APTISI Transactions on Management (ATM)
Vol. 10, No. 1, January 2026, pp. 45∼55
E-ISSN: 2622-6804 P-ISSN: 2622-6812, DOI: 10.33050

IPFS Based Secure and Decentralized Web Architecture A Systematic Review

Dhimas Tribuana[1], Apriani Sijabat[2], Titih Nursugiharti[3], Rizky Charles Wijaya[4*]
[1]Doctor of Management Science, Indonesian Computer University, Indonesia
[2]Faculty of Science Education Doctoral Study Program, Padang State University, Indonesia
[3]Manuscripts, Literature and Oral Traditions, National Research and Innovation Agency, Indonesia
[4]Department of Statistics, Adi-Journal Incorporation, USA
[1]dhimas.75423008@mahasiswa.unikom.ac.id, [2]aprianisijabat@gmail.com, [3]tinus.brata@gmail.com, [4]charlesboy10@adi-journal.org
***Corresponding Author**

Article Info

Article history:

Received December 01, 2025
Revised January 05, 2026
Accepted January 13, 2026

Keywords:

IPFS
SLR
P2P
Security
Web 3.0

ABSTRACT

The rapid development of digital technology has driven a transition from Web 2.0 to Web 3.0, where decentralization, user autonomy, and data security have become fundamental priorities. This transition introduces critical challenges in distributed systems, peer-to-peer networking, and security engineering, particularly concerning fault tolerance, data integrity, and resilience against centralized failures. Traditional centralized web architectures often suffer from single points of failure, making them vulnerable to cyberattacks and censorship. **This study investigates** the InterPlanetary File System (IPFS) as a content-addressed, peer-to-peer distributed storage architecture that enhances decentralized web infrastructures by enabling immutable data validation, node redundancy, and improved resistance to system-level attacks. **This study adopts** a Systematic Literature Review (SLR) approach to examine the application of IPFS in developing secure and decentralized websites within the Web 3.0 ecosystem. Following PRISMA-guided procedures, recent peer-reviewed studies are systematically analyzed to identify architectural patterns, security mechanisms, and system-level challenges associated with decentralized web hosting. **The findings** are synthesized to assess the implications of IPFS for data integrity, system resilience, and fault tolerance in distributed environments. **These results lead** to the conclusion that integrating IPFS into website development represents a strategic step toward creating a more transparent, resilient, and decentralized web ecosystem aligned with the core principles of Web 3.0.

Corresponding Author:

DOI: https://doi.org/10.33050/atm.v10i1.2580

1. INTRODUCTION

The growing reliance on centralized web infrastructures has increasingly exposed digital platforms to systemic risks, including data breaches, service outages, and unilateral control over information flows. While contemporary web platforms enable large-scale interaction and content creation, their underlying architectures often concentrate data ownership and governance within a small number of service providers, resulting in diminished user control, heightened censorship risks, and vulnerability to infrastructure failures or cyberattacks

[1]. These limitations have intensified calls for alternative web architectures that emphasize transparency, resilience, and decentralized control.

Decentralized web paradigms have emerged in response to these structural challenges by rethinking how data is stored, accessed, and verified across networks. Rather than relying on server-centric models characteristic of earlier web architectures [2], decentralized systems promote peer-to-peer interaction and user-driven content management, extending the participatory model popularized during the social-media-driven era of interactive platforms [3]. This shift has become central to the vision of Web 3.0, which prioritizes open participation, cryptographic trust, and distributed governance mechanisms.

Within the Web 3.0 ecosystem, the InterPlanetary File System (IPFS) has gained significant attention as a decentralized, content-addressed storage protocol designed to eliminate dependence on centralized servers [4, 5]. By identifying data through cryptographic hashes rather than physical locations, IPFS enables intrinsic verification of content integrity, facilitates distributed replication, and supports censorship-resistant access to information [6, 7]. These characteristics position IPFS as a critical infrastructural component for decentralized web applications that require long-term data availability and user sovereignty.

From an engineering and systems perspective, however, the adoption of IPFS introduces a range of technical challenges that remain highly relevant to IEEE research and practice [8]. The content-addressed design of IPFS raises important questions regarding routing efficiency, replication strategies, and interoperability with existing web protocols [9]. Furthermore, decentralized content retrieval must balance security and resilience against performance constraints such as latency, throughput, and scalability, particularly under dynamic network conditions [10–12]. These challenges underscore the need for systematic evaluation of IPFS-based architectures beyond isolated implementations or proof-of-concept systems [13].

