RESEARCH ARTICLE

Comparison of cloud storage in terms of privacy and personal data - Sync, pCloud, IceDrive and Egnyte

[version 1; peer review: awaiting peer review]

Elissa Mollakuqe, Ersan Hamdiu, Nida Santuri Fishekqiu, Samir Jakupi, Jusuf Qarkaxhija

Faculty of Computer Sciences, AAB College, 10000, Pristina, Republic of Kosovo, Kosovo (Serbia and Montenegro)

v1 **First published:** 28 Jun 2024, **4**:128
https://doi.org/10.12688/openreseurope.16631.1
Latest published: 28 Jun 2024, **4**:128
https://doi.org/10.12688/openreseurope.16631.1

Abstract

The cloud, essentially a network of interconnected computers, has revolutionized data storage and sharing. Cloud storage, an integral part of this ecosystem, offers a virtual storage space spanning numerous physical devices. This technology relies on internet-based platforms hosted in data centers provided by service giants like Apple iCloud, Microsoft OneDrive, and Google Cloud Storage. While cloud storage enhances accessibility and convenience, it also introduces heightened risks, primarily due to the transfer of essential services to third-party providers. These risks encompass challenges related to security, privacy, data support, service availability, and regulatory compliance. Cloud storage, characterized by remote data transmission and storage on networked servers, offers a paradigm shift in data management. Users access these remote storage systems *via* the internet, paying providers based on usage rates. In this paper, we evaluate the security features of four Cloud Storage providers: Sync, pCloud, IceDrive, and Egnyte, with a specific focus on privacy and personal data protection. This paper presents a comprehensive analysis of privacy and security aspects in four prominent Cloud Storage services: Sync, pCloud, IceDrive, and Egnyte. The primary objective is to underscore the significance of privacy in the realm of Cloud Storage. Employing methods such as analysis and synthesis, comparative analysis, and empirical meta-analysis, this research delves into the core characteristics of these platforms, focusing on security, compliance, governance, and data protection.

Keywords

Cloud storages, privacy, sync, pCloud, IceDrive, Egnyte

Open Peer Review

Approval Status *AWAITING PEER REVIEW*

Any reports and responses or comments on the article can be found at the end of the article.

This article is included in the COST Actions gateway.

This article is included in the Cloud-based Technologies collection.

Corresponding author: Elissa Mollakuqe (elissamollakuqe@gmail.com)

Author roles: Mollakuqe E: Conceptualization, Investigation, Methodology, Project Administration, Writing – Original Draft Preparation; **Hamdiu E**: Resources, Writing – Review & Editing; **Fishekqiu NS**: Methodology, Writing – Original Draft Preparation, Writing – Review & Editing; **Jakupi S**: Resources, Writing – Original Draft Preparation, Writing – Review & Editing; **Qarkaxhija J**: Resources, Writing – Original Draft Preparation, Writing – Review & Editing

Competing interests: No competing interests were disclosed.

Grant information: This project has received funding from the European Union's Framework Programme for Research & Innovation as part of the COST Action [CA 19130 Fintech and AI in Finance], as supported by the COST Association (European Cooperation in Science and Technology).
The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

How to cite this article: Mollakuqe E, Hamdiu E, Fishekqiu NS *et al.* **Comparison of cloud storage in terms of privacy and personal data - Sync, pCloud, IceDrive and Egnyte [version 1; peer review: awaiting peer review]** Open Research Europe 2024, **4**:128 https://doi.org/10.12688/openreseurope.16631.1

First published: 28 Jun 2024, **4**:128 https://doi.org/10.12688/openreseurope.16631.1

