





# Leveraging IPFS for Secure Distributed Blockchain-Based Data Infrastructure and Enhanced Security

Sandy Setiawan<sup>1\*</sup> , Muchlisina Madani<sup>2</sup> , Sondang Visiana Sihotang<sup>3</sup> , Elisa Ananda Natalia<sup>4</sup> ,

Novita Khairunnisa<sup>5</sup> , Kristina Vaher<sup>6</sup> 

<sup>1</sup>Department of Entrepreneurship, Bina Nusantara University, Indonesia

<sup>2,5</sup>Faculty of Computer Science, REY Incorporation, Indonesia

<sup>3,5</sup>Faculty of Economics and Business, University of Raharja, Indonesia

<sup>4</sup>Faculty of Computer Systems, University of Raharja, Indonesia

<sup>6</sup>Faculty of Computer Systems, ilearning incorporation, Estonia

<sup>1</sup>sandy.setiawan@binus.ac.id <sup>2</sup>muchlisina@raharja.info <sup>3</sup>sondang@raharja.info <sup>4</sup>elisa.ananda@raharja.info

<sup>5</sup>novita.khairunnisa@raharja.info <sup>6</sup>vaheer.kristin@ilearning.ee

\*Corresponding Author

## Article Info

### Article history:

Received month dd, 2025-06-19

Revised month dd, 2025-07-30

Accepted month dd, 2025-08-01

### Keywords:

IPFS

Data Security

Public Gateway

Latency of Access

Digital Sensor



## ABSTRACT

**In an increasingly digital world**, where centralized storage systems dominate and censorship risks are growing, the InterPlanetary File System (IPFS) has emerged as a promising decentralized data storage solution. **This research aims** to evaluate the potential and challenges of implementing IPFS, **using a descriptive qualitative approach** that includes both a comprehensive literature review and technical simulations. The literature review highlights IPFS's advantages, particularly in areas such as data integrity, resistance to censorship, and efficient content distribution. However, it also identifies key challenges, such as high latency and the dependency on node availability. To further investigate these issues, technical simulations were conducted using a private IPFS network, testing file access latency under different network conditions. **The results indicate** that the fastest average latency occurs when all nodes are active, at 150 ms, while the highest latency is observed when files are accessed through a public gateway, with an average of 540 ms. These findings demonstrate that IPFS has substantial potential to create a more open, decentralized digital ecosystem that resists centralized control. However, for large-scale adoption to be feasible, significant improvements in infrastructure, particularly node availability and latency management, are required to fully support IPFS's widespread implementation.

*This is an open access article under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license.*



DOI: <https://10.34306/bfront.v5n1.826>

This is an open-access article under the CC-BY license (<https://creativecommons.org/licenses/by/4.0/>)

©Authors retain all copyrights

## 1. INTRODUCTION

The need for secure, open, and censorship-free data storage has become increasingly evident as the volume of digital information continues to grow [1]. Despite the widespread adoption of traditional, centralized cloud-based file sharing systems, they have come under heightened scrutiny due to vulnerabilities such as data manipulation, restricted access, and reliance on single points of failure.

In many cases, large corporations and governments control these digital platforms, which results in a loss of data sovereignty, increased surveillance, and the potential for content removal [2]. As a response,

decentralized approaches are gaining traction as they offer greater autonomy and resilience in data transmission, reducing the risks associated with centralized control.

The InterPlanetary File System (IPFS) provides a revolutionary decentralized storage solution by shifting from location-based addressing to content-based addressing [3]. Operating on a peer-to-peer (P2P) network, IPFS distributes files across multiple nodes, which are identified using cryptographic hashes, unlike traditional systems that depend on centralized servers [4]. This decentralized model increases data redundancy, minimizes reliance on intermediaries, and strengthens protection against censorship [5]. By allowing users to access content directly from the network, IPFS fosters an open and accessible digital environment, free from the constraints imposed by central authorities.

One of IPFS's key strengths is its ability to enhance data integrity and transparency. Each modification to content results in the generation of a new cryptographic hash, ensuring that the data is immutable, verifiable, and resistant to tampering [6]. This feature is particularly valuable in applications requiring trustless verification, such as open-source projects, legal documentation, and scientific research. Furthermore, IPFS optimizes content delivery by storing frequently requested data closer to the user, thereby improving data retrieval efficiency, reducing bandwidth costs, and enhancing overall speed [7].

