APTISI Transactions on Management (ATM)
Vol. 10, No. 1, 2026, pp. 11∼20
E-ISSN: 2622-6804 P-ISSN: 2622-6812, DOI:10.33050

A Comparative Analysis of Traditional and Decentralized Storage Systems in the Digital Age

Po Abbas Sunarya[1], Desy Apriani[2], Ruli Supriati[3], Danang Surya Budi[4*], John Edwards[5]
[1,4]Faculty of Economics and Business, University of Raharja, Indonesia
[2, 3]Faculty of Science and Technology, University of Raharja, Indonesia
[5]Department of Economics and Business, Pandawan Incorporation, New Zealand
[1]abas@raharja.info, [2]desy@raharja.info, [3]ruli@raharja.info, [4]danang.surya@raharja.info, [5]j.edwards@pandawan.ac.nz
***Corresponding Author**

Article Info

Article history:

Received August 26, 2025
Revised December 21, 2025
Accepted December 24, 2025

Keywords:

Storage Systems
Data Storage
IPFS
Cloud Storage
Scalability

ABSTRACT

The background of this research originates from the critical role of data storage in the advancement of modern digital technology, where centralized traditional cloud storage models have become dominant due to their accessibility and ease of data management. However, the challenges faced by these models include limited scalability, high operational costs, and vulnerabilities related to data security and privacy. In response to these limitations, the InterPlanetary File System (IPFS) has emerged as a decentralized storage solution that offers an alternative approach to data storage and distribution. **The objective of this study** is to compare IPFS and traditional cloud storage based on four key aspects: scalability, security, cost, and performance. **The methodology** involves a literature review and case studies of IPFS implementation in various practical scenarios. **The findings** reveal that while IPFS offers superior decentralization and resistance to data censorship, it still suffers from inefficiencies in data retrieval and challenges in large-scale adoption. The results show that traditional cloud storage demonstrates advantages in access speed and integration capabilities but remains constrained by higher costs and the risks associated with data centralization. **The conclusion** emphasizes the need for continued research to enhance the efficiency of IPFS and to explore hybrid storage models that integrate the benefits of both decentralized and centralized technologies.

Corresponding Author:

DOI: https://doi.org/10.33050/atm.v10i1.2531

1. INTRODUCTION

Data storage is a core component of modern digital infrastructure. Although traditional cloud platforms offer wide accessibility, they continue to face challenges related to security, scalability, and rising costs. Key threats include insider attacks, traffic hijacking, data loss, and insecure interfaces [1, 2]. Security also remains a major barrier for cloud adoption in sensitive scientific and business applications [3].

To address these weaknesses, decentralized storage through the IPFS has emerged as an alternative. InterPlanetary File System (IPFS) uses a P2P network and content-addressing based on cryptographic hashing, enabling data access through unique identifiers rather than centralized locations [4]. This approach improves resistance to censorship and cyberattacks but still faces limitations in retrieval speed, search efficiency, and

adoption [5, 6]. Cost and scalability are additional concerns, as cloud services rely on subscription models that increase with storage and bandwidth demands and may experience slowdowns during traffic spikes. Grounded in P2P distribution, distributed trust, and content-addressable networks, this study compares IPFS and cloud storage in terms of scalability, security, cost efficiency, and performance. It also examines IPFS adoption challenges and the potential integration of decentralized and traditional storage systems [7].

In addition to its technological significance, data storage infrastructure plays an important role in supporting the achievement of the United Nations Sustainable Development Goals. Efficient, secure, and scalable data storage systems contribute to sustainable digital development by strengthening industry, innovation, and digital infrastructure as reflected in Sustainable Development Goal 9. Reliable storage technologies enable organizations to innovate, expand digital services, and support economic growth through resilient and adaptive information systems.

Data security, privacy, and equitable access to information are also closely related to the objective of building peaceful, just, and strong institutions as outlined in Sustainable Development Goal 16. Storage systems that promote transparency, accountability, and user control over data help reduce the risks associated with centralized authority and information asymmetry. From an environmental and economic perspective, optimized data storage architectures support responsible consumption and production in line with Sustainable Development Goal 12 by reducing unnecessary resource usage and operational inefficiencies. In this context, decentralized technologies such as IPFS offer an alternative paradigm that aligns technological advancement with sustainability objectives, making the comparison between traditional cloud storage and decentralized storage systems a strategically relevant research topic.

2. LITERATURE REVIEW

2.1. Traditional Cloud Storage

Traditional cloud storage refers to an internet-based data storage model in which information is stored and managed on centralized servers operated by third-party service providers. Widely adopted platforms such as Google Drive, Dropbox, and Amazon Web Services (AWS) enable users to access, synchronize, and share data across multiple devices with minimal local infrastructure requirements [8]. This centralized architecture offers high availability, efficient data management, and seamless integration with other digital services, making cloud storage a fundamental component of modern business and digital ecosystems.

