APTISI Transactions on Management (ATM)
Vol. 10, No. 2, May 2026, pp. 177∼190
E-ISSN: 2622-6804 | P-ISSN: 2622-6812, DOI: 10.33050

Using IPFS for Automatic Digital Intellectual Property Registration in Web3 Platforms

Yusuf Tojiri[1*], Maulana Arif Komara[2], Alfri Adiwijaya[3], Nasrul Hidayat[4], Cristiano Gatot Wagner[5], Marviola Hardini[6]
[1]Faculty of Management, STIE Yasa Anggana Garut, Indonesia
[2,3,4,6]Faculty of Economics and Business, Universitas Raharja, Indonesia
[5]Department of Education, Ilearning Incorporation, Colombia
[1]yusuftojiri@stieyasaanggana.ac.id, [2]maulana.arif@raharja.info, [3]alfri.adiwijaya@raharja.info, [4]nasrul.hidayat@raharja.info,
[5]cwagner_gatot@ilearning.co, [6]marviola@raharja.info
***Corresponding Author**

Article Info

Article history:

Submission February 02, 2026
Revised February 22, 2026
Accepted March 30, 2026
Published May 15, 2026

Keywords:

IPFS
Decentralized Storage
Digital Intellectual Property
Web3
Digital Certificate

ABSTRACT

This study proposes an IPFS-based system for automatic digital intellectual property registration within Web3 platform environments. The rapid development of digital technology has encouraged the transformation of Intellectual Property Rights (IPR) protection from manual systems to more secure and efficient digital mechanisms. However, current IPR registration processes remain centralized, slow, and vulnerable to data tampering. Based on this issue, **this study aims** to design and test an automatic IPR registration system using the InterPlanetary File System (IPFS) as a decentralized storage solution. **This research employs** a software engineering method with a prototyping approach that includes the design of a user interface, integration of the IPFS API, implementation of an automatic hash-generation system, metadata storage in a database, and issuance of digital certificates. **Testing results show** that the system can automatically register digital works, generate unique and consistent file hashes, upload files to IPFS with an average upload time of less than two seconds, and provide global accessibility through a distributed network. In addition, the system is capable of validating the authenticity of a work by matching the hash and metadata listed in the digital certificate. **Based on these findings**, it can be concluded that the use of IPFS in digital IPR registration systems is effective in enhancing security, efficiency, and transparency, although further development is required in relation to integration with national legal frameworks and formal legal recognition.

Corresponding Author:

DOI: https://doi.org/10.33050/atm.v10i2.2616

1. INTRODUCTION

In the emerging Web3 ecosystem, decentralized storage technologies such as IPFS are increasingly explored for digital intellectual property documentation. The rapid advancement of digital technology has transformed how intellectual works are created, distributed, and consumed, leading to new challenges in ensuring ownership protection [1]. In the era of Web3, where decentralization, transparency, and user control

are central principles, conventional Intellectual Property Rights (IPR) systems remain largely centralized, often characterized by complex administrative procedures, high costs, and slow processing times [2, 3]. As a result, creative industry actors including software developers, writers, musicians, and digital artists face increasing risks such as forgery, plagiarism, unauthorized distribution, and data loss, which complicate the protection and enforcement of their rights in digital environments [4].

To address these challenges, the InterPlanetary File System (IPFS), a peer-to-peer distributed storage system, offers a promising alternative for developing secure and decentralized IPR registration mechanisms [5]. IPFS utilizes a content-addressable architecture in which each file is assigned a unique cryptographic hash, enabling immutable, tamper-resistant, and globally accessible data storage [6]. This study aims to design and evaluate an IPFS-based system for automatic IPR registration, where digital files are securely stored, metadata is systematically recorded, and unique hashes are generated as verifiable proof of ownership. The system further incorporates timestamping and audit trail mechanisms to ensure transparency and traceability of creation and registration events, thereby enhancing trust in the verification process [7, 8].

This research is motivated by the limited availability of practical implementations of IPFS-based IPR systems, particularly in developing countries such as Indonesia, where intellectual property registration is still dominated by centralized administrative institutions [9]. Existing studies predominantly focus on blockchain-based solutions, which, although strong in immutability and transparency, often emphasize transaction recording rather than efficient file storage and face challenges related to scalability, latency, and operational costs [10, 11]. In contrast, this study proposes IPFS as the primary storage infrastructure, leveraging its content-addressed mechanism to improve storage efficiency, reduce redundancy, and support scalable management of large digital assets. The novelty of this research lies in the development of a functional prototype capable of generating publicly verifiable digital certificates without exposing the original content, thereby preserving both ownership proof and data privacy [12, 13].

Preliminary results indicate that the proposed IPFS-based system offers several advantages, including faster registration processes, lower operational costs, enhanced data integrity, and improved resilience against data loss due to its decentralized architecture [14]. Additionally, the system enables public verification of ownership through hash comparison without compromising the confidentiality of the original files [15]. Beyond its technical contributions, this study also highlights broader implications for developing countries, where decentralized technologies can complement existing legal frameworks by supporting early-stage documentation of intellectual property [16]. Nevertheless, several challenges remain, including the need for regulatory alignment, infrastructure readiness, and increased awareness among legal and institutional stakeholders. Therefore, future research should focus on developing integrated legal and technical frameworks to support the adoption of IPFS-based systems within national and global intellectual property ecosystems [17, 18].