Introduction

Cloud storage is a service model that involves the transmission and remote storage of data on external storage systems. This data is securely backed up and managed on these remote servers, allowing users to access it over a network, typically the internet. Users subscribe to cloud storage services and are billed periodically, often on a monthly basis, based on the amount of storage they consume[1,2]. These cloud storage providers offer a convenient and scalable solution for individuals and businesses to store and access their data, without the need for on-premises hardware and infrastructure[3]. The digital era has ushered in a transformative age of data management, where the cloud, an intricate network of interconnected computers, has taken center stage[4]. Cloud storage stands as a fundamental element in the ongoing technological transformation, granting users the capability to securely store and retrieve their data from any location equipped with an internet connection. It is a virtual repository that spans across a multitude of physical storage devices, empowering individuals and organizations alike to harness the power of remote data storage. Leading technology companies such as Apple, Microsoft, Google, and many others have ventured into this realm, providing users with the convenience of cloud-based storage solutions[5]. This innovation has brought about unparalleled levels of accessibility, flexibility, and scalability. IThas also introduced a complex landscape of challenges, most notably pertaining to the security and privacy of sensitive data. In this digital landscape, data has become a valuable asset, and protecting it has become paramount[4]. With essential services increasingly entrusted to third-party cloud storage providers, ensuring the confidentiality, integrity, and availability of data has become a multifaceted challenge. Privacy concerns, regulatory compliance, and the evolving threat landscape have made the evaluation of cloud storage services a critical endeavor. This paper delves into the realm of cloud storage, specifically focusing on the security and privacy aspects of popular cloud storage providers. By conducting a comprehensive analysis, we aim to shed light on the critical considerations users and organizations should take into account when entrusting their data to these platforms. Through an exploration of various criteria, including secure collaboration, compliance, governance, and data security, we seek to provide insights into the strengths and weaknesses of different cloud storage services. As we embark on this journey through the cloud, it becomes increasingly evident that safeguarding personal and sensitive data is of paramount importance. The evolving landscape of technology and the dynamic nature of cyber threats require a thorough understanding of the security measures and privacy safeguards offered by cloud storage providers. This paper endeavors to equip readers with the knowledge needed to make informed decisions and navigate the intricate terrain of cloud storage in an era where data privacy and security stand as pillars of the digital age. In this paper, we present the characteristics of security for four Cloud Storages: Sync, pCloud, IceDrive and Egnyte by using their properties in terms of privacy and personal data. We define the model that we used to analyze cloud storages. By using these models, we start our research to obtain the results. Here we give one detailed analysis of comparison of cloud storages in terms of privacy. We finish the paper with conclusions.

Cloud storages and their properties

The term "cloud computing" emerged relatively recently in the information technology (IT) industry, but it has deep roots in decades of innovation in areas such as virtualization, utility computing, distributed computing, networking, and software services[6]. The concept of a cloud represents an IT environment meticulously designed to offer scalable and precisely measured resources from a remote location, Table 1. Over time, it has evolved into a contemporary paradigm for information exchange and the delivery of internet-based services[7]. This evolution has led to the provision of more secure, adaptable, and scalable services for consumers, effectively operating as a service-oriented architecture that minimizes end-user administrative burdens[3].

At its most basic level, cloud storage can be as simple as a single user gaining access to a single server. In this scenario, a user uploads their data through a terminal and stores it on the server for safekeeping. However, if the server were to encounter a malfunction, retrieving the data files would be an insurmountable challenge until the server is back online[8]. Cloud storage addresses this vulnerability through the principles of redundancy and replication, ensuring data availability and durability[5].

Sync. Sync.com is a comprehensive file-sharing and collaboration solution tailored for small and medium-sized businesses. This platform encompasses collaboration features, data backup, and recovery tools all in one package. It offers the flexibility of both cloud-based and on-premises deployment options and provides mobile apps compatible with Android and iOS devices for seamless accessibility.

One of Sync.com's notable features is its robust access control, enabling users to tightly manage shared documents. This control extends to setting passwords, defining expiration dates, monitoring uploads, and receiving email notifications about document interactions[9].

A standout aspect of Sync.com is its unwavering commitment to data security through zero-knowledge encryption. This means that your data remains perpetually safe, secure, and

Table 1. Characteristics of cloud storage.

Characteristics of cloud storage	
SaaS	services are offered as a web application and consumers are able to access services at any time and from any place
IaaS/HaaS	Consumer receives: storage, Virtual machine, network in virtualized form and build their infrastructure on them
PaaS	consumers receive hosted applications according to API programming frameworks and deploy systems in them

private. Furthermore, Sync.com's secure cloud storage complies with a wide array of data privacy regulations in the United States, Canada, and the European Union, including Health Insurance Portability and Accountability Act (HIPAA), Personal Information Protection and Electronic Document Act (PIPEDA), and EU-safeguard standards. Users can exercise granular control over access permissions, whether read-only or read-write, adding an extra layer of security[10].

Sync.com offers valuable data backup and recovery capabilities, allowing users to restore documents to earlier versions. This feature provides a crucial safety net in cases of virus or ransomware attacks, as well as accidental deletions. According to their *Terms of Service as of May 12, 2021, retrieved from Sync's official website on June 17, 2022*, this functionality offers a valuable lifeline for data recovery. Additionally, Sync.com introduces Fault Storage, allowing users to seamlessly archive documents to the cloud directly from their system or hardware storage, enhancing data management and accessibility[11]. The criteria selected for evaluating cloud platforms, namely "Secure Collaboration," "Compliance, Governance, and Privacy," and "Data Security," are crucial aspects that organizations consider when adopting cloud services. These criteria collectively address key concerns related to the confidentiality, integrity, and availability of data on cloud platforms. By focusing on secure collaboration, compliance, governance, and data security, organizations can make informed decisions about which cloud platform aligns best with their security and operational requirements. Additionally, these criteria align with industry best practices and standards for cloud security, making them widely recognized and accepted in the field.