Beyond transparency, IPFS plays a critical role in combating international censorship. Unlike traditional web hosting, which depends on centralized hosting providers and domain name systems (DNS), IPFS enables the decentralized hosting of websites and digital materials. This ensures that content remains accessible even in regions with stringent censorship laws [8]. As a result, IPFS has become a preferred choice for journalists, activists, and organizations advocating for digital rights and the freedom of information [9].

As the demand for robust and decentralized infrastructure grows with the evolving digital landscape, IPFS offers a promising solution to address the shortcomings of conventional file-sharing systems. By leveraging IPFS, we can create a distributed internet that prioritizes accessibility, data integrity, and resistance to censorship [10]. This study explores the latest advancements in IPFS technology, its practical applications, and its potential to shape the future of the digital ecosystem. With IPFS, we can build a more open, transparent, and censorship-resistant digital infrastructure that aligns with the evolving needs of the global community [11].

## 2. LITERATURE REVIEW

### 2.1. Overview of IPFS

The InterPlanetary File System (IPFS) is a peer-to-peer decentralized storage protocol designed to address the limitations of traditional centralized storage systems [12]. By employing content-based addressing, IPFS enables efficient and censorship-resistant distribution of data. The design and implementation of IPFS as a foundational storage layer for the decentralized web have been extensively evaluated [13]. A study showcasing IPFS's global adoption reports that the protocol spans over 2,700 Autonomous Systems across 152 countries, highlighting its broad acceptance and usage [14]. However, challenges related to latency and access speed persist, particularly in networks with constrained infrastructure.

### 2.2. Censorship and Security Vulnerabilities in IPFS

A significant vulnerability within IPFS is its susceptibility to censorship attacks via Kademlia's Distributed Hash Table (DHT). Research has demonstrated that such attacks can prevent the retrieval of specific content, although a mitigation system has been proposed that successfully detects these attacks with a detection rate of 99.6% and achieves 100% mitigation effectiveness [15].

### 2.3. Challenges and Scalability Issues in IPFS

In exploring IPFS as a decentralized cloud storage solution, researchers have highlighted its advantages in ensuring data integrity and decentralization. However, user adoption, scalability, and integration with existing systems remain substantial bottlenecks [16].

### 2.4. Cyber Share System and Integration with Blockchain

To address these challenges, the Cyber Share system was developed to share cybersecurity data using a private IPFS network, thus reducing reliance on a central server, alleviating server load, and ensuring the confidentiality, integrity, and availability of shared data [17]. Furthermore, the integration of IPFS with

blockchain technology has been proposed to optimize big data architecture, overcoming the limitations of centralized storage systems such as Hadoop, particularly in terms of data availability and resilience against attacks [18].

### 3. RESEARCH METHOD

This study employs a descriptive qualitative approach to explore the potential and challenges of implementing the InterPlanetary File System (IPFS) technology as a decentralized data storage solution [19]. The aim of this approach is to provide a comprehensive analysis of the features, operations, and relevance of IPFS in the contemporary digital landscape [20].

#### 3.1. Research Phases

The research is divided into two main stages: a literature review and technical simulation [21]. The literature review involves an in-depth analysis of existing research, focusing on the architecture, benefits, and challenges of the InterPlanetary File System (IPFS). It explores key studies on decentralized storage technologies and their potential applications across various industries, including healthcare, digital rights, and supply chain management. The review also highlights the limitations and gaps in current research, providing a solid foundation for the subsequent technical simulations. These simulations aim to evaluate IPFS's performance under different network conditions by building a private IPFS node network and measuring the access latency. The findings from both stages will contribute to a comprehensive understanding of IPFS's potential and challenges in real-world applications.

The first phase of the study involves a literature review, where various relevant and current scientific sources are examined. Special attention is given to journals published since 2021 and indexed in reputable databases such as Google Scholar and arXiv. The review focuses on IPFS's architecture, its advantages and disadvantages, and its implementation in real-world systems [22]. The literature review provides the theoretical foundation for the study, offering insights into IPFS's evolution and application.

