Blockchain Frontier Technology (B-Front)
Vol. 5, No. 2, 2026, pp. 136∼146
E-ISSN: 2808-0009 P-ISSN: 2808-0831, DOI:10.34306

Decentralized Data Storage Using IPFS for Sustainable Blockchain Availability Improvement

Aswadi Jaya[1], Muh Fahrurrozi[2], Susy Alestriani Sibagariang[3], Vinkan Likita[4], Henry Zainarthur[5]*
[1]Department of English Education, PGRI University Palembang, Indonesia
[2]Faculty of Social Sciences and Economics, Hamzanwadi University, Indonesia
[3]Department of Economic Education, Universitas HKBP Nommensen Pematangsiantar, Indonesia
[4]Faculty of Economic and Business, University of Raharja, Indonesia
[5]Faculty of Economic and Business, Eduaward Incorporation, United Kingdom
[1]aswadijaya@univpgri-palembang.ac.id, [2]fahrurrozi@hamzanwadi.ac.id, [3]susysibagariang@gmail.com, [4]vinkan@raharja.info
[5]henry.zthur7@eduaward.co.uk
***Corresponding Author**

Article Info

Article history:

Submission, 30-06-2025
Revised, 27-10-2025
Accepted, 10-11-2025

Keywords:

IPFS
Distributed
Data Availability
Decentralized
Blockchain

ABSTRACT

The rapid expansion of digital ecosystems has highlighted the limitations of centralized data storage systems, which often struggle with data loss, censorship, and single points of failure. To address these challenges, **this study explores** the InterPlanetary File System (IPFS) as a decentralized data management solution that enhances security, availability, and sustainability in distributed information environments. Using the **IPFS-KI framework**, a descriptive–qualitative methodology, this research examines the architectural design, operational mechanisms, and real-world implementations of IPFS. Through literature analysis, node simulations, and case-based evaluation, **the study investigates** IPFS performance in maintaining data integrity, fault tolerance, and resilience against network disruptions and censorship. **The findings reveal** that IPFS provides improved data reliability, transparency, and scalability compared to conventional centralized architectures, although certain limitations remain in terms of node stability and hidden centralization. **This study contributes** to a broader understanding of how decentralized storage technologies like IPFS can support the development of more secure, equitable, and sustainable digital infrastructures.

DOI: https://10.34306/bfront.v5i2.860

1. INTRODUCTION

In the era of rapid digital transformation, the reliance on centralized data storage systems has revealed several critical weaknesses [1, 2]. Traditional client–server architectures, such as those based on the HTTP protocol, remain highly dependent on a single point of control. This dependency makes them vulnerable to data loss, censorship, system downtime, and cyberattacks [3, 4]. When a central server fails or becomes compromised, the entire data ecosystem risks losing accessibility, integrity, and continuity [5]. Moreover, centralized infrastructures are often inefficient in regions with unstable internet connectivity or limited technical resources, further restricting equal access to information [6, 7].

In response to these limitations, decentralized approaches have emerged as an innovative alternative for improving data distribution and resilience [8]. Among the most promising technologies in this domain is the InterPlanetary File System (IPFS), a peer-to-peer protocol designed to enable content-addressed storage and distribution [9, 10]. Unlike traditional systems that locate files through server addresses, IPFS retrieves content using cryptographic hashes derived from the data itself. This mechanism allows users to access files from any node that stores a copy, thereby ensuring higher data redundancy, integrity, and resistance to tampering or censorship.

Understanding how IPFS contributes to sustainable and reliable data management is essential for advancing distributed information systems. While prior studies have highlighted its technical potential, comprehensive analyses of its real-world impact on data availability and sustainability remain limited [11, 12]. Recent studies have shown that integrating IPFS with blockchain can improve data validation speed, reduce packet loss, and maintain transparency and energy efficiency, making it particularly relevant for applications requiring verifiable audit trails, such as digital archives, IoT ecosystems, and supply chain traceability [13]. This research, therefore, seeks to bridge that gap by providing both theoretical and empirical insights into the performance of IPFS in distributed environments.

Furthermore, the relevance of this study aligns with the United Nations Sustainable Development Goals (SDGs), particularly SDG 9 [Industry, Innovation, and Infrastructure] and SDG 16 [Peace, Justice, and Strong Institutions]. SDG 9 emphasizes the development of resilient, inclusive, and sustainable technological infrastructures an aspect directly reflected in the potential of IPFS to enhance data availability, fault tolerance, and long term digital resilience. SDG 16 highlights the importance of transparency, accountability, and secure access to information. By reducing single points of failure and mitigating risks of censorship and data manipulation, decentralized storage technologies such as IPFS contribute significantly to strengthening institutional trust and ensuring equitable access to digital information. Therefore, this research not only advances technological innovation but also supports global efforts to build secure, sustainable, and inclusive digital ecosystems.