From a managerial and operational perspective, traditional cloud storage provides several advantages, including reliable performance, scalability, and ease of use. Cloud providers employ advanced technologies such as load balancing, redundancy, and automatic scaling to maintain service stability during periods of high demand [9, 10]. These capabilities allow organizations to focus on core business activities without the burden of managing physical storage infrastructure. Additionally, the standardized interfaces and extensive ecosystem support offered by cloud services facilitate rapid deployment and integration with enterprise applications.

Despite these benefits, traditional cloud storage also presents notable challenges. The reliance on centralized servers creates potential vulnerabilities related to data security, privacy, and service availability. Data stored in cloud platforms remains under the control of service providers, raising concerns regarding unauthorized access, data monitoring, and censorship [11, 12]. Furthermore, subscription-based pricing models can lead to increasing operational costs as data volumes and bandwidth usage grow over time. These limitations highlight the need for organizations to carefully assess risk, compliance requirements, and long-term cost implications when adopting traditional cloud storage solutions.

2.2. InterPlanetary File System (IPFS)

IPFS is a P2P based storage system designed to provide an alternative to centralized storage models, IPFS implements a content addressing mechanism, which assigns each file a unique cryptographic identity known as a CID. This approach allows data to be retrieved directly from the node storing it, without reliance on a specific server location [13]. A key advantage of IPFS is its resilience against censorship and centralized attacks. Since files uploaded to IPFS are replicated across multiple nodes within the network, the system is more robust against server failures and more efficient in distributing digital content. Additionally, IPFS reduces bandwidth usage by enabling data retrieval from the nearest available node, thereby improving the efficiency of information delivery [14].

The Figure 1 above illustrates the basic concept of a conventional cloud storage system. In this model, various types of data such as documents, music, videos, images, contacts, and other files are stored centrally

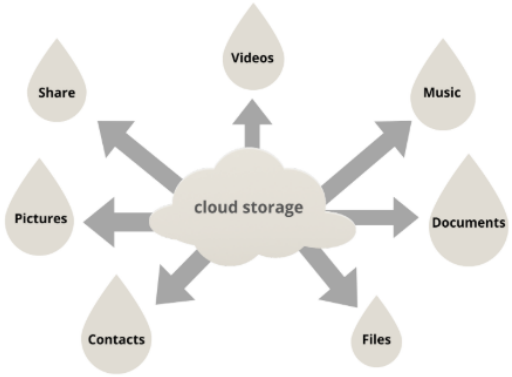

Figure 1. Traditional Cloud Storage Architecture

within a single cloud service and can be accessed and shared over the internet at any time [15, 16]. This aligns with discussions in the literature that emphasize the advantages of cloud storage in terms of accessibility and system integration. However, despite the effectiveness of this centralized method, it presents several critical challenges, including security threats, high operational costs, and issues related to censorship or system failures. Consequently, the IPFS, a decentralized storage system, offers a P2P-based solution that is more resistant to censorship and more efficient in data distribution, addressing the shortcomings of traditional cloud models [17].

Despite its numerous advantages, IPFS also faces several challenges. One of the main limitations is the lack of an efficient search mechanism as found in traditional cloud storage systems. Since IPFS does not utilise a centralized directory system, file searches can only be performed if the user knows the file's CID [18, 19]. Additionally, IPFS access speed remains a challenge, especially when the number of nodes storing a particular file decreases, leading to potential high latency in data retrieval [20].

2.3. Comparison Between IPFS and Traditional Cloud Storage

Based on various studies, several fundamental differences exist between IPFS and traditional cloud storage systems. From the perspective of security and privacy, IPFS offers more decentralized data control compared to traditional cloud services managed by service providers. This decentralized model enables users to retain full control over their data without the risk of third-party intervention [21, 22]. In terms of scalability, IPFS enables more efficient data distribution compared to traditional cloud storage. The P2P system in IPFS reduces the load on a single central server, whereas in traditional cloud systems, the larger the amount of stored data, the greater the burden placed on the central server [23].

In terms of operational cost, IPFS has an advantage as it does not rely on centralized server infrastructure, which typically incurs high maintenance expenses. However, in practice, IPFS users often depend on pinning services such as Filecoin or IPFS Cluster to maintain data availability, which can introduce additional costs [24, 25]. In terms of performance and access speed, traditional cloud systems tend to be faster and more stable because their server infrastructure is optimized for efficient data access. In contrast, IPFS faces challenges in access speed, particularly when files are not widely replicated across the network or when the nodes storing the data are offline. Overall, although IPFS offers a revolutionary approach to data storage systems, its implementation still faces challenges in terms of search efficiency and large-scale adoption. Therefore, a hybrid approach that combines the strengths of both IPFS and traditional cloud storage may serve as a more optimal solution in the future [26].