##### 3.1.1. Technical Simulation

The second phase involves conducting technical simulations to evaluate the performance of IPFS. A private IPFS node network is built within a local environment consisting of multiple interconnected virtual nodes [23]. To assess the system's performance under different network conditions, the study tests file access times in three scenarios:

1. When all nodes are active.
2. When some nodes are inactive.
3. When files are accessed via an IPFS public gateway.

Each scenario is tested five times to obtain reliable average results. A terminal-based timekeeping tool records access times in milliseconds.

#### 3.2. Data Collection and Analysis

The data collected during the study falls into two categories:

1. **Secondary data:** Obtained from the literature review, which is analyzed descriptively.
2. **Primary data:** Obtained from the technical simulation process. These data are subjected to simple quantitative analysis.

The results from both stages are synthesized to draw conclusions about the effectiveness of IPFS as a decentralized storage solution, particularly in terms of its potential to enhance data integrity, reduce reliance on centralized systems, and promote censorship resistance. Additionally, the findings suggest directions for future development, including improvements in infrastructure to address latency and node availability issues, as well as exploring IPFS's integration with other emerging technologies like blockchain and IoT to further optimize data management and scalability [24, 25].

### 3.3. State of the Art (SOTA) Matrix

The development of InterPlanetary File System (IPFS)-based decentralized storage technologies has garnered significant attention in recent years [26, 27, 28]. Various studies have explored the capabilities [29, 30], challenges, and future directions of IPFS in multiple domains [5, 31], including data integrity [32, 33], censorship resistance [34, 35], decentralized governance [36, 37], and integration with blockchain technologies [38, 39, 40]. The following table summarizes key studies that contribute to the state of the art in IPFS-based decentralized storage [41], providing insights into the methodologies, results, and future research opportunities identified by these works [42, 8, 43].

Table 1. Summary of State of the Art (SOTA) on IPFS-Based Decentralized Storage Technologies

No	Method (X)	Result (Y)	Future Work	Future Work
1	System study and IPFS erasure simulation	Feasible content erasure without affecting other nodes	Decentralized content deletion model	Integration with high-privacy systems
2	Censorship attack analysis on IPFS DHT	Censorship possible by disrupting the DHT; detection and mitigation system proposed	Identification of censorship gaps and solutions in IPFS	Strengthen routing table and early detection mechanisms
3	Social and technical observation of IPFS	Supports social resilience in open communities	Sociotechnical approach to IPFS decentralization	Combine technical and social evaluations of IPFS
4	Implementation of web annotations using IPFS + Ethereum	Decentralized annotation system successfully tested	Integration of IPFS with Ethereum for anti-censorship annotations	Application for digital journalism use cases
5	Legal	technological analysis of Web3/IPFS	Legal and sociotechnical perspective on IPFS use	Study Web3-IPFS adoption in repressive regions
6	Study of IPFS as off-chain storage	IPFS improves blockchain scalability and storage efficiency	Off-chain blockchain storage optimization using IPFS	Testing systems under high transaction volume
7	Architecture review and global IPFS deployment	IPFS used by thousands of nodes in 152 countries	Real-world usage statistics of IPFS	Optimization of content lookup algorithms

The table 1 summarizes key prior studies relevant to the development of IPFS-based decentralized storage technologies [44]. These studies focus on various advancements [45], challenges [46], and future directions for improving IPFS performance and adoption in different applications [47]. The research highlights the potential of IPFS in areas such as decentralization [48, 49], censorship resistance, and its integration with other technologies like blockchain.

Delegated content erasure model within IPFS, which allows content to be removed from the system

without affecting other nodes, thus enhancing decentralization. Vulnerabilities of IPFS, particularly related to censorship attacks on the Distributed Hash Table (DHT), and proposed a mitigation system.

Social and technical resilience of IPFS, particularly its potential to support community autonomy in open environments. The use of IPFS as an off-chain storage solution for blockchain technologies and discussed the challenges associated with latency and node availability.

This matrix presents an overview of these studies, offering insights into the current state of IPFS technology and suggesting areas for further research and development.

## 4. RESULT AND DISCUSSION

### 4.1. Literature Review and Conceptual Analysis

The InterPlanetary File System (IPFS) is a solution to conventional centralized data storage systems that are vulnerable to disruption and censorship. A key feature of IPFS is content-based addressing, where files are accessed based on their cryptographic hash rather than their physical storage location. This ensures that files remain accessible even if the server location changes or becomes unavailable. Additionally, IPFS distributes files across multiple nodes, creating a more resilient data network and eliminating single points of failure.