The main objectives of this study are as follows:

1. To examine the mechanisms of the InterPlanetary File System (IPFS) that enhance data availability within decentralized networks.
2. To evaluate the sustainability and security performance of IPFS through simulation and case-based observation.
3. To identify the major implementation challenges and propose recommendations for overcoming scalability and hidden centralization issues.

Through these objectives, the study aims to contribute to the development of more resilient, transparent, and accessible information infrastructures that leverage decentralized technologies.

2. LITERATURE REVIEW

2.1. Overview of IPFS and Its Core Architecture

The IPFS is a Peer-to-peer (P2P) protocol that enables decentralized data storage and distribution through content-based addressing rather than traditional server-based systems [14, 9]. Each file stored in IPFS is assigned a cryptographic hash generated from its content, functioning as a unique digital fingerprint that ensures data integrity and immutability [15].

This design allows users to access content from any node containing a copy, thereby eliminating reliance on central servers and improving fault tolerance [16, 17]. The Merkle Directed Acyclic Graph (Merkle DAG) structure used by IPFS supports version control and duplication minimization, making it effective for secure file sharing, digital preservation, and distributed applications [18, 19].

2.2. Data Availability in Distributed Networks

A prior study used four linked nodes with authentication keys to assess data availability in a decentralized IPFS configuration [20]. The system was around three times more dependable than a centralized storage setup, according to the results [21]. The current study, which expands the analysis by simulating comparable circumstances to assess IPFS efficacy in preserving data accessibility during network outages, uses this discovery as a crucial point of reference [22, 23].

2.3. Security, Integrity, and Resistance to Censorship

IPFS strengthens digital security and freedom of information by eliminating central control points that are vulnerable to censorship or cyberattacks [24]. Because IPFS relies on content hashes instead of domain-based URLs, it minimizes exposure to Distributed Denial-of-Service (DDoS) and Man-in-the-Middle (MITM) attacks. The integration of IPFS with blockchain technology enhances data integrity, verification, and traceability. This combination enables secure, transparent, and tamper-resistant data-sharing systems essential features for sectors like healthcare, IoT, and public administration [25, 26].

2.4. Integration of IPFS and Blockchain for Sustainable Data Systems

The synergy between blockchain and IPFS creates a powerful infrastructure for secure and transparent data management. Blockchain offers immutable record-keeping, while IPFS provides efficient distributed storage. Together, they enable decentralized applications that ensure authenticity, reliability, and cost efficiency [27, 28]. Studies have shown that blockchain IPFS integration improves data validation speed and reduces packet loss, while maintaining transparency and energy efficiency. This hybrid architecture is particularly relevant for applications requiring verifiable audit trails, such as digital archives, IoT ecosystems, and supply chain traceability [25, 29].

2.5. Challenges and Directions for IPFS Development

What technical and operational challenges arise in implementing IPFS-based distributed networks?. Found that IPFS is actually a decentralized system, but because many nodes are hosted on large cloud services, it is more centralized [30]. This can reduce the expected decentralization and put pressure on the principles of a decentralized web.

3. RESEARCH METHOD

This study uses the IPFS-KI framework, a descriptive–qualitative methodology, to better understand the function and effects of IPFS technology in distributed information systems. This method is appropriate for analyzing IPFS, a relatively new and empirically understudied technology, since it prioritizes interpretation and contextual analysis above solely numerical measurement [31]. Six steps make up the research process: literature review, IPFS architectural analysis, node simulation, implementation case study, assessment of disruption resilience, and findings synthesis. The goal of each step is to gradually make clearer how IPFS supports data availability and sustainability in both real-world and simulated scenarios [32, 12].

To provide a clearer overview of the methodological design, Table 1 presents the main components of the IPFS-KI framework, along with their focus areas and expected outcomes.

As shown in Table 1, the IPFS-KI framework serves as a structured roadmap for conducting both theoretical and empirical analysis throughout the study. Each component builds upon the previous one beginning with knowledge identification to establish conceptual grounding, followed by architectural observation and practical validation. The later stages emphasize security evaluation and synthesis, ensuring that the research captures not only the operational performance of IPFS but also its broader implications for data sustainability and resilience.

