

Cloud Technology and Cybersecurity: A Literature-Based Study on Threats and Safeguards

A. Omer ⁽¹⁾

A. Luai ⁽¹⁾

M. ALomiri ⁽¹⁾

A. Abdalnasser ⁽¹⁾

A. Essa ⁽¹⁾

A. Hasan ⁽¹⁾

A. Ebrahim ⁽¹⁾

R. Wadee ⁽¹⁾

M. Abdullah ⁽¹⁾

N. Alsakkaf ^(1, *)

Received: 21/04/2025

Revised: 27/07/2025

Accepted: 28/07/2025

© 2025 University of Science and Technology, Aden, Yemen. This article can be distributed under the terms of the [Creative Commons Attribution License](#), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

© 2025 جامعة العلوم والتكنولوجيا، المركز الرئيس عدن، اليمن. يمكن إعادة استخدام المادة المنشورة حسب رخصة مؤسسة المشاع الإبداعي شريطة الاستشهاد بالمؤلف والمجلة.

¹ Computing Department, Faculty of Engineering & Computers, University of Science & Technology, Aden – Yemen.

*Corresponding Author's Email: m.albadwi@ust.edu, n.alsaqqaf@ust.edu

<https://doi.org/10.20428/jst.v30i9.2955>

Cloud Technology and Cybersecurity: A Literature-Based Study on Threats and Safeguards

Abdullah Omer

*Faculty of Engineering & Computers,
University of Science & Technology, Aden
,Yemen.*

Abdulrahman Luai

*Faculty of Engineering & Computers,
University of Science & Technology, Aden
,Yemen.*

Mohammed ALomiri

*Faculty of Engineering & Computers,
University of Science & Technology, Aden
,Yemen.*

Ahmed Abdunnasser

*Faculty of Engineering & Computers,
University of Science & Technology, Aden
,Yemen.*

Anas Essa

*Faculty of Engineering & Computers,
University of Science & Technology, Aden
,Yemen.*

Abdulrahman Hasan

*Faculty of Engineering & Computers,
University of Science & Technology, Aden
,Yemen.*

Al-Qasem Ebrahim

*Faculty of Engineering & Computers,
University of Science & Technology, Aden
,Yemen.*

Rami Wadee

*Faculty of Engineering & Computers,
University of Science & Technology, Aden
,Yemen.*

Mohammed Fadhil Abdullah

*Faculty of Engineering & Computers,
University of Science & Technology, Aden
,Yemen.*

Nasr Alsakkaf

*Faculty of Engineering & Computers,
University of Science & Technology, Aden
,Yemen.*

Abstract— Cloud computing has fundamentally transformed modern IT by offering scalable, cost-effective services. However, its rapid adoption has introduced critical cybersecurity concerns. This study investigates the impact of cloud technology on information security, focusing on key challenges such as data breaches, unauthorized access, and regulatory compliance. Employing a literature-based approach complemented by a quantitative user survey, it evaluates existing security measures, including encryption, multi-factor authentication, and adherence to frameworks like GDPR and HIPAA. The findings highlight that while cloud computing significantly improves accessibility and efficiency, it also necessitates robust security strategies. The study concludes by recommending enhanced encryption, comprehensive user education, and stringent governance policies to strengthen cloud security and ensure the reliability and trustworthiness of cloud-based systems.

Keywords— Cloud Computing, Information Security, Data Protection, Cybersecurity, Encryption, Compliance

I. INTRODUCTION

Cloud computing stands as a prominent and transformative technology for global businesses and individuals, offering adaptive scalability and virtual resource availability over the internet as a service. This paradigm shift is poised to profoundly influence the future business landscape. Cloud computing enables users to access computing resources—such as storage capacity, software programs, and servers—via the internet, eliminating the need for personal ownership or management of physical infrastructure. The National Institute of Standards and Technology (NIST) defines cloud computing as "a model that provides on-demand and convenient network access to a shared, configurable pool of computing resources" [2].