The obtained results for Sync Storage according to Secure Collaboration criteria are presented on Table 2.

The obtained results for Sync Storage according to compliance, governance, and privacy criteria are presented on Table 3.

Table 2. Secure Collaboration on Sync.

Secure Collaboration	
Secure Collaboration	- User Authentication - Two-factor Authentication - End-to-end encryption - AES-256 bit encryption - Password protected - SSL/TLS encryption - Client-Side Encryption - Virtual Private Network

Table 3. Compliance, governance, and privacy on Sync.

Compliance, Governance, and Privacy	
Compliance, Governance, and Privacy	Sync data governance workflow covers all stages of the content lifecycle: ● Define ○ Identification: Recognize the types of data requiring governance. ○ Protection Levels: Determine the appropriate level of safeguarding for each data type. ○ Storage and Retention Policies: Establish policies for storage duration and retention. ○ Ownership: Clearly define data ownership responsibilities. ● Control ○ Data Protection Policies: Develop and enforce policies for safeguarding data. ○ Access Controls: Implement access controls to regulate who can access data. ○ Monitoring: Continuously monitor data usage and activities. ○ Activity Detection: Employ mechanisms to detect and track data-related activities. ○ Rules: Set rules for creating, storing, and sharing data. ○ Roles and Responsibilities: Define roles and assign responsibilities for data governance. ● Alert ○ Alert Configuration: Configure alerts for detecting unusual or suspicious activities. ○ Response: Act upon alerts promptly. ○ Policy Review: Regularly review and update data governance policies. ● Monitor ○ Usage Monitoring: Continuously monitor data usage and user activities. ○ Incident Response: Be prepared to respond effectively to data-related incidents. ● Protect ○ Security Measures: Implement robust security measures to safeguard data. ○ Encryption: Utilize encryption techniques to protect data in transit and at rest. ○ Incident Response Plans: Establish comprehensive incident response plans to address data breaches and security incidents effectively.

The obtained results for Sync according to *Terms of Service as of May 12, 2021, retrieved from Sync's official website on June 17, 2022* cloud storage according to data security criteria are presented on Table 4.

PCloud. pCloud is a personal cloud storage service that allows us to save our files and folders. The software is compatible with nearly all devices and operating systems (iOS, Android, MacOS, Windows, and all Linux distributions). The application generates a secure virtual drive, allowing us to increase our local storage capacity. Every change we make to our pCloud platform will be immediately visible on other pCloud-connected devices. We have direct file access to any update and all of our devices are instantaneously synchronized[12].

The obtained results for pCloud Storage according to Secure Collaboration criteria are presented on Table 5.

The obtained results for pCloud Storage according to compliance, governance, and privacy criteria are presented on Table 6.

Table 4. Data security on Sync.

Data Security	
Data Security	• Comprehensive end-to-end encryption, SOC 2 (Service Organization Control Type 2) Type 1 certification • Absence of third-party tracking • Adherence to HIPAA compliance standards • Alignment with GDPR compliance requirements • Conformance with PIPEDA compliance regulations

Table 5. Secure collaboration on pCloud.

Secure Collaboration	
Secure Collaboration	- User Authentication properties - Two-step Login Verification properties - Verification - TLS/SSL encryption - Encryption in Transit - Password protected - Private Key Encryption - Client-Side Encryption - Swiss Data Protection

Table 6. Compliance, governance, and privacy on pCloud.

Compliance, Governance, and Privacy	

Compliance, Governance, and Privacy	The data governance workflow within pCloud encompasses every phase of the content lifecycle:
	• Authentication
	  ○ User authentication
	  ○ Two-step Login Verification
	  ○ Make secure connection over internet using TLS/SSL encryption
	• Define
	  ○ Level of access in data
	  ○ Access management and control
	  ○ Data encryption
	  ○ Classification of data
	• Alert
	  ○ Unknown device
	  ○ Limited internet connection
	  ○ Public line of connection
	  ○ Scan for viruses

The obtained results for IceDrive Cloud Storage according to Data Security criteria are presented on Table 7.

IceDrive. IceDrive is a cloud storage, focused on privacy and security. Its main selling point is its hermetic encryption with zero knowledge[13]. Almost all devices and operating systems are compatible with the program (Windows, Mac, and Linux) there is a desktop app, mobile (Android and iOS) devices can access mobile apps but only Windows users can utilize a virtual disk[14]. Activities you would need to carry out on files—edit, delete, and upload—feel equally quick for files. Icedrive provides real-time file synchronization[15].

The obtained results for IceDrive Cloud Storage according to secure collaboration criteria are presented on Table 8.

The obtained results for IceDrive Cloud Storage according to compliance, governance, and privacy criteria are presented on Table 9.

The obtained results for IceDrive Cloud Storage according to Data Security criteria are presented on Table 10.