The first is a literature study that aims to build a solid theoretical foundation on IPFS concepts and architecture, particularly with regard to decentralized storage and information sustainability. Sources include official IPFS documentation, white papers, peer-reviewed journals, and technological articles [33]. The second is an analysis of IPFS architecture, focusing on its core principles, such as addressable content. This is an analysis that aims to demonstrate the architecture's capabilities for building secure and anti-fire systems.

In the third stage, simulations of several IPFS nodes are performed to observe system behavior under network conditions that are restricted. These simulations evaluate IPFS's ability to maintain data availability and redundancy in the event of connection loss or node failure [34, 35]. In the fourth stage, case study analysis is performed to evaluate the benefits and effectiveness of IPFS implementations in the real world. Implementations such as digital archiving, static websites, and remote communication projects are evaluated [36].

The fifth step involves evaluating IPFS's resilience against censorship, cyberattacks like DDoS, and node loss, sometimes including blockchain integration to enhance data integrity and reliability [37, 38]. The final stage synthesizes the findings into a comprehensive narrative, highlighting how IPFS tackles data sustainability and availability challenges while noting issues such as scalability limits and adoption barriers [39].

Table 1. IPFS-KI Framework Components and Research Focus

Framework Component	**Description**	**Research Output**
Knowledge Identification (KI)	Analyze existing literature and IPFS studies to build conceptual understanding and identify research gaps.	Established theoretical foundation and conceptual framework for IPFS analysis.
Infrastructure Observation (IO)	Examine IPFS architecture through simulations and network analysis.	Empirical data on system performance, redundancy, and accessibility.
Practical Implementation (PI)	Test IPFS applications in real-world projects such as digital archiving and web hosting.	Validation of IPFS practicality and sustainability in real environments.
Security and Integrity Evaluation (SIE)	Assess IPFS resilience against censorship, cyberattacks, and blockchain integration.	Comprehensive understanding of IPFS robustness and security capabilities.
Synthesis and Recommendation (SR)	Integrate findings to draw conclusions and propose recommendations for sustainable adoption.	Strategic insights and implementation guidelines for decentralized data systems.

Based on Table 2 data authenticity, immutability, and resistance to manipulation are all improved by integrating IPFS with blockchain. IoT connectivity, medical data security, and environmental data reliability have all improved as a result of this combination. The symmetric security paradigm and the integrated system design, which support decentralized operations, are the primary advances. Future research is expected to focus on large-scale validation, real-world deployment, and the development of adaptive decentralized systems that can react to changing network conditions.

4. RESULT AND DISCUSSION

The infographic below outlines the main features of distributed information systems and offers a thorough summary of the IPFS research findings. It outlines the primary elements influencing data resilience, dependability, and accessibility as well as the difficulties encountered during IPFS implementation. The purpose of this visual description is to make the technology's advantages and disadvantages in real-world applications easier to comprehend.

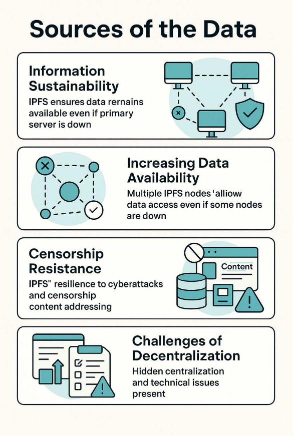
Sources of the Data
Information Sustainability
IPFS ensures data rernains available even if primary server is down
Increasing Data Availability
Multiple IPFS nodes 'alliow data access even if some nodes are down
Censorship Resistance
IPFS" resilience to cyberattacks and censorship content addressing
Content
Challenges of Decentralization
Hidden centralization and technical issues present

Figure 1. Core Concepts of IPFS for Distributed Information Systems

Table 2. Comparative Analysis of Recent Research on IPFS and Decentralized Data Storage

Title	Method (X, Y)	Novelty	Future Work
IPFS and blockchain based reliability and availability for river streamflow data	X: Integration of IPFS and Blockchain Y: Reliability and data availability improvement	Decentralized real time data storage	Development of a real-time river monitoring system
Enhancing data integrity in blockchain physical systems using blockchain	X: Blockchain Framework Y: Tracking and integrity verification via ICSF	Design of an integrated ICSF framework	Integration of IPFS into decentralized storage systems
Blockchain and data sharing review	X: Technical literature review Y: Secure dat a sharing	System review of blockchain-based data communication	Prototype implementation of IPFS in data systems
Data management and resilience in IoT using blockchain-IPFS	X: Application of IPFS & Blockchain Y: Data resilience and reliability in IoT networks	Architecture for blockchain–IoT data storage	Improvement of data performance in large-scale networks
Decentralized secure data service with hybrid blockchain IPFS	X: Symmetric blockchain-IPFS model Y: Privacy and data integrity verification	Formal model for integrated data storage systems	Adaptation of models for distributed energy systems
Integrated distributed data management system	X: Security review Y: Integration of IPFS–DLT	High-level data security	Implementation of IPFS–DLT integration in manufacturing systems
Blockchain-based security framework for IoT	X: Blockchain framework Y: Secure IoT data sharing	Advanced IoT data protection system	Integration of blockchain–IPFS for large-scale IoT data management