IPFS has seen global adoption, with thousands of nodes in over 150 countries using the technology. Notable applications of IPFS include long-term document storage, censorship-resistant journalism platforms, and integration with blockchain and smart contract technologies.

However, IPFS is not without its challenges. One significant issue is the potential disruption of the hash routing system, which allows attacks on the Distributed Hash Table (DHT) to alter file distribution. Moreover, the speed of the network remains limited, especially when files are accessed through public gateways or when the node storing the files is offline. This limitation is particularly problematic for applications requiring high-speed access, such as streaming or real-time services, where high latency can degrade performance.

The advantages and disadvantages of IPFS, based on the literature review, are summarized in the following table:

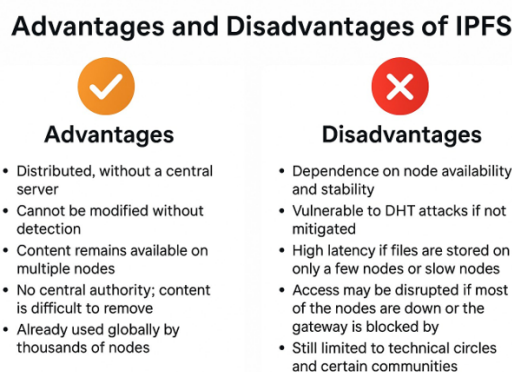


Figure 1. Comparison of Advantages and Disadvantages of IPFS Based on Literature Review

From Figure 1, it is evident that IPFS offers key advantages such as decentralization, immutability, and global availability. However, it also faces challenges like node dependency, high latency, and vulnerability to DHT attacks. These limitations impact its performance, especially in high-speed or real-time applications, highlighting the need for infrastructure improvements and broader adoption.

### 4.2. Technical Simulation Results

Technical simulations were conducted using a private IPFS network composed of multiple virtual nodes to assess the real-world performance of IPFS. The simulations were performed under three different network conditions:

1. All nodes are active (ideal conditions),
2. Some nodes are inactive (partially unavailable), and

### 3. Files are accessed via an IPFS public gateway.

Each scenario was tested five times to ensure reliability and consistency in the results, with multiple tests conducted to account for any variations in network conditions or node availability. The results from these tests were then averaged to provide a more accurate representation of the system's performance under each scenario. The average latency for each scenario is presented in Table 2, which highlights the differences in access times based on varying network conditions and node availability.

Table 2. Average IPFS File Access Latency Based on Network Conditions

Scenario	Latency 1 (ms)	Latency 2 (ms)	Latency 3 (ms)	Latency 4 (ms)	Latency 5 (ms)
All Nodes Active	140	150	155	145	160
Some Nodes Inactive	310	330	320	305	335
Public IPFS Gateway	530	550	560	535	525

From Table 2, we observe that when all nodes in the IPFS network are active and properly functioning, the files are accessed quickly due to the efficient connection and close proximity of the storage nodes. Under these conditions, the average access latency is approximately 150 milliseconds (ms). This scenario is ideal for applications requiring reliable and quick data access.

However, when some nodes are inactive or unavailable, the performance of the DHT decreases, causing a significant increase in latency. In this case, the system has to search additional nodes for the requested files, resulting in a latency of about 320 ms, nearly double the latency when all nodes are active. This demonstrates that node availability plays a crucial role in the speed and reliability of IPFS.

The worst-case scenario occurs when files are accessed via a public IPFS gateway, with the highest observed latency at around 540 ms. This high latency can be attributed to several factors:

1. **High user request queues:** Public gateways often serve large numbers of users, causing delays in request processing.
2. **Limited bandwidth:** Public gateways have limited bandwidth, leading to slower data transfer speeds.
3. **File cache availability:** If requested files are not cached at the public gateway, they must be retrieved directly from the IPFS network, adding further delays.

While public gateways offer open access to the IPFS network without the need to join a private network, their performance is slower compared to private networks where nodes are actively managed and maintained.

### 4.3. Interpretation and Discussion

The simulation results indicate that the lowest access latency occurs when all nodes in the IPFS network are active and interconnected. In this optimal scenario, the storage nodes are in close proximity, and the system efficiently retrieves files through the DHT, resulting in low latency.

