Blockchain Frontier Technology (B-Front)
Vol. 5, No. 2, 2026, pp. 183∼193
E-ISSN: 2808-0009 P-ISSN: 2808 0831, DOI:10.34306

Comparative Analysis of Cloud Storage Architectures for Scalability and Security

Wahyu Nur Wahid[1*], Fitri Nurdianingsih[2], Jonathan Parker[3]

[1]Faculty of Economic and Business, Alfabet Inkubator Indonesia, Indonesia
[2]Department of English Education, State University of Semarang, Indonesia
[3]Faculty of Economic and Business, Rey Incorporation, USA
[1]nur.wahid@raharja.info, [2]fitrinurdianingsih22@students.unnes.ac.id,[3]p.jonparker@rey.zone,
***Corresponding Author**

Article Info

Article history:

Submission, 26-06-2025
Revised, 08-12-2025
Accepted, 30-12-2025

Keywords:

IPFS
Data Integrity
Distributed Systems
Cloud Storage
Decentralization

ABSTRACT

This study compares the scalability and security of the InterPlanetary File System (IPFS) and traditional cloud storage platforms. As global data traffic continues to rise, traditional centralized cloud services, like AWS S3 and Google Cloud Storage, face increasing challenges in terms of scalability, security, and data sovereignty. In contrast, IPFS offers a decentralized, content-addressed storage model that enhances data integrity and resilience. This **research uses** a combination of qualitative and quantitative methods, including a literature review, performance benchmarking, and security assessments. The **evaluation** involved testing various file sizes, monitoring data availability over seven days, and conducting fault tolerance simulations. The **findings** reveal that traditional cloud platforms provide stable, predictable performance, low latency, and high availability, making them suitable for enterprise applications. However, IPFS with its decentralized architecture, excels in ensuring data integrity and resilience in distributed environments, although it experiences performance variability and lacks built-in encryption and access control. **These** factors make IPFS less viable in regulated settings. The **study concludes** that IPFS and traditional cloud storage should not be seen as alternatives, but as complementary systems. A hybrid approach, combining the strengths of both, can support scalable, secure, and sustainable digital infrastructures, aligning with SDG 9, which promotes innovation and resilient infrastructure development

DOI: http://10.34306/bfront.v5i2.857

1. INTRODUCTION

In the digital era, data has become one of the most valuable assets in modern society. Rapid advances in internet connectivity, cloud services, artificial intelligence, and smart devices have significantly increased the volume of digital data generated every second. Businesses, governments, academic institutions, and individuals increasingly rely on the ability to store, access, and protect data efficiently [1]. To address these demands, traditional cloud storage providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform have developed robust, centralized infrastructures capable of managing massive volumes of information. Despite their maturity and reliability, centralized cloud architectures raise critical concerns related to data sovereignty [2].

One of the major driving forces behind the search for alternative storage architectures is the exponential growth of global data traffic. According to the Cisco Annual Internet Report, global IP traffic reached 396 exabytes per month in 2022 and is projected to continue increasing rapidly in the coming years. This growth places significant pressure on centralized infrastructures, which must continuously scale server capacity, bandwidth, and redundancy mechanisms to maintain performance and availability.

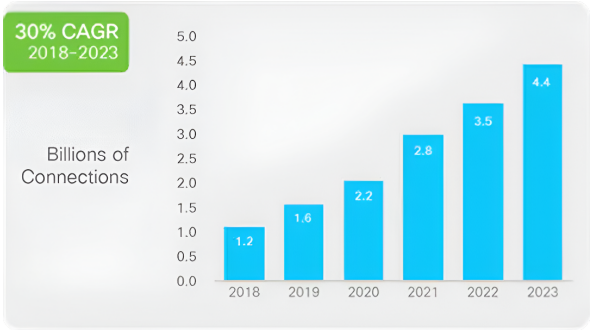

Figure 1. Global IP Traffic Growth, 2018–2023
Source: Cisco Annual Internet Report, 2023.

As shown in Figure 1 while traditional cloud storage services attempt to address these challenges through automated scaling and integrated security tools, they fundamentally rely on location-addressed architectures, where data is retrieved based on server locations [3]. In contrast, decentralized storage technologies such as the IPFS adopt a content-addressed and peer-to-peer architecture, in which files are identified and retrieved using cryptographic hash values rather than fixed server addresses [3]. This architectural shift enables improved data integrity, resistance to tampering, and enhanced availability across distributed networks. As a result, IPFS has gained increasing attention in domains such as decentralized finance, digital preservation, and censorship-resistant publishing [4]. Although prior studies have discussed the conceptual advantages and limitations of both centralized cloud storage and IPFS, empirical comparisons that simultaneously evaluate scalability and security using experimental benchmarking remain limited. Most existing works focus either on theoretical analysis or on isolated use cases, leaving a gap in systematic, data-driven evaluations between these two storage paradigms under comparable conditions [5].

This study conducts a distributed systems of IPFS and traditional cloud storage solutions with a focus on scalability and security as two critical pillars of modern data infrastructure. The research aims to investigate whether IPFS can function as a viable alternative or a complementary solution to traditional cloud systems, particularly in scenarios requiring decentralization, resilience, and data immutability. To guide the analysis, this study is structured around the following research questions:

- RQ1: How do IPFS and traditional cloud storage systems compare in terms of scalability under varying data loads and network conditions?
- RQ2: What are the key differences in security characteristics between IPFS and traditional cloud storage, particularly regarding data integrity, access control, and resilience to failures?
- RQ3: Based on experimental results, what implications do these differences have for the adoption of hybrid storage models in modern digital infrastructures?