Egnyte. Egnyte stands as an enterprise-level file sharing and collaboration solution, enabling users to securely access, share,

Table 7. Data security on pCloud.

Data Security	
Data Security	GDPR (General Data Protection Regulation) ISO 9001:2015 certification ISO 27001:2013 certification SSAE 18 SOC 2 Type II compliance SSAE 16 SOC 2 Type II compliance

Table 8. Secure collaboration on IceDrive.

Secure Collaboration	
Secure Collaboration	User Authentication Twofish protocol Zero-knowledge encryption two-factor authentication

Table 9. Compliance, governance, and privacy on IceDrive.

Compliance, Governance, and Privacy	

Compliance, Governance, and Privacy	IceDrive's data governance workflow encompasses every phase of the content lifecycle:
	• Control
	  ○ Control over personal data access to add and delete or even delete the account completely
	  ○ Classification of sensitive data
	• Define
	  ○ Access & Content Sharing Controls
	  ○ Access management and control
	  ○ Data protection
	• Alert
	  ○ Stay on Top of Issues
	  ▪ Limited support options
	  ▪ External Links
	  ▪ Customer Support
	  ▪ Restricted Collaboration

and collaborate with colleagues and partners from various devices[16]. It seamlessly blends the key attributes of security, scalability, and control for IT administrators, while simultaneously offering an intuitive file sharing experience for end-users.

Egnyte's distinct advantage lies in its ability to provide enterprise-grade file sharing without the risks associated with unauthorized cloud providers, the complexities of VPN setups, or vulnerabilities in security[17]. It ensures optimal performance within office environments while facilitating powerful collaboration across different devices[18].

Egnyte's infrastructure adopts a hybrid approach, which establishes a secure environment for users to generate and store files in the cloud. Data is securely housed within SOC2-certified data centers, and it can be augmented by on-premises infrastructure[19]. This hybrid setup ensures uninterrupted access, even in low-bandwidth scenarios, guaranteeing data availability and continuity for users[20].

The obtained results for Egnyte Cloud Storage according to Secure Collaboration criteria are presented on Table 11.

The obtained results for Egnyte Cloud Storage according to Compliance, Governance, and Privacy criteria are presented on Table 12.

The obtained results for Egnyte Cloud Storage according to Data Security criteria are presented in Table 13.

Table 10. Data Security on IceDrive.

Data Security	
Data Security	Twofish Encryption Client-side Encryption Zero-knowledge Encryption

The evolution of cloud computing has provided scalable, flexible, and secure services for consumers, enhancing information exchange and internet-based services. Cloud storage is achieved through redundancy and repetition concepts, ensuring data safety even in server malfunctions. *Secure Collaboration on Sync* - Tailored for the needs of small and medium-sized businesses, it provides a comprehensive suite encompassing collaboration, data backup, and recovery solutions. Its features include user authentication, two-factor authentication, end-to-end encryption, AES-256 bit encryption, password protection, SSL/TLS encryption, client-side encryption, and virtual private networks.

Compliance, Governance, and Privacy on Sync - Sync.com's data governance workflow covers data classification, access controls, monitoring, alert setup, and incident response, ensuring compliance with data privacy regulations such as HIPAA, PIPEDA, and EU safeguards.

Data Security on Sync- Sync.com boasts end-to-end encryption, SOC 2 Type 1 compliance, no third-party tracking, HIPAA, GDPR, and PIPEDA compliance.

pCloud is a personal cloud storage service compatible with various devices and operating systems. It offers secure collaboration features, including user authentication, two-step login verification, TLS/SSL encryption, encryption in transit, password protection, private key encryption, client-side encryption, and Swiss data protection.

Compliance, Governance, and Privacy on pCloud - pCloud's data governance workflow includes access management, data encryption, and alert setups.

Data Security on pCloud - Complies with a range of stringent standards, including GDPR, ISO 9001:2015, ISO 27001:2013, SSAE 18 SOC 2 Type II, and SSAE 16 SOC 2 Type II, ensuring the highest levels of data security and quality management.

Table 11. Secure Collaboration on Egnyte.

Secure Collaboration	
Secure Collaboration	• User Authentication: Ensuring secure user identification and access. • Two-Step Login Verification: Adding an extra layer of security for user logins. • Login Credentials Password Policy Management: Enforcing password policies to enhance login security. • Active Directory/LDAP/Single Sign-On Integration: Streamlining user management by integrating with these authentication systems. • Roles-Based Administration: Assigning specific roles and permissions to users based on their responsibilities. • Repository Permissions: Controlling access to data repositories with granular permissions. • Encryption in Transit: Safeguarding data during transmission over networks. • Encryption at Rest: Protecting data while it's stored on servers or in the cloud. • Egnyte Object Store File Encryption and Key Management: Ensuring encryption and secure key management for files stored in Egnyte's Object Store. • Application & Data Vulnerability Detection: Identifying and addressing vulnerabilities in both applications and data to enhance overall security.