Despite a growing body of research, uncertainty remains regarding the practical viability of IPFS for real-world decentralized website development, including its usability, performance consistency, and compatibility with widely adopted web technologies [14]. Rather than developing or experimentally testing a specific prototype, this study adopts a Systematic Literature Review (SLR) approach to synthesize empirical and analytical findings from recent peer-reviewed studies. Through comparative analysis, this research evaluates the security, performance, and architectural characteristics of IPFS-based web infrastructures relative to traditional centralized hosting models [15].

The primary objective of this study is to assess whether IPFS can effectively support the development of secure, tamper-resistant, and censorship-resilient web architectures [16, 17]. Existing studies have explored IPFS performance under various conditions, including network disruptions, unauthorized data modification attempts, and multi-user access scenarios [18–20]. By consolidating insights from these studies, this review aims to clarify the conditions under which IPFS can serve as a viable alternative to traditional hosting systems, particularly for organizations and individuals seeking greater control over their digital assets [21, 22].

Beyond technical considerations, decentralized web technologies align with broader socio-economic objectives, particularly the United Nations Sustainable Development Goals (SDGs). Web 3.0 infrastructures contribute to SDG 9 and SDG 16 by promoting resilient, secure, and transparent digital systems [23, 24]. In Indonesia, national digital transformation strategies emphasize infrastructure development to support sustainable growth and inclusive connectivity, reinforcing the relevance of evaluating decentralized web technologies such as IPFS [25, 26].

2. LITERATUR REVIEW

2.1. The Transition of Web Architectures Toward Decentralized Paradigms

However, Web 2.0 was susceptible to issues including data manipulation, censorship, and privacy violations due to its heavy reliance on centralized servers managed by third parties [27]. As a result, Web 3.0 arose as a decentralized system that gives people complete control over their data. To provide a clear analytical foundation, this study adopts a theoretical lens grounded in distributed systems and security engineering [28, 29]. Within this framework, decentralized web infrastructure is examined through three interrelated dimensions:

- Architectural decentralization, which emphasizes Peer to Peer (P2P) communication and content-addressed storage.
- System resilience, encompassing fault tolerance, redundancy, and availability [30].
- Security assurance, including data integrity, immutability, and resistance to unauthorized modification.

This framework is used to organize and interpret the reviewed studies, enabling a structured analysis of how IPFS contributes to Web 3.0 infrastructure beyond descriptive characteristics.

Guided by this theoretical framework, the review is analytically driven by the following research questions:

- (RQ1) How does IPFS architecture, as a distributed system, enhance data integrity and tamper resistance in decentralized web environments?
- (RQ2) What system-level resilience and fault-tolerance properties are enabled by IPFS-based P2P networking?
- (RQ3) What technical limitations and performance trade-offs are identified across existing studies when IPFS is applied to large-scale Web 3.0 infrastructures?

Web 3.0 builds a more secure and equitable digital economy by utilizing blockchain technology and other decentralized protocols.

2.2. Content-Addressed Storage and Decentralized Architectural Design

IPFS is a P2P network and protocol intended for data sharing and storage in scattered environments [31]. Unlike conventional HTTP, IPFS employs content addressing rather than location addressing. This method makes the data unidentifiable by giving each file in IPFS a distinct cryptographic hash [32, 33]. 4 IPFS also permits data redundancy among several network nodes, boosting the system's dependability and resistance to malfunctions. IPFS can enhance data security, file distribution efficiency, and lessen reliance on central servers, according to a number of earlier research [34, 35]. IPFS and end-to-end encryption work together to create secure web delivery and storage systems.

2.3. Using Decentralized Technology for Website Security

Building on prior studies in distributed systems and security engineering, this research adopts a conceptual framework that positions IPFS as a content-addressed P2P storage layer within the Web 3.0 ecosystem [36, 37]. From a distributed systems perspective, IPFS contributes through node-level redundancy, fault tolerance, and decentralized routing. From a networking standpoint, the P2P architecture enables resilient content distribution without reliance on centralized servers [38, 39]. In terms of security engineering, content-based hashing and cryptographic verification mechanisms ensure data integrity, immutability, and resistance to unauthorized modification.

Based on this framework, this study conceptualizes the relationship between IPFS architectural characteristics (content addressing and P2P distribution) and system-level outcomes, including security robustness, availability, and resilience against single points of failure [40, 41]. This analytical structure provides a theoretical foundation that guides the research design and evaluation process.

Accordingly, the study addresses the following research questions:

- (RQ1) How does IPFS architecture enhance data integrity and tamper resistance compared to traditional centralized web hosting models?
- (RQ2) To what extent does P2P content distribution in IPFS improve system resilience and fault tolerance?
- (RQ3) What security and performance trade-offs emerge when IPFS is applied to decentralized website development in the Web 3.0 context?