When some nodes are down, the DHT's efficiency is reduced, leading to longer search times for the requested files. This results in an increase in latency, as the system must search additional nodes to retrieve the data. This finding highlights the critical importance of node availability for ensuring the speed and reliability of IPFS.

The highest latency occurs when files are accessed through a public IPFS gateway. Public gateways, while providing open access to the network, suffer from limitations such as user request queues, limited bandwidth, and the unavailability of cached files, which result in significantly slower data retrieval.

In conclusion, the simulation results suggest that IPFS performs best under conditions where all nodes are operational, and private network configurations offer superior performance compared to public gateways. Future improvements to IPFS could focus on enhancing node availability, reducing latency, and addressing the limitations of public gateways, particularly for real-time applications.

## 5. MANAGERIAL IMPLICATION

The findings of this study offer several important implications for IT managers, digital policymakers, and data infrastructure administrators. These implications not only contribute to improving organizational



efficiency but also align with global sustainability objectives, particularly the United Nations Sustainable Development Goals (SDGs), such as SDG 9 (Industry, Innovation, and Infrastructure), SDG 12 (Responsible Consumption and Production), and SDG 16 (Peace, Justice, and Strong Institutions).

### 5.1. Adoption of Decentralized Storage Infrastructure

IT managers should consider integrating IPFS into their organization's digital infrastructure as an alternative to traditional centralized cloud storage solutions. IPFS offers distributed file storage, which can significantly mitigate the risks associated with service outages and improve data accessibility, particularly in scenarios where content distribution across multiple locations is crucial. By leveraging IPFS, organizations can enhance their data resiliency and operational continuity, especially during disruptions in centralized storage systems. This aligns with SDG 9, which calls for building resilient infrastructure and fostering innovation. IPFS can contribute to more sustainable and accessible digital infrastructure globally.

### 5.2. Enhancing Data Integrity and Security

IPFS uses cryptographic hashing to ensure each file has a unique, tamper-proof identifier, thereby providing a high level of data integrity. This makes it especially suitable for industries requiring strong validation and immutability of digital content, such as legal, academic, and financial sectors. IT managers can leverage IPFS to establish a solid foundation for securing critical data workflows, ensuring the authenticity and reliability of sensitive digital assets. In the context of SDG 16, IPFS enhances transparency and strengthens institutions by ensuring data integrity and security, critical components of good governance.

### 5.3. Reducing Operational Costs through Bandwidth Optimization

Organizations can significantly reduce bandwidth consumption by utilizing the peer-to-peer nature of IPFS. With content-based retrieval, files that are frequently accessed can be cached closer to the user, lowering the load on central servers and reducing associated data transfer costs. This bandwidth optimization offers long-term savings, particularly for high-volume or media-heavy applications. By strategically using IPFS, organizations can enhance their cost-efficiency in managing digital content distribution. This approach promotes more responsible consumption and production (SDG 12), as it optimizes resources and reduces the environmental impact of data storage and transfer.

### 5.4. Ensuring Continuity in High-Censorship Environments

For organizations operating in regions with stringent digital regulations or potential internet censorship, IPFS offers a resilient method for ensuring content remains online and accessible. By adopting IPFS, organizations can safeguard the continuity of communication and information access, even in the event that traditional hosting services or DNS systems are compromised or blocked. This feature is especially important for organizations in sensitive sectors such as media, human rights, and international communication. Supporting access to information, particularly in high-censorship environments, aligns with SDG 16, which emphasizes the importance of peace, justice, and strong institutions, ensuring access to information remains unimpeded.

### 5.5. Planning for Technical Integration and Capacity Building

The implementation of IPFS requires a shift in architectural thinking and specific technical expertise. IT managers must prepare for this transition by allocating resources for team training, infrastructure deployment, and gradual integration. Building internal competencies will be critical to ensuring the long-term sustainability and reliability of IPFS within the organization's digital strategy. As the adoption of decentralized technologies grows, having the technical capacity to manage and scale IPFS-based infrastructure will be a significant advantage for organizations aiming to stay ahead in the evolving digital landscape. This capacity-building effort contributes to SDG 9 by fostering innovation and technological advancements that can contribute to economic and social development.

## 6. CONCLUSION

As concerns over data integrity, censorship resistance, and the reliance on centralized systems continue to grow, this research highlights the promise of the InterPlanetary File System (IPFS) as a decentralized storage solution capable of addressing these issues. The literature review and technical simulations demonstrate that IPFS offers substantial benefits in areas such as data immutability, content addressing, and peer-to-peer distribution.

