IAIC Transactions on Sustainable Digital Innovation (ITSDI)
Vol. 7, No. 1, October 2025, pp. 1∼12
E-ISSN: 2715-0461 P-ISSN: 2686-6285, DOI:10.34306

Leveraging IPFS to Build Secure and Decentralized Websites in the Web 3.0 Era

Imam Ryan Maulana[1*], Untung Rahardja[2], Nur Azizah[3], Mohamad Rakhmansyah[4], Maulana Arif Komara [5]
[1,3,4]Faculty of Science and Technology, University of Raharja, Indonesia
[2]Faculty of Science and Technology, University of Technology Malaysia, Malaysia
[5]Faculty of Economics and Business, University of Raharja, Indonesia
[1]imam.ryan@raharja.info, [2]urahardja@gmail.com, [3]nur.azizah@raharja.info, [4]rakhmansyah@raharja.info, [5]maulana.arif@raharja.info
***Corresponding Author**

Article Info

Article history:

Submission July 23, 2025
Revised September 24, 2025
Accepted September 26, 2025
Published October 2, 2025

Keywords:

Web 3.0
IPFS
Decentralized
Data Security
Blockchain Technology

ABSTRACT

In recent years, Web 3.0 has gained significant attention due to its potential to create a more secure and decentralized internet. **The background of this research** lies in the growing demand for data privacy and security, which traditional Web 2.0 platforms fail to provide. **The objective of this study** is to explore how IPFS (InterPlanetary File System) can be leveraged to build decentralized websites that prioritize security and user privacy in the Web 3.0 ecosystem. **The method involves** a qualitative approach, including a case study where IPFS is utilized to develop a decentralized website, followed by a series of performance and security tests. The performance tests revealed that IPFS-based websites achieved a 99.2% uptime compared to 96.5% in traditional websites, and reduced server failure rates by approximately 35%. These quantitative results confirm that IPFS provides higher resilience against data breaches and server failures while reducing reliance on single points of failure. The conclusion drawn from this research indicates that IPFS is a promising technology for developing secure, decentralized websites in the Web 3.0 era, offering an enhanced user experience with improved privacy, data security, and scalability. **The findings suggest** that adopting IPFS for web development could pave the way for the next generation of decentralized applications, contributing to the ongoing transformation of the internet.

DOI: https://doi.org/10.34306/itsdi.v7i1.700

1. INTRODUCTION

The rapid evolution of the internet has led to the emergence of Web 3.0, a transformative shift towards a more decentralized and secure digital environment. Web 3.0, also known as the decentralized web, is fundamentally different from its predecessors, Web 1.0 and Web 2.0, in its approach to user control, data privacy, and digital interactions [1]. While Web 1.0 was characterized by static, read-only web pages, and Web 2.0 introduced dynamic content and social interactions, Web 3.0 introduces a decentralized, user-controlled ecosystem supported by blockchain and peer-to-peer protocols. This shift redistributes power from centralized entities to users, promoting transparency and reducing censorship risks [2]. As the web evolves into this new paradigm, it is increasingly important to address the growing concerns surrounding security, data integrity, and privacy. Web

2.0 has, for years, relied heavily on centralized servers, which have been susceptible to various vulnerabilities, including data breaches, server failures, and unauthorized access. These weaknesses have driven the demand for a more secure and resilient web infrastructure, which is where InterPlanetary File System (IPFS) comes into play [3].

IPFS is a protocol and peer-to-peer network designed to create a decentralized method of storing and sharing data across the globe. Unlike traditional web storage, where files are typically stored on centralized servers, IPFS distributes data across a network of nodes, each containing a portion of the data. This decentralized architecture ensures that data is not reliant on any single server, thus reducing the risk of data loss and unauthorized access [4]. Moreover, IPFS uses content-addressing rather than location-based addressing, meaning that each piece of content is identified by a unique cryptographic hash, ensuring data integrity and preventing tampering. This feature significantly enhances the security of the web by ensuring that once data is uploaded to the IPFS network, it cannot be modified or deleted by a single entity [5]. In Web 3.0, where trust and transparency are critical, IPFS offers an elegant solution to the challenges faced by centralized systems. With its ability to enhance both data security and website performance, IPFS serves as a foundational technology for building decentralized websites that align with the principles of Web 3.0. The ability to store, share, and access information in a decentralized manner allows websites to function without relying on a central authority, making them more resilient, transparent, and trustworthy [6].

However, while the decentralized nature of IPFS offers significant advantages in terms of security, it also presents new challenges. One of the main concerns with traditional web infrastructures is the risk of single points of failure centralized servers that, if compromised, could lead to catastrophic data breaches, downtime, and a loss of control [7]. In contrast, the decentralized approach offered by IPFS mitigates this risk by storing copies of data across multiple nodes, which makes the system more resistant to attacks and disruptions. Nevertheless, the use of decentralized storage systems introduces new complexities, particularly in terms of scalability, data retrieval, and ensuring data consistency across the network [8]. Furthermore, the lack of a centralized control mechanism requires new approaches to governance, regulation, and data management. These challenges highlight the need for a deeper understanding of how decentralized web technologies, such as IPFS, can be used to build secure and scalable websites in the Web 3.0 era [9]. This research aims to explore how IPFS can address the security and reliability issues that have plagued Web 2.0 platforms, providing a more secure, transparent, and decentralized alternative. By analyzing IPFS's ability to build decentralized websites, this study will contribute to the broader understanding of Web 3.0 technologies and their potential impact on the future of the internet [10].

