International Journal of Computer Techniques – IJCT Volume 12 Issue 5, October 2025

Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

An Analytical Study on User Trust and Data Privacy in Cloud Storage Services

Govinda Shrinivas Harbyashi
Department of Computer Applications
Sinhgad Institute of Business Administration and Research
Pune, India
gsh494950@gmail.com

Shriyal Shrikant Mali
Department of Computer Applications
Sinhgad Institute of Business Administration and Research
Pune, India
malishriyal@gmail.com

Prof. Rubina sheikh
Assistant Professor
Department of Computer Applications
Sinhgad Institute of Business Administration and Research
Pune, India
rubina.sk@gmail.com

Prof. Kalyani Alisetty
Assistant Professor
Department of Computer Applications
Sinhgad Institute of Business Administration and Research
Pune, India
koukuntla.kalyani@gmail.com

Abstract— **This project digs into what makes people trust cloud storage providers. It explores which privacy features matter most, which company's users rely on, and what can be done to make cloud storage safer and more trustworthy. The study is based on responses from a Google Form survey, backed by insights from existing academic research on cloud data privacy.**

The findings are clear: users feel safest when providers offer strong encryption (especially end-to-end or zero-knowledge), multi-factor authentication (MFA), and compliance with global privacy laws like GDPR and ISO 27018. This addresses the major concern that while traditional encryption offers a layer of security, it may not withstand internal attacks from cloud providers themselves.

Among all providers, Google Drive, Microsoft OneDrive, and Apple iCloud are the most trusted overall. However, privacy-focused services like MEGA and Sync.com are popular with users who want total control over their encryption keys. Indian companies like Jio Cloud and CtrlS are slowly gaining trust for local data hosting and support for India's DPDPA 2023, but users feel they need stronger international certifications to compete globally.

A key theme that emerged is the need for "data control," which includes both the ability to move data to a new provider (data mobility) and the right to have your data permanently deleted (data withdrawal). Based on our findings, we recommend that providers improve trust by offering user-controlled encryption (BYOK), publishing third-party security audits, simplifying their privacy policies, and designing systems with privacy as the default.

I. Introduction

In today's world, our digital lives—photos, documents, and projects—live on the cloud. We use services like Google Drive, OneDrive, and iCloud every day, often without a second thought. But the truth is, the more we store online, the more we rely on someone else's system. This automatically raises questions about privacy, control, and security.

When we upload our data, we're trusting these companies not to peek at it, lose it, or share it. Yet, with reports of data breaches affecting over 60% of cloud users, that trust is often shaken. Every time we sign up, we click the "I agree" box on Terms of Service (TOS) agreements that are non-negotiable and rarely read, which can seriously impact our legal rights.

This research aims to answer a simple but vital question: "What exactly makes users trust a cloud storage provider?"

We also explore whether users trust global giants like Google and Microsoft more than Indian providers like Jio Cloud, especially now that India has its own Digital Personal Data Protection Act (DPDPA), 2023. A central part of this is understanding the user's demand for data control—the right to take your data with you or have it erased completely, preventing issues like vendor lock-in [8].

In short, this project looks at how trust is built—whether through technology, legal compliance, or brand reputation—and what providers can do to make users feel their data is truly safe.

II. Literature Review

A. Technology & Security

Encryption is the backbone of trust [9]. However, while standard encryption protects data from outside hackers, it often fails to prevent internal attacks from the cloud provider itself, who may hold the decryption keys [10]. To solve this, researchers propose advanced methods.

Some suggest a three-layer architecture using fog computing, where data is split and stored across local, fog, and cloud servers using algorithms like the Hash-Solomon code, making it impossible for any single entity to reconstruct the full data [11].

Other approaches focus on protocols that ensure File Assured Deletion (FADE), giving users proof that their data is truly gone when they delete it [12].