3. RESEARCH METHODS

3.1. Research Approach

This study applies a Systematic Literature Review (SLR) to synthesize empirical and analytical studies on IPFS-based decentralized web architectures [42]. Methodological rigor is ensured through transparent literature selection and structured analysis following PRISMA guidelines, without system prototyping or experimentation [43]. The SLR approach is suitable for identifying trends, challenges, and innovations in IPFS applications for secure and decentralized Web 3.0 websites [44–46]. The review follows four PRISMA stages: identification, screening, full-text evaluation, and synthesis [47].

3.2. Literature Selection Criteria

To ensure the relevance, quality, and consistency of the selected literature, this study defines a set of inclusion and exclusion criteria that guide the literature screening and selection process. These criteria are systematically summarized in Table 1, providing a clear framework for identifying studies that are most relevant to the research objectives.

Table 1. Inclusion and Exclusion Criteria

Criteria	Description
Inclusion	An article that explicitly discusses IPFS, decentralization, and Web 3.0. Scientific studies published between 2021–2025 in reputable journals (Scopus, IEEE, ACM, Elsevier). Studies involving website security, distributed systems, and P2P technologies
Exclusion	Blog articles, opinions, or unverified sources that have not undergone peer-review. Research prior to 2021 or articles not available in English or Indonesian.

The literature selection process is conducted in two sequential stages based on the inclusion and exclusion criteria presented in Table 1. The first stage involves a screening of titles and abstracts to ensure initial relevance to the research topic. Articles that pass this stage proceed to the second stage, which consists of a full-text evaluation focusing on methodological quality and the contribution of each study to the research objectives.

3.3. Stages of SLR Implementation

To provide a clear and structured overview of SLR process, this study outlines the key stages involved in literature selection and analysis. The stages of the SLR implementation are summarized in Table 2, illustrating the step-by-step process from study identification to synthesis and reporting.

Table 2. Literature Selection and Analysis Process

Level	Process Description
Study Identification	Collection of articles from databases such as IEEE Xplore, Scopus, and Google Scholar using keywords: “IPFS”, “Web 3.0”, “decentralized website”, and “secure P2P hosting”.
Title and Abstract Screening	Initial screening based on title and abstract to ensure relevance to the research topic and fulfillment of inclusion criteria.
Full Text Evaluation	A thorough review of the article’s content, methodology, findings, and reliability of sources.
Synthesis and Reporting	Grouping the results based on categories such as IPFS architecture, data security, and website implementation, followed by narrative analysis and visualization of findings trends.

As summarized in Table 2, the literature selection process follows a structured multi-stage approach to ensure relevance and rigor. It begins with systematic database searches using predefined keywords [48], followed by title and abstract screening to assess inclusion criteria. Eligible studies then undergo full-text evaluation to examine methodological quality and source reliability [49]. Finally, the selected literature is synthesized to identify patterns related to IPFS architecture, data security, and decentralized web implementation [50].

3.4. SLR Process Flow Diagram

To enhance clarity and transparency in the research methodology, this study includes a visual representation of the SLR process. Figure 1 depicts the workflow from planning to data extraction, covering key stages such as literature identification, screening, eligibility assessment, and synthesis. The figure visually organizes the systematic approach used to ensure comprehensive inclusion of relevant studies, minimize bias, and uphold methodological rigor. This visualization not only strengthens the transparency and replicability of the review process but also helps readers better understand the structured steps involved in conducting an SLR. It serves as a guide to the systematic, replicable process that underpins the analysis and synthesis of existing literature on IPFS and Web 3.0 technologies.

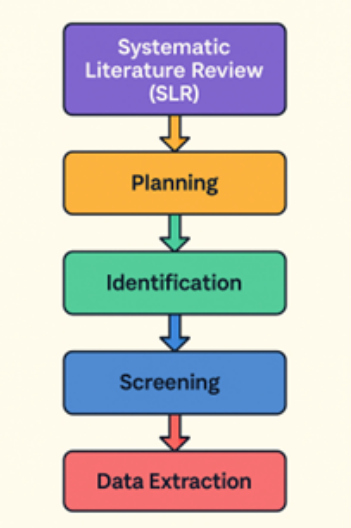

Figure 1. Systematic Literature Review (SLR) Process

The research process is described in Figure 1, which begins with the identification of literature and ends with the production of organized and responsible findings. This representation encourages process transparency and makes it easier for other researchers to replicate the findings.