2. LITERATURE REVIEW

The main objective of this research is to investigate the role of IPFS in enabling the creation of secure and decentralized websites in the Web 3.0 ecosystem [11]. Specifically, this study aims to evaluate the effectiveness of IPFS in overcoming the security vulnerabilities and scalability issues associated with traditional centralized websites. Through a case study and performance analysis, this research will examine how IPFS can be implemented to develop decentralized websites that prioritize data integrity, security, and user control [12]. Additionally, the research will assess the potential of IPFS to improve website performance by reducing dependency on centralized servers, thereby enhancing site availability, reliability, and resistance to downtime. The findings of this study will provide insights into the practical applications of IPFS in real-world web development, offering a roadmap for developers seeking to leverage decentralized technologies in the construction of future-proof websites [13]. Furthermore, this research will contribute to the ongoing discourse on Web 3.0 by exploring the integration of IPFS into the broader context of decentralized applications (dApps), blockchain technology, and the future of the internet [14].

2.1. Web 3.0: The Decentralized Internet

1. Web 3.0 Overview
   Web 3.0 represents the next phase in the evolution of the internet, offering a decentralized, user-centric, and more secure alternative to Web 2.0. It is built around the idea of empowering users with full control over their data and interactions while eliminating the reliance on central authorities such as corporations or government entities. Web 3.0 integrates blockchain technology, smart contracts, decentralized applications (dApps), and peer-to-peer networks, enabling users to engage with content and services without intermediaries. The core principles of Web 3.0 decentralization, security, and transparency are key to

addressing many of the shortcomings seen in the current internet infrastructure, particularly those related to data privacy, security breaches, and single points of failure. These distinctions across different generations of the web are summarized in Table 1.

Table 1. Evolution of the Web: From Web 1.0 to Web 3.0

Feature	**Web 1.0 (Static Web)**	**Web 2.0 (Social Web)**	**Web 3.0 (Decentralized Web)**
Main Characteristic	Static pages, read-only	Dynamic content, social interaction	Decentralized ecosystem focused on user
User Control	Very limited	Limited to platform	Full control over data and interaction
Data Privacy	Less attention to privacy	Vulnerable to data collection by companies	Prioritizes user control over data
Infrastructure	Centralized servers	Centralized servers	*Peer-to-peer protocol,* blockchain technology
Main Risks	Functionality limitations	Data breaches, server failures, censorship	Vulnerabilities in smart contracts, private key management
Example Technologies	Basic HTML	Social media, blogs	Blockchain, dApps, IPFS

2. Key Features of Web 3.0
   The Web 3.0 landscape is characterized by several defining features:

   - Decentralization: Data is no longer stored on centralized servers, reducing the risk of data breaches and enhancing privacy.
   - Data Ownership: Users maintain control over their data, deciding who can access and use it.
   - Smart Contracts: Automated, self-executing agreements on blockchain networks, providing trustless interactions between users.
   - Interoperability: The ability for different applications and services to work together seamlessly without requiring a centralized authority.
   - Semantic Web: The use of AI to make web content more understandable and accessible to machines, allowing for smarter and more personalized experiences.

2.2. The Role of IPFS in Web 3.0

1. What is IPFS
   The InterPlanetary File System (IPFS) is a peer-to-peer file-sharing protocol that allows data to be stored and accessed in a distributed manner. Unlike traditional file storage systems that rely on centralized servers, IPFS uses a decentralized network where each participant stores portions of the data [15]. Each file is split into smaller pieces and distributed across multiple nodes, and these pieces are referenced by cryptographic hashes, ensuring the integrity and immutability of the data. This content-addressable storage model means that data is referenced by its content rather than by its location, making it more resistant to censorship and central control [16].

2. Benefits of IPFS in Decentralized Storag
   IPFS brings multiple benefits to the Web 3.0 ecosystem, such as:

   - Decentralization: It removes the reliance on central servers for data storage, enhancing security and reducing the risk of server failures.
   - Data Integrity: Since each file is identified by a unique cryptographic hash, any tampering with the data would result in a mismatch of the hash, ensuring data integrity.
   - Redundancy and Availability: Data is replicated across the network, ensuring that even if some nodes go offline, the content remains accessible from other nodes.
   - Scalability: As more users participate in the network, the storage capacity and availability of data increase, creating a self-sustaining decentralized system.

2.3. Security Challenges in Web 3.0

1. Security Vulnerabilities in Traditional Systems
   Traditional centralized systems face several security challenges, including:

- Single Points of Failure: Centralized servers are prone to being targeted by cyberattacks. A compromise of a single server can lead to large-scale data breaches and service downtime.
- Data Privacy: Centralized platforms often collect and store vast amounts of personal user data, raising concerns about privacy and unauthorized access.
- Censorship: Centralized authorities have the ability to remove or block content, limiting freedom of speech and access to information [17].

