectural model. Early works, such such as Buyya, Broberg, and Goscinski (2010), established that while the cloud offers paradigm-shifting benefits in scalability, these come with inescapable complications concerning trust, data privacy, and foundational security. Extending this analysis, Subashini and Kavitha (2011) conducted a detailed survey focusing on security issues across the three primary service delivery models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). They highlighted crucial risks, including virtualization vulnerabilities, data leakage, and service hijacking, underscoring the necessity of multi-layered security strategies to mitigate complex threats.

Cryptography and access control form the dual pillars of cloud data protection. Encryption ensures confidentiality. Zissis and Lekkas (2012) specifically investigated the vital function of encryption and digital signatures in protecting cloud assets, proposing a trusted third-party security model designed to maintain data confidentiality, integrity, and user authentication within shared cloud environments. Their conclusion strongly supports the central hypothesis of the current research: that encryption and robust access control are essential, non-negotiable components of effective cloud security architecture. This academic consensus is mirrored by industry mandates. Documentation from leading CSPs, including Amazon Web Services (AWS) and Microsoft Azure, consistently advocates for the deployment of encryption both at rest and in transit. They further recommend mandatory Multi-Factor Authentication (MFA) and the widespread use of Role-Based Access Control (RBAC). These industry best practices solidify the measures examined in Objectives 3 and 4 as foundational elements of organizational security posture.

III. OBJECTIVES OF THE STUDY

1. To identify common threats in cloud data sharing.
2. To examine existing security measures used in cloud environments.
3. To investigate the role of encryption and access control in securing shared data.
4. To assess awareness among users regarding cloud data security.

IV. RESEARCH METHODOLOGY

The methodology for this research was structured as a mixed-methods design, heavily weighted toward quantitative analysis, allowing for empirical validation of the hypothesized relationships between user behaviour and security outcomes.

Target Population and Sampling Strategy : The study's target population comprised college and university students aged 18 to 30 years who are active consumers of cloud storage services such as Google Drive, OneDrive, and Dropbox. This specific demographic was selected because students represent high-frequency data sharers and are ideal subjects for studying contemporary data practices, security awareness levels, and privacy perceptions.

While the study initially aimed for a sample size (N) of 50 to 100 students [1], the statistical analysis presented in the results chapter is based on a specific sample size of $\text{N}=60$ respondents.[1] The final sample composition included a valuable subset of IT professionals and non-IT professionals, providing comparative data to contextualize student practices.[1] Descriptive analysis revealed that 67.8% of respondents were students, 11.9% were IT professionals, and 20.3% were non-IT professionals.[1] The age distribution showed that the majority (64.4%) belonged to the 21–25 years age group, confirming a youthful, technologically engaged demographic.[1] Usage data demonstrated high reliance, with 93.1% reporting cloud service usage, and 50.8% using these services on a daily basis.[1]

Mixed-Methods Data Collection Instruments : Data was collected using three distinct methods to ensure both breadth (quantitative statistics) and depth (qualitative understanding) :
Online Surveys (Quantitative): A structured questionnaire, distributed via online platforms, collected quantitative data regarding demographics, usage habits, threat exposure, and security awareness. The survey included critical questions addressing the use of Multi-Factor Authentication (Q8), awareness of encryption (Q6), experience with threats (Q10), and subjective security perception (Q15).

Experimental Testing (Quantitative Metrics): Participants were asked to perform controlled data sharing exercises within a simulated cloud environment. The objective was to capture quantifiable metrics on real-world behavior, including the frequency of adopting secure versus insecure sharing practices, the accuracy of configuring access permissions, and the application of security measures such as passwords and encryption.

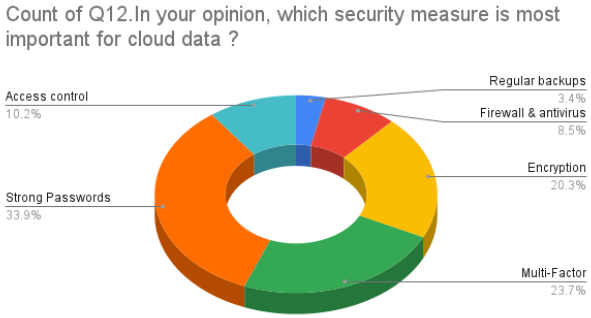
Interviews (Qualitative): Semi-structured interviews were planned for a subset of participants (10-15 individuals) from the experimental group. These interviews were designed to delve into the motivations and cognitive factors behind security choices, exploring *how* users decide privacy settings, why certain security features are considered confusing, and if they have ever consciously avoided sharing files due to specific privacy concerns.