4. RESULTS AND DISCUSSION

4.1. Overview of Research Findings

To provide a concise overview of the studies selected in this systematic literature review, this section summarizes key information from the relevant publications, including authors, research methods, publication year, data sources, and main findings. The summary of the selected literature is presented in Table 3, which highlights how IPFS and related Web 3.0 technologies have been applied across different research contexts.

Table 3. Summary of Selected Literature on IPFS and Web 3.0

Writer	Article Title	Method	Year	Source	Research Result
[51]	Decentralized File Sharing: Leveraging Blockchain and IPFS for Secure Data Storage	Experiments and Case Studies	2024	IEEE Xplore	IPFS and blockchain enhance data security in decentralized storage systems, although scalability and access speed remain challenges. These technologies support secure and efficient Web 3.0 applications.
[52]	Scalable Blockchain Model Using Off-chain IPFS Storage for Healthcare Data Security and Privacy	Experimental	2022	Scopus	Integrating IPFS and blockchain secures health data by using off-chain storage and on-chain verification. This approach ensures privacy, immutability, auditability, scalability, and reduces risks of centralized data storage.
[53]	IPFS Based Decentralised Twitter Using Web 3.0 Technologies	Experimenting with prototype development	2023	Google Scholar	This paper presents a Web 3.0 based decentralized Twitter using IPFS for distributed data storage and blockchain for data integrity. The system enhances user data control, reduces censorship and centralization, but still faces scalability and access speed challenges.

Writer	Article Title	Method	Year	Source	Research Result
[54]	Efficient and Secure Distributed Data Storage and Retrieval Using Interplanetary File System and Blockchain	Framework analysis & system evaluation	2024	ResearchGate	IPFS with blockchain enhances secure, decentralized, and efficient distributed storage and retrieval, improving data integrity and performance in Web 3.0 environments.
[19]	Decentralized Data Storage Using IPFS for Sustainable Blockchain Availability Improvement	Qualitative literature & case evaluation	2024	Google Scholar	IPFS improves data reliability, transparency, and scalability compared to centralized systems, while revealing challenges in node stability and system resilience.

Beyond aggregating existing findings, this SLR provides new insights by revealing consistent cross-study patterns and unresolved technical tensions in IPFS-based systems. As summarized in Table 3, this SLR identifies several important observations. First, while most studies confirm that IPFS enhances data integrity and censorship resistance, this SLR identifies a recurring trade-off between decentralization and performance scalability that is insufficiently addressed in isolated case studies. Second, the review highlights that security guarantees in IPFS are predominantly content-centric, whereas network-level attack resilience and adaptive routing security remain underexplored across application domains. Third, by comparing results from social media, healthcare, and content hosting use cases, this study uncovers a research gap in domain-specific optimization strategies for IPFS deployment, suggesting that a one-size-fits-all architecture is inadequate for large-scale Web 3.0 systems. These synthesized insights extend prior work by shifting the discussion from isolated implementations toward system-level design implications relevant to IEEE research on distributed systems and secure networking.

However, despite the advantages of this system in terms of security and openness, scalability and availability speed continue to be major obstacles, especially in large-scale applications like decentralized social media (like decentralized Twitter) [55, 56]. Several investigations show that although IPFS offers decentralization, when the amount of data or the number of nodes increases, the pace of data retrieval from a distributed network may go down.

4.2. Security, Privacy, and Data Integrity

The reviewed studies consistently indicate that IPFS enhances data integrity and security in decentralized storage systems through content-addressed mechanisms that enable reliable detection of unauthorized modifications. When combined with blockchain-based verification, these systems further strengthen transparency and auditability. As a result, reliance on centralized control points is reduced, thereby lowering systemic security risks and improving overall resilience.

4.3. Scalability and Performance Challenges

Stability and performance issues are one of the main issues that cloud-based systems, IPFS, and Blockchain must cope with, particularly when handling massive data volumes and numerous users. As the number of nodes in the network grows, IPFS may undergo performance deterioration, which affects data processing time and access speed. The issue is the effectiveness of the network for managing huge transactions and storing data in a decentralized system. Decentralization and security are provided by IPFS, however scalability is still a significant challenge because poorly managed data distribution and management might impede data retrieval.

Some of the suggested solutions to this problem include network optimization and the use of a strategic node that is more effectively dispersed, as well as the use of extra layers to expedite the process of data retrieval and verification. Additionally, this is crucial to guarantee system performance, which is ideal in huge applications like Web 3.0-based social media platforms.