Table 12. Compliance, Governance, and Privacy on Egnyte.

Compliance, Governance, and Privacy	

Compliance, Governance, and Privacy	Egnyte's data governance workflow comprehensively addresses every phase of the content lifecycle:
	• Discover
	  ○ Automate Sensitive Data Classification
	• Define
	  ○ Access & Content Sharing Controls
	  ○ Permissions Browser
	  ○ Content Safeguards
	• Remediate,
	  ○ Address and Resolve Issues
	  ○ Ransomware
	  ○ Behavioral Analytics
	• Alert
	  ○ Stay on Top of Issues
	  ▪ Unusual Access
	  ▪ Compromised Accounts
	  ▪ Ransomware Infection
	  ▪ Public Link
	  ▪ Open Access
	  ▪ External Sharing
	  ▪ Report,
	  ▪ Share Progress & Support Regulatory Compliance
	  ▪ Audit Reports
	  ▪ Responding to Requests for Personal Data
	• Retire
	  ○ Delete or Archive Stale Data
	  ○ Minimize Your Data, Minimize Your Risk

Table 13. Data Security on Egnyte.

Data Security	
Data Security	SOC 2: Demonstrating adherence to high standards of security, availability, processing integrity, confidentiality, and privacy. ISO 27001: Certifying its robust information security management system. Financial Services: Meeting the stringent compliance requirements specific to the financial sector. Healthcare: Complying with healthcare industry standards to secure sensitive patient information. EU Customers: Addressing the specific needs and regulations relevant to European Union customers.

IceDrive - emphasizes privacy and security, supporting multiple devices and operating systems. Its features include Twofish protocol, zero-knowledge encryption, two-factor authentication, and real-time file synchronization.

Compliance, Governance, and Privacy on IceDrive - IceDrive's data governance workflow covers data control, access management, data protection, and alert setups.

Data Security on IceDrive - ensures data security through Twofish encryption, client-side encryption, and zero-knowledge encryption.

Egnyte provides enterprise-grade file sharing and collaboration capabilities within a hybrid infrastructure. It prioritizes security in collaboration through features such as user authentication, two-step login verification, password policy

management, integration with active directory/LDAP/single sign-on, and robust encryption measures for data both in transit and at rest.

Compliance, Governance, and Privacy on Egnyte-Egnyte's data governance workflow covers data discovery, access controls, issue remediation, alerting, and data retirement.

Data Security on Egnyte - maintains compliance certifications like SOC 2, ISO 27001, and serves various sectors, including financial services, healthcare, and EU customers.

Methods

This study utilized a comprehensive evaluation framework to analyze the security and privacy features of four cloud storage services: Sync, pCloud, IceDrive, and Egnyte. The data collection process involved a systematic review of each platform's documentation, user manuals, and security whitepapers. Additionally, direct interactions with each service were conducted to verify the features and performance claims. The evaluation criteria were divided into three main categories: secure collaboration, compliance, governance, and privacy, and data security. For secure collaboration, we examined aspects such as user authentication, two-factor authentication, encryption standards, password policy management, and integration with directory services like Active Directory and LDAP. Compliance, governance, and privacy were assessed based on each service's adherence to industry standards and regulations, including GDPR, HIPAA, and ISO27001, and their ability to define, control, alert, and remediate potential security incidents. Data security was evaluated through encryption methods, both in transit and at rest, zero-knowledge encryption protocols, and the presence of compliance certifications. Each feature was meticulously tested where applicable, and qualitative assessments were supported by quantitative data when available. The comparison aimed to provide a detailed understanding of how each platform addresses critical security and privacy challenges. This methodical approach ensures that the study's findings are robust, replicable, and provide valuable insights for users and organizations considering these cloud storage options.

Study design

The study was designed as a comparative analysis of four cloud storage platforms with a focus on their security and privacy features. The design involved multiple phases:

- **Literature Review and Preliminary Research:** Initial research included a review of existing literature, user manuals, security whitepapers, and industry reports on cloud storage services. This phase helped identify key evaluation criteria and set the groundwork for a comprehensive analysis.

- **Criteria Selection:** Based on the literature review and industry standards, three primary criteria were chosen for evaluation: secure collaboration, compliance, governance, privacy, and data security. These criteria were selected due to their relevance in assessing the security and privacy of cloud storage services.

- **Data Collection:** Information was gathered through systematic reviews of each platform's documentation and direct interactions with the services. This involved setting up accounts, testing features, and verifying performance claims. Specific attention was given to user authentication processes, encryption methods, compliance with regulations, and overall data security measures.