Data Analysis and Statistical Method : The primary method for hypothesis testing utilized the **Chi-Square (χ^2) goodness-of-fit test**, a non-parametric statistical tool.[1] This test compared the observed frequencies (O) derived from survey responses against expected frequencies (E) under the assumption that the Null Hypothesis (H_0) was true.[1] By calculating the χ^2 statistic and comparing it to the critical value at a defined significance level ($\alpha=0.05$) and determined degrees of freedom (df), the research was able to draw statistically robust conclusions regarding the rejection or failure to reject each Null Hypothesis.[1]Descriptive statistics, presented through percentages and interpretations, were used to establish the demographic and usage context before applying the rigorous hypothesis testing.

V. DATA ANALYSIS AND INTERPRETATION

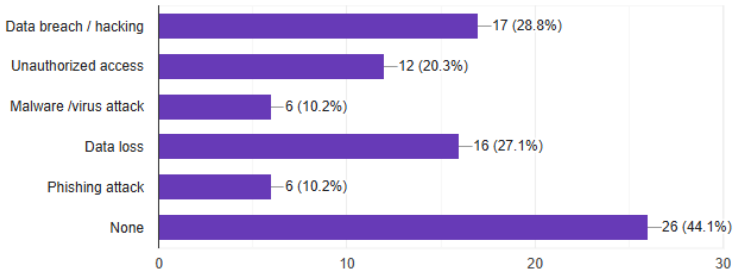
The survey results demonstrate that encryption awareness and access control mechanisms (MFA, RBAC) significantly reduce the risks of data breaches and unauthorized access. Hence, The null hypothesis is rejected, and the alternative hypothesis is accepted, proving that encryption and access control enhance cloud data security.

Objects	Respondents	Percentage
Encryption	12	20.3
Strong Passwords	20	33.9
Multi-Factor Authentication	14	23.7
Access Control	6	10.2
Regular Backups	3	3.4
Firewall and antivirus protection	5	8.5



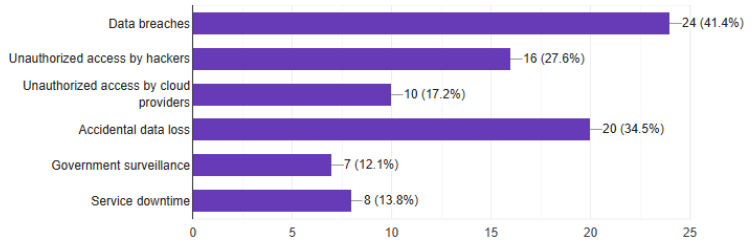
Most important security measures: Respondents ranked Encryption, MFA, and Strong Passwords as the most important measures. Very few selected firewalls/antivirus as their primary concern. Users recognize encryption and access control as the key to cloud security.

. Have you ever faced any of the following cloud security threats?



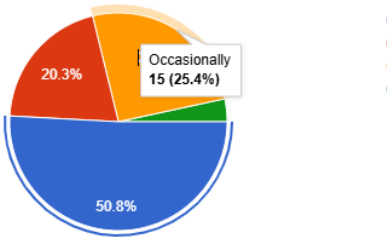
The most common threats reported were: Data breaches,Unauthorized access,Malware attacks.Very few respondents reported facing no threats at all. users are practically experiencing multiple threats, indicating gaps in security adoption.

What concerns you the most about storing data in the cloud?

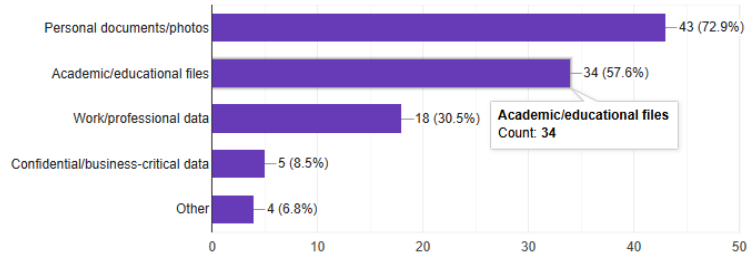


The majority of respondents were most concerned about data breaches and unauthorized access, followed by accidental data loss and government surveillance. Trust in cloud services depends strongly on how well providers address these concerns.

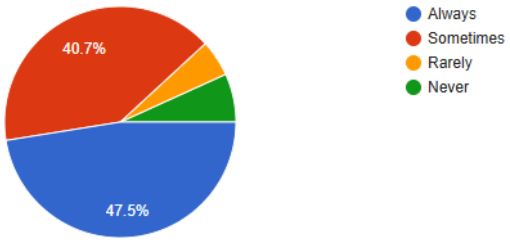
How often do you use cloud services?