4.4. Application in Web 3.0 Ecosystem

IPFS and Blockchain implementation in Web 3.0 is crucial to building a transparent and safe decentralized platform [57]. In the Web 3.0 system, IPFS can be utilized to safely store material, giving users complete control over their data. A platform designed using IPFS allows for more data protection, user control,

and transparency by substituting a distributed network for a centralized server. But implementing Web 3.0 with IPFS and Blockchain on big platforms like decentralized social media needs a more robust infrastructure to handle massive amounts of data. For Web 3.0 to be implemented successfully, particularly on a big scale, access speed and ability remain a challenge [58].

4.5. Conclusion of Results

Overall, beyond reaffirming established advantages of IPFS, this systematic review uncovers several novel analytical insights that are not explicitly articulated in individual studies. First, a consistent cross-study pattern reveals that security benefits in IPFS-based systems are predominantly achieved at the data layer through content addressing and cryptographic hashing, whereas network-layer security and adaptive routing mechanisms remain comparatively underexplored. Second, the synthesis exposes a contradiction in scalability findings: while experimental studies report acceptable performance in controlled environments, application-oriented studies in social media and large-scale content delivery consistently document latency degradation and node coordination challenges. Third, this review identifies a significant research gap in domain-specific deployment strategies, as most studies assume a generic IPFS architecture without tailoring design choices to application requirements. These insights demonstrate that current IPFS research emphasizes architectural feasibility over systematic optimization, thereby highlighting critical directions for future IEEE-focused research on distributed systems and decentralized networking. By continuously improving infrastructure and network solutions to solve problems, this technology has significant potential to build a safer and more effective decentralized platform in the future scalability and quick access.

5. MANAGERIAL IMPLICATIONS

The findings of this study provide several important managerial implications for decision-makers, technology managers, and system architects involved in the development and governance of decentralized web infrastructure. First, managers responsible for digital platform strategy should recognize that adopting IPFS is not merely a technological shift, but a strategic architectural decision. IPFS-based systems offer clear advantages in terms of data integrity, censorship resistance, and resilience against single points of failure. However, these benefits come with performance and scalability trade-offs. Therefore, managerial decisions should prioritize hybrid deployment strategies, combining decentralized storage with adaptive caching and selective centralization to balance security and performance requirements.

Second, from an operational management perspective, the results highlight the need for proactive governance of node availability and content persistence. Managers overseeing decentralized systems should implement clear policies for content pinning, node incentive mechanisms, and redundancy management to ensure data availability and service reliability. Without such governance mechanisms, the decentralized nature of IPFS may lead to inconsistent performance and reduced user experience, particularly in large-scale applications.

Third, at the organizational and policy interface, managers and policymakers should collaborate to align decentralized web adoption with regulatory requirements related to data sovereignty, privacy, and digital resilience. The study suggests that IPFS can support compliance with emerging data governance frameworks by enabling distributed data control and reducing dependence on centralized infrastructure providers. Consequently, managerial leadership is required to translate these technical capabilities into organizational policies, risk management frameworks, and long-term digital infrastructure strategies that support sustainable and secure Web 3.0 adoption.

Fourth, from a financial and investment perspective, the adoption of IPFS requires managers to reassess cost structures and long-term return on investment in digital infrastructure. While decentralized storage can reduce dependency on centralized cloud providers and associated vendor lock-in risks, it may introduce new operational costs related to node maintenance, incentive mechanisms, and performance optimization. Therefore, managers should conduct comprehensive cost–benefit analyses that account for both direct infrastructure expenses and indirect strategic benefits, such as improved data sovereignty, system resilience, and reduced exposure to centralized service disruptions.

Fifth, the findings underscore the importance of organizational capability development and change management in decentralized web adoption. Successful implementation of IPFS-based architectures demands not only technical expertise, but also cross-functional coordination between IT teams, security specialists, legal units, and business stakeholders. Managers should invest in workforce upskilling, establish interdisciplinary

governance structures, and promote organizational awareness of decentralized system principles to mitigate operational risks and ensure effective integration into existing digital ecosystems.

Finally, from a long-term strategic innovation perspective, the study highlights that IPFS adoption should be viewed as an evolving capability rather than a one-time infrastructure decision. As decentralized web technologies continue to mature, managers should remain adaptive by monitoring advancements in routing optimization, incentive models, and hybrid architectural frameworks. Proactive engagement with research communities and industry consortia will enable organizations to continuously refine their decentralized strategies, ensuring alignment with emerging standards and sustaining competitive advantage in the Web 3.0 landscape.