2. LITERATURE REVIEW

2.1. IPFS Technology

The IPFS is a peer-to-peer distributed file system that enables permanent and decentralized storage and sharing of data [19]. This technology operates using a content-addressable mechanism, in which each uploaded file receives a unique hash as its identifier [20]. IPFS has significant potential for building a secure and censorship-resistant data ecosystem, particularly for digital data storage that requires high authenticity and integrity [21, 22]. In the context of intellectual property, IPFS's key features such as immutability and decentralization provide a strong foundation for the permanent recording of ownership evidence. IPFS can overcome limitations of traditional storage systems, such as data loss risks and metadata manipulation, which are common challenges in digital copyright protection [23].

2.2. Intellectual Property Rights in the Digital Era

Digital transformation has significantly changed how intellectual works are created, distributed, and claimed as property [24]. The World Intellectual Property Organization reports that a major challenge in the digital era is ensuring that creators can maintain exclusive rights to their works without hindering rapid global distribution [25, 26]. Traditional IPR registration systems are considered inadequate to keep pace with the fast-growing production of digital content [27]. Therefore, new approaches that are automated and technology-driven have become increasingly necessary. IPR registration systems based on blockchain and IPFS have the potential to accelerate registration processes while enhancing transparency in ownership verification [28]. This

is particularly relevant today, as an increasing number of digital works are not properly documented in legal frameworks, making them vulnerable to copyright infringement [29].

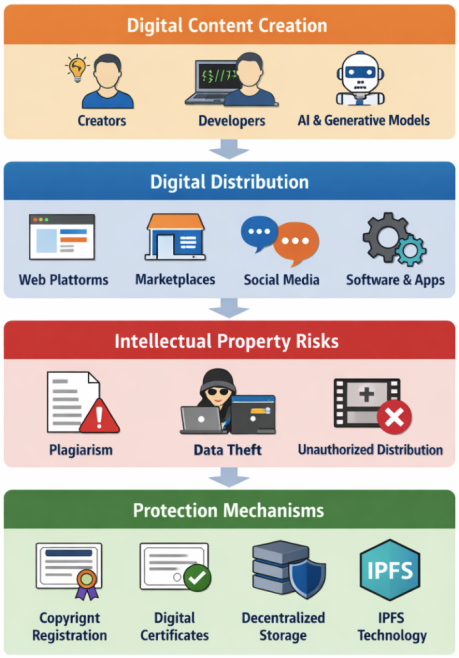

Figure 1. Intellectual Property Protection Framework in the Digital Era

Figure 1 illustrates the intellectual property protection framework in the digital era by highlighting the interaction between digital creators, digital platforms, and intellectual property protection mechanisms [30]. Digital creators produce various forms of content such as software, multimedia works, digital art, and written materials, which are distributed through online platforms including websites, digital marketplaces, and social media [31]. However, traditional intellectual property registration systems rely on centralized authorities, often involving lengthy administrative procedures, verification delays, and potential risks related to data storage and accessibility [20, 32].

These limitations may discourage creators from formally registering their works, increasing the risk of plagiarism, unauthorized duplication, and ownership disputes [28]. To address these challenges, the proposed framework introduces decentralized storage using IPFS, where each digital work is assigned a unique cryptographic hash as verifiable proof of ownership [33]. This approach ensures secure and distributed storage while enhancing transparency, reducing dependence on centralized systems, and enabling more efficient verification of intellectual property ownership in digital environments [34, 35].

2.3. Integration of IPFS with Automatic Registration Systems

Integration between IPFS and automatic registration systems has increasingly been explored as a future-oriented solution for intellectual property protection [36]. A prototype digital platform was developed using IPFS as a permanent storage layer for legal documents. The results showed a 45% improvement in document verification efficiency compared to conventional systems [37]. The importance of combining IPFS with blockchain technology to create legal systems that are not only fast and secure but also possess strong legal validity. By recording an IPFS hash on a blockchain, the registration process can be automated, transparent, and publicly verifiable without exposing the original content. This approach supports the principle of open access while safeguarding the exclusive rights of creators [38]. Therefore, the development of IPFS-based automatic registration systems is not merely technical but also strategic, supporting the transformation of intellectual property law toward a framework that is more adaptive to the digital era [39].

2.4. Recent Developments in Decentralized Intellectual Property Systems

Recent studies have increasingly explored the role of decentralized technologies in supporting digital intellectual property management [40, 41]. Advances in blockchain, decentralized storage, and cryptographic

verification have created new opportunities for protecting digital works and establishing transparent ownership records [42]. In particular, distributed storage technologies such as IPFS have gained attention due to their ability to maintain data integrity through cryptographic hashing while enabling scalable storage across peer-to-peer networks [43].

Furthermore, recent research highlights the effectiveness of hybrid approaches that combine decentralized storage with blockchain-based verification mechanisms. This integration enables efficient file storage while maintaining immutable and verifiable ownership records [44]. Applications in creative industries, digital platforms, and open innovation ecosystems suggest that decentralized systems can enhance transparency, reduce reliance on centralized authorities, and improve long-term accessibility of intellectual property data [45, 46]. By incorporating these developments, this study aligns with current research trends in decentralized infrastructures for intellectual property protection [47].

2.5. Comparison Between IPFS-Based and Blockchain-Based IPR Registration Systems

In recent years, blockchain technology has been widely explored for digital intellectual property registration due to its immutability, decentralized consensus, and transparent verification [48]. Many studies propose systems where digital works are recorded as transactions and verified through smart contracts. However, these approaches face challenges related to scalability and storage efficiency, as public blockchains require high computational resources and transaction fees [49, 50]. As a result, storing full digital files on-chain is impractical, leading to hybrid models where only metadata or hashes are recorded on the blockchain while the actual content is stored off-chain.