- **Data Analysis:** The data collected from the evaluations were analyzed using both qualitative and quantitative methods. Qualitative data, such as user experience and compliance documentation, were categorized and coded to identify recurring themes and patterns. Quantitative data, such as the number of security features and compliance certifications, were statistically analyzed to compare the performance of each cloud storage service. The combination of these methods provided a holistic view of the security and privacy features of each platform.

- **Feature Testing and Validation:** Each cloud storage service was subjected to rigorous testing to validate the claimed features. Secure collaboration features were tested by simulating user scenarios that involved authentication, encryption, and data sharing. Compliance, governance, and privacy measures were assessed by reviewing adherence to standards and the ability to manage security incidents. Data security was tested by examining encryption protocols and certifications.

- **Comparison and Analysis:** The collected data was organized into a comparative table (Table 14), highlighting the strengths and weaknesses of each platform across the selected criteria. Qualitative assessments were supported by quantitative data where applicable, providing a comprehensive overview of each service's capabilities.

- **Synthesis and Reporting:** The final phase involved synthesizing the findings into a coherent narrative, summarizing the key insights and providing recommendations for users and organizations. This phase also included identifying areas for future research and potential improvements in cloud storage security and privacy.

This structured approach ensured a thorough and unbiased evaluation of each cloud storage service, providing stakeholders with valuable information to make informed decisions regarding their data security and privacy needs.

Ethical considerations

This study was conducted with a focus on maintaining high ethical standards. All interactions with the cloud storage services were conducted using dummy data to ensure no real user data was compromised, and no personal or sensitive information was used or disclosed during the testing and evaluation processes. The study aimed to provide a transparent and unbiased evaluation of each cloud storage service, with

Table 14. Comparison of Sync, pCloud, Icedrive and Egnyte.

	Sync	pCloud	Icedrive	EGNYTE
Secure collaboration	User Authentication Two-factor Authentication End-to-end encryption AES-256 bit encryption Password protected TLS encryption ClientSide Encryption	User Authentication Two-step Login VerificationTLS/SSL encryption Encryption in Transit Password protected Private Key Encryption Client-Side Encryption Swiss Data Protection	User Authentication Twofish protocol Zero-knowledge encryption two-factor authentication	User Authentication Two-Step Login Verification Login Credentials Password Policy Management Active Directory/LDAP/Single Sign-On Integration Roles-Based Administration Repository Permissions Encryption in Transit Encryption at Rest Egnyte Object Store File Encryption and Key Management Application & Data Vulnerability Detection
Compliance, governance, and privacy	Control Define Alert	Authentication Define Alert	Control Define Alert	Discover[17] Define[17] Remediate[17] Alert[17] Report[17] and Retire[17]
Data security	End-to-end encryption SOC 2 Type 1 No third-party tracking HIPPA compliance GDPR compliance PIPEDA compliance	General Data Protection Regulation (GDPR) ISO 9001:2015 ISO 27001:2013 SSAE 18 SOC 2 Type II SSAE 16 SOC 2 Type II	Twofish Encryption Client-side Encryption Zero-knowledge Encryption	Egnyte Compliance Certifications SOC 2 ISO27001 Financial Services Healthcare EU Customers

all findings based on publicly available information and verifiable tests. Although no human subjects were involved, the principles of ethical research, such as honesty and integrity, were strictly adhered to. The researchers have no affiliations or financial interests in any of the cloud storage services evaluated, ensuring an unbiased and impartial assessment. This structured approach ensured a thorough and unbiased evaluation, providing stakeholders with valuable information to make informed decisions regarding their data security and privacy needs.

Results

Assessing cloud storage providers for privacy and personal data protection

The information was collected evaluating by four different cloud storages: Sync, pCloud, IceDrive and Egnyte by using three different criteria of comparing: secure collaboration; compliance, governance, and privacy; and data security. This study utilized a comprehensive evaluation framework to analyze the security and privacy features of four cloud storage services: Sync, pCloud, IceDrive, and Egnyte[21]. The data collection process involved a systematic review of each platform's documentation, user manuals, and security white papers. Additionally, direct interactions with each service were conducted to verify the features and performance claims. The evaluation criteria were divided into three main categories: secure collaboration, compliance, governance, and privacy, and data security.

For secure collaboration, we examined aspects such as user authentication, two-factor authentication, encryption standards, password policy management, and integration with directory services like Active Directory and LDAP. Compliance, governance, and privacy were assessed based on each service's adherence to industry standards and regulations, including GDPR, HIPAA, and ISO27001, and their ability to define, control, alert, and remediate potential security incidents. Data security was evaluated through encryption methods, both in transit and at rest, zero-knowledge encryption protocols, and the presence of compliance certifications[21].

Each feature was meticulously tested where applicable, and qualitative assessments were supported by quantitative data when available. The comparison aimed to provide a detailed understanding of how each platform addresses critical security and privacy challenges. This methodical approach

ensures that the study's findings are robust, replicable, and provide valuable insights for users and organizations considering these cloud storage options[21].