Figure 1 illustrates four essential dimensions of the IPFS framework, encompassing data persistence, fault tolerance, resistance to censorship, and decentralization constraints. This visual representation clarifies how IPFS strengthens data reliability while revealing the technical and structural limitations that still affect its deployment in distributed information environments.

4.1. Research on Information Sustainability through Decentralized Architecture

Research on decentralized data systems highlights that IPFS enhances information sustainability by eliminating reliance on centralized servers. Through its peer-to-peer structure and content based addressing, IPFS distributes data across multiple nodes, ensuring accessibility and integrity even during server or network disruptions. This decentralized model promotes long term data resilience and transparency, addressing the vulnerability of conventional centralized architectures.

The use of content-based addressing further strengthens data integrity by enabling each file to be retrieved based on its cryptographic hash rather than its location. This approach ensures that data can be accessed from any node storing a valid copy, making the system more resistant to tampering, modification, or unauthorized deletion. Such characteristics support the preservation of digital information over long periods, even under challenging network conditions.

Overall, this decentralized model promotes long-term data resilience, transparency, and accessibility. By addressing the inherent weaknesses of traditional client server architectures, IPFS offers a sustainable alternative for managing distributed information. These advantages make decentralized storage particularly relevant for applications requiring high reliability, such as digital archives, public information systems, and resource-limited environments.

4.2. Increasing Data Availability in Limited Conditions

This study evaluated how IPFS maintains data availability despite network interruptions through a controlled simulation to ensure transparency in the experimental procedure. Four IPFS nodes, each set up on different virtual environments with the same storage capacity (1 GB) and linked via a local network, were used in the simulation. To guarantee consistent system behavior, IPFS version 0.23.0 was utilized [40]. The percentage of successful data retrieval attempts relative to all queries is known as the Data Retrieval Success Rate (DRSR). The average amount of time (measured in milliseconds) needed to obtain a file from available nodes is known as the Average latency (AL). The number of different nodes that successfully supplied the same material is known as the Redundancy Factor (RF). According to the findings, IPFS maintained a 95% DRSR while two nodes were unavailable and a 100% DRSR when one node failed. Under low connectivity, the average latency rose marginally from 215 ms to 290 ms, but the redundancy factor stayed constant at 3.0, suggesting that content copies were regularly dispersed among several nodes. By contrast, once the primary server was removed, the centralized server model was unable to deliver any material. These results validate IPFS's enhanced access continuity and almost thrice increased fault tolerance in decentralized settings. A more transparent and reliable investigation of IPFS performance under various network conditions is ensured by the quantitative information that backs up the qualitative observations.

4.3. Enhancing Data Integrity and Anti-Censorship Mechanisms in IPFS

IPFS reinforces the integrity and accessibility of digital information by decentralizing data storage and eliminating reliance on a single authority. Through its peer-to-peer structure and content-based addressing, data cannot be easily suppressed, altered, or removed by external entities [41]. This architecture prevents content blocking that typically occurs in centralized systems dependent on domain-based URL [42]. Moreover, when integrated with blockchain technologies such as Ethereum, IPFS achieves higher transparency and verifiability, allowing each transaction and data modification to be securely recorded and authenticated [43]. Together, these mechanisms provide a robust defense against censorship, tampering, and unauthorized manipulation within distributed networks.

4.4. Real Implementation Case Study

IPFS Digital archiving projects, static website creation, and data sharing platforms in remote areas are some of the IPFS implementations [44]. These implementations demonstrate that IPFS effectively sustains data accessibility without dependence on centralized servers. An increased number of participating nodes enhances content delivery speed and overall network responsiveness, reflecting the scalability and operational efficiency of decentralized storage environments.

IPFS supports long-term preservation by ensuring that stored files cannot be easily altered or deleted, making it suitable for historical and governmental records. Meanwhile, static websites hosted on IPFS benefit from improved resilience and reduced server dependency, particularly in regions with inconsistent connectivity. Remote communities also leverage IPFS-based data-sharing systems to facilitate access to educational materials, health information, and administrative documents without relying on centralized internet service providers.