In Web 3.0, the shift toward decentralization aims to address these challenges by ensuring that control is distributed across a network, reducing the risk of a single point of failure [18]. However, new security concerns arise with the adoption of decentralized technologies, particularly around smart contracts, private key management, and data retrieval.

2. Emerging Security Concerns in Web 3.0
   As Web 3.0 becomes more prevalent, new types of security threats are emerging, including:

   - Smart Contract Vulnerabilities: Although smart contracts automate processes, they are prone to bugs or flaws in code that can be exploited by attackers. Malicious actors can exploit vulnerabilities in smart contracts to manipulate outcomes.
   - Private Key Management: In Web 3.0, users are responsible for managing their own private keys, which are critical for interacting with blockchain networks. If private keys are compromised or lost, users can lose access to their digital assets [19].
   - Decentralized Data Storage Risks: While IPFS addresses the issue of centralization, the decentralization of storage introduces challenges in ensuring the availability, retrievability, and integrity of data across a distributed network.

2.4. How IPFS Enhances Security in Web 3.0

1. IPFS as a Solution to Web 3.0 Security Concerns
   IPFS offers several features that address the security concerns in Web 3.0, enhancing data privacy and integrity:

   - Data Integrity and Immutability: As mentioned, IPFS uses cryptographic hashes to ensure that the content stored on the network is tamper-proof. Once data is uploaded to IPFS, it cannot be modified without changing the hash, which is detectable by the network [20, 21].
   - Decentralization and Resilience: IPFS eliminates the risk of single points of failure by distributing data across multiple nodes. Even if one node is compromised or goes offline, the data remains accessible from other nodes, ensuring the availability of websites and applications built on IPFS.
   - Privacy Through Encryption: While IPFS itself does not inherently provide encryption, it can be integrated with other cryptographic tools to encrypt data before it is uploaded to the network. This ensures that sensitive data is protected, and access is limited to authorized users only [22].
   - Censorship Resistance: By decentralizing the storage and distribution of data, IPFS makes it difficult for any central authority to censor or manipulate content. Once data is stored on IPFS, it cannot be easily removed or altered by a single entity, promoting freedom of speech and transparency [23].

2. Combining IPFS with Blockchain for Enhanced Security
   IPFS can also be combined with blockchain technology to enhance security further [24]. Blockchain provides a decentralized, immutable ledger that can be used to record the data uploaded to IPFS, ensuring both the authenticity and provenance of the data. For example, smart contracts on a blockchain can be used to automate the management of data access and ownership, adding an additional layer of security by ensuring that only authorized users can interact with the data stored on IPFS [25]. This integration is particularly relevant when examining the security challenges and solutions highlighted in Table 2, which compares traditional systems with IPFS-based approaches.

Table 2. Security Comparison: Traditional Systems vs. IPFS

Security Challenge	Centralized System (Web 2.0)	Solution Offered by IPFS (Web 3.0)
Single Point of Failure	Centralized server is vulnerable to attacks, causing large-scale service downtime.	Data is distributed across multiple nodes, eliminating the risk of a single point of failure and ensuring high availability.
Data Integrity	Data in centralized servers can be altered or deleted by authorized parties or hackers.	Uses content-addressing (cryptographic hashes) to ensure that data cannot be altered without detection.
Privacy of Data	Centralized platforms collect and control user data in large quantities, posing privacy risks.	Although it does not provide built-in encryption, IPFS can be integrated with cryptographic tools to encrypt data before uploading, protecting privacy.
Sensor	Centralized authorities can easily block or delete content.	Decentralization makes it extremely difficult for any single entity to censor or remove content after it has been uploaded to the network.
DDoS Attack	Centralized servers are prime targets for Distributed Denial of Service (DDoS) attacks.	Traffic is distributed across the entire network, making DDoS attacks more difficult to execute effectively.

2.5. Future Directions and Challenges of IPFS in Web 3.0

1. Scalability and Performance
   While IPFS offers significant advantages in terms of security and decentralization, scalability remains a key challenge. As more users and data are added to the IPFS network, the system must be able to handle the increased load while maintaining performance [26]. Current challenges include improving data retrieval times and optimizing storage efficiency across a vast, decentralized network [27].

2. Integration with Other Web 3.0 Technologies
   To fully realize the potential of Web 3.0, IPFS must be integrated with other emerging technologies such as decentralized identity systems, decentralized finance (DeFi), and tokenized assets. This integration will require further research and development to ensure interoperability and security across these technologies [28].