3. RESEARCH METHODOLOGY

3.1. Type of Research

This study is a descriptive and qualitative research that aims to analyze and compare IPFS and traditional cloud storage based on aspects of scalability, security, cost, and performance. The research methods used are literature study and simulation experiments, where data is obtained through literature analysis and performance testing of both storage systems in a controlled environment [27, 28].

3.2. Data Sources

The data in this study is obtained from two main sources Primary Sources direct testing of IPFS and traditional cloud services such as Google Drive, Dropbox, and AWS to evaluate access speed, storage efficiency, and network resource consumption [29]. Secondary Sources scientific journals, conference papers, books, and technical reports related to IPFS and traditional cloud storage. on the concept of IPFS, and a study highlighting the advantages of IPFS in decentralized architecture [30, 31].

3.3. Data Collection Techniques

The data collection methods in this study were conducted through the following approaches:

Literature Study gathering information from relevant scientific publications regarding the characteristics, advantages, and challenges of both IPFS and traditional cloud storage [32]. Simulation Experiments conducting trials of data storage and access using IPFS and traditional cloud services to measure speed, latency, and bandwidth consumption. Comparative Analysis using parameters such as security, scalability, cost, and performance as key indicators in evaluating the strengths of each technology [33, 34].

3.4. Data Analysis Method

The data obtained were analyzed using a quantitative and qualitative approach, through the following methods:

- Performance Analysis Measuring access speed in IPFS and traditional cloud storage using tools such as ping, traceroute, and bandwidth benchmarking. Calculating latency in both systems by comparing the loading times of files with varying sizes [35].
- Security Analysis Reviewing the risks of cyberattacks, including man-in-the-middle attacks, DDoS, and data breaches, in both systems [36]. Identifying the encryption mechanisms and data protection methods used in each platform [37].
- Cost Analysis Comparing cost models between traditional cloud services (e.g., storage and bandwidth costs for Google Drive, Dropbox, and AWS) and IPFS-based solutions, including the use of pinning services such as Filecoin or IPFS Cluster.
- Scalability Analysis This analysis evaluates the ability of both systems to handle increasing numbers of users and growing data volumes [38]. It also investigates the efficiency of data replication and redundancy within the P2P network architecture of IPFS compared to traditional cloud storage systems [39, 40].

3.5. Research Limitations

Despite the comprehensive comparative analysis conducted in this study, several limitations must be acknowledged to ensure transparency and proper interpretation of the findings. These limitations define the scope of the research and indicate areas where the results should be interpreted with caution.

The experimental evaluation was performed in a controlled and relatively limited network environment. Performance measurements for IPFS and traditional cloud storage were conducted under predefined bandwidth conditions and geographically constrained nodes [41, 42]. As a result, the observed access speed, latency, and throughput may not fully represent real-world performance in heterogeneous global networks, where variations in connectivity, congestion, and node distribution can significantly affect system behavior.

The cloud service providers examined in this study were limited to Google Drive, Dropbox, and AWS S3. Although these platforms represent dominant and architecturally mature cloud storage solutions, they do not capture the full diversity of existing cloud services with different pricing models, security mechanisms, and optimization strategies. Consequently, the comparative results should not be generalized to all cloud storage platforms without careful consideration.

The decentralized nature of IPFS introduces inherent variability in performance due to fluctuating node availability, replication levels, and geographic distribution of peers. Since network participation and node churn cannot be fully controlled or predicted, the reported IPFS performance may vary over time and across different deployment scenarios [43]. Additionally, the absence of advanced optimization mechanisms such as automated pinning strategies, incentive-based replication, or blockchain-integrated persistence layers means that the evaluated IPFS implementation reflects a baseline configuration rather than a fully optimized system.

The security analysis in this study focused primarily on architectural characteristics, data integrity mechanisms, and general threat considerations. In-depth technical evaluations, including penetration testing,

cryptographic verification, and adversarial simulations, were beyond the scope of this research. Furthermore, the study employed a qualitative-dominant comparative approach supported by limited quantitative metrics, which may not capture fine-grained performance variations under diverse workloads and access patterns. Future research incorporating large-scale empirical testing and longitudinal analysis would enhance the robustness and generalizability of the findings.