The effectiveness of these implementations is further enhanced by the increasing number of active IPFS nodes participating in content distribution. As more nodes replicate and store content, retrieval speeds improve, and overall network responsiveness becomes more stable. This demonstrates the underlying scalability and operational efficiency of the IPFS architecture, reinforcing its potential as a sustainable alternative to centralized data storage infrastructures.

4.5. Hidden Centralization and Sustainability Implications

Despite IPFS's decentralized, peer-to-peer architecture, this study finds that a major obstacle is the persistence of disguised centralization. Major cloud service providers like AWS, Google Cloud, or Azure continue to host a sizable percentage of IPFS nodes [45]. Because service outages, pricing regulations, or access limitations from these providers could still affect global data accessibility, this dependency compromises the network's independence [46]. While IPFS removes single points of failure at the protocol level, it indirectly reintroduces vulnerability through centralized hosting practices, creating a contradiction in decentralized designs [47]. Because only well-funded or technically skilled users can maintain stable nodes, this reliance on commercial infrastructures leads to unequal participation [48]. When a result, the diversity and resilience needed for real decentralization are diminished when the global node distribution becomes concentrated in particular areas and service platforms [49]. In order to overcome this obstacle, community-based and edge-hosted nodes should be given priority in sustained decentralization, allowing individuals and small businesses to engage with the IPFS ecosystem without relying on cloud infrastructure [50]. A more distributed and balanced network could be achieved by integrating edge computing, promoting open node incentives, and streamlining node deployment on low-power hardware. IPFS can better fulfill its objective of guaranteeing long-term data sustainability, censorship resistance, and equal access to information by reducing disguised centralization [38]. This broader viewpoint supports the claim that decentralization needs to take governance and infrastructure into account in addition to protocol design [42].

In addition to demonstrating technical improvements in data availability, resilience, and integrity, the findings of this study also align with several Sustainable Development Goals (SDGs). The enhanced reliability and decentralized architecture of IPFS directly support SDG 9 (Industry, Innovation, and Infrastructure) by promoting innovative digital infrastructure capable of withstanding system failures and reducing reliance on centralized data centers. Furthermore, the platform's ability to maintain transparency, resist censorship, and secure information integrity reflects the principles of SDG 16 (Peace, Justice, and Strong Institutions), which emphasizes accountable and trustworthy information systems. The collaborative nature of decentralized networks, which requires participation from diverse stakeholders to increase node distribution, also contributes to SDG 17 (Partnerships for the Goals) by encouraging multi-stakeholder cooperation in building sustainable and equitable technological ecosystems.

5. MANAGERIAL IMPLICATION

The findings of this study highlight that adopting IPFS can significantly enhance organizational data resilience, security, and autonomy. By implementing decentralized storage, institutions can reduce their dependence on centralized servers, thereby minimizing the risks of system downtime, censorship, and data breaches. This approach is especially beneficial for organizations operating in environments with limited infrastructure, as IPFS ensures continuous data accessibility even under unstable network conditions.

Integrating IPFS with blockchain frameworks further strengthens data integrity and traceability, making it a valuable solution for sectors that require verifiable and tamper-resistant records, such as education, governance, and public archives. To ensure successful adoption, organizations should initiate implementation through small-scale pilot projects while gradually expanding usage based on performance evaluations.

Moreover, management must invest in staff training to develop technical understanding of decentralized storage operations, as human competence plays a vital role in maintaining the network's stability. Promoting community-based node participation and reducing reliance on commercial cloud providers will also help preserve the principles of true decentralization. By aligning these managerial strategies, organizations can move toward more transparent, secure, and sustainable information ecosystems.

These managerial implications are also closely aligned with the Sustainable Development Goals (SDGs), particularly SDG 9 (Industry, Innovation, and Infrastructure), which emphasizes the advancement of resilient and innovative digital infrastructures. The decentralization approach supported by IPFS also contributes to SDG 16 (Peace, Justice, and Strong Institutions) by enhancing transparency and ensuring the integrity of information systems that are resistant to censorship and manipulation. Furthermore, the collaborative nature of decentralized node networks reflects SDG 17 (Partnerships for the Goals), highlighting the importance of multi-stakeholder cooperation in developing secure, inclusive, and sustainable digital ecosystems.

6. CONCLUSION

The findings of this study demonstrate that the InterPlanetary File System (IPFS) has significant potential to strengthen data sustainability and availability within decentralized environments. Through its peer-to-peer architecture and content-based addressing, IPFS ensures continuous access to information even when multiple nodes fail or disconnect. When integrated with blockchain, the system benefits from enhanced authenticity, integrity, and protection against censorship and cyberattacks, making it a reliable solution for organizations and communities operating in areas with limited connectivity.