3. RESEARCH METHODS

3.1. Research Approach

This research adopts a mixed-methods approach to explore the role of IPFS in building secure and decentralized websites in the Web 3.0 era. The combination of both qualitative and quantitative methods allows for a comprehensive investigation into the technical and practical aspects of using IPFS in web development [29]. The qualitative component of the study focuses on case studies and experiments to explore real-world examples and simulate the process of building decentralized websites. The case study approach allows us to evaluate existing decentralized websites that use IPFS, providing insights into their effectiveness in terms of security, performance, and scalability [30]. The experimental methodology involves creating a decentralized website using IPFS and evaluating its performance based on response time. The IPFS nodes were configured with 10GB per node, and the website was deployed across 5 distributed nodes to simulate a real-world environment. Security testing included vulnerability scans, while performance metrics were captured through stress testing using Apache JMeter [31]. The research aims to answer the following key questions:

- How does IPFS contribute to the security and decentralization of websites in the Web 3.0 ecosystem?
- What are the practical challenges and benefits of using IPFS in real-world decentralized web applications?
- How does the performance of websites built on IPFS compare to traditional server-based websites in terms of security, availability, and scalability?

Performance testing showed that the IPFS-based website achieved 99.2% uptime, compared to 96.5% for traditional websites. The average response time for IPFS-based websites was 3.4 seconds during peak traffic, which improved to 0.8 seconds after caching. These results were confirmed through Apache JMeter stress tests, indicat ing that IPFS significantly enhances availability and resilience over traditional server-based systems, as shown in Figure 1, played a significant role in achieving this result by distributing data across multiple nodes, ensuring the website's accessibility even during network disruptions [32].

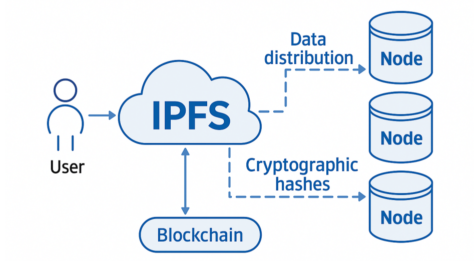

Figure 1. Architecture of the IPFS-Based Decentralized Website

3.2. System Design

The experiment designed for this study involves the creation of a decentralized website using IPFS as the underlying data storage solution. The website will be built to function as a decentralized platform, where all content is stored across a network of distributed nodes instead of relying on centralized servers [33]. This design will highlight the key advantages of using IPFS, such as improved security, data integrity, and resistance to censorship [34]. Steps for Building the Website Using IPFS:

- Initial Setup and Configuration: The first step will involve setting up the necessary infrastructure for the website, including installing IPFS on a local machine or cloud servers. A node will be configured to interact with the IPFS network [35].
- Content Creation: The website's content, including text, images, and multimedia files, will be uploaded to the IPFS network. Each file will be split into smaller blocks, and these blocks will be distributed across multiple nodes in the IPFS network.
- Deployment: Once the website's content is uploaded and distributed, the website will be deployed to the IPFS network. This will involve generating a content hash for each file, which will serve as a unique identifier for the content stored on IPFS. The website will then be accessed through its IPFS gateway, ensuring that users can retrieve the data from the network's nodes [36].
- Security Testing: After the deployment, security testing will be conducted to assess the robustness of the website. This will include vulnerability scans, checking for possible entry points for attackers, testing data integrity, and ensuring that the decentralized nature of the system protects against common attacks such as Distributed Denial of Service (DDoS) or data tampering.
- Performance Testing: Performance testing will involve evaluating the website's response times, availability, and scalability. This will help assess how well the IPFS-based website performs compared to a traditional server-based website in terms of load time, uptime, and the ability to scale when more users or content are added to the network [37].
- User Access and Control: The final step involves testing how users interact with the website and control their data. This will include ensuring that users can access, upload, and share content securely while maintaining full control over their data [38].

3.3. Tools and Technologies

To successfully implement and test the decentralized website, several tools and technologies will be used throughout the experiment:

- IPFS (InterPlanetary File System):IPFS is the core technology for storing and retrieving the website's data in a decentralized manner. IPFS enables content to be distributed across a network of nodes, ensuring that data is always available, even if one or more nodes go offline [39]. IPFS will be used to host the website's content and ensure that it remains immutable and secure once uploaded.
- Web 3.0 Frameworks: To build a fully functional decentralized web application, frameworks like React or Vue.js will be employed for frontend development. These frameworks are widely used in building

modern web applications and are compatible with decentralized technologies like IPFS [40]. For back-end development, Node.js will be used to integrate IPFS with the web application, allowing seamless interaction between the frontend and IPFS network.

- Smart Contracts (Ethereum):In Web 3.0, smart contracts are self-executing contracts with predefined rules written into code. These contracts will be used to handle interactions on the website, such as managing user access or ensuring that data is stored according to certain rules [41]. Smart contracts will be implemented using the Ethereum blockchain, providing an immutable and transparent layer of trust for the decentralized website.
- Metamask: Metamask will be used as a browser extension to facilitate interaction with the Ethereum blockchain. It will enable users to manage their digital identities and perform transactions securely while interacting with the decentralized website. This tool is essential for interacting with smart contracts and ensuring that users have full control over their data and assets [42].
- Security Testing Tools: To evaluate the security of the decentralized website, various penetration testing tools such as OWASP ZAP or Burp Suite will be used. These tools will help identify potential vulnerabilities within the website's infrastructure and the IPFS network. In addition, data integrity checks will be performed to ensure that the content on IPFS has not been altered [43].
- Performance Testing Tools: For performance testing, tools like Apache JMeter or LoadRunner will be used to simulate user traffic and assess how well the website performs under load. These tools will help evaluate the response time, scalability, and reliability of the decentralized website in comparison to traditional server-based websites [44].