4. RESULTS AND DISCUSSION

4.1. Performance Comparison Between IPFS and Traditional Cloud Storage

To enhance analytical robustness, the average access times reported in Table 1 were computed from multiple trials and supplemented with variance measurements to assess performance consistency [44, 45]. Additional metrics such as standard deviation, latency fluctuations, and throughput efficiency were also considered to provide a more comprehensive quantitative comparison across platforms [46]. The testing involved uploading and downloading files of 100 MB, 500 MB, and 1 GB using both IPFS and cloud platforms such as Google Drive and Dropbox, with the comparative results of file access time for each platform clearly summarized in Table 1.

Table 1. Comparison of File Access Time Between Google Drive, Dropbox, and IPFS

File size	Google Drive (second)	Dropbox (second)	IPFS (second)
100 MB	2,1	2,3	3,7
500 MB	5,6	6,1	9,4
1 GB	10,8	11,3	15,2

The difference in access speed between traditional cloud services and IPFS must be interpreted in the context of the testing environment, which involved controlled bandwidth settings and geographically limited nodes [47]. These constraints influenced retrieval performance and indicate that real-world results may vary under broader, heterogenous network conditions [48]. This is primarily due to their centralized architecture, which allows data to be retrieved directly from servers equipped with infrastructure optimized for speed [49]. In contrast, IPFS relies on the number of nodes storing a given file, meaning that when replication is low across the network, access speed may decrease [50].

4.2. Data Security and Privacy

Security is a key advantage of IPFS over traditional cloud storage. While cloud data can be encrypted, it remains under the control of service providers. IPFS uses cryptographic CIDs, ensuring data integrity since any modification changes the CID. However, IPFS faces security challenges, including the absence of built-in encryption and the risk of data loss if files are not actively pinned. Despite these limitations [51], IPFS offers strong censorship resistance because data in a P2P network cannot be controlled by a single authority.

4.3. System Scalability

In terms of scalability, traditional cloud storage is more stable due to its support from large server infrastructures distributed across various global locations. Services like AWS and Google Cloud utilize load balancing and auto-scaling, which allow systems to remain optimized even during traffic surges [52]. In contrast, IPFS employs a decentralized scalability model, where system performance improves as the number of nodes in the network increases [53]. However, in low-participation environments, IPFS may experience bottlenecks in data access. Additionally, since IPFS lacks an automatic garbage collection mechanism, nodes storing large numbers of files may face limitations in storage capacity [54, 55].

4.4. Cost Analysis

Cost is one of the key factors in selecting a storage system. Traditional cloud services typically apply a subscription-based model for capacity and bandwidth, where users are charged based on the amount of storage used and the volume of data uploaded or downloaded. For example, Table 2 provides a comparison of storage costs among major cloud providers, including Google Drive, Dropbox, and AWS S3, highlighting differences in monthly storage pricing and outbound data transfer charges [56].

IPFS is fundamentally free to use, however, in order to ensure data persistence and availability, users often rely on pinning services such as Filecoin or Pinata, which introduce their own cost models. In certain

Table 2. Cloud Storage Cost Comparison

Service	Storage Cost (per month)	Data Transfer Cost
Google Drive	$9.99 for 2 TB	No charge within the Google ecosystem
Dropbox	$11.99 for 2 TB	No charge within the Dropbox ecosystem
AWS S3	$0.023 per GB	$0.09 per GB for outbound data transfer

scenarios, these costs may be lower than those associated with traditional cloud storage services. Nonetheless, users are responsible for actively managing their data to maintain its availability.

4.5. Strengths and Weaknesses of Each System

Based on the analysis, it can be concluded that both IPFS and traditional cloud storage systems have their respective strengths and weaknesses, as systematically summarized in Table 3, which compares key aspects such as access speed, security, privacy, scalability, and cost.

Table 3. Comparison of IPFS and Traditional Cloud Storage Systems

Aspects	IPFS	Traditional Cloud
Access Speed	Slower Performance with a Low Number of Nodes.	Faster Access Due to Centralized Infrastructure.
Security	Resistant to Censorship, as it is Based on Content Identifiers (CID).	Service Availability Depends on the Provider.
Privacy	Full Control Remains with the User.	Subject to Service Policy Regulations.
Scalability	Reliant on Network Participation.	High Scalability Achieved Through Load Balancing.
Cost	Free of Charge, Unless Pinning Services are Utilized.	Operates on a Fixed-Cost Subscription Model.

Based on the comparison between the IPFS and traditional cloud storage, it is evident that each approach offers distinct advantages and limitations depending on user needs. Traditional cloud services excel in access speed, stability, and scalability, owing to their centralized infrastructure and mature load balancing technologies. However, this model presents challenges related to increasing operational costs and potential privacy risks, which are subject to the policies of service providers. Conversely, IPFS adopts a decentralized approach that grants users full control over their data and offers greater resilience against censorship and data manipulation. While cost-effective in general use, IPFS often requires supplementary services such as pinning to ensure consistent data availability. Therefore, a hybrid approach that integrates both systems may represent an ideal strategy for developing secure, efficient, and flexible data storage solutions in the future.