6. CONCLUSION

This study demonstrates that the integration of IPFS and blockchain offers a powerful solution for building decentralized systems that are more secure and verifiable for Web 3.0-based applications. By utilizing IPFS for data storage and blockchain for verification, this approach enables users to maintain greater control over their data, reduces dependence on centralized servers, and enhances data security and privacy. Despite its strong potential in terms of transparency and data integrity, the primary challenges identified relate to scalability and access speed, particularly when applied to systems handling large volumes of data.

The main topic of this study is how IPFS and blockchain can be integrated to produce a more decentralized and secure data storage system. Although the results validate the efficacy of both systems, a number of limitations are still apparent. Scalability becomes a significant issue, particularly on systems with lots of users and a lot of data, where slower data retrieval and performance degradation might happen. However, if performance and large-scale data management issues are sufficiently resolved to enable wider acceptance, the use of IPFS and blockchain is still very relevant to the advancement of Web 3.0.

Building on the identified scalability and performance limitations, several directions for future research and system development are proposed. From a technical perspective, further investigation into adaptive routing and caching mechanisms within IPFS is recommended to reduce latency and improve throughput under high network dynamics. Hybrid architectural designs that combine decentralized storage with strategically placed gateway nodes may also help balance performance efficiency and decentralization. In addition, future studies should conduct large-scale performance benchmarking under realistic workloads and explore performance-aware incentive mechanisms to enhance network stability. In real-world Web 3.0 deployments, testing IPFS and blockchain implementations in large-scale applications, including decentralized social media platforms, will further support system readiness and stability.

7. DECLARATIONS

7.1. About Authors

Dhimas Tribuana (DR) https://orcid.org/0009-0002-8504-0740

Apriani Sijabat (AS) https://orcid.org/0000-0002-0044-052X

Titih Nursugiharti (TN) https://orcid.org/0000-0002-5775-8627

Rizky Charles Wijaya (RW) https://orcid.org/0009-0003-8655-1339

7.2. Author Contributions

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

REFERENCES

[1] M. C. Lacity and E. Carmel, "Web2 versus web3 information privacy: An information systems discipline perspective," in *Human Privacy in Virtual and Physical Worlds: Multidisciplinary Perspectives*. Springer Nature Switzerland Cham, 2024, pp. 111–140.

[2] T. T. Haile, "Web's progression: Moving from passive content consumption to active content creation and content validation," *International Journal of Business and Management*, vol. 18, no. 6, p. 136, 2023.

[3] E. C. Ramos and C. M. Ramos, "User-generated content and its impact on purchase intent for tourism products: A comparative analysis of millennials and centennials on tiktok," *Future Internet*, vol. 17, no. 3, p. 105, 2025.

[4] I. R. Maulana, U. Rahardja, N. Azizah, M. Rakhmansyah, and M. A. Komara, "Leveraging ipfs to build secure and decentralized websites in the web 3.0 era," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 7, no. 1, pp. 1–12, 2025.

[5] U. Narayanan, V. Paul, and S. Joseph, "Decentralized blockchain based authentication for secure data sharing in cloud-iot: Deblock-sec," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 2, pp. 769–787, 2022.

[6] N. P. Patil, Y. D. Mane, A. Vasoya, A. Agrawal, and S. Raut, "Secure file sharing using blockchain and ipfs with smart contract-based access control," 2024.

[7] H. Herman, W. Achmad, N. Aulia, S. Rusdian, and T. Green, "Utilizing ipfs for decentralized data storage a security and censorship resistance solution," *Blockchain Frontier Technology*, vol. 5, no. 2, pp. 124–135, 2026.

[8] M. J. H. Faruk, P. Raya, M. K. Siam, J. Q. Cheng, H. Shahriar, A. Cuzzocrea, and P. G. Bringas, "A systematic literature review of decentralized applications in web3: Identifying challenges and opportunities for blockchain developers," in *2024 IEEE International Conference on Big Data (BigData)*. IEEE, 2024, pp. 6240–6249.

[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] D. Trautwein, Y. Wei, Y. Psaras, M. Schubotz, I. Castro, B. Gipp, and G. Tyson, "Ipfs in the fast lane: Accelerating record storage with optimistic provide," in *IEEE INFOCOM 2024-IEEE Conference on Computer Communications*. IEEE, 2024, pp. 1920–1929.

[11] 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.

[12] R. Shi, R. Cheng, B. Han, Y. Cheng, and S. Chen, "A closer look into ipfs: Accessibility, content, and performance," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 8, no. 2, pp. 1–31, 2024.

[13] G. Mandinyenya and V. Malele, "Comparative security and performance evaluation of ipfs and filecoin for off-chain blockchain storage," *The Indonesian Journal of Computer Science*, vol. 14, no. 4, 2025.