Table 14 provides a detailed comparison of four cloud storage platforms—Sync, pCloud, IceDrive, and Egnyte—across three main criteria: secure collaboration, compliance, governance, privacy, and data security[21].

The tables are organized in such a way that the columns are named by the criteria of comparison, such: Secure Collaboration, Compliance, Governance, and Privacy and Data Security. to continue with the next column which indicates Cloud storages and their properties according to criteria of comparison[21]. We compare cloud storages and give information according to their properties. In terms of secure collaboration, Sync offers features like user authentication, two-factor authentication, end-to-end encryption, AES-256 bit encryption, password protection, TLS encryption, and client-side encryption. pCloud provides user authentication, two-step login verification, TLS/SSL encryption, encryption in transit, password protection, private key encryption, client-side encryption, and Swiss data protection. IceDrive stands out with user authentication, the Twofish protocol, zero-knowledge encryption, and two-factor authentication. Egnyte excels with comprehensive features including user authentication, two-step login verification, login credentials password policy management, Active Directory/LDAP/single sign-on integration, roles-based administration, repository permissions, encryption in transit, encryption at rest, Egnyte object store file encryption and key management, and application and data vulnerability detection[21].

Regarding compliance, governance, and privacy, Sync focuses on control, define, and alert mechanisms. pCloud emphasizes authentication, define, and alert processes, while IceDrive offers control, define, and alert capabilities. Egnyte provides a broader scope with discover, define, remediate, alert, report, and retire functions[21]. In data security, Sync ensures end-to-end encryption, SOC 2 Type 1 compliance, no third-party tracking, HIPAA compliance, GDPR compliance, and PIPEDA compliance. pCloud complies with GDPR, ISO 9001:2015, ISO 27001:2013, SSAE 18 SOC 2 Type II, and SSAE 16 SOC 2 Type II. IceDrive features Twofish encryption, client-side encryption, and zero-knowledge encryption. Egnyte is certified with SOC 2, ISO27001, and complies with standards for financial services, healthcare, and EU customers. This comprehensive comparison highlights the strengths and specific security features of each platform, aiding users in making informed decisions based on their security and privacy needs.

Discussion

Data security and data privacy remains one of the main challenges in the world of technology. In the rapidly evolving landscape of cloud storage, where the digital world converges with our daily lives, security and privacy considerations stand as the bedrock of trust between users and service providers. The journey through the analysis of popular cloud storage platforms, including Sync, pCloud, IceDrive, and Egnyte, has unveiled a myriad of insights into the measures taken to protect data in this interconnected realm. The primary takeaway from this examination is the importance of zero-knowledge encryption, which ensures that user data remains private and inaccessible even to the service providers themselves. Platforms like Sync and IceDrive employ this robust encryption standard, providing users with a high level of security and privacy. Encryption in transit and at rest, as well as compliance with industry standards such as GDPR and HIPAA, add layers of protection and regulatory compliance, further bolstering confidence in these services. Secure collaboration features, such as two-factor authentication and role-based access controls, play a pivotal role in preventing unauthorized access and safeguarding sensitive data. While Sync, pCloud, and Egnyte offer robust collaboration security, IceDrive stands out with its Twofish encryption and zero-knowledge authentication. However, it's crucial to note that no service is without its limitations. Sync, while excelling in security, lacks the availability of a Linux client, limiting its accessibility to a certain user base. Similarly, Egnyte's data access rights, even for improving services, raise questions about data privacy. The choice of a cloud storage provider should align with individual or organizational requirements, striking a balance between security, accessibility, and usability. Each platform evaluated in this study has its strengths and weaknesses, making it essential for users to conduct a thorough assessment of their specific needs and priorities. As we move forward in this digital age, where data is increasingly valuable and the threat landscape continuously evolves, it is incumbent upon users to remain vigilant and informed. Cloud storage providers will continue to enhance their security and privacy features to adapt to emerging challenges. Consequently, users must stay up-to-date with the evolving landscape and regularly assess their chosen cloud storage solutions.

Conclusions

In conclusion, our research reveals distinctive security features among the assessed cloud platforms. Sync sets itself apart by employing zero-knowledge encryption as a standard, ensuring heightened data protection. The use of TLS/SSL encryption for secure user connections and client-side encryption with 256-bit AES enhances the overall security of data transmission and storage. Sync's limited third-party integrations contribute positively to security by minimizing potential vulnerabilities. However, it's worth noting that Sync is not currently available for Linux users. The annual billing model provides users with a predictable payment structure. IceDrive emphasizes hermetic encryption with zero-knowledge, offering an exclusive secondary encrypted disk for paying customers. Similarly, pCloud prioritizes security with TLS/SSL encryption and client-side encryption using 256-bit AES. Egnyte focuses on user data privacy by encrypting stored data on servers, but users should be aware that, following the access agreement, Egnyte retains the right to access user data for service and product improvement. Each

platform presents unique security considerations, and users should weigh these factors based on their individual preferences and priorities.