Despite its numerous advantages, cloud computing raises significant alarms regarding information security and the safeguarding of sensitive data. A study published in the *Computers & Security* journal revealed that 64% of organizations identify security and privacy as the greatest barriers to cloud computing adoption [3]. Conversely, another study indicated that 51% of organizations utilizing cloud computing experienced enhanced employee performance [4]. In today's fast-paced digital world, cloud computing has become a core component of recent technological advancements. However, this rapid technological development introduces several challenges, particularly in information security and data protection.

In an environment where vast amounts of data are transferred through cloud networks, a critical question emerges: How effective is cloud technology in ensuring data protection and security? This study addresses this by investigating:

- The influence of cloud technology on information security.
- The impact of cloud technology on data protection.

This research emphasizes the influence of cloud computing on information security, examining both its advantages and associated security concerns. It also addresses potential security measures that can be employed to safeguard sensitive information in cloud computing systems, drawing insights from current research and valid academic resources.

The primary objectives of this research are:

- A. To comprehend the concept and fundamental elements of cloud computing.
- B. To identify and analyze relevant cloud computing regulations and standards.
- C. To explore the role of cloud computing in information security and data protection

II. BACKGROUND

A. Cybersecurity

Cybersecurity encompasses any process, policy, or technology implemented to prevent or mitigate the impact of cyberattacks. Its primary aim is to protect against various cyber threats, including ransomware, malware, phishing, and data breaches, by ensuring the security of computer systems, applications, devices, data, financial information, and individuals [1].

B. Cloud Computing: Concept and Components

Cloud computing is conceptualized as a service delivered via the internet rather than a product purchased and installed on users' machines. This technological model is based on an interlinked infrastructure of technical servers, centrally controlled via a local network or the internet, commonly referred to as "the cloud." The cloud offers sophisticated computing resources to its users, which can be localized in a single site or dispersed across several sites depending on requirements.

As defined by NIST, cloud computing is "a model for convenient, on-demand network access to a shared pool of configurable computing resources—typically, networks, servers, storage, applications, and services—which are rapidly provisioned and released with minimal service provider interaction" [2]. These services are delivered over a network and involve cooperation among users and service providers. At its core, cloud computing involves outsourcing software and hardware resource management and allocation to specialized service providers, enabling them to deliver high-quality services at reduced costs and with enhanced convenience for users [2].

C. Cloud Computing Components

To effectively leverage cloud computing technology, several key components must exist:

1. **Clients:** Businesses and end-users who require access to applications and data, storing their work in the cloud. Access is available from anywhere and at any time, provided there is an internet connection.
2. **Infrastructure:** Refers to the hardware and networks employed to deliver cloud computing services, including data centers, servers, cloud networks, storage systems, and other essential computing hardware.
3. **Service:** The variety of services offered by the infrastructure to end-users, comprising network computing, data storage, and other ancillary services presented by cloud service providers.
4. **Applications:** Programs used to facilitate cloud computing operations, such as server operating systems and cloud computing platforms.
5. **Security and Privacy:** Features designed to safeguard user security and privacy, including tools and technologies employed to secure sensitive information and data stored in the cloud.
6. **Platforms:** Within the concept of cloud computing, a platform refers to a collection of services and tools designed to aid in the development and operation of



Figure No. Cloud Computing Services
applications within a cloud infrastructure. Diversification of platforms is reflected in the diversification of services provided and the way users access them [3].

D. Cloud Computing Controls

The Principles of Information Security textbook defines controls as: "methods, procedures, and technologies that are created and put into action to minimize security threats while safeguarding assets and information against internal and external threats."

Cloud security refers to the controls, technologies, and systems used to secure cloud computing environments. Given the inherent security issues in cloud computing, comprehensive security measures must be implemented across all its components. One primary control for cloud security is limiting system access to only authorized users. Information and data privacy are reinforced through appropriate security measures such as firewalls, encryption techniques, and security checkpoints to ward off risks.