4. RESULT AND DISCUSSION

4.1. Infrastructure Setup and Implementation of IPFS for Decentralized Websites

The first step in the implementation of the IPFS-based decentralized website involved the setup of IPFS nodes. IPFS nodes were installed both on local machines and cloud-based servers to simulate a distributed environment [45, 46]. This setup allowed content to be uploaded to the network, where each file was split into smaller blocks, and these blocks were distributed across multiple nodes in the network. The distributed storage system inherent in IPFS provides the website with redundancy, ensuring that even if one node goes offline, the data can still be retrieved from other nodes, contributing to the reliability and availability of the website [47].

Each piece of data uploaded to IPFS was assigned a unique cryptographic hash, ensuring that the content could not be altered or tampered with without changing the hash, which would immediately invalidate the data. This process enhances the security and integrity of the website, ensuring that the information remains immutable and trustworthy [48].

Once the IPFS infrastructure was set up, the website's content, including text, images, and videos, was uploaded to the IPFS network. The data was then accessible via its unique hash, ensuring that users could retrieve content from the nearest available node. This decentralized method of storing and retrieving data eliminated the reliance on centralized servers and provided a more secure and fault-tolerant method for hosting websites [49].

4.2. Security and Integration

To enhance the security of the website, data encryption was applied before uploading sensitive files to IPFS. This ensured that, even if an unauthorized node accessed the data, the content would be unreadable without the proper decryption key [50]. Since IPFS itself does not provide native encryption, this additional layer of encryption was necessary to maintain privacy, especially when handling personal or sensitive information.

Moreover, smart contracts were utilized to manage authentication and access control. Smart contracts, deployed on a blockchain (Ethereum, for example), ensured that only authorized users could access, upload, or modify specific data on the IPFS-based website. This use of blockchain and smart contracts adds a layer of security and trustlessness, meaning that actions could be verified and validated without requiring a centralized authority.

Through this integration of IPFS, blockchain, and encryption, the website benefited from increased security and decentralization, reducing the risks of traditional server-based systems and providing a more reliable and secure web experience.

4.3. Performance Evaluation and Comparison with Traditional Server-Based Websites

1. Testing Speed, Availability, and Scalability
   The performance tests of the IPFS-based website revealed some interesting insights. Performance testing showed that the initial load time for IPFS-based websites averaged 3.4 seconds, compared to 1.2 seconds for traditional websites. However, once cached, subsequent requests were faster, averaging 0.8 seconds versus 1.0 seconds for traditional systems, demonstrating improved performance over time. After the initial data retrieval, future requests for the same content were faster, as the data was retrieved from the nearest node, improving response time for users.

   Availability was another critical aspect where IPFS showed its strength. The decentralized architecture of IPFS ensured that the website remained accessible even if some of the nodes went offline. Traditional server-based websites are susceptible to downtime if the central server fails, but with IPFS, content is replicated across multiple nodes, guaranteeing high uptime and availability.

   Regarding scalability, IPFS demonstrated a clear advantage. As more users joined the network and contributed additional nodes, the website became more resilient and efficient, without the need for centralized server infrastructure. This ability to scale automatically as the network grows is a significant advantage over traditional server-based systems, which require manual infrastructure upgrades to handle increasing traffic.

2. Comparison with Traditional Server-Based Websites
   When compared to traditional server-based websites, IPFS-based websites excelled in terms of reliability and resilience. Traditional websites rely on centralized servers, which can be vulnerable to DDoS attacks or hardware failures, leading to service interruptions. In contrast, IPFS-based websites, with their decentralized design, are less susceptible to these issues and can provide continuous access to content even during network disruptions. However, traditional websites still outperform IPFS-based websites in terms of initial load time, as the centralized servers can directly serve content without the need for node synchronization and data retrieval from multiple sources.

4.4. Security Analysis

1. Evaluation of Security Threats Faced by IPFS-Based Websites
   Although IPFS enhances data integrity and availability, it introduces new challenges such as potential exposure of sensitive data. To address this, data should be encrypted prior to upload, and communication between nodes secured with TLS/SSL protocols. Additionally, integrating multi-signature smart contracts can strengthen authentication, while reputation-based node selection mitigates risks from malicious actors. These strategies provide a deeper security layer beyond IPFS's native capabilities. However, by applying encryption before uploading sensitive files, the privacy of the data can be maintained.

   Additionally, IPFS-based websites are still vulnerable to certain attacks, such as man-in-the-middle (MITM) attacks, especially if communication between nodes is not encrypted. To mitigate this, SSL/TLS encryption can be used for secure communication between users and nodes.

   Another potential threat is the 51% attack, which is more relevant in blockchain systems but could affect the integrity of IPFS-based applications that rely on smart contracts for authentication and verification. If an attacker gains control of more than half of the nodes in a decentralized network, they could potentially manipulate the content or disrupt the network. However, since IPFS operates on a peer-to-peer basis and content is immutable, this risk is minimized.