B. Trust & Reputation Models

Lack of transparency is a major barrier to cloud adoption [13]. To address this, some studies propose reputation-based trust frameworks [14]. These models calculate a provider's trustworthiness based on measurable factors like server workload, request rejection rates, and user feedback [15]. This creates a more objective way for users to choose a reliable provider, rather than relying on marketing claims alone.

C. Policy and Data Control

Legal scholars point out that most users agree to non-negotiable Terms of Service (TOS) agreements without reading them, creating a huge information imbalance [16]. The concept of data control has emerged as a critical user right, consisting of:

- Data Mobility: The ability to move your data to a different provider without being "locked in" by proprietary formats [17].
- Data Withdrawal: The right to have your data completely removed from a provider's servers, including from third parties [18].

This literature confirms that trust isn't just about strong passwords. It's a combination of verifiable technology (like fog computing), objective reputation scores, and clear, enforceable policies that give users real control over their data.

III. Methodology And Data Source

To get real opinions, an online survey was conducted using Google Forms and shared with students and professionals.

The survey collected data about:

- Cloud storage services people use most (Google Drive, OneDrive, MEGA, Jio Cloud, etc.).
- Features that build their trust (Encryption, MFA, Compliance, Local Data Hosting).
- Their awareness of privacy laws like GDPR, ISO 27018, and DPDPA 2023.

The questionnaire also included open-ended questions on what improvements they would like to see.

Around 182 responses were received. The collected data was analysed, and user opinions were compared with the actual privacy laws and technologies each company claims to follow.

IV. Survey Results and Analysis

The survey responses clearly showed which provider is most trusted by the users and why.

A. Most Trusted Providers:

- Google Drive: 92.9% of users trust it most, citing its brand reputation, constant updates and visible GDPR/ISO certifications.
- Microsoft OneDrive: Trusted by 47.3%, known for strong corporate security and Office 365 integration.
- Apple iCloud: 20.3% of users trust, mainly due to Apple's privacy-focused marketing and encryption features.
- MEGA & Sync.com: Trusted by 1.6% and 2.2% users respectively, valued for their zero knowledge, privacy-first approach.
- Indian Providers (Jio Cloud, CtrlS, Cyfuture): Only 15–20% of users trust. It is mainly preferred for local data hosting due to compliance with Indian laws.

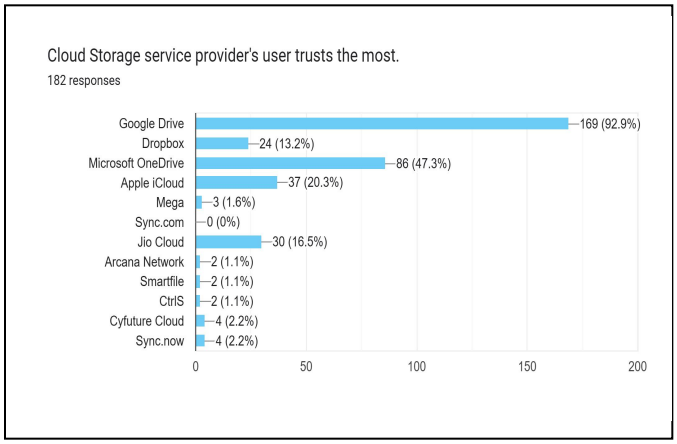


Fig.1: User trust in service provider

B. Feature Importance(1-5):

Based on a 5-point rating scale, here's what users value the most

Table I User Ratings of Key Cloud Storage Security Features

SR. No	Features	Average Rating
1.	Encryption	4.3
2.	MFA (Multi-Factor Authentication)	4.0
3.	Compliance (GDPR/ISO)	3.8
4.	Transparency & Control	3.7
5.	Local Hosting (DPDPA)	3.5

Table I shows rating for Encryption & MFA higher than compliance labels. This shows users clearly prioritize technical protection *Figures and Tables*