By addressing these research questions through a combination of literature review, performance benchmarking, and qualitative security assessment, this study seeks to provide objective insights for researchers, practitioners, and policymakers regarding the evolving landscape of data storage architectures [6, 7].

As a response to these challenges, decentralized storage technologies such as the IPFS are gaining attention. IPFS offers a content addressable storage model that is distributed across networks, which addresses some of the key issues of centralized cloud systems, such as data immutability, resilience, and data sovereignty [8]. This study explores how such decentralized solutions could contribute to more sustainable digital infrastructure [9, 10]. The infrastructure shift toward decentralized and distributed systems aligns with SDGs 9 (Industry, Innovation, and Infrastructure), which aims to foster innovation and build resilient infrastructure.

By leveraging decentralized technologies, organizations can improve data management scalability while also reducing dependence on centralized cloud providers, leading to more sustainable, secure, and transparent infrastructure.

2. LITERATURE REVIEW

2.1. The Evolution of Data Storage Technologies

Data storage technologies have undergone significant transformation over the past decades, evolving from physical storage media such as magnetic tapes and hard disk drives to large-scale cloud-based platforms [11]. Traditional cloud storage providers, including AWS, Google Cloud, and Microsoft Azure, have become the backbone of contemporary digital services by offering high availability, elastic scalability, and managed infrastructure [12]. These platforms enable organizations to handle rapidly increasing data volumes efficiently while reducing the complexity associated with on premise infrastructure management [13].

Despite these advantages, recent studies have identified inherent limitations within centralized cloud storage models, particularly in relation to data sovereignty, long-term operational costs, and dependency on single service providers [14, 15]. The growing frequency of large-scale data breaches and concerns regarding vendor lock-in have further intensified critical discussions surrounding centralized data governance and control [16]. In response to these challenges, decentralized storage systems have emerged as an alternative paradigm. By distributing data across multiple nodes rather than relying on centralized servers, decentralized storage aims to enhance system resilience, data availability, and fault tolerance under adverse conditions [17]. However, empirical comparative studies that systematically evaluate decentralized and centralized storage models especially in terms of scalability and security remain limited, indicating a need for further investigation [18].

2.2. IPFS and Decentralized Storage

IPFS represents a decentralized approach to data storage that seeks to address several structural limitations of centralized systems [19, 20]. Distributed systems traditional cloud storage, which relies on location-based addressing and centralized data centers, IPFS employs a content addressable storage mechanism in which each file is identified by a unique cryptographic hash [21]. This design enhances data integrity, as any modification to stored content results in a different hash value, making unauthorized alterations immediately detectable [22].

Recent developments have expanded the applicability of IPFS through integration with blockchain technologies, enabling its use in smart contracts, decentralized applications, and distributed data management frameworks [23]. These characteristics position IPFS as a promising infrastructure for applications that require transparency, immutability, and distributed trust. Nevertheless, despite its architectural advantages, IPFS continues to face adoption challenges, particularly in enterprise environments [24, 25]. The absence of native encryption and built-in user access control mechanisms poses a significant barrier for deployment in regulated sectors that demand strict compliance, auditing, and confidentiality requirements [26]. In addition, usability constraints and the lack of standardized governance models may limit organizational scalability and broader adoption [27]. While IPFS adoption has increased in areas such as supply chain management and decentralized finance (DeFi), these limitations suggest that IPFS currently functions more effectively as a complementary technology rather than a full replacement for traditional cloud storage in enterprise contexts [28].

2.3. Scalability Comparison: IPFS vs Traditional Cloud

Scalability is a critical factor in evaluating modern data storage solutions. Traditional cloud service providers utilize auto-scaling mechanisms, globally distributed data centers, and Service Level Agreements (SLAs) to maintain stable performance under varying workloads [29, 30]. These managed infrastructures enable cloud platforms to deliver predictable throughput, controlled latency, and consistent service quality, which are essential for enterprise applications and high traffic digital services [31].

In contrast, IPFS achieves scalability through horizontal expansion by distributing data across a peer-to-peer network [32]. While this decentralized approach allows IPFS to scale organically as network participation increases, its performance is inherently influenced by network conditions, node availability, and data replication strategies [33]. Prior studies indicate that IPFS performs effectively in decentralized and geographically distributed environments, such as blockchain based systems and collaborative data networks. However, it may experience performance limitations in latency sensitive or high-throughput scenarios where controlled infrastructure, bandwidth management, and predictable service guarantees are required [34, 35]. Consequently,

traditional cloud platforms continue to dominate enterprise deployments where scalability consistency, operational support, and performance predictability remain critical requirements [36].

2.4. Security Implications in Decentralized and Centralized Storage

Security considerations play a fundamental role in the design and selection of data storage systems, encompassing confidentiality, integrity, and availability [37]. Traditional cloud providers invest extensively in comprehensive security frameworks [38]. These features are typically integrated into cloud service architectures, offering organizations centralized security management and regulatory compliance support.

Decentralized storage systems such as IPFS address security from a different perspective. Through its content-addressing mechanism and distributed architecture, IPFS inherently enhances data integrity and resistance to tampering, as any unauthorized modification alters the content hash and invalidates the reference [39]. However, IPFS does not provide native encryption or fine-grained access control by default, requiring additional application layer security mechanisms to protect sensitive data [39]. This distinction highlights a fundamental trade off between decentralization and managed security services [40]. While IPFS excels in ensuring data immutability and censorship resistance, traditional cloud platforms remain more suitable for environments that demand security management, regulatory compliance, and controlled data access.