[14] 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.

[15] M. H. R. Chakim, M. A. D. Yuda, R. Fahrudin, D. Apriliasari *et al.*, "Secure and transparent elections: Exploring decentralized electronic voting on p2p blockchain," *ADI Journal on Recent Innovation*, vol. 5, no. 1Sp, pp. 54–67, 2023.

[16] T. Rahman, S. I. Mouno, A. M. Raatul, A. K. Al Azad, and N. Mansoor, "Verifi-chain: a credentials verifier using blockchain and ipfs," in *International Conference on Information, Communication and Computing Technology*. Springer, 2023, pp. 361–371.

[17] T. Eldem, "Decentralisation as resistance: Web3's potential in countering digital censorship and redefining cyber sovereignty," *ELTE LJ*, p. 161, 2024.

[18] S. R. Mallick, R. K. Lenka, and S. Sobhanayak, "Secure and scalable dual blockchain and ipfs driven iot ecosystem for next gen healthcare systems," *Scientific Reports*, vol. 15, no. 1, p. 41064, 2025.

[19] A. Jaya, M. Fahrurrozi, S. A. Sibagariang, V. Likita, and H. Zainarthur, "Decentralized data storage using ipfs for sustainable blockchain availability improvement," *Blockchain Frontier Technology*, vol. 5, no. 2, pp. 136–146, 2026.

[20] B. John and J. John, "A comparative study of ipfs and blockchain integration for scalable data storage," 2023.

[21] G. Perboli, F. Merlo, and C. Vandoni, "Decentralizing the future: Value creation in web 3.0 and the metaverse," *Open Research Europe*, vol. 5, p. 226, 2025.

[22] D. Niham, L. Elle, A. Yuriah, and I. Alifaddin, "Utilization of big data in libraries by using data mining," *International Journal of Cyber and IT Service Management*, vol. 3, no. 2, pp. 79–85, 2023.

[23] P. P. Ray, "Web3: A comprehensive review on background, technologies, applications, zero-trust archi-

tectures, challenges and future directions," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 213–248, 2023.

[24] J. von der Assen, C. Killer, A. De Carli, and B. Stiller, "Performance analysis of decentralized physical infrastructure networks and centralized clouds," in *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2024, pp. 1–6.

[25] Indonesia Investment Authority, "Indonesia digital transformation: A strategic investment," https://www.ina.go.id/ina-in-the-news/indonesia-digital-transformation-a-strategic-investment, 2025, accessed: 2026-01-08.

[26] M. Shen, Z. Tan, D. Niyato, Y. Liu, J. Kang, Z. Xiong, L. Zhu, W. Wang, and X. Shen, "Artificial intelligence for web 3.0: A comprehensive survey," *ACM Computing Surveys*, vol. 56, no. 10, pp. 1–39, 2024.

[27] D. Krause, "Web3 and the decentralized future: Exploring data ownership, privacy, and blockchain infrastructure," *Privacy, and Blockchain Infrastructure (December 19, 2024)*, 2024.

[28] V. Sitharamulu, G. Sucharitha, S. B. Gole, H. R. Battu, O. Osman, and J. Rasheed, "Semantic data sharing and pricing in web 3.0 using blockchain," *Discover Computing*, vol. 28, no. 1, p. 291, 2025.

[29] B. Alotaibi, "Cybersecurity attacks and detection methods in web 3.0 technology: A review," *Sensors*, vol. 25, no. 2, p. 342, 2025.

[30] D. Bucher, J. J. Hunhevicz, B. Byers, M. Honic-Eser, C. De Wolf, and D. Hall, "Decentralized data networks for lifecycle management in the built environment," *Journal of Information Technology in Construction*, vol. 30, pp. 826–851, 2025.

[31] N. Azizah, V. Hartajaya, and S. Riady, "Comparison of replication strategies on distributed database systems," *International Journal of Cyber and IT Service Management*, vol. 2, no. 1, pp. 20–29, 2022.

[32] M. Mazmudar, S. Veitch, and R. A. Mahdavi, "Peer2pir: Private queries for ipfs," in *2025 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2025, pp. 4438–4456.

[33] 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.

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

[35] S. Setiawan, M. Madani, E. A. Natalia, N. Khairunnisa, K. Vaher *et al.*, "Leveraging ipfs for secure, distributed blockchain data infrastructure and enhanced security," *Blockchain Frontier Technology*, vol. 5, no. 1, pp. 90–100, 2025.