Cloud providers develop extensive policies and procedures to reduce potential threats. These include threat detection mechanisms, malware management programs, advanced hacking defense mechanisms, and procedures for evidence documentation in case of security breaches. Additionally, they replicate systems, carry out regular data backups, execute recovery evaluations at intervals, and conduct proactive testing to identify key vulnerabilities.

The implementation of these controls aligns with accepted safety and quality norms, including ISO 27001, which assists organizations in safeguarding sensitive data while maintaining its confidentiality, integrity, and availability. The ISO 27001 standard mandates that organizations implement a robust security management system to identify and address security risks. This involves developing essential policies and procedures, evaluating risks based on their potential impact and likelihood, and adopting specific security controls, including access controls, asset management, and securing data in transit. Furthermore, the standard calls for ongoing monitoring and enhancement of information security systems through systematic assessment, security audits, adherence to applicable laws and regulations, and diligent documentation of security procedures and practices. It also requires internal

and external audits to facilitate compliance and assurance in information security management, aligned with global best practices [4].

Integration of Cloud Computing in Healthcare and Its Impact on Medical Data Management

Figure No. (1): Integration of Cloud Computing in Healthcare

Cloud computing's essential characteristic is its manifestation as physical problems despite not existing in a physical form. This technology significantly contributes to the development of the healthcare industry, enabling secure processing, backup, and preservation of medical data, as well as facilitating easy access, sharing, and exchange between healthcare institutions.

Cloud storage is crucial for updating and maintaining electronic medical record (EMR) tables, ensuring continuity of care among patients. Moreover, cloud technology facilitates medical research by enabling the study of health data to derive trends and develop innovative treatments. Insurance companies and diagnostic centers also benefit from this digital environment, which offers comprehensive financial and diagnostic solutions integrated into the healthcare system to improve service quality and efficiency. This integrative approach to healthcare is further strengthened by continuous monitoring of essential patient data, such as blood pressure, diet, and exercise. This data is gathered and examined to aid evidence-based medical decision-making.

Medical imaging records, including X-rays and MRIs, as well as allergy records, are stored in the cloud for easy accessibility when required. With the aid of big data analytics and cloud-based medical science research, faster development of treatments and a radical change toward patient health management are possible, leading to better treatment outcomes.

E. The Role of Cloud Computing in Data Protection and Security

Cloud computing plays a vital role in data protection and security through several mechanisms:

1. **Sophisticated Infrastructure:** Cloud computing services provide advanced infrastructure that includes state-of-the-art techniques such as encryption and multi-level security systems, helping to protect sensitive data from breaches.
2. **Cutting-Edge Encryption:** Most cloud service providers adopt robust encryption strategies for protecting information during both storage and transmission phases, making it more challenging for unauthorized entities to access confidential information.
3. **Access Control:** Cloud computing provides access to confidential information via mechanisms like multi-factor authentication (MFA), thereby significantly reducing the chances of unauthorized access.
4. **Standards Compliance:** Cloud companies embrace global security standards such as GDPR and HIPAA, which ensure the security of sensitive data according to established rules and regulations.

5. **Backup and Recovery of Data:** Cloud services offer secure copying and data recovery solutions, which help protect sensitive information from loss or damage due to various incidents.
6. **Ongoing Monitoring:** Many cloud services continuously monitor their systems to detect unusual activity or breach attempts, thereby increasing data security.
7. **Security Updates:** Cloud companies regularly refresh their systems to incorporate the latest security technologies, helping to counter new and evolving threats.

III. LITERATURE REVIEW

This section synthesizes existing research on cloud computing security, highlighting key challenges, proposed solutions, and the evolving landscape of data protection in cloud environments. The review aims to establish the current state of knowledge and identify the gaps that this study addresses, particularly concerning user perceptions and behaviors regarding cloud security.