3. RESEARCH METHOD

This study adopts a comparative qualitative–quantitative research design to analyze and evaluate the performance of IPFS and traditional cloud storage platforms, namely AWS S3 and Google Cloud Storage, with a specific focus on scalability and security aspects. The methodological framework is aligned with the research questions formulated in the Introduction, ensuring consistency between the problem formulation, experimental setup, and analytical interpretation. A multi method approach is employed, consisting of a systematic literature review, controlled performance benchmarking, and a structured security assessment. This design allows the study to capture both empirical performance measurements and architectural characteristics of centralized and decentralized storage systems.

3.1. Centralized Cloud Architecture and Research Workflow

Each virtual machine is managed by a Virtual Machine Manager, while system performance, resource utilization, and fault conditions are continuously supervised by a virtual machine monitor. The virtual machines operate on top of multiple physical servers (Server 1 to Server n), enabling horizontal scaling, redundancy, and fault isolation. This architecture represents the centralized cloud storage model evaluated during the benchmarking phase and serves as a reference for comparison with the decentralized IPFS architecture [41].

The centralized cloud distributed systems architecture supports predictable scalability management through explicit orchestration and resource allocation mechanisms. Load balancing and virtual machine management enable workloads to be distributed efficiently across available resources, minimizing performance degradation under increasing demand. This controlled environment provides a stable foundation for evaluating scalability indicators such as throughput stability and latency behavior during the benchmarking process.

System monitoring components play an essential role in maintaining service reliability and availability throughout the experiments. Continuous observation of resource utilization, system health, and fault conditions allows the infrastructure to respond dynamically to disruptions. These distributed systems characteristics are particularly relevant for assessing data availability and fault tolerance, as they reflect how centralized cloud platforms sustain operational continuity through redundancy and automated recovery mechanisms.

The centralized control model also introduces specific implications for security and governance evaluation. Integrated authentication mechanisms, identity and access management, and centralized policy enforcement enable fine-grained control over data usage and permissions. These architectural features provide a concrete basis for analyzing security aspects such as access control effectiveness, compliance readiness, and resistance to unauthorized access, which differ fundamentally from the decentralized trust model of IPFS.

This architectural representation into the research workflow, the study establishes a methodologically consistent baseline for comparison. Clearly defining orchestration, monitoring, and fault-handling mechanisms on the cloud side ensures that observed differences in scalability and security performance can be attributed to architectural design choices rather than experimental inconsistencies. This approach strengthens the validity and interpretability of the comparative analysis between centralized cloud storage and decentralized IPFS systems.

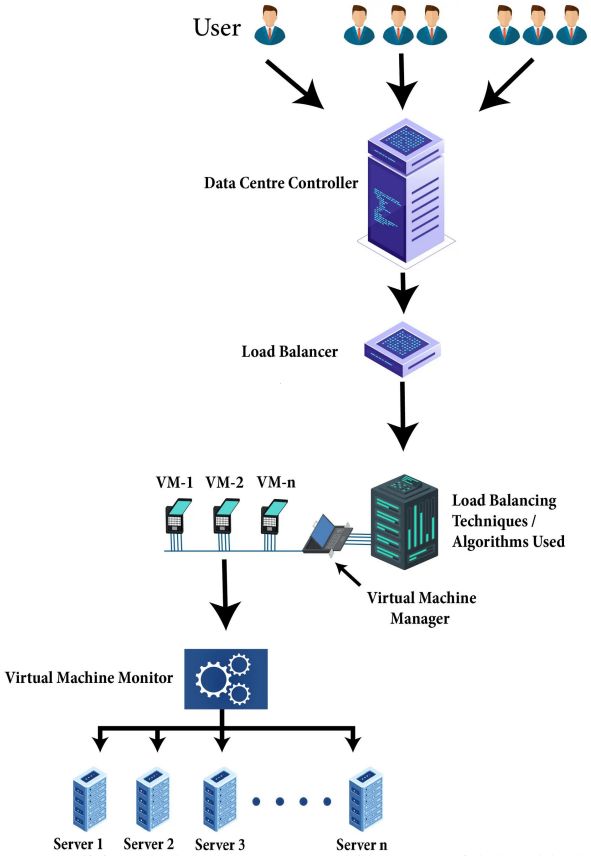

Figure 2. Traditional cloud storage architecture with load balancing.

Figure 2 illustrates the conceptual architecture of the traditional centralized cloud storage environment used as the baseline model in this study. Multiple users submit service requests that are first handled by a Data Centre Controller, which coordinates incoming traffic and forwards requests to a Load Balancer. The load balancer distributes workloads across multiple Virtual Machines (VM-1 to VM-n) using predefined load balancing techniques and algorithms.

This architectural representation is essential for ensuring methodological fairness in the comparative evaluation. By explicitly modeling request routing, load balancing, virtual machine management, and monitoring layers, the study establishes a clear baseline for how scalability and fault tolerance are achieved in centralized cloud environments. This baseline architecture allows performance metrics such as latency, throughput stability, availability, and failure recovery to be interpreted in relation to well-defined control and orchestration mechanisms, thereby enabling a structured and consistent comparison with the decentralized IPFS architecture examined in this study [42].