Furthermore, this research also contributes to global development priorities by aligning with key Sustainable Development Goals (SDGs), particularly SDG 9 (Industry, Innovation, and Infrastructure) and SDG 16 (Peace, Justice, and Strong Institutions). The adoption of decentralized storage technologies such as IPFS supports the establishment of resilient digital infrastructures, strengthens transparency, and reduces reliance on centralized authorities all of which are essential components of sustainable and equitable digital ecosystems. These contributions highlight the broader relevance of this study in advancing secure, inclusive, and future-ready information systems at a global scale.

Despite its promising advantages, achieving full decentralization still requires addressing several challenges, including scalability limitations, indexing latency, and hidden centralization caused by cloud-hosted nodes. Future research should explore hybrid node infrastructures that combine cloud and local resources, community driven participation mechanisms, and the integration of emerging technologies such as artificial intelligence and edge computing. Collaboration among researchers, developers, and policymakers will also be essential in developing standardized governance frameworks and interoperability protocols. Through these efforts, IPFS can progress toward becoming a fully decentralized, sustainable, and globally accessible data ecosystem.

7. DECLARATIONS

7.1. About Authors

Aswadi Jaya (AJ) https://orcid.org/0000-0001-5706-0977

Muh Fahrurrozi (MF) https://orcid.org/0000-0002-4402-4384

Susy Alestriani Sibagariang (SA) https://orcid.org/0009-0009-1890-5442

Vinkan Likita (VL) https://orcid.org/0009-0009-6435-8494

Henry Zainarthur (HZ) https://orcid.org/0009-0001-7510-9321

7.2. Author Contributions

Conceptualization: AJ, MF, and SA; Methodology: VL; Software: HZ; Validation: AJ and MF; Formal Analysis: SA and VL; Investigation: HZ; Resources: AJ; Data Curation: MF; Writing Original Draft Preparation: SA and VL; Writing Review and Editing: HZ; Visualization: AJ; All authors, AJ, MF, SA, VL and HZ, 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] P. Goswami, N. Faujdar, S. Debnath, A. K. Khan, and G. Singh, "Investigation on storage level data integrity strategies in cloud computing: classification, security obstructions, challenges and vulnerability," *Journal of Cloud Computing*, vol. 13, no. 1, p. 45, 2024.

[2] N. Janssen, T. Ilayperuma, J. Jayasinghe, F. Bukhsh, and M. Daneva, "The evolution of data storage architectures: examining the secure value of the data lakehouse," *Journal of Data, Information and Management*, vol. 6, no. 4, pp. 309–334, 2024.

[3] G. Airlangga and A. Liu, “A study of the data security attack and defense pattern in a centralized uav–cloud architecture,” *Drones*, vol. 7, no. 5, p. 289, 2023.

[4] J. Alonso, L. Orue-Echevarria, V. Casola *et al.*, “Understanding the challenges and novel architectural models of multi-cloud native applications–a systematic literature review. j cloud comp 12, 6 (2023),” 2023.

[5] S. Singh, S. B. Verma, B. K. Gupta, and A. Agrawal, “Decentralization and federated approach for personal data protection and privacy control.” *Journal of Information Assurance & Security*, vol. 19, no. 5, 2024.

[6] N. Gozzi, N. Comini, and N. Perra, “Bridging the digital divide: mapping internet connectivity evolution, inequalities, and resilience in six brazilian cities,” *EPJ Data Science*, vol. 13, no. 1, p. 69, 2024.

[7] X. Chen, K. Chen, M. Wang, and R. Li, “Roles of wireless networks in bridging the rural smart infrastructural divide,” *Infrastructures*, vol. 8, no. 11, p. 159, 2023.

[8] 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.

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

[10] 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.

[11] F. Zhang and L. Zhang, “A cryptographic blockchain-ipfs framework for secure distributed database storage and access control,” *Informatica*, vol. 49, no. 30, 2025.

[12] K. Shibano, K. Ito, C. Han, T. T. Chu, W. Ozaki, and G. Mogi, “Secure processing and distribution of data managed on private interplanetary file system using zero-knowledge proofs.” *Electronics (2079-9292)*, vol. 13, no. 15, 2024.

[13] T. W. E. Suryawijaya, “Strengthening data security through blockchain technology: Exploring successful implementations in digital transformation in indonesia,” *JSKP: Jurnal Studi Kebijakan Publik*, vol. 2, no. 1, pp. 55–68, 2023. [Online]. Available: https://jurnal.kemendagri.go.id/index.php/jskp/article/view/1682

[14] A. Maariz, M. A. Wiputra, and M. R. D. Armanto, “Blockchain technology: Revolutionizing data integrity and security in digital environments,” *International Transactions on Education Technology (ITEE)*, vol. 2, no. 2, pp. 92–98, 2024.