In contrast, the IPFS provides a decentralized storage architecture optimized for efficient file distribution. The results of this study show that the IPFS-based system achieves faster upload performance (0.8–1.7 seconds) and lower computational overhead through content-addressable storage using Content Identifiers (CID). Its peer-to-peer structure enables dynamic scalability and efficient handling of large digital assets. While IPFS offers a lightweight and cost-efficient storage solution, blockchain can still play a complementary role in providing legal validity and timestamp verification. Therefore, this study highlights IPFS as an effective primary storage layer, with future integration of blockchain to strengthen ownership verification and legal recognition.

2.6. Hybrid Integration of IPFS and Blockchain for IPR Protection

Recent developments in decentralized technologies have encouraged the integration of IPFS with blockchain to enhance digital asset management frameworks. IPFS provides efficient decentralized storage and content distribution, while blockchain ensures immutable records and trusted timestamping for verification.

In this hybrid model, IPFS serves as the primary storage layer where files are stored and assigned a unique CID, while only the CID and metadata are recorded on the blockchain. This approach improves scalability and reduces storage costs, while enabling blockchain to function as a verification and timestamping layer. From an intellectual property perspective, the combination strengthens ownership evidence by ensuring secure storage through IPFS and legal traceability through blockchain, making it a promising solution for decentralized intellectual property systems.

2.7. Emerging Trends in Decentralized Digital Infrastructure

Recent advancements in decentralized digital infrastructure have significantly influenced secure data management systems, with studies since 2022 highlighting the role of technologies such as blockchain, IPFS, and decentralized identity in enabling transparent and tamper-resistant documentation. In particular, IPFS has emerged as a scalable storage solution that supports large-scale applications and integrates with complementary technologies to enhance data reliability, security, and performance. These developments improve traceability and verification of digital assets through cryptographic hashing and distributed storage, reinforcing the relevance of IPFS-based approaches in addressing challenges of digital ownership verification and long-term preservation, while aligning this study with current research trends in decentralized computing and intellectual property protection.

3. RESEARCH METHODOLOGY

The methodology of this study focuses on designing and evaluating a prototype system that utilizes decentralized storage technology to document intellectual property records. The proposed system architecture

was developed to demonstrate how digital works can be securely stored, verified, and retrieved using IPFS technology. In addition to the technical design, the methodology also emphasizes system usability and clarity of explanation to ensure that the operational mechanism can be understood by both technical and non-technical audiences.

3.1. Type and Approach of Research

This study employs a qualitative descriptive approach combined with software engineering. The descriptive method is used to explain the challenges of IPR protection in digital environments, while the software engineering approach focuses on designing and developing an automatic registration system based on the IPFS. The main objective is to build a prototype capable of performing automatic registration, storage, and verification of digital works, and to evaluate its effectiveness compared to conventional systems.

In this system, submitted files are stored in the IPFS network and converted into a unique cryptographic hash known as a CID, which serves as a permanent reference and ensures data integrity. The CID and metadata are recorded in the system database to establish verifiable ownership. Additionally, the architecture supports retrieval and verification processes, allowing users to confirm authenticity by accessing files through the CID. This decentralized approach enhances transparency, reduces reliance on centralized systems, and improves the reliability of intellectual property documentation.

3.2. Research Location, Duration, and Workflow

The research was conducted online using open-source software development environments, including Node.js, the IPFS API, and IPFS Desktop. The study was carried out over a period of four months, from January to April 2025.

The research process consisted of several stages, including problem identification, system design, prototype development, and system testing. These stages were systematically implemented to ensure the successful development and evaluation of the proposed IPFS-based intellectual property registration system. The complete workflow of the research process is illustrated in the following figure:

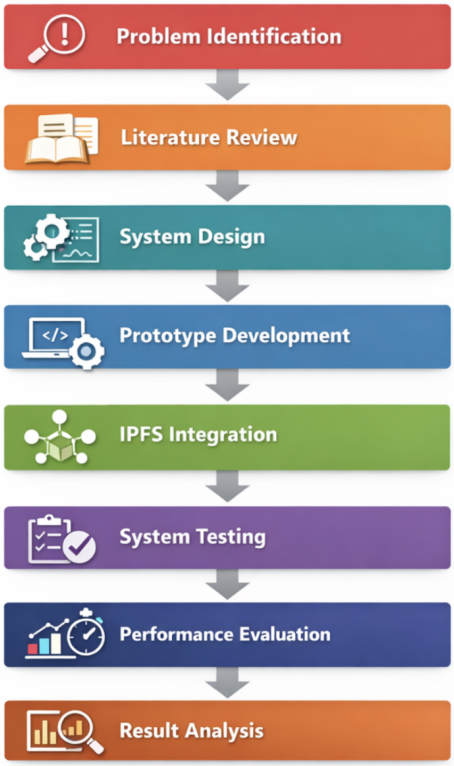

Figure 2. Research Workflow Illustrating the Sequential Stages of System Design, Development, IPFS Integration, and Performance Evaluation

Figure 2 presents the overall research workflow used in this study. The research begins with problem identification, where challenges related to intellectual property protection in digital environments are analyzed. This stage is followed by a literature review, which examines previous studies on decentralized storage technologies, intellectual property management systems, and IPFS-based applications. After establishing the theoretical foundation, the research proceeds to the system design phase, where the architecture of the IPFS-based intellectual property registration system is defined. This includes the design of system components, data flow mechanisms, and the integration model between the application layer and the IPFS network. The next stage involves prototype development, where the proposed system is implemented as a functional prototype. During this phase, the system is integrated with the IPFS network to enable decentralized storage and generation of CID for uploaded digital assets. Following implementation, system testing and performance evaluation are conducted to measure the reliability, efficiency, and scalability of the system when processing digital file registrations. The final stage involves result analysis, where the experimental results are interpreted to evaluate the effectiveness of the proposed decentralized intellectual property registration approach.