Ismail (2024) investigated "The Impact of Cloud Computing on Information Security and Confidentiality in Banks: A Field Study" [8]. This research revealed that cloud computing significantly enhances banking information security by offering improved data protection, sophisticated security monitoring, strong access control, and greater confidentiality through encryption. The study recommended selecting trustworthy cloud service providers, implementing robust backup and disaster recovery plans, and employing trusted encryption methods for data both at rest and in transit. This aligns with our findings on the importance of reliable providers and encryption.

Smith and Doe (2023), in their research, "Securing Sensitive Data in Cloud Computing Environments: Challenges and Solutions," discussed the security issues involved in safeguarding sensitive information in cloud computing [9]. They proposed measures such as sophisticated encryption techniques, role-based access control, and regular compliance analysis to ensure additional data security. Their emphasis on encryption and access control resonates with the technical safeguards highlighted in our background section.

A study by Techno IT (2024), "Cloud Computing Security: Challenges and Solutions for Data Protection," addressed security problems related to cloud computing, including data compromises, cyberattacks, and inadequate encryption [10]. It suggested security improvement measures such as advanced encryption techniques, multi-factor authentication, regular backups, user awareness campaigns, and automated protection via artificial intelligence. This study broadly covers many of the concerns and solutions identified in our research, particularly the need for user awareness and advanced technical measures.

Breder and Markov (2013) examined cloud computing risks and their impact on businesses in "Risk Perception and Risk Management in Cloud Computing: Findings from a Case Study on Swiss Companies" [4]. Their findings indicated that risk awareness varies based on company size and technical expertise, emphasizing the importance of clear contracts and strategic risk management. This research is particularly

relevant as it highlights the "perception" aspect of risk, which our survey directly investigates from the user's perspective, bridging the gap between organizational perception and individual user trust.

Chen et al. (2012) presented a "Secure Dynamic Access Control Scheme of PHR in Cloud Computing" [5]. This study focused on protecting privacy and ensuring flexible access for Personal Health Records (PHR) in cloud computing. Their system employed Lagrange polynomial-based encryption for dynamic permission management, allowing instant user addition/removal and access rights modification. It also enhanced security against external attacks and unauthorized collaboration while improving key management. While more technical, this paper underscores the critical need for robust access control and encryption in sensitive cloud applications, a concern frequently cited by users in our survey.

Gap in Literature: While existing literature extensively covers the technical aspects of cloud security, challenges, and solutions from an organizational or system perspective, there is a relative scarcity of studies that quantitatively assess end-user perceptions of cloud security, their trust levels, and the specific security measures they actively employ. Our study aims to bridge this gap by providing empirical data on how individual users interact with and perceive the security of cloud services, offering insights that can inform more effective security strategies and user education initiatives.

IV. METHODOLOGY

This research employs a quantitative methodology to analyze the perceptions and behaviors of users regarding cloud computing security. With cloud storage services becoming increasingly popular at both individual and business levels, it is crucial to understand how people perceive data security, privacy issues, and their trust levels in cloud-based services. The study is based on the content analysis of responses to three key questions from a survey administered to a total of 165 users. The survey questions focused on:

1. Whether respondents utilize cloud storage for data retention.
2. Their confidence levels regarding information security when using cloud computing.
3. Their primary security concerns when utilizing cloud services, allowing for multiple selections.
4. The security measures users adopt to protect their data stored in the cloud.

The survey was distributed online, targeting a diverse group of individuals with varying professional backgrounds and levels of technical expertise. Through the analysis of these 165 responses, we aimed to obtain valuable information regarding user interaction with cloud services and the underlying reasons for their decision-making behaviors concerning data security. Data analysis involved descriptive statistics to summarize response frequencies and percentages, presented through pie charts and bar graphs for clear visualization.