3.2. Benchmarking Metrics and Tools

Performance evaluation in this study focused on scalability-related metrics, including upload speed, download speed, latency, data availability, and fault tolerance. These metrics were selected because they represent critical indicators of storage system performance under increasing data loads and varying network conditions. Upload and download speeds reflect throughput efficiency, latency indicates responsiveness, while data availability and fault tolerance capture system reliability and resilience in real-world usage scenarios.

Data availability and fault tolerance were evaluated through longitudinal monitoring and simulated failure scenarios. Data availability was measured as the percentage of successful file access attempts over a seven-day observation period, while fault tolerance was assessed by intentionally introducing node or service disruptions and observing system behavior and recovery. These metrics provided insight into how each storage model handles partial failures, network instability, and redundancy, offering a comprehensive view of scalability beyond raw throughput performance.

Table 1. Performance Benchmark Metrics and Tools

Metric	Definition	Tool/Method Used
Upload Speed	Time taken to upload files (MBps)	Custom Python Script, cURL
Download Speed	Time taken to retrieve files (MBps)	wget, cURL
Latency	Response time during file retrieval (ms)	Ping, Traceroute
Data Availability	File accessibility rate (%) over 7 days	Cron Job Monitoring
Fault Tolerance	System behavior during failure scenarios	Simulated Node Shutdown

As summarized in Table 1, the selected benchmarking metrics are designed to capture both performance scalability and system resilience across storage platforms. Upload speed, download speed, and latency represent core throughput and responsiveness indicators, while data availability and fault tolerance evaluate system stability under prolonged operation and failure conditions [43]. By applying consistent tools and measurement procedures for each metric, the study ensures comparability between centralized cloud storage and decentralized IPFS environments, allowing observed differences to be attributed to architectural characteristics rather than measurement bias.

3.3. Data Analysis Techniques

Quantitative data obtained from the performance benchmarking experiments were analyzed using statistical averaging and variance calculations to assess consistency and performance stability across different test [44]. Metrics such as upload speed, download speed, and latency were computed from repeated measurements to minimize random fluctuations and provide representative performance values for each storage platform. This approach allows a more objective comparison between IPFS, AWS S3, and Google Cloud Storage under comparable conditions [43].

To support interpretability, the quantitative results were further visualized using graphical representations, including bar charts and line graphs. These visual tools were employed to highlight performance trends across varying file sizes and network environments, as well as to illustrate differences in performance variability between decentralized and centralized storage architectures [45]. Visualization helped identify patterns that were not immediately evident from numerical summaries alone, particularly regarding performance consistency and scalability behavior [46].

Security-related data were analyzed using qualitative assessment techniques, focusing on a comparative evaluation of key security dimensions across the tested platforms. These dimensions included compliance with recognized industry standards, encryption mechanisms, access control models, data integrity assurance, and exposure to potential system vulnerabilities. The qualitative analysis aimed to contextualize technical features within practical deployment considerations, especially for enterprise and regulated environments.

The dataset was normalized to enable fair comparisons across heterogeneous storage systems. Performance patterns were identified by examining results across different file sizes and network conditions. Finally, the strengths and weaknesses of each storage model were evaluated based on established scalability and security criteria, forming the basis for the comparative discussion and conclusions presented in this study.

4. RESULT AND DISCUSSION

4.1. Scalability Performance Analysis

The first objective of this study was to evaluate the scalability performance of IPFS and traditional cloud storage platforms under increasing data loads [47]. Quantitative benchmarking tests were conducted through upload and download trials for each platform across three file sizes (5 MB, 50 MB, and 500 MB) under controlled network conditions.

The narrow variance observed in cloud platforms can be attributed to centralized resource provisioning, managed bandwidth allocation, and automated load balancing. It should be noted that the cloud services were tested under standard service conditions without intentional bandwidth throttling. However, peak global traffic loads were not simulated, representing a limitation of the controlled environment. Regarding download performance, AWS S3 and Google Cloud Storage consistently maintained low latency (below 80 ms), whereas IPFS latency fluctuated between 120 ms and 200 ms, particularly for larger file sizes. Nevertheless, during simulated geographically distributed access [32].

Table 2. Scalability Performance Benchmark Results

Platform	File Size	Avg Upload Speed (MBps)	Std. Dev. (MBps)	Avg Download Speed (MBps)	Avg Latency (ms)
AWS S3	5 MB	80.2	±2.8	92.4	58
AWS S3	50 MB	78.5	±3.1	89.7	63
AWS S3	500 MB	75.6	±3.7	85.2	74
Google Cloud Storage	5 MB	76.8	±3.0	90.1	60
Google Cloud Storage	50 MB	74.2	±3.5	87.3	66
Google Cloud Storage	500 MB	71.9	±4.1	82.8	78
IPFS	5 MB	58.4	±7.2	70.6	118
IPFS	50 MB	47.9	±8.9	63.4	152
IPFS	500 MB	39.6	±12.7	55.1	198

As shown in Table 2 traditional cloud services exhibited highly stable and predictable throughput. AWS S3 achieved an average upload speed of approximately 78 MBps with low variance, while Google Cloud Storage averaged 74 MBps. In contrast, IPFS demonstrated significantly higher performance variance, with upload speeds ranging from 35 MBps to 60 MBps, depending on peer availability and replication strategy.

4.2. Data Availability and Fault Tolerance Analysis

Beyond throughput and latency, this study evaluated data availability and fault tolerance to assess system resilience. Data availability was measured as the percentage of successful file retrievals over a continuous seven-day period, while fault tolerance was examined through ten simulated failure scenarios.