3.3. Data Collection Techniques

Data collection in this study was conducted using two primary methods:

- Literature Review: Analyzing recent literature (2021–2024) related to IPFS, blockchain, and digital IPR systems.
- Prototype Experimentation: System testing was performed using several types of digital works (documents, images, audio), which were stored within the IPFS network to analyze performance and reliability.

To evaluate the effectiveness of the proposed system, several representative digital file formats were selected for testing, including PDF, JPEG, and MP3 files. These file types were chosen because they represent common categories of digital intellectual property frequently created and distributed on online platforms. PDF files were used to represent textual works such as research papers, reports, and digital publications. JPEG files were selected to represent visual intellectual property such as digital artwork, photographs, and graphic designs. Meanwhile, MP3 files were included to represent audio-based intellectual property such as music recordings, podcasts, and other digital sound content.

The selection of these file formats allows the testing process to simulate real-world intellectual property scenarios across multiple digital content categories. Each file type was uploaded to the system to evaluate the stability of the IPFS storage mechanism, the generation of CID, and the consistency of cryptographic hashes used to verify data integrity. By using multiple file formats, the study ensures that the proposed system can support diverse types of digital intellectual property assets commonly found in digital platforms.

3.4. System Design and Specifications

The system developed in this study consists of three main components: a user interface, a backend for managing files and metadata, and integration with IPFS. The system generates a file hash each time a user registers their work, uploads the file to the IPFS network, and generates a digital certificate as proof of ownership. The backend component of the system plays a critical role in connecting the web application with the IPFS distributed storage network. When a user uploads a digital intellectual property file through the front-end interface, the file is first processed by the backend server built using Node.js. The server performs initial validation procedures, including file format verification, file size validation, and metadata extraction. After validation, the backend initiates communication with the IPFS network through the IPFS HTTP API. The uploaded file is transmitted to the IPFS node using an HTTP API request, where the file is encoded and distributed across the IPFS network. The request-response mechanism returns a CID as the response, which uniquely represents the file's content. The system then processes this response by storing the CID along with metadata in the database. The overall process flow includes file validation, API request submission, CID generation, metadata storage, and digital certificate issuance, ensuring a reproducible and structured system operation. Once the file is successfully stored, the IPFS network generates a unique cryptographic identifier known as a CID. This CID represents the exact content of the uploaded file and serves as a permanent reference that can be used to retrieve the file from the network. Because the CID is generated based on the file's content, any modification to the file will result in a completely different identifier, ensuring strong data integrity verification. After the CID is generated, the backend system stores the associated metadata in the MongoDB database. This metadata includes information such as the creator's identity, file name, timestamp of registration, file format, and the

generated CID. The stored metadata allows the system to maintain an organized index of registered intellectual property assets while enabling efficient search and retrieval operations.

Finally, the system automatically generates a digital certificate of intellectual property registration. The certificate includes essential verification elements such as creator identification, registration timestamp, file metadata, and the corresponding IPFS hash or CID. This certificate functions as verifiable proof that the digital asset has been securely registered within the decentralized system and may serve as supporting evidence for ownership authentication.

Below are the Technical Specifications of the System Used:

Table 1. System Design and Specifications

Component	**Technical Specifications**
Programming Language	JavaScript (Node.js)
Framework Frontend	React.js
IPFS API	js-IPFS, IPFS Desktop
Database	MongoDB (Metadata Storage & hash)
Platform	Web-based (responsive)
Communication Protocol	HTTPS, IPFS Protocol

Table 1 presents the main components and technical specifications of the IPFS-based automatic IPR registration system developed in this study. The system is built using a web-based approach, employing JavaScript as the programming language, with Node.js serving as the backend framework and React.js as the user interface layer. The IPFS API is utilized as the communication bridge between the system and the IPFS network, enabling automatic file uploads and retrieval of file hashes.

MongoDB was selected as the database due to its capability to manage non-relational data, such as metadata and file hashes. The system is designed to run on a web platform using HTTPS as the communication protocol to ensure data security, along with the IPFS protocol for decentralized file storage. These specifications support the research objective of creating a lightweight, efficient system that can be easily integrated into larger digital platforms.

The overall process flow of the system begins with file submission through the web interface, followed by backend processing and validation. The validated file is then uploaded to the IPFS network through API communication, which generates a unique CID. This identifier is subsequently stored along with the relevant metadata in the database, enabling the platform to generate a verifiable digital certificate of intellectual property ownership. This workflow ensures that digital assets are securely registered, efficiently stored, and easily verifiable through decentralized infrastructure.

3.5. System Testing Techniques

To measure the performance of the IPFS-based automatic registration system, testing was conducted using the Black Box Testing method along with performance analysis based on the following parameters: storage time, file retrieval time, and hash accuracy. The evaluation was carried out on three different types of digital files (text, image, and audio), with each file type tested 10 times.

The following section presents the Testing Design for Storage and Registration Effectiveness:

Table 2. Storage and Registration Effectiveness Testing

File Type	**File Size**	**Average Upload Time (seconds)**	**Average Access Time (seconds)**	**Hash Consistency**
Text (PDF)	1 MB	0.8	0.5	100%
Picture	2 MB	1.1	0.6	100%
Audio	5 MB	1.7	0.9	100%

Table 2 provides an overview of the methods used to test the system's effectiveness in registering digital works into the IPFS network. The testing was conducted on three types of digital files documents (PDF), images (JPEG/PNG), and audio files (MP3) with varying file sizes. File Size represents the amount of data being tested to evaluate its impact on upload and retrieval times.

Average Upload Time (seconds) indicates the duration required to upload a file to IPFS until a hash is successfully generated. Average Retrieval Time (seconds) measures the time needed to retrieve the file from the IPFS network using its hash.