5. MANAGERIAL IMPLICATIONS

The findings of this study provide several important managerial implications for decision-makers, particularly Information Technology (IT) managers, system architects, and organizational leaders responsible for digital infrastructure planning. Selecting an appropriate data storage system is no longer solely a technical decision but a strategic managerial choice that directly influences operational efficiency, cost management, data governance, and long-term organizational resilience.

For organizations that prioritize high availability, rapid access speed, and seamless system integration, traditional cloud storage remains the most suitable option. Cloud platforms such as AWS, Google Drive, and Dropbox offer mature infrastructures supported by load balancing and auto-scaling mechanisms, enabling stable performance even under high traffic conditions. From a managerial perspective, this makes traditional cloud storage ideal for mission-critical business applications, customer-facing platforms, and real-time data processing environments where performance consistency is essential. However, managers must carefully consider the long-term financial implications of subscription-based pricing models, especially for organizations experiencing rapid data growth.

IPFS presents a strategic opportunity for organizations seeking to enhance data sovereignty, privacy, and resistance to censorship. Because IPFS allows users to retain full control over their data without reliance on centralized service providers, it is particularly relevant for sectors handling sensitive or regulated information, such as research institutions, digital media platforms, and organizations operating in environments with strict data governance requirements. Nevertheless, managers should recognize that IPFS adoption requires additional technical competencies, including node management, encryption implementation, and the use of pinning services to ensure data availability. Consequently, successful IPFS deployment demands careful planning, skilled human resources, and clearly defined operational procedures.

From a cost management perspective, managers must evaluate storage solutions not only based on initial expenses but also on total cost of ownership. While IPFS is fundamentally free to use, hidden costs may arise from maintaining data persistence through pinning services, infrastructure monitoring, and network participation. Conversely, traditional cloud services offer predictable pricing but can become costly over time due to bandwidth charges and increasing storage demands. Therefore, managerial decisions should incorporate long-term financial projections, usage patterns, and scalability requirements to avoid unforeseen budget overruns.

The study highlights the strategic value of adopting a hybrid storage model that integrates both IPFS and traditional cloud storage. In this approach, organizations can leverage cloud storage for high-performance and frequently accessed data, while utilizing IPFS for archival, decentralized, or privacy-sensitive data. This hybrid strategy enables managers to balance performance, security, and cost efficiency, while also reducing dependency on a single storage paradigm. From a governance perspective, such integration supports risk diversification and enhances system resilience against service disruptions or policy changes by cloud providers.

Managers should view decentralized storage technologies such as IPFS not merely as alternative tools but as part of a broader digital transformation strategy. Continuous monitoring of technological developments, regulatory frameworks, and interoperability standards is essential to ensure that storage architectures remain adaptable and future-ready. Investing in staff training, developing internal guidelines for decentralized data management, and aligning storage decisions with organizational objectives will enable managers to maximize the strategic benefits of both centralized and decentralized storage systems.

6. CONCLUSION

This study contributes to the discourse on decentralized storage by demonstrating how IPFS challenges traditional assumptions in centralized cloud models, particularly in relation to data ownership, trust, and infrastructure governance. Conventional cloud platforms such as AWS, Google Cloud, and Microsoft Azure continue to dominate the market due to their centralized architectures, which enable efficient data access, mature management capabilities, and high reliability. These characteristics support the development of digital infrastructure and innovation, thereby contributing to the advancement of sustainable digital transformation and the objectives of Sustainable Development Goal 9. However, centralized cloud systems also face notable limitations, including high operational costs, security and privacy concerns, and the inherent risks associated with data centralization.

IPFS offers a decentralized alternative by distributing data across P2P network nodes, enhancing resistance to censorship and system failures while eliminating single points of failure. Its scalability model, which is driven by network participation rather than server provisioning, presents a more cost-efficient approach to data distribution and supports more responsible use of digital infrastructure resources in line with Sustainable Development Goal 12. In terms of security, while traditional cloud systems apply encryption under provider-controlled environments, IPFS ensures data integrity through tamper-resistant content identifiers, strengthening user control and data sovereignty. These characteristics align with the principles of transparency, accountability, and trust that underpin Sustainable Development Goal 16, although additional encryption mechanisms must still be implemented by users.

Despite its advantages, IPFS remains more suitable for applications that prioritize privacy, decentralization, and cost efficiency, whereas traditional cloud platforms continue to outperform in terms of access speed, stability, and operational reliability due to their mature infrastructures. Ensuring data availability in IPFS often requires supplementary services such as Filecoin or Pinata, which introduces additional managerial and technical considerations. Therefore, future research should focus on the development of hybrid storage frameworks that integrate centralized and decentralized systems through standardized interoperability protocols, automated

data routing, and optimized cost models. Such hybrid approaches offer a balanced pathway toward secure, innovative, and sustainability-oriented data storage ecosystems that support long-term advancements in digital infrastructure.