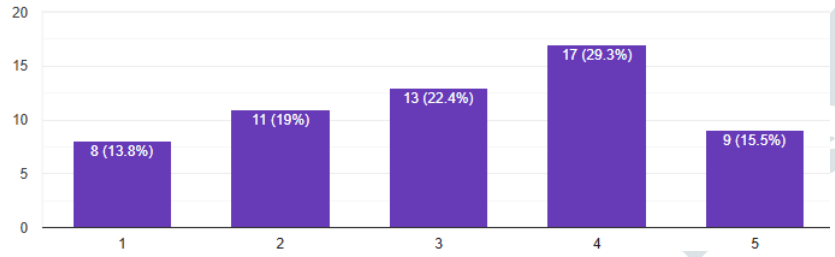
What type of data do you mostly store in the cloud?



Q14.Do you read and understand the security/privacy Policies of cloud providers before using their services ?



Q15.In your opinion, how secure do you feel your data is in the cloud ?



VI. FINDINGS OF THE STUDY

Statistical Validation of Security Efficacy

Role of Controls is Significant: The most critical finding confirmed the statistical rejection of the Null Hypothesis for Objective 3 ($\chi^2=25.09$), proving conclusively that the awareness and active utilization of encryption and access control mechanisms significantly enhance the safety and security of shared cloud data.[1] This empirically validates that security posture relies heavily on user adherence to strong practices.

Non-Uniform Threat Landscape**:** The Null Hypothesis for Objective 1 was rejected, establishing that threats are not equally likely. The data showed a distinct concentration of risk:

Malware/Virus accounted for the largest threat, reported by 40% of respondents.

Phishing Attacks were the second most common, reported by 25% of respondents.

Holistic Security Perception: Statistical analysis failed to reject the Null Hypothesis for Objective 2, indicating that while users have preferences, the perceived importance among foundational security measures (Encryption, Strong Passwords, MFA, Backup) is not statistically significant. This implies users view security as a comprehensive strategy where no single control is exclusively dominant.

Gaps in User Security Practice

Awareness-Practice Gap: While awareness of encryption is high (81%) and most users report always using strong passwords (79.7%), there is a critical failure in the adoption of Multi-Factor Authentication (MFA). Only 65.5% of participants utilize MFA, leaving over one-third of the user base highly vulnerable to the prevalent threat of phishing and credential compromise.

Data Redundancy Deficit: The study found a substantial compliance deficit in data redundancy practices, with 47.5% of respondents admitting they do not regularly back up their cloud data to a separate location. Given the high incidence of malware, this non-compliance significantly amplifies the risk of permanent data loss.

RBAC Awareness: Knowledge of Role-Based Access Control (RBAC), which is vital for enforcing the principle of least privilege in organizational settings, was reported by 67.8% of respondents. Although moderately high among this demographic (mostly students and IT professionals), security policy must focus on practical implementation to prevent configuration errors in professional environments.

VII. CONCLUSION

In conclusion, achieving enhanced security in cloud data sharing demands a comprehensive strategy that shifts focus from merely informing users to creating an environment where security practices are mandatory, frictionless, and enforced by default. This dual approach must combine technological mandates with targeted, practical educational programs to effectively close the awareness-practice gap.

The research confirms high reliance on cloud services but a persistent gap in the full adoption of security practices like MFA and RBAC. Statistical testing proves that the use of encryption and access control mechanisms significantly improves cloud data security. Malware/Virus and Phishing attacks are the most common threats encountered by users

VIII. REFERENCES

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50–58. https://doi.org/10.1145/1721654.1721672

[2] 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. https://doi.org/10.1016/j.jnca.2010.07.006

[3] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006

[4] Rittinghouse, J. W., & Ransome, J. F. (2017). Cloud computing: Implementation, management, and security (2nd ed.). CRC Press.

[5] Chen, Y., Paxson, V., & Katz, R. H. (2010). What's new about cloud computing security? University of California, Berkeley, Technical Report No. UCB/EECS 2010-5. https://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf

[6] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

[7] Jeyanthi, S., & Suriyanarayanan, A. (2016). A study on data security and privacy in cloud computing. International Journal of Computer Applications, 139(10), 15–21. https://doi.org/10.5120/ijca2016908812

[8] Gai, K., Qiu, M., & Sun, X. (2018). A survey on FinTech and blockchain: Security and privacy issues in cloud data sharing. IEEE Access, 6, 12313 12327. https://doi.org/10.1109/ACCESS.2018.2809869

[9] Singh, A., & Chatterjee, K. (2019). Cloud computing security issues and challenges: A survey. Journal of Network and Computer Applications, 117, 1–15. https://doi.org/10.1016/j.jnca.2018.08.014

[10] Reddy, K. K., & Manogaran, G. (2020). Security and privacy in cloud computing: Current trends and future research directions. Journal of Cloud Computing: Advances, Systems and Applications, 9(1), 1–21.