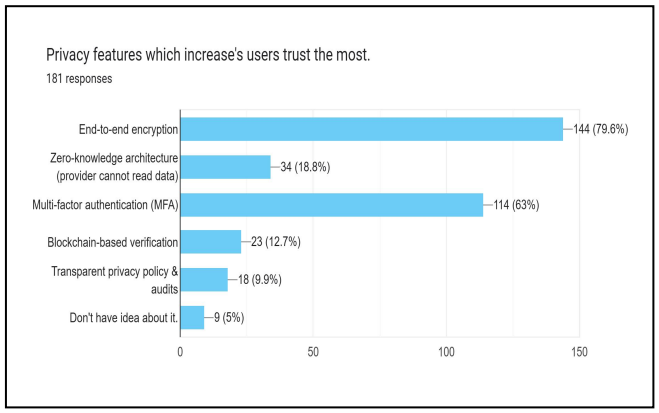
C. Awareness of Laws:

Our Study states that

- 60% of the users were aware of **GDPR**.
- 30% users knew about **ISO 27018**.
- Only 20% users had heard of India's DPDPA 2023.

This confirms that most users rely more on brand reputation than on specific legal details.

Fig.2: Privacy features



D. Key Takeaway: Trust is a mix of strong technology, a reputable brand, and visible compliance. Users may not know each and every law, but they can tell when a provider takes their privacy seriously.

V. What Makes Users Trust

Digging deeper into the results, a few key themes emerged about what builds user trust.

1. Encryption and MFA are the Foundation

Fig.2:Privacy feature which increase's users trust

These two features are non-negotiable for most users. Encryption ensures that even if data is breached, it remains unreadable. MFA reassures them that their account is safe from unauthorized logins. Many users specifically mentioned "end-to-end" or "zero-knowledge" encryption as the gold standard because it prevents even the provider from accessing their files.

2. Compliance Acts as a Trust Signal

Seeing logos for GDPR or ISO makes users feel safer, but only if they are clearly displayed. Around 60% said these certifications increase their trust, though many admitted they don't fully understand the technical details. They act as a signal that the company is serious about following rules.

3. Transparency and Control Are Crucial

Users want to know who can access their data, where it's stored, and how to get it back or delete it forever. This reflects the growing demand for "data control"—the ability to move data freely (data mobility) and demand its deletion (data withdrawal). Companies that explain this in simple language earn more trust.

4. Brand Reputation Often Outweighs All Else

Many users trust providers like Google or Microsoft simply because they are global leaders with a proven track record. Even if smaller, privacy-focused providers offer better security, users often hesitate due to a lack of brand familiarity.

5. Local Data Hosting Is a Key Advantage for Indian Providers

Some users in India explicitly stated they prefer Jio Cloud or CtrlS because keeping data within the country feels safer. However, they also said these providers need to be more transparent about their security audits and global certifications to be fully trusted.

VI. Provider Comparison: Acts & Technologies

Table 2 shows a comparison of various major cloud providers, their compliance and security technologies used as per the public documentation available online.

Table II: Comparison of Cloud Providers

Providers	Compliance/Act	Key Security Technologies Used
Google Drive	GDPR, ISO 27018, SOC 2/3	AES-256 encryption, MFA, Audit Logs, BYOK options
Microsoft OneDrive	GDPR, ISO 27001/27018	Conditional Access, DLP, Azure AD, MFA, Customer Lockbox
Apple iCloud	GDPR, ADP (Advanced	End-to-end encryption (optional), HSMs
MEGA	GDPR (NZ Region)	Zero-knowledge, client-side encryption
Sync.com	GDPR	End-to-end encryption, zero-knowledge
Jio Cloud	DPDPA 2023 (India)	Encryption at rest, Local data hosting
CtrlS	ISO 27001, RBI/IRDAI	SOC operations, Tier-IV data center security
Cyfuture Cloud	GDPR, HIPAA	Multi-layer encryption, Tier-III data

- Global Leaders (Google, Microsoft) align closely with user values by offering both visible compliance and strong, configurable security.
- Privacy Specialists (MEGA, Sync.com) lead on zero-knowledge encryption but need stronger brand recognition to attract the mass market.
- Indian Providers (Jio Cloud, CtrlS) excel at local hosting but need to enhance transparency and pursue more global certifications to build wider trust.