7. DECLARATIONS

7.1. About Authors

Po Abbas Sunarya (PS) https://orcid.org/0000-0002-3869-2837

Desy Apriani (DA) https://orcid.org/0000-0001-6967-0369

Ruli Supriati (RS) https://orcid.org/0009-0005-0315-5088

Danang Surya Budi (DS) https://orcid.org/0009-0003-7328-0939

John Edwards (JW) https://orcid.org/0009-0004-0067-0490

7.2. Author Contributions

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

REFERENCES

[1] N. Asiri, "Security and privacy issues in cloud storage," *arXiv Preprint*, 2024.

[2] E. Susetyono, D. S. Priyarsono, A. Sukmawati, and P. Nurhayati, "A structural model of risk governance and maturity in ultra microfinance soes," *International Journal of Cyber and IT Service Management (IJCITSM)*, vol. 5, no. 2, pp. 156–170, 2025.

[3] N. Soveizi, F. Turkmen, and D. Karastoyanova, "Security and privacy concerns in cloud-based scientific and business workflows: A systematic review," *Future Generation Computer Systems*, vol. 148, pp. 184–200, 2023.

[4] D. Trautwein, A. Raman, G. Tyson, I. Castro, W. Scott, M. Schubotz, and Y. Psaras, "Design and evaluation of ipfs: A storage layer for the decentralized web," in *Proceedings of the ACM SIGCOMM 2022 Conference*. ACM, 2022, pp. 739–752.

[5] L. Balduf, S. Henningsen, M. Florian, S. Rust, and B. Scheuermann, "Monitoring data requests in decentralized data storage systems: A case study of ipfs," *arXiv Preprint*, 2021.

[6] M. Hardini, V. Agarwal, D. Apriani, I. A. Widjaya, E. Setiawaty, and N. Nurasiah, "Application of database normalization in increasing data storage efficiency," *International Transactions on Artificial Intelligence*, vol. 3, no. 2, pp. 201–211, 2025.

[7] M. Bin Saif, S. Migliorini, and F. Spoto, "Efficient and secure distributed data storage and retrieval using interplanetary file system and blockchain," *Future Internet*, vol. 16, no. 3, p. 98, 2024.

[8] T. V. Doan, Y. Psaras, J. Ott, and V. Bajpai, "Toward decentralized cloud storage with ipfs: Opportunities, challenges, and future considerations," *IEEE Internet Computing*, vol. 26, no. 6, pp. 7–15, 2022.

[9] Z. Yao, B. Ding, Q. Bai, and Y. Xu, "Minerva: Decentralized collaborative query processing over interplanetary file system," *arXiv Preprint*, 2023.

[10] T. Handra, S. Purnama, A. J. Kusumo, and D. Bennet, "Blockchain in digital transformation: Enhancing security, transparency, and efficiency in modern systems," *Blockchain Frontier Technology*, vol. 4, no. 1, pp. 23–28, 2024.

[11] S. Singh, A. Tah, and S. Saha, "Storage and organisation of geospatial data in distributed blockchain using ipfs," in *Emergent Converging Technologies and Biomedical Systems*. Springer, 2024, pp. 583–596.

[12] A. Erica, S. Wulandari, and R. Widayanti, "Data security transformation: The significant role of blockchain technology," *Blockchain Frontier Technology*, vol. 3, no. 2, pp. 107–112, 2024.

[13] I. G. A. K. Warmayana, Y. Yamashita, and N. Oka, "Decentralized materials data management using blockchain, non-fungible tokens, and interplanetary file system in web3," *Journal of Applied Data Sciences*, vol. 5, no. 2, pp. 45–60, 2023.