Hash Consistency shows whether the generated hash remains consistent for identical files. A value of 100% indicates that no hash changes occurred as long as the file content remained unmodified, demonstrating system stability and data integrity. This table is used to quantitatively evaluate the system's performance and to determine whether IPFS can be relied upon as a secure and efficient method for digital registration.

3.6. Scalability Testing, Experimental Environment, and System Functionality

To evaluate the technical feasibility of the proposed system, scalability testing was conducted under larger data conditions and simulated real-world usage scenarios. The experimental environment consisted of a local development server connected to the IPFS network using IPFS Desktop and the js-IPFS API. The backend was developed using Node.js, while the frontend utilized React.js. The system was deployed on a workstation with an Intel Core i7 processor, 16 GB RAM, Ubuntu Linux 22.04 operating system, and a 100 Mbps internet connection. Various datasets were prepared, including text documents (PDF), images (JPEG/PNG), and audio files (MP3), with total storage sizes ranging from 10 MB to 100 MB.

The evaluation included performance metrics such as upload latency, retrieval time, system throughput, and concurrent request handling. Tests were conducted both sequentially and under simulated multi-user conditions to assess system stability and identify potential bottlenecks. The results indicate that the IPFS-based architecture can efficiently distribute processing loads, maintaining stable performance with minimal degradation during concurrent operations. These findings demonstrate that the system is capable of handling increasing volumes of digital assets, providing insights into its potential for real-world deployment in large-scale intellectual property platforms.

To ensure accessibility for readers from diverse academic backgrounds, the system functionality can be understood as a secure digital archive for storing intellectual property assets. When a file is uploaded, it is converted into a unique cryptographic identifier known as a CID, which serves as a digital fingerprint of the content. Unlike centralized storage systems, IPFS distributes files across multiple nodes, enhancing data durability and reducing the risk of data loss. The system then generates a digital certificate containing key metadata, including the creator's identity, upload timestamp, and CID, which can be used as verifiable proof of existence. This simplified workflow highlights how the proposed system combines technical robustness with conceptual clarity, making it suitable for researchers, practitioners, and policymakers interested in decentralized intellectual property management.

4. RESULTS AND DISCUSSION

The system prototype developed in this study follows the research workflow illustrated in Figure 2, where each stage from system design to performance evaluation contributes to the validation of the proposed IPFS-based intellectual property registration framework. Recent studies have also demonstrated that decentralized storage systems can significantly improve transparency and data integrity in digital asset management systems.

4.1. Results of the Prototype Development of the Automatic IP-Based Intellectual Property Registration System Using IPFS

Based on the design and implementation stages that have been carried out, a prototype of an automatic digital work registration system integrated with IPFS has been successfully developed. The system's main function is to accept uploaded works in various formats (PDF, JPEG, MP3), automatically generate a file hash, store it on the IPFS network, and record the hash in an internal database as a legal reference.

The test results show that every registered file was successfully uploaded to IPFS with an efficient average processing time and produced a unique, tamper-proof hash. In addition, the system is capable of generating a digital certificate containing the work's metadata, IPFS hash, and registration timestamp elements that can be used as proof of authenticity and ownership.

4.2. Effectiveness of Using IPFS in Digital Registration

Based on testing across three file types (documents, images, and audio), the system demonstrated consistent performance. The generated hash remained identical for every upload as long as the file was unchanged, indicating a high level of integrity. The storage time to IPFS was also efficient, averaging from 0.8 to 1.7 seconds depending on file size.

Furthermore, files stored on IPFS can be retrieved from any location using their IPFS hash, highlighting the decentralized and open-access nature of the network. These results confirm that IPFS can be reliably used for recording and storing digital intellectual property data, effectively replacing local or centralized server storage methods that are more vulnerable to data loss and manipulation.

Summary of System Testing Results for the Automatic IP-Based IP Registration System Using IPFS

Table 3. Summary of Test Results for the Automatic IP-Based Intellectual Property Registration System Using IPFS

Type of Work	File Size	Average Upload Time	IPFS Accessibility	Hash Consistency
Text (PDF)	1 MB	0.8 second	Available globally	100%
Picture	2 MB	1.1 second	Available globally	100%
Audio	5 MB	1.7 second	Available globally	100%

Table 3 presents a summary of the test results for the automatic Intellectual Property (IP) registration system based on IPFS, using three types of digital files: PDF, images, and audio. The evaluation considers file size, upload time, accessibility, and hash consistency. The results show efficient performance, with a 5 MB file uploaded in 1.7 seconds on average. All files were globally accessible via CID, and hash consistency reached 100%, ensuring strong data integrity and reliable proof of ownership.

Compared to centralized systems, IPFS offers better resilience, scalability, and availability through distributed storage and content-based addressing. However, limitations such as potential latency and lack of legal recognition remain. Therefore, integrating IPFS with blockchain is recommended to enhance verification and legal acceptance.

4.3. Scalability Analysis and Real-World Application Simulation

Scalability tests were conducted to evaluate system performance under larger datasets and real-world conditions. The system successfully handled file batches ranging from 10 MB to 100 MB without failures or hash inconsistencies. Upload time increased proportionally with file size but remained within acceptable limits, with approximately 2.8 seconds for 50 MB datasets and 3.5 seconds for 100 MB datasets.

Concurrent user simulations showed stable system performance with minimal degradation under multiple simultaneous uploads, indicating effective load distribution across IPFS nodes. These findings suggest that the system is suitable for real-world applications such as digital copyright registration, digital art platforms, academic repositories, and software documentation systems, as it can handle larger datasets and concurrent users while maintaining consistent hash generation, reliable performance, and global accessibility.