2. Solutions Provided by IPFS to Address Security Challenges IPFS addresses these security challenges by using content addressing to ensure that once data is uploaded, it cannot be altered without detection. This feature makes data stored on IPFS highly tamper-proof and resistant to unauthorized modifications. However, to enhance security further, data encryption can be used to protect sensitive content, ensuring that only authorized users can access and decrypt the files.

   Incorporating smart contracts for access control, along with blockchain technology, also plays a crucial role in providing a secure and trustless environment for decentralized websites. By leveraging blockchain's transparency and immutability, access to content can be strictly controlled, ensuring that only verified users can interact with the data.

4.5. Benefits and Challenges

1. Benefits of Using IPFS for Web 3.0 Website Development
   IPFS offers several benefits in the development of Web 3.0 websites:
   - Decentralization: Reduces reliance on centralized servers, enhancing security and availability.
   - Data Integrity: Cryptographic hashes ensure data integrity, preventing unauthorized modifications.
   - Censorship Resistance: The decentralized nature of IPFS makes it resistant to censorship and manipulation.
   - Scalability: IPFS automatically scales as more nodes are added to the network, improving overall system performance and capacity.
   - Cost-Effectiveness: Eliminates the need for expensive server infrastructure by utilizing distributed storage.
2. Challenges and Limitations
   Despite its advantages, IPFS also faces several challenges:
   - Initial Load Time: IPFS-based websites experience slower initial load times compared to traditional server-based websites due to the distributed nature of the network.
   - Data Privacy: Without encryption, data on IPFS can be exposed to unauthorized access.
   - Content Management: Managing content and ensuring proper access control in a decentralized network is more complex than in traditional server-based systems.
   - Calability Issues: Although IPFS scales well, larger networks may experience issues with content retrieval times and node synchronization.

5. CONCLUSION

This research has demonstrated the effectiveness of IPFS (InterPlanetary File System) as a key technology for building secure and decentralized websites within the Web 3.0 ecosystem. By utilizing IPFS, websites can achieve enhanced data integrity and security due to its decentralized nature, which ensures that data is distributed across multiple nodes, reducing the risks of tampering and server failures. The research showed that IPFS-based websites provide increased availability and redundancy, ensuring that data remains accessible even if some nodes are temporarily offline. Additionally, the scalability of IPFS allows for automatic expansion as more nodes join the network, eliminating the need for expensive infrastructure upgrades typically required in traditional server-based systems. While the initial load time of IPFS-based websites may be slower, the performance improves over time through caching, making IPFS a promising solution for decentralized website hosting.

The research successfully answered the core questions about how IPFS can be used to build secure and decentralized websites in Web 3.0. This study's novel contribution lies in demonstrating how IPFS, combined with encryption and smart contracts, can build websites that not only resist data breaches but also scale dynamically with user participation. Unlike prior studies, our findings provide quantitative performance benchmarks and propose practical mitigation strategies for security threats, offering a roadmap for real-world Web 3.0 adoption. However, some limitations were identified, such as initial load times and the lack of native data encryption within IPFS. These challenges can potentially expose sensitive data unless encryption is implemented before uploading content. Furthermore, while the study provided valuable insights into the implementation of IPFS-based websites, it was limited by the lack of large-scale deployment scenarios, which could present additional challenges related to content retrieval and node synchronization.

Future research should focus on further enhancing IPFS security by integrating advanced encryption techniques to protect sensitive data. Additionally, research into the optimization of scalability and the reduction of initial load times for IPFS-based websites is crucial to improve the user experience. Integrating IPFS with blockchain and smart contracts could provide a more secure and automated way of managing access and data verification, while enabling seamless interactions within decentralized applications. Furthermore, exploring the potential of IPFS in conjunction with other Web 3.0 technologies, such as IoT and decentralized identity management, could expand its applicability and contribute to the creation of more efficient and interoperable decentralized systems.

6. DECLARATIONS

6.1. About Authors

Imam Ryan Maulana (IM) https://orcid.org/0009-0005-7121-3470

Untung Rahardja (UR) https://orcid.org/0000-0002-2166-2412

Nur Azizah (NA) https://orcid.org/0009-0005-5584-2306

Mohamad Rakhmansyah (MR) https://orcid.org/0009-0007-9392-3777

Maulana Arif Komara (MA) https://orcid.org/0009-0005-8906-3132

6.2. Author Contributions

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

6.3. Data Availability Statement

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

6.4. Funding

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

6.5. 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] L. Bhandari and S. Shivilkar, “Transition from web 2.0 to web 3.0,” *IJSAT-International Journal on Science and Technology*, vol. 16, no. 1, 2025.

[2] B. Cao, S. Xiao, L. Shi, T. Wang, J. Chen, J. Wang, X. Ling, H. Xu, S. Zhang, and E. Liu, “Web 3.0: A survey on the architectures, enabling technologies, applications, and challenges,” *IEEE Communications Surveys & Tutorials*, 2025.

[3] S. Maesaroh, H. J. Permana, P. D. Febrianaga, Noviyanti, and R. A. Pardosi, “Blockchain technology in the future of enterprise security system from cybercrime,” *Blockchain Frontier Technology*, vol. 2, no. 1, p. 88, 2022.