VII. The Trust Gap: MNCs vs. Indian Providers

There's a noticeable trust gap between big global companies and local Indian providers.
Here's why:

MNC Providers (Google, Microsoft, Apple):

- Reasons to trust: They have a strong global reputation,
- provide frequent security updates, and display multiple certifications like GDPR, ISO, and SOC reports. Their long history and massive infrastructure give users a sense of stability and reliability.
- The challenge: Their privacy policies can be complex and hard to
- understand, and users sometimes worry about data being used for advertising.

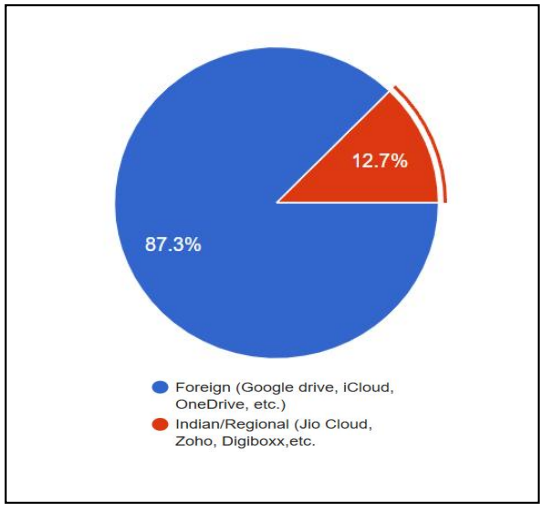


Fig.3: Proportion Chart

Indian / Regional Providers (Jio Cloud, CtrlS, Cyfuture) :

- Reasons to trust: They are appreciated for keeping data hosted locally, which aligns with data sovereignty concerns and India's DPDPA 2023. This is a significant advantage for government and regulated industry clients.
- The challenge: Many users feel that the providers don't communicate their compliance or security audits
- clearly. Survey comments showed people want to trust Indian providers but hesitate due to a lack of publicly available third-party verification.

The core reasons for the trust gap are:

- Visibility: MNCs prominently display compliance badges and audit reports; Indian providers often don't.
- Verification: Global players are regularly audited by third parties; regional ones often rely on self-claims.
- Reputation: MNCs are perceived as having more experience and resources to handle global cyber threats.
- This gap isn't permanent. If Indian providers start adopting global standards, publishing their audit results, and offering features like end-to-end encryption, they can earn the same level of trust over time.

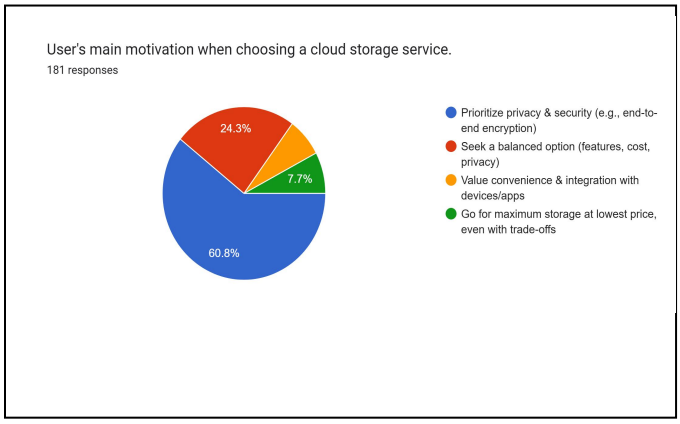


Fig.4: User Motivation for Cloud Storage

The pie chart presents user motivations for choosing a cloud storage service, based on 181 survey responses. The majority, 60.8%, prioritize privacy and security, specifically features like end-to-end encryption. In contrast, only 24.3% seek a balanced option, and smaller segments value either convenience/integration (7.7%) or the lowest price, even with trade-offs.