Platform	Availability Rate (%)	Downtime Incidents	Primary Cause
AWS S3	100%	0	Centralized redundancy
Google Cloud Storage	100%	0	Multi-zone replication
IPFS (High Replication)	96%	2	Temporary peer unavailability
IPFS (Low Replication)	92%	5	Limited peer hosting

Table 3. Data Availability Results Over a 7-Day Observation Period

The fault tolerance results in Table 3 show that IPFS is inherently resilient to localized failures, as content remains accessible as long as at least one peer hosts the data. However, coordinated peer unavailability led to temporary access delays, highlighting the dependency of IPFS resilience on network health and replication strategy. In contrast, cloud platforms demonstrated seamless recovery due to centralized redundancy.

4.3. Security Evaluation Results

From a security perspective, traditional cloud storage platforms provide comprehensive, integrated security frameworks. These include AES-256 encryption at rest and in transit, centralized Identity and Access Management (IAM), detailed audit logging, and compliance with international standards such as ISO/IEC 27001 and GDPR. Such features are enabled by default and managed directly by the service providers, making them well-suited for regulated industries requiring strict governance and accountability.

In contrast, IPFS relies on content-addressing and immutability, where data integrity is ensured through cryptographic hash verification. Any modification to stored content results in a new hash, making unauthorized tampering immediately detectable. This mechanism provides strong guarantees for data integrity and provenance. However, IPFS does not natively support encryption or fine grained access control, requiring these security layers to be implemented at the application level or through third party integrations [48].

This limitation represents a significant barrier to IPFS adoption in regulated enterprise environments, where confidentiality [49]. While IPFS is inherently more resistant to censorship and centralized attacks due to its decentralized architecture, traditional cloud platforms remain superior for use cases requiring controlled access, compliance auditing, and end-to-end managed security [50].

Synthesizing the scalability, availability, and security results reveals clear architectural trade-offs between the two storage paradigms. Traditional cloud platforms leverage location-addressed storage, centralized infrastructure, and managed services to deliver predictable performance, strong governance, and compliance-ready security. These characteristics make them ideal for enterprise workloads involving high transaction volumes, low latency requirements, and sensitive data. Conversely, IPFS employs a content-addressed, peer-to-peer architecture, which shifts scalability from centralized resource provisioning to network-wide participation. This design enhances data integrity, resilience to censorship, and distributed availability but introduces performance variability and additional security integration requirements. Consequently, IPFS excels in decentralized applications, open data repositories, blockchain ecosystems, and collaborative research environments where data immutability and resilience are prioritized over strict access control. Importantly, the findings indicate that IPFS and traditional cloud storage should not be viewed as direct substitutes. Instead, they can function as complementary components within hybrid storage architectures. For example, latency-sensitive and frequently updated datasets can be stored on traditional cloud platforms, while immutable metadata, archival records, or cryptographic proofs can be stored on IPFS to ensure long-term integrity and transparency.

IPFS ability to scale effectively in distributed networks and provide a more resilient solution for data management highlights its potential as a complementary technology to traditional cloud solutions. As organizations face increasing pressure to manage massive volumes of data efficiently, hybrid storage solutions, combining the strengths of both centralized cloud systems and decentralized technologies like IPFS, are emerging as a practical approach to meet the evolving demands of modern infrastructures. These hybrid models can contribute to the goals outlined in SDGs 9, helping organizations to build more resilient, sustainable, and innovative infrastructure.

5. MANAGERIAL IMPLICATIONS

The findings of this study provide several important managerial implications for decision-makers responsible for designing and managing data storage infrastructures in modern digital organizations. As organizations increasingly depend on complex data storage systems, balancing performance, scalability, security, and operational requirements becomes essential. This study emphasizes the need for a nuanced approach to storage infrastructure design, particularly with the growing relevance of decentralized technologies alongside traditional cloud-based systems. The following subsections offer managerial strategies for integrating centralized and decentralized storage systems, aiming to optimize operational effectiveness and support long-term organizational goals.

5.1. Cloud Storage in Enterprise and Compliance-Driven Environments

Managers in enterprise and compliance-driven environments should recognize that traditional cloud storage platforms, such as AWS S3 and Google Cloud Storage, remain the most appropriate choice for latency-sensitive operations, high-throughput workloads, and regulated data handling. Their integrated security mechanisms, predictable scalability, and compliance readiness make them suitable for operational systems that require strict access control, continuous availability, and standardized governance. From a managerial perspective, this implies that centralized cloud storage should continue to serve as the backbone for core business processes and mission-critical applications.

Moreover, as data governance and security regulations become more stringent, organizations must ensure that their cloud infrastructure adheres to the required standards. Cloud platforms like AWS and Google Cloud offer a comprehensive set of compliance certifications that ease the process of regulatory adherence. For decision-makers, it is essential to recognize the long-term value of relying on these centralized platforms for sensitive data, which will enable them to meet both internal and external compliance requirements, thus supporting business continuity and reducing risk exposure.

5.2. Strategic Value of IPFS for Data Integrity and Resilience

The results highlight that IPFS offers distinct strategic value when data integrity, immutability, and resilience against centralized failures are prioritized. Managers overseeing blockchain-based systems, digital

archiving, research data repositories, or provenance-sensitive applications can leverage IPFS as a complementary storage layer rather than a full replacement for cloud infrastructure. By utilizing IPFS for immutable records, audit trails, metadata storage, or long-term archival content, organizations can enhance transparency and trust while reducing dependency on centralized control. However, managers must also account for the absence of native encryption and access control in IPFS by allocating additional resources for application layer security integration and governance policies.