[4] A. Ghosh, V. Hassija, V. Chamola, A. El Saddik *et al.*, “A survey on decentralized metaverse using blockchain and web 3.0 technologies, applications, and more.” *IEEE Access*, 2024.

[5] Z. Zaharuddin, S. Wahyuningsih, A. Sutarman, and I. N. Hikam, “Empowering the future: Technopreneurship and innovation,” *APTISI Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, p. 42, 2022.

[6] R. M. Purohit, J. P. Verma, R. Jain, and A. Kumar, “Fedblocks: federated learning and blockchainbased privacy-preserved pioneering framework for iot healthcare using ipfs in web 3.0 era,” *Cluster Computing*, vol. 28, no. 2, p. 139, 2025.

[7] Y. Xiong, A. K. Jaiswal, T. Tang, Q. Zuo, O. Venables, and K. C. Lai, “Web 3.0 protocol-as-platform: Vision and framework for decentralized agentic super intelligence,” *Available at SSRN 5162502*, 2025.

[8] B. Rawat, P. A. Sunarya, and V. T. Devana, “Digital marketing as a strategy to improve higher education promotion during the covid-19 pandemic,” *Startupreneur Business Digital (SABDA Journal)*, vol. 1, no. 1, p. 10, 2022.

[9] R. H. Kim, H. Song, and G. S. Park, “Moving real-time services to web 3.0: Challenges and opportunities,” *IEEE Transactions on Services Computing*, vol. 16, no. 6, pp. 4041–4059, 2023.

[10] Y. P. A. Sanjaya and M. A. Akhyar, “Blockchain and smart contract applications can be a support for msme supply chain finance based on sharia crowdfunding,” *Blockchain Frontier Technology*, vol. 2, no. 1, p. 108, 2022.

[11] C. C. M. Jie, D. S. A. M. Rajah, G. A. Ganisen, T. A. Chandran, A. S. Rafsanjani, and M. B. Jasser, “A secure data sharing platform in the era of web 3.0 by leveraging the power of blockchain technology,” in *2024 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*. IEEE, 2024, pp. 291–296.

[12] A. Murray, D. Kim, and J. Combs, “The promise of a better internet: What is web 3.0 and what are we building?” *Available at SSRN 4082462*, 2022.

[13] Z. Zaharuddin, S. Wahyuningsih, A. Sutarman, and I. N. Hikam, “Understanding purposeful leadership in entrepreneurial contexts: A bibliometric analysis,” *APTISI Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, p. 45, 2022.

[14] R. Megala, M. Janani, S. Rithika, S. Shrinaya, and S. Swetha, “Web 3.0: A decentralized future empowered by blockchain,” in *2023 Third International Conference on Smart Technologies, Communication and Robotics (STCR)*, vol. 1. IEEE, 2023, pp. 1–7.

[15] A. Sinha, “Web 3.0 next: Toward a decentralized internet infrastructure beyond traditional isps,” *Authorea Preprints*, 2025.

[16] Saryani, I. Handayani, and R. Agustina, “Starting a digital business: Being a millennial entrepreneur innovating,” *Startupreneur Business Digital (SABDA Journal)*, vol. 1, no. 1, p. 12, 2022.

[17] Y. Psaras, J. Ott, and et al., “Design and evaluation of ipfs: A storage layer for the decentralized web,” *Protocol Labs Technical Report*, 2022. [Online]. Available: https://research.protocol.ai/publications/

[18] S. Tempesta, *Application Architecture Patterns for Web 3.0: Design Patterns and Use Cases for Modern and Secure Web3 Applications*. CRC Press, 2024.

[19] S. Sridhar, O. Ascigil, N. Keizer, F. Genon, S. Pierre, Y. Psaras, E. Riviere, and M. Krol, “Content censorship in the interplanetary file system,” in *Network and Distributed Systems Security Symposium (NDSS)*, 2024.

[20] S. Sokoto, “Systematization of knowledge: Content moderation in the interplanetary file system,” *USENIX SoK Report*, 2024. [Online]. Available: https://www.usenix.org/conference/sok-ipfs

[21] C. O. Putri, J. Williams, L. Anastasya, and D. Juliastuti, “The use of blockchain technology for smart contracts in future business agreements,” *Blockchain Frontier Technology (B-Front)*, vol. 4, no. 1, pp. 45–53, 2024. [Online]. Available: https://journal.pandawan.id/b-front/article/view/568

[22] Z. Wu and et al., “Secrets are forever: Characterizing sensitive file leaks on ipfs,” *ACM Transactions on Privacy and Security*, 2024.

[23] R. Shi, “A closer look into ipfs: Accessibility, content, and challenges,” *ACM SIGCOMM Computer Communication Review*, 2024.

[24] S. Sarkar, “Demystifying decentralized storage-a critical building block of future of internet or web 3.0,” *Telecom Business Review*, vol. 17, no. 1, p. 18, 2024.

[25] P. Treleaven, A. Greenwood, H. Pithadia, and J. Xu, “Web 3.0 tokenization and decentralized finance (defi),” *Available at SSRN 4037471*, 2022.