However, several challenges remain in its implementation. Notably, latency issues—especially when nodes are offline or when files are accessed via public gateways—underscore the need for improved infrastructure and enhanced node availability. The simulation results indicate that fully connected private IPFS networks provide the fastest response times (average of 150 ms), while public gateway access results in the highest latency (average of 540 ms).

In conclusion, IPFS presents a significant step toward creating a more open, transparent, and censorship-resistant digital ecosystem. Nevertheless, further advancements are required in terms of infrastructure support, scalability, and integration with existing systems to enable more widespread deployment. Future research and organizational initiatives should focus on addressing these technical limitations and exploring IPFS in dynamic, complex network environments to fully realize its potential in the digital ecosystem.


## 7. DECLARATIONS

### 7.1. About Authors


Sandy Setiawan (SS)  <https://orcid.org/0009-0001-2203-6579>

Muchlisina Madani (MM)  <https://orcid.org/0009-0001-8858-9547>

Sondang Visiana Sihotang (SV)  <https://orcid.org/0009-0008-4042-5798>

Elisa Ananda Natalia (EA)  <https://orcid.org/0009-0005-4863-3557>

Novita Khairunnisa (NK)  <https://orcid.org/0009-0007-4174-825X>

Kristina Vaher (KV)  <https://orcid.org/0009-0009-6790-0680>

### 7.2. Author Contributions

Conceptualization: SS, MM, and SV; Methodology: EA; Software: NK; Validation: SS and MM; Formal Analysis: SV and EA; Investigation: MM; Resources: SS; Data Curation: SV; Writing Original Draft Preparation: EA and SV; Writing Review and Editing: EA; Visualization: SS; All authors, SS, MM, SV, EA, NK, and KV, 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] S. Sridhar, O. Ascigil, N. Keizer, F. Genon, S. Pierre, Y. Psaras, E. Rivière, and M. Król, "Content censorship in the interplanetary file system," *arXiv preprint arXiv:2307.12212*, 2023.
- [2] 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.
- [3] T. Eldem, "Decentralisation as resistance: Web3's potential in countering digital censorship and redefining cyber sovereignty," *ELTE Law Journal*, no. 2, pp. 161–172, 2024.
- [4] P. B. Natarajan, "Exploring decentralized computing using solid and ipfs for social media applications," 2024.
- [5] D. E. Rose, J. Van Der Merwe, and J. Jones, "Digital marketing strategy in enhancing brand awareness and profitability of e-commerce companies," *APTISI Transactions on Management*, vol. 8, no. 2, pp. 160–166, 2024.