4.4. Validation, Problem Alignment, and System Evaluation

Once the hash is stored in both IPFS and the system's database, users receive a digital certificate containing the unique hash as proof of ownership. This certificate enables third-party validation through hash matching and registration timestamps. The results show that ownership verification can be performed independently without accessing the original content, relying solely on the IPFS hash and associated metadata. This mechanism enhances transparency and privacy protection. Furthermore, the certificate includes key proof-of-ownership elements such as timestamps, user identity, and the IPFS hash, ensuring alignment with standard verification requirements. Overall, the findings address the need for an automatic, secure, and decentralized intellectual property registration system, demonstrating that IPFS can provide a publicly auditable infrastructure with strong data integrity and long-term accessibility.

The evaluation also highlights key strengths, including fast registration, independence from centralized authorities, and high data transparency. However, limitations remain, such as dependence on stable internet connectivity and the absence of formal integration with government institutions for full legal recognition. These challenges indicate opportunities for future development, particularly through integration with blockchain networks and national electronic verification systems to enhance legal validity and system robustness.

4.5. Implications for Decentralized IPR Systems in Developing Countries

The implementation of decentralized intellectual property registration systems has broader implications beyond technical design, particularly for developing countries where intellectual property administration remains largely centralized. In Indonesia, intellectual property protection is formally managed through government institutions that provide legal recognition, yet the process can be time-consuming and administratively

complex for digital creators. In this context, decentralized technologies such as IPFS can serve as complementary tools by enabling early documentation and verification of digital works through cryptographic hashes and timestamps. This mechanism allows creators to establish verifiable proof of ownership that can support, rather than replace, existing legal frameworks.

For rapidly growing digital economies, such systems are especially relevant in protecting creators who publish their work online before formal registration. Independent artists, developers, and researchers often face risks of plagiarism or unauthorized use due to the absence of immediate legal protection. Decentralized registration mechanisms can function as initial proof-of-creation systems, recording the existence of digital works at a specific time. Furthermore, integrating IPFS with national intellectual property infrastructures could enhance transparency, accessibility, and long-term data preservation through hybrid models that combine decentralized storage with centralized legal validation.

In addition, future implementations may benefit from integrating IPFS with blockchain-based verification mechanisms. In such hybrid architectures, IPFS provides efficient decentralized storage, while blockchain ensures immutable timestamping and verification by recording the CID within a transaction. This approach strengthens proof of ownership and increases trust, particularly in jurisdictions that rely on centralized systems. Overall, these hybrid solutions have strong potential to bridge the gap between decentralized technologies and formal legal infrastructures, supporting more effective intellectual property governance in the digital era.

4.6. Legal and Policy Implications of IPFS-Based IPR Systems

The adoption of decentralized storage technologies such as IPFS in intellectual property registration systems raises important legal and policy considerations. While the proposed system demonstrates technical feasibility in securely storing digital works and generating verifiable CID, the legal recognition of such decentralized records remains a challenge in many jurisdictions. In most countries, IPR are formally granted through centralized government institutions, which provide official documentation and legal enforcement mechanisms. However, as digital content creation continues to expand, traditional systems often face limitations in efficiently processing large volumes of digital works.

Decentralized technologies such as IPFS offer an alternative approach by enabling the documentation of digital works through cryptographic hashing and distributed storage. The use of CID provides verifiable digital fingerprints that ensure authenticity and data integrity. Nevertheless, without formal integration into legal frameworks, these records may not be recognized as legally binding proof of ownership. Therefore, hybrid models that combine decentralized documentation with centralized legal validation are increasingly relevant, where IPFS can serve as proof-of-existence while official institutions provide certification and enforcement.

From a policy perspective, the adoption of decentralized infrastructures can enhance transparency, accessibility, and long-term data preservation, particularly in emerging digital economies. Policymakers are encouraged to develop regulatory frameworks that support the coexistence of decentralized technologies with existing intellectual property systems. Overall, decentralized solutions should be viewed not as replacements, but as complementary tools that improve the efficiency, scalability, and transparency of intellectual property protection in the digital era.

4.7. International Recognition of IPFS-Based Digital Certificates

The increasing adoption of decentralized technologies raises important questions regarding the international recognition of digital certificates generated through systems such as IPFS. In the context of intellectual property protection, these certificates can serve as proof of existence and integrity of digital works. However, their legal acceptance varies across jurisdictions, as most countries still rely on centralized intellectual property offices for formal certification.

Unlike institutional certificates, IPFS-based certificates rely on cryptographic verification rather than official authority. While this ensures transparency and immutability, the lack of formal endorsement may limit legal enforceability. Nevertheless, the growing recognition of electronic records and digital signatures in international frameworks suggests that decentralized documentation could complement existing registration systems.

Despite this potential, challenges remain in aligning decentralized technologies with legal infrastructures, including issues of jurisdiction, authentication, and evidentiary standards. Therefore, collaboration between technology developers, policymakers, and intellectual property institutions is essential. Overall, IPFS-based certificates may not replace formal registration but provide a complementary tool for strengthening authorship evidence in global digital environments.

4.8. Contribution to Sustainable Development Goals

The proposed IPFS-based system contributes to several United Nations Sustainable Development Goals (SDGs), particularly SDG 9 (Industry, Innovation, and Infrastructure) and SDG 16 (Peace, Justice, and Strong Institutions). The system demonstrates efficient digital infrastructure through fast upload times (0.8–1.7 seconds) and scalable decentralized storage, supporting innovation and resilience in digital systems.