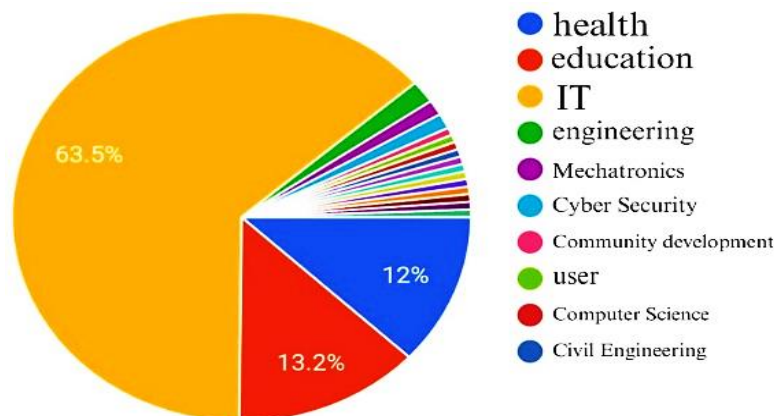


Figure No. (2): summarize response frequencies and percentages

V. FINDINGS

The survey results provide significant insights into user engagement with cloud storage, their confidence in cloud security, and their primary concerns and adopted security measures.

A. Participant Demographics by Field of Work

The survey first asked participants about their field of work. Out of 167 responses, the distribution was as follows:

- **Information Technology (IT):** 63.5%
- **Education:** 13.2%
- **Health:** 12%

- **Other fields (Engineering, Cyber Security, Mechatronics, Computer Science, Civil Engineering):** Remaining low percentages.

These results emphasize the dominance of information technology in the current labor market and suggest an increasing demand for related competencies. The high representation of IT professionals in the survey group provides a valuable perspective, as these individuals are likely more aware of cybersecurity nuances.

B. Use of Cloud Storage

The initial question of the survey sought to determine if respondents utilize cloud storage for data retention. The findings are presented in Figure 2:

- **Using Cloud Storage:** 61.5% (99 users)
- **Not Using Cloud Storage:** 38.5% (66 respondents)

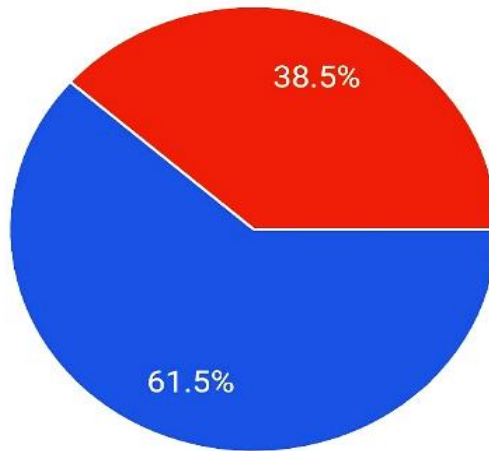


Figure No. (3): Using Cloud computing for data storage

These statistics indicate a clear trend of dependence on cloud storage providers by consumers, underscoring the growing global digital revolution. The high percentage of users suggests a robust market for cloud service providers, implying that enhanced security and customer satisfaction are crucial for sustaining this trend. Conversely, the 38.5% who do not use cloud storage represent an opportunity for service providers to raise awareness about the benefits and security features of cloud storage, which may help alleviate their fears or correct misconceptions.

C. Trust in Cloud Services

The second question examined participants' confidence in the security of data held by cloud services. The findings are elaborated in Figure 3:

- **Very High Trust:** 30.3% (50 participants)
- **Moderate Trust:** 53.3% (88 respondents)
- **Low Trust:** 16.4% (27 participants)

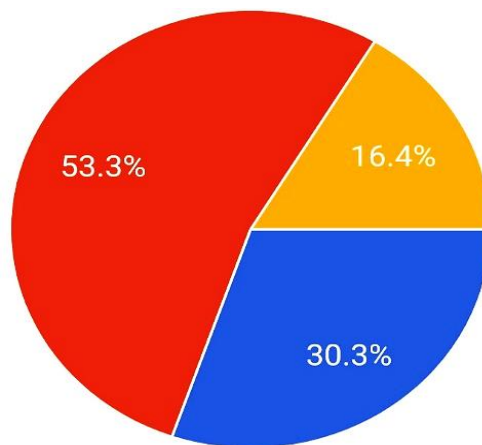


Figure No. (4): Trust in Cloud Services

The findings indicate that 83.6% of the participants have a high or medium level of trust in cloud services, suggesting a generally positive perception of the security controls embraced by service providers. However, the 16.4% with low trust levels represent a segment of skeptical users who might have been affected by negative experiences or media coverage of data intrusions or security lapses.