- [6] K. V. A. Anthony and T. Mathu, "Decentralized social media using blockchain and ipfs," in *2024 4th International Conference on Pervasive Computing and Social Networking (ICPCSN)*. IEEE, 2024, pp. 560–565.
- [7] Y. Farooqui, D. Patel, M. Kumar, R. Mehta, and R. Vyas, "Towards a decentralized future: The role of deverse in publishing evolution," in *2024 Parul International Conference on Engineering and Technology (PICET)*. IEEE, 2024, pp. 1–6.
- [8] A. Nuche, O. Sy, and J. C. Rodriguez, "Optimizing efficiency through sustainable strategies: The role of management and monitoring in achieving goals," *APTISI Transactions on Management*, vol. 8, no. 2, pp. 167–174, 2024.
- [9] D. Rani, N. S. Gill, P. Gulia, M. Yahya, T. A. Ahanger, M. M. Hassan, F. B. Abdallah, and P. K. Shukla, "A secure digital evidence preservation system for an iot-enabled smart environment using ipfs, blockchain, and smart contracts," *Peer-to-Peer Networking and Applications*, vol. 18, no. 2, pp. 1–29, 2025.
- [10] 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, pp. 4068–4076.
- [11] H. R. Hasan, K. Salah, I. Yaqoob, R. Jayaraman, S. Pesic, and M. Omar, "Trustworthy iot data streaming using blockchain and ipfs," *IEEE Access*, vol. 10, pp. 17 707–17 721, 2022.
- [12] T. Nododile and C. Nyirenda, "A hybrid blockchain-ipfs solution for secure and scalable data collection and storage for smart water meters," 2025.
- [13] S. I. Al-Hawary, J. R. N. Alvarez, A. Ali, A. K. Tripathi, U. Rahardja, I. H. Al-Kharsan, R. M. Romero-Parra, H. A. Marhoon, V. John, and W. Hussian, "Multiobjective optimization of a hybrid electricity generation system based on waste energy of internal combustion engine and solar system for sustainable environment," *Chemosphere*, vol. 336, p. 139269, 2023.
- [14] E. Daniel and F. Tschorsch, "Passively measuring ipfs churn and network size," in *2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*. IEEE, 2022, pp. 60–65.
- [15] 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*, pp. 1–22, 2024.
- [16] D. S. S. Wuisan, R. A. Sunardjo, Q. Aini, N. A. Yusuf, and U. Rahardja, "Integrating artificial intelligence in human resource management: A smartpls approach for entrepreneurial success," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 334–345, 2023.
- [17] T. Chain, A.-S. Oh, and S.-S. Shin, "Blockchain and ipfs-based iot massive data-management model," 2024.
- [18] M. Kaur, S. Gupta, D. Kumar, M. S. Raboaca, S. Goyal, and C. Verma, "Ipfs: An off-chain storage solution for blockchain," in *Proceedings of International Conference on Recent Innovations in Computing: ICRIC 2022, Volume 1*. Springer, 2023, pp. 513–525.
- [19] S. Lestari, S. Watini, and D. E. Rose, "Impact of self-efficacy and work discipline on employee performance in sociopreneur initiatives," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 2, pp. 270–284, 2024.
- [20] T. V. Doan, Y. Psaras, J. Ott, and V. Bajpai, "Towards decentralised cloud storage with ipfs: Opportunities, challenges, and future directions," pp. arXiv–2202, 2022.
- [21] H. Wijayanto, M. J. Andara, D. Wiraguna, N. Agitha, and M. Rahaman, "Blockchain-based supply chain solution using ipfs and qr technology for traditional weave in west nusa tenggara," *JURNAL INFOTEL*, vol. 16, no. 4, pp. 740–757, 2024.
- [22] I. Maria *et al.*, "Unlocking success: Human resource management for startupreneur," *Startupreneur Business Digital (SABDA Journal)*, vol. 3, no. 1, pp. 89–97, 2024.
- [23] V. Estrada-Galiñanes, A. ElRouby, and L. M.-A. Theytaz, "Efficient data management for ipfs dapps," 2024.
- [24] Z. Ullah, G. Husnain, M. I. Mohmand, M. Qadir, K. J. Alzahrani, Y. Y. Ghadi, and H. K. Alkahtani, "Blockchain-iot: A revolutionary model for secure data storage and fine-grained access control in the internet of things," *IET Communications*, vol. 18, no. 19, pp. 1524–1540, 2024.
- [25] T. K. Andiani and O. Jayanagara, "Effect of workload, work stress, technical skills, self-efficacy, and social competence on medical personnel performance," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 2, pp. 118–127, 2023.