Furthermore, the use of IPFS can significantly improve the overall resilience of data storage systems, particularly when centralized platforms face outages or performance bottlenecks. However, implementing IPFS also requires careful consideration of the technical challenges involved in ensuring secure and efficient access to decentralized data. Managers must be proactive in investing in encryption solutions, secure key management, and data access protocols to safeguard the integrity of decentralized records. This approach allows organizations to capitalize on the strengths of both centralized and decentralized storage systems, providing a more robust and adaptable data storage infrastructure.

5.3. Hybrid Storage Architectures for Balancing Performance, Security, and Decentralization

Finally, this study suggests that hybrid storage architectures represent a pragmatic managerial strategy for balancing performance, security, and decentralization. From an operational standpoint, managers can optimize system design by storing frequently accessed and dynamically updated data in traditional cloud environments, while assigning immutable or less time-sensitive data to IPFS-based storage. Such an approach enables organizations to exploit the strengths of both architectures while mitigating their respective limitations.

This hybrid approach not only provides operational efficiency but also ensures data security and compliance in various environments. By strategically adopting a hybrid storage model, organizations can create a more flexible, cost-effective, and resilient infrastructure. It enables businesses to maintain critical data in high-performance cloud environments while benefiting from the decentralized advantages of IPFS, thus enhancing transparency, data integrity, and long-term resilience. For this model to succeed, ongoing monitoring, performance evaluation, and regular updates to security protocols will be crucial in maintaining the system's effectiveness and alignment with organizational goals. This flexibility enables businesses to stay agile in response to evolving industry demands and technological advancements. By adopting a hybrid storage approach, companies can ensure that their data infrastructure remains both scalable and future-ready.

6. CONCLUSION

This study has provided a comparative analysis of the InterPlanetary File System (IPFS) and traditional cloud storage solutions by examining two critical dimensions, namely scalability and security, through a combination of literature review, controlled benchmarking, and qualitative security assessment. The findings indicate that traditional cloud platforms such as AWS S3 and Google Cloud Storage deliver more stable and predictable performance under controlled, high-throughput conditions, supported by mature infrastructure, automated scaling, and integrated security services. In contrast, IPFS demonstrates a decentralized architecture that offers strong advantages in data integrity, content immutability, and resistance to censorship, particularly in geographically distributed and peer-based access scenarios.

Despite its architectural strengths, the results also reveal that IPFS currently faces significant limitations for enterprise-scale adoption. The absence of native encryption and built-in access control mechanisms represents a critical security gap for regulated and compliance-driven environments, while performance variability caused by peer availability affects scalability consistency in controlled settings. Conversely, traditional cloud systems maintain superior reliability and compliance readiness due to centralized governance, standardized security controls, and predictable service-level agreements. These findings suggest that IPFS and traditional cloud storage are not direct substitutes, but rather complementary technologies whose effectiveness depends on application context and operational requirements.

Based on these insights, future research should further investigate hybrid storage architectures that integrate the strengths of both systems, such as deploying traditional cloud storage for latency-sensitive and frequently updated data, while leveraging IPFS for immutable data, archival content, or provenance-critical metadata. Expanding experimental evaluations to larger and more diverse network topologies, incorporating detailed fault tolerance and data availability metrics, and conducting advanced security testing including simulated cyberattacks would enhance the robustness of future studies. Additionally, improvements in IPFS usabil-

ity, governance frameworks, and enterprise integration mechanisms are essential to bridging the gap between decentralized storage technologies and mainstream data infrastructure adoption.

7. DECLARATIONS

7.1. About Authors

Wahyu Nur Wahid (WN) https://orcid.org/0009-0008-7236-2402
Fitri Nurdianingsih (FN) https://orcid.org/0000-0001-9806-7761
Jonathan Parker (JP) https://orcid.org/0009-0000-8585-3245

7.2. Author Contributions

Conceptualization: WN, and FN; Methodology: JP; Software: WN; Validation: JP and FN; Formal Analysis: WN ; Investigation: JP; Resources: FN; Data Curation: FN; Writing Original Draft Preparation: JP and FN; Writing Review and Editing: WN; Visualization: JP; All authors, WN, FN, and JP, have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

REFERENCES

[1] A. Badshah, A. Daud, R. Alharbey, A. Banjar, A. Bukhari, and B. Alshemaimri, "Big data applications: overview, challenges and future," *Artificial Intelligence Review*, vol. 57, no. 11, p. 290, 2024.
[2] M. M. Merlec and H. P. In, "Blockchain-based decentralized storage systems for sustainable data self-sovereignty: A comparative study," *Sustainability*, vol. 16, no. 17, p. 7671, 2024.
[3] Cisco, "Cisco annual internet report (2018-2023) white paper," 2023, accessed: 2025-12-27. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
[4] A. Ruangkanjanases, A. Khan, O. Sivarak, U. Rahardja, and S.-C. Chen, "Modeling the consumers' flow experience in e-commerce: The integration of ecm and tam with the antecedents of flow experience," *SAGE Open*, vol. 14, no. 2, p. 21582440241258595, 2024.
[5] K. Manikandan, V. Pamisetty, S. R. Challa, V. B. Komaragiri, K. Challa, and K. Chava, "Scalability and efficiency in distributed big data architectures: A comparative study," *Metallurgical and Materials Engineering*, vol. 31, no. 3, pp. 40–49, 2025.
[6] A. Ayesha, "A comparative study of efficient healthcare applications addressing scalability challenges in cloud computing," in *2025 International Conference on Next Generation Communication & Information Processing (INCIP)*. IEEE, 2025, pp. 956–960.
[7] S. Maheswari, N. Rajkumar, R. Geetha, K. Theja, M. Malleswari *et al.*, "A comparative analysis of iot platform tools: Security and scalability preferences in device management using ahp," in *2025 International Conference on Visual Analytics and Data Visualization (ICVADV)*. IEEE, 2025, pp. 380–385.
[8] R. Afzaal and H. B. U. Haq, "A review and comparative study of cloud computing and the internet of things," *Spectrum of Engineering and Management Sciences*, vol. 3, no. 1, pp. 18–27, 2025.
[9] S. S. Vellela, N. Malathi, S. Gorintla, K. K. Priya, T. S. Rao, R. Thommandru, and K. N. S. Rao, "A novel secure and scalable framework for a cloud-based electronic health record management system," in *2025 3rd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT)*. IEEE, 2025, pp. 131–135.