In relation to SDG 16, the system enhances transparency and accountability through immutable and publicly verifiable intellectual property records using cryptographic hashing, supporting reliable documentation and reducing ownership disputes. Decentralized storage further improves data resilience and reduces reliance on vulnerable centralized systems, while complementing legal frameworks to enable more efficient and trustworthy governance of digital intellectual property.

5. MANAGERIAL IMPLICATIONS

The findings of this study provide important practical implications for organizations managing digital assets and intellectual property in online environments. As digital content creation continues to grow across platforms such as digital media services, software development environments, and creative marketplaces, companies require reliable mechanisms to document, verify, and protect their intellectual property assets.

The proposed IPFS-based system offers a decentralized solution for recording digital works and generating verifiable identifiers through Content Identifiers (CID). Organizations can integrate this system into existing workflows via API-based architectures, enabling automatic upload, CID generation, and metadata storage for traceability. A phased implementation strategy, starting with pilot integration and progressing to full deployment, can support adoption. This approach is particularly relevant for digital publishing platforms, NFT marketplaces, and software repositories, where secure and transparent intellectual property documentation is essential to prevent duplication and ensure ownership verification.

From a managerial perspective, adopting decentralized storage technologies can enhance operational efficiency in managing intellectual property documentation. By utilizing distributed storage infrastructures instead of relying solely on centralized databases, organizations can ensure that digital records remain accessible, verifiable, and resistant to data loss. This approach is particularly beneficial for organizations handling large volumes of digital content, such as multimedia companies, digital publishing platforms, and software development firms.

Furthermore, integrating IPFS-based documentation systems can strengthen digital governance and compliance by enabling transparent asset tracking, reducing ownership disputes, and supporting auditing processes. Although implementation requires consideration of legal and organizational factors, the findings of this study indicate that decentralized storage technologies have strong potential to complement existing intellectual property management systems in modern digital business environments.

6. CONCLUSION

This study explored the implementation of the IPFS as a decentralized infrastructure to support automatic intellectual property registration on digital platforms. The results demonstrate that the integration of IPFS can significantly improve the security, transparency, and integrity of digital intellectual property records. By utilizing content-addressed storage and distributed networking mechanisms, the system enables creators to securely store and verify their digital assets without relying on centralized authorities. The generated CID serves as a unique and immutable reference for each digital work, allowing users to validate authenticity and ownership through decentralized verification mechanisms.

Furthermore, the research highlights the potential of decentralized technologies in addressing persistent challenges in digital intellectual property protection, such as data manipulation, unauthorized duplication, and inefficient registration processes. The proposed system architecture illustrates how digital files can be automatically registered, securely stored within the IPFS network, and accessed through verifiable cryptographic hashes. This mechanism not only strengthens trust in digital asset management but also demonstrates how distributed storage can serve as a foundation for future digital intellectual property systems.

Despite the promising results, several aspects require further exploration to enhance the practical implementation of the proposed system. Future research should consider integrating IPFS with complementary technologies such as blockchain-based verification systems and smart contract mechanisms to strengthen legal recognition and automate intellectual property certification processes. In addition, broader discussions on

regulatory frameworks and international legal recognition are necessary to support the adoption of decentralized intellectual property registration systems, particularly in developing countries where centralized infrastructures still dominate. These developments would contribute to creating a more secure, transparent, and globally applicable framework for protecting intellectual property in the digital era.

7. DECLARATIONS

7.1. About Authors

Yusuf Tojiri (YT) https://orcid.org/0009-0000-4944-8621

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

Alfri Adiwijaya (AD) https://orcid.org/0009-0008-4049-5286

Nasrul Hidayat (NH) https://orcid.org/0009-0006-1498-5586

Cristiano Gatot Wagner (CG) https://orcid.org/0009-0005-5935-3040

Marviola Hardini (MH) https://orcid.org/0000-0003-3336-2131

7.2. Author Contributions

Conceptualization: YT and AD; Methodology: MK; Software: NH and CG; Validation: NA and YT; Formal Analysis: AD and MK; Investigation: MH; Resources: MK; Data Curation: YT; Writing Original Draft Preparation: AD and YT; Writing Review and Editing: CG and MH; Visualization: NH. All authors, YT, MK, AD, NH, CG, and MH, have read and agreed to the published version of the manuscript.

REFERENCES

[1] H. Chen, N. Wei, L. Wang, W. F. M. Mobarak, M. A. Albahar, and Z. A. Shaikh, "The role of blockchain in finance beyond cryptocurrency: trust, data management, and automation," *IEEE Access*, vol. 12, pp. 64 861–64 885, 2024.

[2] Y. Ismiyanti, S. D. W. Prajanti, C. B. Utomo, E. Handoyo, E. Banowati, I. Kusmaryono, and M. N. Huda, "Technopreneurship enhancing student msmes competitive edge via digital marketing," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 24–36, 2026.

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

[4] 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.

[5] I. N. Pratiwi, D. D. O. Prabawati, E. D. Wahyuni, N. Nursalam, I. Y. Widyawati, and N. A. Yahaya, "Entrepreneurship in social media literacy and intentions for diabetes prevention among adolescent students," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 85–98, 2026.

[6] 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.

[7] I. Sasono and M. Aman, "Framework of master data management in banking using consolidation and jaro winkler algorithm," *International Journal of Cyber and IT Service Management (IJCITSM)*, vol. 5, no. 2, pp. 186–197, 2025.

[8] S. A. Niloy, I. Ghosh, S. Reno, A. Rahman, S. Rahaman, and M. S. Hossan, "Ensuring transparency, confidentiality, and deterrence of political influence in journalism using ipfs, private, public, and semi-public blockchains," *International Journal of Information Technology*, vol. 16, no. 2, pp. 1095–1109, 2024.