- [26] K. Balamurugan, M. Azhagiri, P. H. Vardhini, E. Jijo, and L. Parthiban, "Utilizing blockchain and interplanetary file system for enhanced user privacy in secure data sharing," in *Blockchain and IoT*. Chapman and Hall/CRC, 2025, pp. 42–60.
- [27] A. A. Ayare, V. A. Jadhav, M. K. Banatwala, S. V. Changlere, A. Mote, P. Joshi, and M. Banatwala, "A systematic review on blockchain-based framework for storing educational records using interplanetary file system," *Cureus Journals*, vol. 2, no. 1, 2025.
- [28] 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.
- [29] B. John, "Decentralized data vaults: Leveraging blockchain for secure cloud storage," 2025.
- [30] H. Belfqih and A. Abdellaoui, "Decentralized blockchain-based authentication and interplanetary file system-based data management protocol for internet of things using ascon," *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, p. 16, 2025.
- [31] K. K. Deepthi, L. S. R. K. Boddu, S. N. C. Yalamanchili, and S. Maganti, "Ipfs based file storage access control and authentication model for secure data transfer using blockchain technique," in *Algorithms in Advanced Artificial Intelligence*. CRC Press, 2025, pp. 520–525.
- [32] B. P. Chintal, "Secure decentralized storage system using blockchain and ipfs," *Available at SSRN 5142864*, 2025.
- [33] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi, "Pemerintah dorong swakelola transparansi data menuju pendidikan," 2023, accessed: 2023-07-30. [Online]. Available: <https://www.kemendikdasmen.go.id/siaran-pers/13029-pemerintah-dorong-swakelola-transparansi-data-menuju-pendidi>
- [34] K. Tiwari and S. Kumar, "A healthcare data management system: blockchain-enabled ipfs providing algorithmic solutions for increased privacy-preserving scalability and interoperability," *The Journal of Supercomputing*, vol. 81, no. 8, p. 895, 2025.
- [35] B. John, "Design and implementation of a blockchain-based decentralized data storage system for secure access control in cloud environments," 2025.
- [36] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi, "Penandatanganan komitmen bersama mendukung pelaksanaan spmb," 2023, accessed: 2023-07-30. [Online]. Available: <https://www.kemendikdasmen.go.id/siaran-pers/13026-penandatanganan-komitmen-bersama-mendukung-pelaksanaan-spmb>
- [37] H. A. Alameen and F. Rabee, "Blockchain-based metadata management in distributed file systems," *Mesopotamian Journal of CyberSecurity*, vol. 5, no. 2, pp. 349–360, 2025.
- [38] M. Tarhouni and F. Chaabane, "An advanced secure medical file-sharing system based on ipfs and blockchain technology," in *Using Blockchain Technology in Healthcare Settings*. CRC Press, 2025, pp. 190–205.
- [39] S. Sharma, S. Sharma, and T. Choudhury, "Enhancing cloud data security through an encrypted and efficient connection model based on blockchain technology," *Scalable Computing: Practice and Experience*, vol. 26, no. 2, pp. 517–530, 2025.
- [40] S. T. S. Alfian, F. Ichsanudin, N. Ndruru *et al.*, "Bitcoin and digital currency: Difficulties, open doors and future works," *Blockchain Frontier Technology*, vol. 2, no. 1, pp. 50–57, 2022.
- [41] M. K. Singh, S. Kumar Pippal, and V. Sharma, "A blockchain-ipfs framework for secure, scalable, and interoperable healthcare data management," *SN Computer Science*, vol. 6, no. 5, pp. 1–13, 2025.
- [42] R. Madhusudhan and S. Rithesh, "Decentralized disaster management in smart cities: Leveraging ipfs, blockchain, and edge computing," in *2025 IEEE 22nd Consumer Communications & Networking Conference (CCNC)*. IEEE, 2025, pp. 1–6.
- [43] H. Rehmanji, A. Shirgaonkar, J. Mistry, A. Shah, K. Bhowmick, and N. Patil, "Priority-based disk space sharing using blockchain."
- [44] H. Kumar, H. Kumar, H. Nandanwar, R. Katarya *et al.*, "Enhancing security and scalability of iomt systems using blockchain: Addressing key challenges and limitations," in *6th International Conference on Deep Learning, Artificial Intelligence and Robotics (ICDLAIR 2024)*. Atlantis Press, 2025, pp. 191–202.
- [45] R. Ahli, M. F. Hilmi, and A. Abudaqa, "Moderating effect of perceived organizational support on the relationship between employee performance and its determinants: A case of entrepreneurial firms in uae,"

- Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 2, pp. 199–212, 2024.
- [46] G. Sujatha, “Medisecure: A decentralized framework for electronic health record management using blockchain and ipfs,” in *Harnessing AI, Blockchain, and Cloud Computing for Enhanced e-Government Services*. IGI Global Scientific Publishing, 2025, pp. 181–220.
- [47] A. Verma, T. Singh, S. Raj, and R. K. Dwivedi, “Blockchain based security enhancement in decentralized storage of ipfs using filecoin,” in *2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*. IEEE, 2025, pp. 390–398.
- [48] V. Agarwal, M. Lohani, A. S. Bist, L. Rahardja, M. Hardini, and G. Mustika, “Deep cnn–real esrgan: An innovative framework for lung disease prediction,” in *2022 IEEE Creative Communication and Innovative Technology (ICCIIT)*. IEEE, 2022, pp. 1–6.
- [49] B. Anupama, N. Sunitha, G. Thejas *et al.*, “Document management across departments in defense using blockchain technology,” in *Artificial Intelligence for Military Applications with Blockchain*. CRC Press, 2025, pp. 19–40.