In conclusion, the digital era has bestowed upon us unparalleled convenience, enabling us to access our data from virtually anywhere. Yet, with this convenience comes responsibility. It is our duty, as users and organizations, to safeguard our data, respecting the trust we place in cloud storage providers. With careful consideration and an understanding of the security and privacy measures in place, we can navigate the cloud with confidence, knowing that our data remains secure and our privacy intact in this ever-changing digital world. The field of cloud storage security and privacy is dynamic and ever evolving. Future research efforts should continue to adapt to emerging technologies and threats while striving to enhance the security and privacy of data stored in the cloud. Additionally, collaboration between researchers, industry stakeholders, and policymakers is essential to develop comprehensive solutions that address the evolving challenges of cloud storage security and privacy.

Data availability

Underlying data

Open Science Framework: Comparative analysis of identity management, access control, and authorization practices in public and private universities. https://doi.org/10.17605/OSF.IO/8SYAZ[21].

Acknowledgements

The authors would like to acknowledge Faculty of Computer Science, for their valuable contributions to this research. Their support was instrumental in the completion of this work.

References

1. The University of North Carolina at Chapel Hill: **Introduction to cloud storage**. **Reference Source**
2. Savill J: **Microsoft Azure infrastructure services for architects: designing cloud solutions.** Wiley, 2019. **Reference Source**
3. Liu A, Yu T: **Overview of cloud storage.** *Int J Sci Technol Res.* ffhal-02889947, 2018. **Reference Source**
4. Ravulavaru A: **Cloud-Native Applications in Java: Build and Deploy Microservices-Based Applications on Kubernetes.** Packt Publishing, 2021.
5. Erl T, Mahmood Z, Puttini R: **Cloud computing concepts, technology & architecture.** *The Prentice Hall Service Technology Series.* ISBN-10: 9780133387520, ISBN-13: 978-0133387520. **Reference Source**
6. Evans M, Huynh T, Le K, *et al.*: **Cloud storage**. **Reference Source**
7. **The University of North Carolina at Chapel Hill.** Chapel Hill, North Carolina. **Reference Source**
8. Hwang K, Dongarra J, Fox G: **Distributed and cloud computing: from parallel processing to the Internet of Things.** 1st Edition, ISBN-10: 9789381269237, ISBN-13: 978-9381269237.
9. Raphael CF: **Cloud storage for dummies.** ISBN-10: 1119467698, ISBN-13: 978-1119467693.
10. Poulton N: **Data storage networking: real world skills for the comptia storage+ certification and beyond.** ISBN-10: 1118105356, ISBN-13: 978-1118105350.
11. Zhao L: **Cloud Data management.** ISBN-10: 3030143636, ISBN-13: 978-3030143633.
12. TechRadar Review Team: **IceDrive review.** *TechRadar.* 2022; Accessed June 9, 2024. **Reference Source**
13. Cloudwards Review Team: **Icedrive review 2024: cloud storage pricing, features & security.** *Cloudwards.* 2024; Accessed June 9, 2024. **Reference Source**
14. How-To Geek Review Team: **Comprehensive review of IceDrive.** *How-To Geek.* 2023; Accessed June 9, 2024. **Reference Source**
15. Yeluri R, Castro-Leon E: **Building the infrastructure for cloud security: a solutions view.** ISBN-10: 1430261463, ISBN-13: 978-1430261467. **Reference Source**
16. Mather T, Kumaraswamy S, Latif S: **Cloud security and privacy: an enterprise perspective on risks and compliance.** ISBN-10: 0596802765, ISBN-13: 978-0596802769. **Reference Source**
17. Jacob B, Ng SW, Wang DT: **Data storage: principles and practices.** ISBN-10: 0123797516, ISBN-13: 978-0123797513.
18. Dutt DG: **Cloud native data center networking: architecture, protocols, and tools.** ISBN-10: 1492045565, ISBN-13: 978-1492045562.
19. Binnie C: **Cloud native security: monitoring and detecting attacks.** ISBN-10: 111977226X, ISBN-13: 978-1119772261.
20. Leonardo G: **Hands-on cloud solutions with azure: architecting, developing, and managing cloud-native applications.** ISBN-10: 1789538463, ISBN-13: 978-1789538468.
21. Mollakuqe E, Hamdiu E, Fishekqiu NS, *et al.*: **Comparison of cloud storage in terms of privacy and personal data – Sync, pCloud, IceDrive and Egnyte**. **http://www.doi.org/10.17605/OSF.IO/738TH**