[14] V. Rajasekar, S. Sondhi, S. Saad, and S. Mohammed, "Efficient and secure distributed data storage and retrieval using interplanetary file system and blockchain," *Future Internet*, vol. 16, no. 3, p. 98, 2024.
[15] E. Daniel and F. Tschorsch, "Passively measuring ipfs churn and network size," *arXiv Preprint*, 2022.
[16] M. S. Aprizal, M. Y. Fadilla, M. R. A. Adha *et al.*, "Ensuring security using blockchain technology," *Blockchain Frontier Technology*, vol. 2, no. 2, pp. 54–57, 2023.
[17] R. K. Dewang, M. P. Yadav, S. Awasthi, and A. Kumar, "Data secure application: An application that allows developers to store user data securely using blockchain and ipfs," *Multimedia Tools and Applications*, vol. 83, pp. 45 491–45 517, 2024.
[18] L. Balduf, M. Korczyński, O. Ascigil, N. V. Keizer, G. Pavlou, B. Scheuermann, and M. Król, "The cloud strikes back: Investigating the decentralisation of ipfs," in *Proceedings of the 2023 ACM on Internet Measurement Conference*. ACM, 2023, pp. 391–405.
[19] B. Irawan and D. Trihatmojo, "Decentralized trusted storage of audio-video log data based on blockchain technology and ipfs," *International Journal of Science, Technology & Management*, vol. 5, no. 2, pp. 473–484, 2024.
[20] S. Jadhav, R. Patil, and A. Deshmukh, "Securing decentralized storage in blockchain: A hybrid cryptographic framework," *Cybernetics and Information Technologies*, vol. 24, no. 2, pp. 16–31, 2024.
[21] I. W. Widayat, A. J. Mantau, and M. Köppen, "An edge computing storage and distributed data-driven bridging framework for smart agriculture using clustered interplanetary file system (ipfs)," in *Advances in Intelligent Networking and Collaborative Systems*. Springer, 2023, pp. 187–198.
[22] I. Sasono and M. Aman, "Framework of master data management in banking using consolidation and jaro winkler algorithm," *International Journal of Cyber and IT Service Management (IJCITSM)*, vol. 5, no. 2, pp. 186–197, 2025.
[23] N. Sangeeta and S. Y. Nam, "Blockchain and interplanetary file system (ipfs)-based data storage system for vehicular networks with keyword search capability," *Electronics*, vol. 12, no. 7, p. 1545, 2023.
[24] T. Haryanto and K. Ramli, "Desain dan analisis sistem cybershare menggunakan four node interplanetary file system (ipfs)," *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 8, no. 2, pp. 71–75, 2023.
[25] J. Siswanto, A. Rahmawati, U. Rahardja, N. D. Putra, M. I. N. Hakim, T. Pinandita, and I. B. Prasetyo, "Short-term prediction of bus station fleet number using a combination of bilstm models," *Automotive Experiences*, vol. 8, no. 1, pp. 205–215, 2025.
[26] J. Shen, Y. Li, Y. Zhou, and X. Wang, "A closer look into ipfs: Accessibility, content, and performance," in *Proceedings of the 2024 ACM SIGMETRICS/IFIP PERFORMANCE Joint International Conference on Measurement and Modeling of Computer Systems*. ACM, 2024.
[27] P. Á. Costa, J. Leitão, and Y. Psaras, "Studying the workload of a fully decentralized web3 system: Ipfs," *arXiv Preprint*, 2022.
[28] N. Fadzil, H. Fadzir, H. Mansor, and U. Rahardja, "Driver behaviour classification: A research using obd-ii data and machine learning," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, pp. 51–61, 2024.
[29] Z. Wu, C. R. Yang, S. Vargas, and A. Balasubramanian, "Is ipfs ready for decentralized video streaming?" in *Proceedings of the ACM Web Conference 2023*. ACM, 2023.
[30] A. Chakraborty, N. Mishra, S. Saha, S. Bhattacharya, and D. Mukhopadhyay, "On the amplification of cache occupancy attacks in randomized cache architectures," *arXiv Preprint*, 2023.
[31] P. A. Sunarya, U. Rahardja, S. C. Chen, Y.-M. Lic, and M. Hardini, "Deciphering digital social dynamics: A comparative study of logistic regression and random forest in predicting e-commerce customer behavior," *Journal of Applied Data Sciences*, vol. 5, no. 1, pp. 100–113, 2024.
[32] 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.
[33] S. Lamichhane and P. Herbke, "Verifiable decentralized ipfs cluster: Unlocking trustworthy data permanency for off-chain storage," in *2024 6th Conference on Blockchain Research and Applications for Innovative Networks and Services*. IEEE, 2024, pp. 1–4.
[34] R. Sivaraman, M.-H. Lin, M. I. C. Vargas, S. I. S. Al-Hawary, U. Rahardja, F. A. H. Al-Khafaji, E. V. Golubtsova, and L. Li, "Multi-objective hybrid system development: To increase the performance of diesel/photovoltaic/wind/battery system." *Mathematical Modelling of Engineering Problems*, vol. 11, no. 3, 2024.
[35] V. Estrada-Galiñanes, A. ElRouby, and L. M. A. Theytaz, "Efficient data management for ipfs dapps,"