VIII. Recommendations

Based on the findings, here are actionable steps cloud providers can take to earn more user trust:

- **Offer Optional End-to-End Encryption (E2EE):** Let users choose a "zero-knowledge" mode where only they hold the encryption keys24. This gives privacy-conscious users full control and confidence that not even the provider can access their files.
- **Provide "Bring Your Own Key" (BYOK) for Enterprises:** Allow organizations to manage their own encryption keys using secure hardware security modules (HSMs). This is a critical feature for regulated industries.
- **Publish Security Audits and Certifications:** Don't just claim compliance. Regularly release third-party audit reports (like SOC 2) and make certifications for

ISO 27001, GDPR, and HIPAA easy to find. Users trust visible evidence.

- **Simplify Privacy Policies:** Replace long legal documents with clear, simple summaries or dashboards. Address the problem of unread and obtuse TOS agreements by showing users exactly how their data is used and protected.
- **Mandate Data Mobility and Withdrawal:** Guarantee in the TOS that users can easily download all their data in a standard format (data mobility) and have it permanently deleted upon request (data withdrawal). This prevents vendor lock-in and builds immense trust.
- **Adopt Privacy-by-Design:** Build systems from the ground up with minimal data collection and maximum security as the default settings, not as an afterthought.
- **Comply with Both Global and Local Laws:** For Indian companies, aligning with both DPDPA 2023 and international standards like GDPR or ISO 27018 is essential for earning both domestic and global trust.

If providers implement these steps, trust will grow because users will have measurable evidence of security, not just promises.

IX. Limitations:

- The survey size is modest, so it shows general trends, not definitive global conclusions.
- Some users might not fully grasp technical terms like "end-to-end encryption."
- The results reflect perceived trust, not hands-on technical audits.
- Even with these limitations, the data gives us a solid foundation for understanding what shapes user trust in the real world.
- Privacy policies and technologies change frequently.
- No technical testing done, only based on provider documents.
- Some findings depend on user perception, not verified data.
- Limited time and resources restricted deeper analysis.

X. Conclusion

This study confirms that user trust in cloud storage is built on a foundation of strong encryption and authentication, reinforced by visible compliance and transparency.

Users overwhelmingly trust global providers like Google Drive and OneDrive because they effectively combine powerful technical security with a proven track record of global certifications. Apple iCloud benefits from strong privacy branding, while services like MEGA and Sync.com appeal to a niche that demands zero-knowledge privacy. Indian providers such as Jio Cloud and CtrlS have a key advantage in local data hosting but must become more transparent about their security practices and gain global certifications to close the existing trust gap.

Ultimately, the gap is not about geography but about assurance. Trust is earned when users feel they have genuine data control—the power to secure, move, and delete their own information. By adopting privacy-by-design principles, offering user-controlled encryption, and simplifying their policies, all providers can build a more secure and reliable cloud ecosystem for everyone.

XI. References

[1] Reddy, S. M., et al. (2024). Enhanced Data Privacy and Security in Cloud Storage: A Robust Authentication Scheme for Cyber-Physical-Social Systems. Journal for Educators, Teachers and Trainers, 15(5), 383-392.

[2] Syed, A., Purushotham, K., & Shidaganti, G. (2020). Cloud Storage Security Risks, Practices and Measures: A Review. Conference Paper.

[3] Vurukonda, N., & Rao, B. T. (2016). A Study on Data Storage Security Issues in Cloud Computing. Procedia Computer Science, 92, 128-135.

[4] Ojha, S., et al. (2024). A method to enhance privacy preservation in cloud storage through a three-layer scheme for computational intelligence in fog computing. MethodsX, 13, 103053.