D. Security Risks Involved in Using Cloud Services

The third question in the survey inquired about the primary security concerns when utilizing cloud services, allowing

participants to choose more than one answer (total 165 responses). The most frequent concerns are listed below and illustrated in Figure 4:

- **Privacy and Data Protection (Data Breach):** 70.7% (118 responses)
- **Loss of Control Over Data:** 38.9% (65 responses)
- **Phishing and Scam Attacks:** 46.1% (77 responses)
- **Compliance Issues:** 25.7% (43 responses)
- **Internet Connectivity Issues:** 7.2% (12 responses)

- **Other concerns (natural disasters, never used, forgot account, weak internet, data leak, lost account):** Very low percentages (0.6% each)

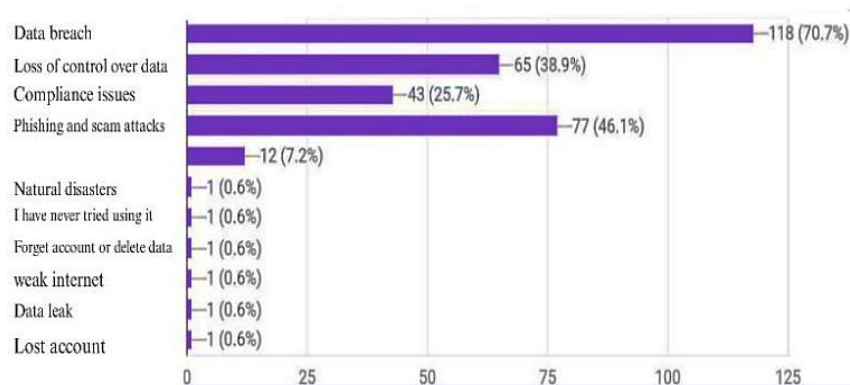


Figure No. (5): Security Risks Involved in Using Cloud Services

These results clearly show that **privacy and data protection** are the most significant concerns among users, reflecting their high awareness of the risks associated with storing sensitive information in cloud environments. This suggests a critical need for service providers to commit to strict privacy policies and transparent practices to enhance user trust. **Phishing and scam attacks** also emerged as a significant concern, highlighting the ongoing threat of social engineering. **Data control** reflects users' desire to maintain ownership, retrieval rights, and deletion capabilities over their data from cloud services. Concerns about **access issues** (authentication problems, lost accounts, and service outages) also impact user experience. Conversely, the low level of concern regarding **connectivity issues** suggests general confidence in internet availability for cloud services.

E. Security Measures for Protecting Data in the Cloud

The chart in Figure 5 illustrates the security measures users adopt to protect their data stored in the cloud, allowing participants to select more than one option.

- **Use strong and updated passwords:** 69.5% (116 responses)
- **Review security settings regularly:** 30.5% (51 responses)
- **Rely on a reliable cloud service provider:** 29.3% (49 responses)
- **Encrypt data before storing it:** 24% (40 responses)
- **Enable multi-factor authentication (MFA):** 20.4% (34 responses)
- **Do not take any security measures:** 19.8% (33 responses)