[10] T. Hidayat, D. Manongga, Y. Nataliani, S. Wijono, S. Y. Prasetyo, E. Maria, U. Raharja, I. Sembiring *et al.*, "Performance prediction using cross validation (gridsearchcv) for stunting prevalence," in *2024 IEEE International Conference on Artificial Intelligence and Mechatronics Systems (AIMS)*. IEEE, 2024, pp. 1–6.

[11] A. Sadique, H. Sehar, S. Nasim, and F. Nasim, "Data exposure risks in hybrid vs. multi-cloud migrations: a comparative analysis," *Journal of Applied Linguistics and TESOL (JALT)*, vol. 8, no. 1, pp. 213–224, 2025.

[12] S. Aslam and T. Fatima, "Optimizing real-time data processing for machine learning: A comparative study of ai-driven architectures," 2025.

[13] S. V. Subramanyam, "Cloud-based enterprise systems: Bridging scalability and security in healthcare and finance," *IJSAT-International Journal on Science and Technology*, vol. 16, no. 1, 2025.

[14] M. Almutairi and F. T. Sheldon, "Iot–cloud integration security: A survey of challenges, solutions, and directions," *Electronics*, vol. 14, no. 7, p. 1394, 2025.

[15] M.-H. Lin, R. Sivaraman, Z. Nan, U. Rahardja, I. Muda, F. S. Fahim, B. S. Bashar, L. Li, and I. Husein, "Capacity optimization design of hybrid energy power generation system." *Mathematical Modelling of Engineering Problems*, vol. 10, no. 4, 2023.

[16] S. Joshi, "Review, tutorials and introduction to cloud platforms for agentic genai: A comparative studies [pre-print]," *Tutorials and Introduction to Cloud Platforms for Agentic GenAI: A Comparative Studies [Pre-Print](February 15, 2025)*, 2025.

[17] S. Ebadinezhad and A. H. A. Alsaroah, "Comparative analysis of edge-based and cloud-based intrusion detection systems: A systematic literature review," in *2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)*. IEEE, 2025, pp. 707–714.

[18] Y. Sanjalawe, S. Al-E'mari, S. Fraihat, and S. Makhadmeh, "Ai-driven job scheduling in cloud computing: a comprehensive review," *Artificial Intelligence Review*, vol. 58, no. 7, p. 197, 2025.

[19] H. Eren, Ö. Karaduman, and M. T. Gençoğlu, "Security challenges and performance trade-offs in on-chain and off-chain blockchain storage: A comprehensive review," *Applied Sciences*, vol. 15, no. 6, p. 3225, 2025.

[20] U. Rahardja, M. A. Ngadi, A. Sutarman, D. Apriani, and E. A. Nabila, "A mapping study research on blockchain technology in education 4.0," in *2022 IEEE Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2022, pp. 1–5.

[21] A. Narayanan, "Adaptive anomaly recognition in distributed cloud infrastructures using advanced neural networks," *Available at SSRN 5637170*, 2025.

[22] M. Oberoi and L. Ahuja, "A comparative analysis on traditional and native cloud security mechanisms," *Available at SSRN 5241572*, 2025.

[23] R. Ayyadurai, K. Parthasarathy, M. Habib *et al.*, "The optimizing financial data transfers in the cloud: A comparative analysis of encryption and machine learning algorithms: Financial data transfers in the cloud data," *International Journal of Digital Innovation, Insight, and Information*, vol. 1, no. 01, pp. 01–13, 2025.

[24] Y. Bentayeb, K. Chaoui, and H. Badir, "Integrating blockchain and edge computing: A systematic analysis of security, efficiency, and scalability." *International Journal of Advanced Computer Science & Applications*, vol. 16, no. 1, 2025.

[25] B. Rawat and R. Bhandari, "Cloud computing applications in business development," *Startupreneur Business Digital (SABDA Journal)*, vol. 2, no. 2, pp. 143–154, 2023.

[26] G. Thakur and A. Ganpati, "Enhancing secure cloud storage: A four-tier architecture with chacha20 encryption, blake3 hashing, and dynamic chunk allocation in multi-cloud environment."

[27] A. Nuthalapati, "Scaling ai applications on the cloud toward optimized cloud-native architectures, model efficiency, and workload distribution," *International Journal of Latest Technology in Engineering, Management & Applied Science*, vol. 14, no. 2, pp. 200–206, 2025.