[5] Kesan, J. P., Hayes, C. M., & Bashir, M. N. (2013). Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences and Market Efficiency. Washington and Lee Law Review, 70(3).

[6] Kaur, R., & Singh, J. (2020). A Review on Data Encryption Techniques in Cloud Computing. International Journal of Computer Applications, 176(9), 1–5.

[7] Li, J., Chen, X., Huang, Q., Tang, S., & Xiang, Y. (2019). Secure Auditing and Deduplication of Encrypted Data in Cloud. IEEE Transactions on Computers, 68(6), 913–926.

[8] Zhang, W., Chen, Y., & Lin, X. (2018). Fog-Based Distributed Data Security Architecture for Cloud Storage. Journal of Network and Computer Applications, 105, 1–9.

[9] Perlman, R. (2017). File Assured Deletion (FADE): Building Secure Deletion into the Cloud. IEEE Security & Privacy, 15(2), 37–44.

[10] Sabherwal, A., & Thakur, A. (2021). Trust and Reputation Management Models for Cloud Computing: A Comprehensive Review. International Journal of Cloud Applications and Computing, 11(4), 45–61.

[11] Noor, T. H., & Sheng, Q. Z. (2014). Trust Management in Cloud Computing: A Critical Review. IEEE Computer, 47(4), 94–98.

[12] Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A Survey on Trust Management for Internet of Things and Cloud Computing. IEEE Communications Surveys & Tutorials, 16(3), 1649–1660.

[13] Alharthi, A., Krotov, V., & Bowman, M. (2017). Addressing the Cloud Computing Transparency Challenge: A Review and Recommendations. Procedia Computer Science, 109, 33–40.

[14] Gai, K., Qiu, M., & Zhao, H. (2018). Security and Privacy Issues in Cloud Computing: A Survey. Future Generation Computer Systems, 88, 254–273.

[15] Rani, P., & Sharma, S. (2022). Data Mobility and Withdrawal Rights under Cloud Service Agreements.

International Journal of Law and Technology, 16(2), 87–101.

[16] Ekwonwune, E. N., et al. (2024). Analysis of Secured Cloud Data Storage Model for Information. Journal of Software Engineering and Applications, 17, 297-320.

[17] Baseer, K. K., et al. (2024). Trust based Reputation Framework for Data Security in Cloud Environment. J. Electrical Systems, 20-7s, 1102-1110.

[18] Monsef M. (2018). Trust and Privacy Concern in the Cloud. ResearchGate.

[19] Utomo & Yasirandi (2024). Exploring Trust, Privacy, and Security in Cloud Storage among Generation Z. ResearchGate.

[20] Mahajan et al. (2011). Depot: Cloud Storage with Minimal Trust. Cornell CS.

[21] Brandenburger et al. (2015). Don't Trust the Cloud, Verify: Integrity and Consistency for Cloud Object Stores. arXiv.

[22] Liu et al. (2013). Secure and Privacy-Preserving Keyword Searching for Cloud Storage. Temple University.

[23] Roslin Dayana et al. (2023). Trust-Aware Cryptographic RBAC in Cloud Storage. Taylor & Francis.

[24] ISO/IEC 27018: Code of practice for protection of PII in public clouds.

[25] Jansen, W., & Grance, T. (2011). NIST Guidelines on Security and Privacy in Public Cloud Computing.

[26] GDPR Article 20 – Data Portability.

[27] Armbrust et al., A View of Cloud Computing.

[28] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing.

[29] Statista, 2024 Cloud Data Breach Statistics.

[30] Solove, D. J. (2013). Privacy self-management and the consent dilemma.

[31] DPDPA 2023, Government of India.

[32] Prior academic works on fog computing, encryption, and reputation models.

[33] ENISA Report on Cloud Security and BYOK Models, 2023.