[15] E. Daniel and F. Tschorsch, “Ipfs and friends: A qualitative comparison of next generation peer-to-peer data networks,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 31–52, 2022.

[16] Z. Yao, B. Ding, Q. Bai, and Y. Xu, “Minerva: Decentralized collaborative query processing over interplanetary file system,” *IEEE Transactions on Big Data*, vol. 11, no. 2, pp. 669–683, 2024.

[17] T. Haryanto, K. Ramli, and A. D. Pramudianto, “Data availability in decentralized data storage using four-node interplanetary file system,” *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 3, pp. 639–645, 2023.

[18] D. Ahmad, N. Lutfiani, A. D. A. R. Ahmad, U. Rahardja, Q. Aini *et al.*, “Blockchain technology immutability framework design in e-government,” *Jurnal Administrasi Publik (Public Administration Journal)*, vol. 11, no. 1, pp. 32–41, 2021.

[19] H. Ko, J. Oh, and S. U. Kim, “Digital content management using non-fungible tokens and the interplanetary file system,” *Applied Sciences*, vol. 14, no. 1, p. 315, 2023.

[20] N. G. Chatzigeorgiou, S. Theocharides, G. Makrides, and G. E. Georghiou, “A review on battery energy storage systems: Applications, developments, and research trends of hybrid installations in the end-user sector,” *Journal of Energy Storage*, vol. 86, p. 111192, 2024.

[21] J. Kaur, R. Rani, and N. Kalra, “Attribute-based access control scheme for secure storage and sharing of ehrs using blockchain and ipfs,” *Cluster Computing*, vol. 27, no. 1, pp. 1047–1061, 2024.

[22] Z. Fauziah, N. P. Anggraini, Y. P. A. Sanjaya, and T. Ramadhan, “Enhancing cybersecurity information sharing: A secure and decentralized approach with four-node ipfs,” *International Journal of Cyber and IT Service Management*, vol. 3, no. 2, pp. 153–159, 2023.

[23] S. Purnama, U. Rahardja, Q. Aini, A. Khoirunisa, and R. A. Toyibah, “Approaching the anonymous deployment of blockchain-based fair advertising on vehicle networks,” in *2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS)*. IEEE, 2021, pp. 1–6.

[24] L. Balduf, M. Korczyński, O. Ascigil, N. V. Keizer, G. Pavlou, B. Scheuermann, and M. Król, “The cloud

strikes back: Investigating the decentralization of ipfs," in *Proceedings of the 2023 ACM on Internet Measurement Conference*, 2023, pp. 391–405.

[25] S. R. Mallick, S. Sobhanayak, and R. K. Lenkar, "Secure and trusted data sharing in smart healthcare using blockchain and iot integration," *Discover Internet of Things*, vol. 5, no. 1, p. 90, 2025.

[26] X. Gao, W. Zhang, B. Zhao, J. Zhang, J. Wang, and Y. Gao, "Product authentication technology integrating blockchain and traceability structure," *Electronics*, vol. 11, no. 20, p. 3314, 2022.

[27] F. Yang, Z. Ding, Y. Yu, and Y. Sun, "Interaction mechanism between blockchain and ipfs," *Blockchain*, vol. 1, no. 2, pp. 24–25, 2023.

[28] F. Yang, Z. Ding, L. Jia, Y. Sun, and Q. Zhu, "Blockchain-based file replication for data availability of ipfs consumers," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1191–1204, 2024.

[29] P. Kang, W. Yang, and J. Zheng, "Blockchain private file storage-sharing method based on ipfs," *Sensors*, vol. 22, no. 14, p. 5100, 2022.

[30] M. Rakhmansyah, M. S. Hadi, S. R. P. Junaedi, F. A. Ramahdan, and S. N. W. Putra, "Integrating blockchain and ai in business operations to enhance transparency and efficiency within decentralized ecosystems," *ADI Journal on Recent Innovation*, vol. 6, no. 2, pp. 157–167, 2025.

[31] K. Nabben, "Decentralized technology in practice: Social and technical resilience in ipfs," in *2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*. IEEE, 2022, pp. 66–72.

[32] R. Zeng, J. You, Y. Li, and R. Han, "An icn-based ipfs high-availability architecture," *Future Internet*, vol. 14, no. 5, p. 122, 2022.