[28] I. G. W. A. Kurniawan, M. Sudiarta, L. M. Wahyuni, I. A. K. Sumawidari, K. Kasiani, M. Bernadetha, M. Zulfan, and F. Sinaga, "The rise of decentralized finance (defi): Opportunities for disruption in traditional financial models," *Journal of Education, Social & Communication Studies*, vol. 2, no. 2, pp. 128–136, 2025.

[29] N. S. Jamithireddy, "Integrating decentralized finance (defi) protocols into sap systems for automated payment processing," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable*

Applications, vol. 16, no. 2, pp. 346–366, 2025.
[30] A. Fernanda, M. Huda, and A. R. F. Geovanni, "Application of learning cloud computing technology (cloud computing) to students in higher education," *International Journal of Cyber and IT Service Management*, vol. 3, no. 1, pp. 32–39, 2023.
[31] R. Ajayi, "Integrating iot and cloud computing for continuous process optimization in real-time systems," *Int J Res Publ Rev*, vol. 6, no. 1, pp. 2540–2558, 2025.
[32] R. Shi, R. Cheng, Y. Fu, B. Han, Y. Cheng, and S. Chen, "Centralization in the decentralized web: Challenges and opportunities in ipfs data management," in *Proceedings of the ACM on Web Conference 2025*, 2025, pp. 4068–4076.
[33] R. Shi, Y. Fu, R. Cheng, B. Han, Y. Cheng, and S. Chen, "The decentralization dilemma: Performance trade-offs in ipfs and breakpoints," in *Proceedings of the 2025 ACM Internet Measurement Conference*, 2025, pp. 662–676.
[34] R. K. Mishra, R. K. Yadav, and P. Nath, "Integration of blockchain and ipfs: healthcare data management & sharing for iot environment," *Multimedia Tools and Applications*, vol. 84, no. 23, pp. 27 229–27 250, 2025.
[35] H. Herman, W. Achmad, N. Aulia, S. Rusdian, and T. Green, "Utilizing ipfs for decentralized data storage a security and censorship resistance solution," *Blockchain Frontier Technology*, vol. 5, no. 2, pp. 124–135, 2026.
[36] S. R. Mallick, R. K. Lenka, and S. Sobhanayak, "Secure and scalable dual blockchain and ipfs driven iot ecosystem for next gen healthcare systems," *Scientific Reports*, vol. 15, no. 1, p. 41064, 2025.
[37] G. Iovane and R. Amatore, "A decentralized storage and security engine (desse) using information fusion based on stochastic processes and quantum mechanics," *Applied Sciences*, vol. 15, no. 2, p. 759, 2025.
[38] B. P. Chintal, "Secure decentralized storage system using blockchain and ipfs," *Available at SSRN 5142864*, 2025.
[39] B. K. Mohanta, A. I. Awad, M. K. Dehury, H. Mohapatra, and M. K. Khan, "Protecting iot-enabled healthcare data at the edge: Integrating blockchain, aes, and off-chain decentralized storage," *IEEE internet of things journal*, 2025.
[40] N. Fahad and K. Gatlin, "Leveraging blockchain for decentralized and secure soc operations," *ResearchGate, Feb*, 2025.
[41] A. Elshamy, A. Alquraan, and S. Al-Kiswany, "A study of orchestration approaches for scientific workflows in serverless computing," in *Proceedings of the 1st workshop on SErverless systems, applications and Methodologies*, 2023, pp. 34–40.
[42] M. Abughazalah, W. Alsaggaf, S. Saifuddin, and S. Sarhan, "Centralized vs. decentralized cloud computing in healthcare," *Applied Sciences*, vol. 14, no. 17, p. 7765, 2024.
[43] M. V. Shevarev and S. V. Suvorov, "Dynamic content-oriented indexing and replication for high-performance storage and analysis of big data in the ipfs network," *Supercomputing Frontiers and Innovations*, vol. 12, no. 2, pp. 74–89, 2025.
[44] G. Mandinyenya and V. Malele, "Comparative security and performance evaluation of ipfs and filecoin for off-chain blockchain storage," *The Indonesian Journal of Computer Science*, vol. 14, no. 4, 2025.
[45] S. O. Adetugboboh, "Developing interoperable blockchain protocols for secure data migration in multi cloud environments," Doctoral dissertation, National College of Ireland, Dublin, 2025.
[46] B. Zhang, R. Shi, X. Li, and M. Zhang, "Decentralized identifiers based iot data trusted collection," *Scientific Reports*, vol. 15, no. 1, p. 4796, 2025.
[47] S. S. Manakhari and A. P. Jadhav, "Enhancing data security with decentralized cloud storage: an ipfs approach," in *World Congress in Computer Science, Computer Engineering & Applied Computing*. Springer Nature Switzerland, Jul. 2024, pp. 27–39.
[48] C. Binkowski, S. Appel, and A. Aßmuth, "Securing 3rd party app integration in docker-based cloud software ecosystems," *arXiv preprint arXiv:2405.11316*, 2024.
[49] S. Matey, D. Raut, R. B. Pansare, and R. Kant, "Prioritizing solutions to address the blockchain technology (bct) adoption barriers in manufacturing industries through the sf-bbwm and sf-codas hybrid framework," *Journal of Modelling in Management*, pp. 1–32, 2025.
[50] G. Bilakanti and S. D. Engineer, "Enhancing cloud security and compliance," *Journal of Cloud Computing and Security*, vol. 10, no. 2, pp. 45–59, 2025.