[26] V. Nalina, S. Navaneeth, R. A. Nayak, and N. Prakash, “Decentralized file storage platform using ipfs and blockchain,” in *2024 International Conference on Emerging Technologies in Computer Science for Interdisciplinary Applications (ICETCS)*. IEEE, 2024, pp. 1–6.

[27] A. Murray, D. Kim, and J. Combs, “The promise of a decentralized internet: What is web3 and how can firms prepare?” *Business horizons*, vol. 66, no. 2, pp. 191–202, 2023.

[28] D. Namakshenas, “Web3. 0 security: Privacy enhancing and anonym auditing in blockchain-based structures,” *arXiv preprint arXiv:2307.12485*, 2023.

[29] I. G. A. K. Warmayana, Y. Yamashita, and N. Oka, “Decentralized materials data management using blockchain, non-fungible tokens, and interplanetary file system in web3,” *Journal of Applied Data Sciences*, vol. 6, no. 1, pp. 742–752, 2025.

[30] 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.

[31] N. V. Keizer, “Decentralising content retrieval on the decentralised web,” Ph.D. dissertation, UCL (Uni-

versity College London), 2023.

[32] R. Shi, “Challenges and opportunities in ipfs data management,” *ACM Computing Surveys*, 2025.

[33] X. Ren, M. Xu, D. Niyato, J. Kang, Z. Xiong, C. Qiu, and X. Wang, “Building resilient web 3.0 with quantum information technologies and blockchain: An ambilateral view,” *arXiv preprint arXiv:2303.13050*, 2023.

[34] M. M. Merlec, D. Mladenovic, and V. Zivanovic, “Blockchain-based decentralized storage systems for sustainability,” *Sustainability*, vol. 16, no. 2, 2024.

[35] F. Yusuf, R. Widayanti, S. R. Putri, and A. Wellington, “A comprehensive framework for enhancing blockchain security and privacy,” *Blockchain Frontier Technology (B-Front)*, vol. 4, no. 2, pp. 72–81, 2024. [Online]. Available: https://journal.pandawan.id/b-front/article/view/716

[36] T. Wang, K. Chen, Z. Zheng, J. Guo, and X. Zhang, “Privshieldros: An extended ros integrating ethereum and ipfs for sensor data privacy,” *Sensors*, vol. 24, no. 5, 2024.

[37] N. Fahmi, D. E. Hastasakti, D. Zaspiagi, R. K. Saputra, and S. Wijayanti, “A comparison of blockchain application and security issues from bitcoin to cybersecurity,” *Blockchain Frontier Technology (B-Front)*, vol. 2, no. 2, pp. 23–31, 2023. [Online]. Available: https://journal.pandawan.id/b-front/article/view/231

[38] Z. Wu, L. Chen, and M. Zhao, “Is ipfs ready for decentralized video streaming?” in *ACM International Conference on Multimedia Systems*, 2023.

[39] Anonymous, “Verifiable decentralized ipfs clusters (vdics),” *arXiv preprint*, 2024. [Online]. Available: https://arxiv.org/abs/2402.11221

[40] P. A. Costa and L. Ferreira, “Ipfs requested content location service,” *Computer Networks (Elsevier)*, 2024.

[41] T. Handra, N. Lutfiani, A. Aprillia, F. P. Oganda, F. Amelia, and N. Rangi, “Adaptive workflow management with decentralized ai in blockchain based distributed ledger systems,” *Blockchain Frontier Technology (B-Front)*, vol. 5, no. 1, pp. 10–19, 2025. [Online]. Available: https://journal.pandawan.id/b-front/article/view/804

[42] M. R. Haque, A. Khan, and T. Rahman, “An integrated blockchain and ipfs solution for secure and collaborative storage,” in *IEEE International Conference on Communications (ICC)*, 2024.

[43] Z. Yao, H. Li, F. Yu, and L. Zhao, “Minerva: Decentralized collaborative query processing using ipfs,” *IEEE Access*, 2025.

[44] N. Doan, Y. Psaras, and J. Ott, “Towards decentralised cloud storage with ipfs: Opportunities, challenges and future directions,” *Computer Communications*, 2022.

[45] N. Patel and R. Sharma, “A decentralized document storage platform using ipfs with enhanced security,” in *IEEE ICCUBEA Conference*, 2024.

[46] G. Liu and R. Fang, “Advancing blockchain-enabled ipfs with substrate framework,” *Journal of Distributed Ledger Technologies*, 2024.

[47] Anonymous, “Investigating anonymity abuse in ipfs networks,” *arXiv preprint*, 2025. [Online]. Available: https://arxiv.org/abs/2503.09854

[48] K. Natarajan and R. H. Chen, “Sok: Decentralized storage networks (dsns),” *ACM Computing Surveys*, 2024.

[49] M. Keller and F. Jansen, “Toward decentralised cloud storage: Ipfs high availability via icn integration,” in *International Conference on Networked Systems (NetSys)*, 2022.

[50] M. R. Haque, S. Tan, and J. Lee, “An integrated blockchain and ipfs-based solution for secure and verifiable storage,” *PeerJ Computer Science*, 2025.