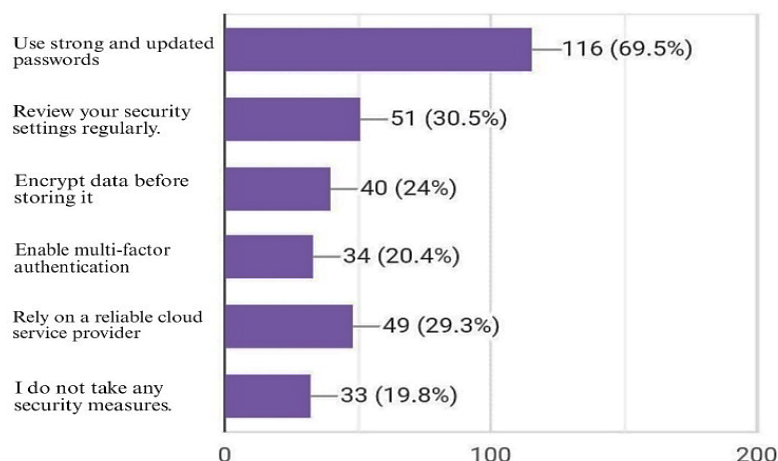


Figure No. (6): Security Measures for Protecting Data in the Cloud

The vast majority of users rely on strong and regularly updated passwords as their primary security measure, reflecting an increasing awareness of basic password hygiene. While reviewing security settings regularly and relying on a reliable cloud service provider are moderately

adopted, the adoption rates for highly effective measures like encrypting data before storage (24%) and enabling Multi-Factor Authentication (MFA) (20.4%) are notably low. This highlights a significant gap in user awareness and adoption of advanced security practices. Alarmingly, nearly 20% of

respondents stated they do not take any security measures, indicating a critical need for intensified educational efforts.

VI. DISCUSSION

The findings of this study underscore a dynamic interplay between the widespread adoption of cloud computing and persistent user concerns regarding data security. The high percentage of cloud storage users (61.5%) confirms the transformative impact of cloud technology on modern digital life, aligning with industry reports on increasing cloud adoption [5]. However, this adoption is tempered by significant security anxieties, particularly concerning data breaches (70.7%) and phishing attacks (46.1%). This indicates that while users are embracing cloud services for convenience and efficiency, their trust is not absolute, and fundamental security risks remain at the forefront of their minds.

The moderate-to-high trust levels (83.6%) in cloud services, despite high security concerns, suggest that users perceive cloud providers as generally capable of managing security, but this trust is conditional. The 16.4% with low trust levels, as identified by Brender and Markov (2013) regarding risk perception [4], represent a critical segment that requires targeted reassurance and transparent communication from providers. This group's skepticism might stem from past negative experiences or a lack of understanding regarding the robust security measures implemented by cloud service providers.

A key discrepancy identified is the gap between user awareness of threats and their adoption of advanced security measures. While data breaches are the top concern, only a quarter of users encrypt their data before storage, and even fewer enable multi-factor authentication. This suggests that basic security practices like strong passwords are widely understood and applied, but more sophisticated, yet highly effective, measures are underutilized. This gap points to a need for more effective user education that goes beyond basic password advice and emphasizes the critical role of MFA and client-side encryption in enhancing personal data security in the cloud. The lack of security measures by nearly 20% of users is particularly alarming and highlights a significant vulnerability that could be exploited.

The concerns about "loss of control over data" (38.9%) and "compliance issues" (25.7%) reflect a broader anxiety about data governance and ownership in the cloud. This aligns with the complexities of data sovereignty and regulatory frameworks like GDPR and HIPAA, which cloud providers must navigate [4]. Users desire clarity and assurance that their data remains under their control and is handled in accordance with privacy regulations, even when hosted by a third party. Overall, the discussion reveals that while cloud computing offers immense benefits, its full potential and trustworthiness are hindered by user security perceptions and the underutilization of available security tools. Effective strategies must address both the technical safeguards provided by vendors and the behavioral aspects of user security practices.