[33] E. K. Andana, O. A. Y. Ludji, and E. Sumarya, "Blockchain-enabled framework for securing iot data transactions," *The Journal of Academic Science*, vol. 2, no. 3, pp. 995–1007, 2025.

[34] L. Balduf, S. Henningsen, M. Florian, S. Rust, and B. Scheuermann, "Monitoring data requests in decentralized data storage systems: A case study of ipfs," in *2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2022, pp. 658–668.

[35] Z. Fauziah, "A secure and decentralized approach with four-node ipfs," *International Journal of Cyber and IT Service Management (IJCITSM)*, vol. 3, no. 2, pp. 1–10, 2023. [Online]. Available: https://iiast.iaic-publisher.org/ijcitsm/index.php/IJCITSM/article/download/139/66

[36] J. Viswanathan and S. U. Kumar, "Blockchain-based decentralized digital forensics case management system using ipfs," in *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*. IEEE, 2024, pp. 1–6.

[37] M. I. Hossain, T. Steigner, M. I. Hussain, and A. Akther, "Enhancing data integrity and traceability in industry cyber physical systems (icps) through blockchain technology: A comprehensive approach," *arXiv preprint arXiv:2405.04837*, 2024.

[38] N. Khairunnisa, F. Christiani, and A. G. Prawiyogi, "Supply chain transparency: Exploring blockchain solutions for enhanced traceability and efficiency," *Blockchain Frontier Technology*, vol. 4, no. 1, pp. 15–22, 2024.

[39] I. C. A. Pilares, S. Azam, S. Akbulut, M. Jonkman, and B. Shanmugam, "Addressing the challenges of electronic health records using blockchain and ipfs," *Sensors*, vol. 22, no. 11, p. 4032, 2022.

[40] M. R. Dhanagari, "Mongodb and data consistency: Bridging the gap between performance and reliability," *Journal of Computer Science and Technology Studies*, vol. 6, no. 2, pp. 183–198, 2024.

[41] 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.

[42] T. Hariguna, Y. Durachman, M. Yusup, and S. Millah, "Blockchain technology transformation in advancing future change," *Blockchain Frontier Technology*, vol. 1, no. 01, pp. 13–20, 2021.

[43] N. A. Santoso, P. Juanta, S. Maulana, K. Toktar, and A. Khanza, "Decentralized file sharing infrastructure with ipfs for censorship resistance in blockchain ecosystems," *Blockchain Frontier Technology*, vol. 5, no. 1, pp. 80–89, 2025.

[44] M. R. Haque, S. I. Munna, S. Ahmed, M. T. Islam, M. M. H. Onik, and A. Rahman, "An integrated blockchain and ipfs solution for secure and efficient source code repository hosting using middleman approach," *arXiv preprint arXiv:2409.14530*, 2024.

[45] I.-C. Lin, Y.-H. Kuo, C.-C. Chang, J.-C. Liu, and C.-C. Chang, "Symmetry in blockchain-powered secure decentralized data storage: Mitigating risks and ensuring confidentiality," *Symmetry*, vol. 16, no. 2, p. 147, 2024.

[46] Z. Zhang, J. Zhao, G. Wang, S.-K. Johnston, G. Chalhoub, T. Ross, D. Liu, C. Tinsman, R. Zhao, M. Van Kleek *et al.*, "Trouble in paradise? understanding mastodon admin's motivations, experiences, and challenges running decentralised social media," *Proceedings of the ACM on Human-Computer Interaction*, vol. 8, no. CSCW2, pp. 1–24, 2024.

[47] M. Hullurappa and S. Addanki, "Building sustainable data ecosystems: A framework for long-term data governance in multi-cloud environments," in *Driving Business Success Through Eco-Friendly Strategies*. IGI Global Scientific Publishing, 2025, pp. 73–92.

[48] R. H. Chowdhury, "Next-generation cybersecurity through blockchain and ai synergy: a paradigm shift in intelligent threat mitigation and decentralised security," *International Journal of Research and Scientific Innovation*, vol. 12, no. 8, 2025.

[49] U. Rahardja, Q. Aini, A. S. Bist, S. Maulana, and S. Millah, "Examining the interplay of technology readiness and behavioural intentions in health detection safe entry station," *JDM: Jurnal Dinamika Manajemen*, vol. 15, no. 1, 2024.

[50] Q. Aini, D. Manongga, U. Rahardja, I. Sembiring, and Y. M. Li, "Understanding behavioral intention to use of air quality monitoring solutions with emphasis on technology readiness," *International Journal of Human–Computer Interaction*, vol. 41, no. 8, pp. 5079–5099, 2025.