[36] V. Netto, T. Cholez, and C.-L. Ignat, "Active sybil attack and efficient defense strategy in ipfs dht," *arXiv preprint arXiv:2505.01139*, 2025.

[37] J. Matter and M. Tran, "Network-level censorship attacks in the interplanetary file system," *arXiv preprint arXiv:2509.06626*, 2025.

[38] J. Liu, Y. Xue, Z. Peng, C. Lin, and X. Huang, "Fairrelay: Fair and cost-efficient peer-to-peer content delivery through payment channel networks," *arXiv preprint arXiv:2405.02973*, 2024.

[39] 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, pp. 125–143, 2024.

[40] N. J. Reddy, K. Vamsi Krishna, J. Abhiram Varma, R. Hurtis, and M. Sheela Devi, "Decentralized file storage system using ipfs and blockchain," in *International Conference on Smart Data Intelligence*. Springer, 2024, pp. 291–304.

[41] 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.

[42] R. Shi, R. Cheng, Y. Fu, B. Han, Y. Cheng, and S. Chen, "Centralization in the decentralized web: Challenges and opportunities in ipfs data management," in *Proceedings of the ACM on Web Conference 2025*, 2025, pp. 4068–4076.

[43] D. Holst, K. Moenck, J. Koch, O. Schmedemann, and T. Schüppstuhl, "Transparent reporting of ai in systematic literature reviews: Development of the prisma-traice checklist," *JMIR AI*, vol. 4, p. e80247, 2025.

[44] J. Zhu, F. Li, and J. Chen, "A survey of blockchain, artificial intelligence, and edge computing for web 3.0," *Computer Science Review*, vol. 54, p. 100667, 2024.

[45] P. Á. Costa, J. Leitão, and Y. Psaras, "Studying the workload of a fully decentralized web3 system: Ipfs,"

in *IFIP International Conference on Distributed Applications and Interoperable Systems*. Springer, 2023, pp. 20–36.

[46] A. Diwate, P. Waghulkar, S. Patle, T. Kadam, M. Tahir, and V. Domde, "Decentralized web hosting platform and framework," *Int. J. Res. Appl. Sci. Eng. Technol*, pp. 2–5, 2023.

[47] M. L. Rethlefsen and M. J. Page, "Prisma 2020 and prisma-s: common questions on tracking records and the flow diagram," *Journal of the Medical Library Association: JMLA*, vol. 110, no. 2, p. 253, 2022.

[48] 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.

[49] M. Hammad, J. Iqbal, C. A. u. Hassan, S. Hussain, S. S. Ullah, M. Uddin, U. A. Malik, M. Abdelhaq, and R. Alsaqour, "Blockchain-based decentralized architecture for software version control," *Applied Sciences*, vol. 13, no. 5, p. 3066, 2023.

[50] S. Millah, A. Waskito, E. A. Natalia, S. H. Lase, and M. Rodriguez, "Decentralized solutions for intellectual property security using the interplanetary file system," *Blockchain Frontier Technology*, vol. 5, no. 1, pp. 49–59, 2025.

[51] M. G. Gowda, N. Raj, P. P, R. Vishrutha, and A. S, "Decentralized file sharing: Leveraging blockchain and ipfs for secure data storage," in *2024 International Conference on Integration of Emerging Technologies for the Digital World (ICIETDW)*, 2024, pp. 1–7.

[52] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain ipfs storage for healthcare data security and privacy," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 152–167, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0743731522000648

[53] M. Mangal and S. Ansari, "Ipfs based decentralised twitter using web 3.0 technologies."

[54] M. B. 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. [Online]. Available: https://www.mdpi.com/1999-5903/16/3/98

[55] Y. Wei, D. Trautwein, Y. Psaras, I. Castro, W. Scott, A. Raman, and G. Tyson, "The eternal tussle: exploring the role of centralization in {IPFS}," in *21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24)*, 2024, pp. 441–454.

[56] M. Cortes-Goicoechea, C. Kiraly, D. Ryajov, J. L. Muñoz-Tapia, and L. Bautista-Gomez, "Scalability limitations of kademlia dhts when enabling data availability sampling in ethereum," in *Proceedings of the 2024 6th Blockchain and Internet of Things Conference*, 2024, pp. 83–91.

[57] J. Xiangjuan, F. Xinwei, Z. Yijie, Y. Heng, C. Xiaofeng, G. Wenfei, L. Weinan, and H. Fanglei, "Integration and innovation of blockchain in web3. 0: current status and standardization prospects," *World Wide Web*, vol. 28, no. 1, p. 7, 2025.

[58] 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.