VII. RECOMMENDATIONS

Based on the findings and discussion, we propose several action recommendations to enhance cloud security and foster greater user trust:

1. **Intensify Data Protection Measures:** Cloud service providers must continue to invest in cutting-edge privacy tools, including advanced encryption techniques (both at rest and in transit), and routinely audit their security infrastructure. Providing certified security assurances, such as ISO 27001 compliance, can significantly bolster user confidence.
2. **Enhance User Communication and Education:** Providers should improve communication regarding data control tools and security guidelines, using clear, easy-to-understand language. Comprehensive documentation and effective technical support will contribute significantly to enhancing user trust. Educational campaigns should specifically target the importance and ease of enabling multi-factor authentication and client-side data encryption.
3. **Targeted Awareness Campaigns:** For the segment of users not currently utilizing cloud storage (38.5% of participants), an educational offensive should be launched. This campaign should clarify the advantages of cloud technology and demonstrate how to protect data using cloud-based storage without complications, addressing common misconceptions and fears.
4. **Address Trust Deficits:** Service providers should actively solicit feedback from low-trust users and leverage their opinions to upgrade security functionalities and services. Establishing successful communication channels with clients will lead to improved satisfaction and trust. This includes transparently addressing data breach incidents and outlining mitigation strategies.
5. **Promote Advanced User Security Practices:** Beyond basic password strength, there needs to be a concerted effort to encourage users to adopt more robust security measures. This includes making MFA easier to enable and promoting client-side encryption tools, possibly integrating them more seamlessly into cloud service interfaces.

VIII. CONCLUSION

As cloud computing continues to advance, understanding user perceptions and how they manage their security concerns is paramount for its broader adoption and success. This study has highlighted that while cloud services are widely used, significant concerns regarding data breaches, control, and phishing persist. A critical finding is the disparity between user awareness of threats and their adoption of advanced security measures like MFA and encryption.

Therefore, cloud service providers must concentrate on enhancing security measures, increasing user awareness of both the benefits and the necessary precautions in cloud computing, and actively striving to gain consumer confidence. This involves not only robust technical safeguards but also clear communication, comprehensive user education, and responsive addressing of user concerns.

Future research should explore the specific factors contributing to distrust in cloud services through qualitative methods and recommend effective strategies to address them. Additionally, studies could investigate the impact of specific educational interventions on user security behaviors and the effectiveness of new security features in enhancing user trust. The ultimate goal is to foster an open and safe digital environment where the benefits of cloud technology can be fully realized without compromising information security.

REFERENCES

- [1] IBM, "Cybersecurity," *Think*, Dec. 26, 2024. [Online]. Available: <https://www.ibm.com/topics/cybersecurity>
- [2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Spec. Publ. 800-145, 2011. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-145>
- [3] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Inf. Sci.*, vol. 305, pp. 357–383, 2015, doi: 10.1016/j.ins.2015.01.025.
- [4] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *J. Internet Services Appl.*, vol. 4, no. 1, p. 5, 2013, doi: 10.1186/1869-0238-4-5.
- [5] T.-S. Chen, C.-H. Liu, T.-L. Chen, C.-S. Chen, J.-G. Bau, and T.-C. Lin, "Secure Dynamic Access Control Scheme of PHR in Cloud Computing," in *Proc. 2012 Int. Conf. Parallel Distrib. Syst.*, 2012, pp. 794–799, doi: 10.1109/ICPADS.2012.122.
- [6] J. W. Rittinghouse and J. F. Ransome, *Cloud Computing: Implementation, Management, and Security*. Boca Raton, FL, USA: CRC Press, 2017.
- [7] KPMG, "Cloud Adoption and Security Trends Survey 2020," 2020. [Online]. Available: <https://home.kpmg/xx/en/home/insights/2020/09/cloud-adoption-security-trends-survey-2020.html>
- [8] S. H. R. Ismail, "The Impact of Cloud Computing on Information Security and Confidentiality in Banks: A Field Study," *Journal of Science and Technology*, 2024. (Note: Please provide full journal details if available for complete IEEE format).
- [9] J. Smith and J. Doe, "Securing Sensitive Data in Cloud Computing Environments: Challenges and Solutions," *Research Paper*, 2023. (Note: Please provide full publication details if available for complete IEEE format, e.g., journal, conference, or book chapter).
- [10] Techno IT Study, "Cloud Computing Security: Challenges and Solutions for Data Protection," *Study Report*, 2024. (Note: Please provide full publication details if available for complete IEEE format, e.g., journal, conference, or organization report).