arXiv Preprint, 2024.
[36] K. Tiwari, N. Dhanda, and R. Verma, "Decentralized file storage system," in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE, 2024, pp. 1–8.
[37] J. Tiago, D. Dias, and L. Veiga, "Adaptive edge content delivery networks for web-scale file systems," in *2022 IEEE 47th Conference on Local Computer Networks*. IEEE, 2022, pp. 323–326.
[38] H. Chen, Y. Lu, and Y. Cheng, "Fileinsurer: A scalable and reliable protocol for decentralized file storage in blockchain," in *2022 IEEE 42nd International Conference on Distributed Computing Systems*. IEEE, 2022, pp. 168–179.
[39] D. Kumari, A. S. Parmar, H. S. Goyal, K. Mishra, and S. Panda, "Healthrec-chain: Patient-centric blockchain enabled ipfs for privacy preserving scalable health data," *Computer Networks*, vol. 241, p. 110223, 2024.
[40] T. Berlec, M. Corn, S. Varljen, and P. Podržaj, "Exploring decentralized warehouse management using large language models: A proof of concept," *Applied Sciences*, vol. 15, no. 10, p. 5734, 2025.
[41] S. I. Abed, O. S. Albeltaji, and H. Alnabriss, "Decentralized storage using inter planetary file system," in *AI in Business: Opportunities and Limitations: Volume 2*. Springer, 2024, pp. 221–230.
[42] T. Ramírez-Gordillo, A. Maciá-Lillo, F. A. Pujol, N. García-D'Urso, J. Azorín-López, and H. Mora, "Decentralized identity management for internet of things (iot) devices using iota blockchain technology," *Future Internet*, vol. 17, no. 1, p. 49, 2025.
[43] H. Yang and S. Park, "Vidblock: A web3. 0-enabled decentralized blockchain architecture for live video streaming." *Applied Sciences (2076-3417)*, vol. 15, no. 3, 2025.
[44] S. Jadhav, G. Choudhari, M. Bhavik, R. Bura, and V. Bhosale, "A decentralized document storage platform using ipfs with enhanced security," in *2024 8th International Conference on Computing, Communication, Control and Automation (ICCUBEA)*. IEEE, 2024, pp. 1–11.
[45] A. K. Chandanan, V. Roy, V. Birchha, C. Raja, A. Varkale, M. M. A. Zahra, P. Agarwal, and S. K. Vishwakarma, "Federated learning-integrated autoencoder model for robust and decentralized pneumonia detection in chest x-rays." *Traitement du Signal*, vol. 42, no. 3, 2025.
[46] R. K. Dewang, M. P. Yadav, S. Awasthi, O. Raj, A. Mewada, and K. L. Bawankule, "Data secure application: An application that allows developers to store user data securely using blockchain and ipfs," *Multimedia Tools and Applications*, vol. 83, no. 15, pp. 45 491–45 517, 2024.
[47] R. Nair, S. N. Zafrullah, P. Vinayasree, P. Singh, M. M. A. Zahra, T. Sharma, and F. Ahmadi, "Blockchain-based decentralized cloud solutions for data transfer," *Computational Intelligence and Neuroscience*, vol. 2022, no. 1, p. 8209854, 2022.
[48] 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, 2024, pp. 27–39.
[49] B. R. Nida, "Blockchain meets cloud: Reinventing decentralization and secure transactions," 2025.
[50] A. Liu and C. Chen, "From real estate financialization to decentralization: A comparative review of reits and blockchain-based tokenization," *Geoforum*, vol. 159, p. 104193, 2025.
[51] K. Zarour, O. A. Bounab, Y. Marir, and I. Boumezbeur, "Blockchain-based architecture centred patient for decentralised storage and secure sharing health data," *International Journal of Electronic Healthcare*, vol. 12, no. 2, pp. 170–190, 2022.
[52] Organisation for Economic Co-operation and Development, *Reshaping Decentralised Development Co-operation*. Paris: OECD Publishing, 2023.
[53] B. Rolando, "The impact of cryptocurrency on the traditional banking system in indonesia: A threat or complement," *Jurnal Akuntansi Dan Bisnis*, vol. 5, no. 1, pp. 15–28, 2025.
[54] N. Sharma and P. G. Shambharkar, "Multi-layered security architecture for iomt systems: integrating dynamic key management, decentralized storage, and dependable intrusion detection framework," *International Journal of Machine Learning and Cybernetics*, pp. 1–48, 2025.
[55] P. Barros, C. P. Agupugo, E. Ejichukwu, K. A. Ogunmoye, and M. D. Hayden, "Decentralized energy security: Cybersecurity challenges and opportunities in distributed renewable energy," 2025.
[56] OECD, "Vocational education and training systems in nine countries," 2023, accessed: 2026-01-06. [Online]. Available: https://www.oecd.org/en/publications/vocational-education-and-training-systems-in-nine-countries_1a86eb6c-en.html