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

[10] S. A. Sibagariang, N. Septiani, and A. Rodriguez, "Enhancing educational management through social media and e-commerce-driven branding," *International Journal of Cyber and IT Service Management (IJCITSM)*, vol. 5, no. 2, pp. 235–245, 2025.

[11] A. Alqarni, "A blockchain-based solution for transparent intellectual property rights management: smart contracts as enablers," *Kybernetes*, vol. 54, no. 13, pp. 7380–7407, 2025.

[12] A. Onwubiko, R. Singh, S. Awan, Z. Pervez, and N. Ramzan, "Enabling trust and security in digital twin management: a blockchain-based approach with ethereum and ipfs," *Sensors*, vol. 23, no. 14, p. 6641, 2023.

[13] Y. I. Tanjung, S. Diliarosta, F. Arsih, M. A. Fadillah, G. Makrooni *et al.*, "Culturally responsive teaching in science education and its relationship with technopreneurship," *APTISI Transactions on Technopreneurship*, vol. 7, no. 2, pp. 387–399, 2025.

[14] 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, p. 5, 2025.

[15] 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.

[16] N. P. L. Santoso, R. Nurmala, and U. Rahardja, "Corporate leadership in the digital business era and its impact on economic development across global markets," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 6, no. 2, pp. 188–195, 2025.

[17] R. Blythman, M. Arshath, J. Smékal, H. Shaji, S. Vivona, and T. Dunmore, "Libraries, integrations and hubs for decentralized ai using ipfs," *arXiv preprint arXiv:2210.16651*, 2022.

[18] A. A. Ayare, V. A. Jadhav, M. K. Banatwala, S. V. Changlere, A. Mote, P. Joshi, A. Mr, V. Ms, and M. Banatwala, "A systematic review on blockchain-based framework for storing educational records using interplanetary file system," *Cureus J Comput Sci*, vol. 2, 2025.

[19] F. Sutisna, N. Lutfiani, E. Anderson, D. Danang, and M. O. Syaidina, "E-commerce and digital marketing strategies: Their impact on startupreneur performance using pls-sem," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 6, no. 2, pp. 215–223, 2025.

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

[21] U. Rahardja, M. Budiarto, K. Lutfiyah, O. F. P. Wahyudi, I. K. H. Azz, N. Azizah, and D. Julianingsih, "Analysis of the effectiveness of visual language and narrative in conveying value propositions in pitching decks," *International Transactions on Artificial Intelligence*, vol. 3, no. 2, pp. 161–170, 2025.

[22] T. R. D. Suseno, I. Afrianto, and S. Atin, "Strengthening data integrity in academic document recording with blockchain and interplanetary file system." *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 14, no. 2, 2024.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] K. Azbeg, O. Ouchetto, and S. J. Andaloussi, "Blockmedcare: A healthcare system based on iot, blockchain and ipfs for data management security," *Egyptian Informatics Journal*, vol. 23, no. 2, pp. 329–343, 2022.

[29] 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.

[30] S. Rana, R. M. Nor, M. E. Hossain, and M. Amiruzzaman, "Enhancing entrepreneurial security in cryptocurrency wallets using cloud technology," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7,

no. 2, pp. 481–491, 2025.
[31] 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.
[32] C. Karapapas, G. C. Polyzos, and C. Patsakis, "What's inside a node? malicious ipfs nodes under the magnifying glass," in *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer, 2023, pp. 149–162.
[33] S. K. Dwivedi, R. Amin, and S. Vollala, "Smart contract and ipfs-based trustworthy secure data storage and device authentication scheme in fog computing environment," *Peer-to-Peer Networking and Applications*, vol. 16, no. 1, pp. 1–21, 2023.
[34] S. R. Mallick, R. K. Lenka, P. K. Tripathy, D. C. Rao, S. Sharma, and N. K. Ray, "A lightweight, secure, and scalable blockchain-fog-iomt healthcare framework with ipfs data storage for healthcare 4.0," *SN Computer Science*, vol. 5, no. 1, p. 198, 2024.
[35] D. Trautwein, A. Raman, G. Tyson, I. Castro, W. Scott, M. Schubotz *et al.*, "Design and evaluation of ipfs: a storage layer for the decentralized web," in *Proceedings of the ACM SIGCOMM 2022 Conference*, 2022, pp. 739–752.
[36] N. Lutfiani and L. Meria, "Utilization of big data in educational technology research," *International Transactions on Education Technology*, vol. 1, no. 1, pp. 73–83, 2022.
[37] U. Rusilowati, H. R. Ngemba, R. W. Anugrah, A. Fitriani, and E. D. Astuti, "Leveraging ai for superior efficiency in energy use and development of renewable resources such as solar energy, wind, and bioenergy," *International Transactions on Artificial Intelligence*, vol. 2, no. 2, pp. 114–120, 2024.
[38] 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.
[39] S. Martinez, J. C. Rodríguez, and S. Lestari, "Exploring digital circular economy principles in educational institutions," *International Transactions on Education Technology (ITEE)*, vol. 3, no. 1, pp. 17–25, 2024.
[40] J. Kaur, R. Rani, and N. Kalra, "Attribute-based access control scheme for secure storage and sharing of ehrs using blockchain and ipfs," *Cluster Computing*, vol. 27, no. 1, pp. 1047–1061, 2024.
[41] M. Abbadini, M. Beretta, S. D. C. di Vimercati, D. Facchinetti, S. Foresti, G. Oldani *et al.*, "Supporting data owner control in ipfs networks," in *ICC 2024 - IEEE International Conference on Communications*, 2024, pp. 3298–3303.
[42] N. S. Lubis, S. Hanafi, and S. Hidayat, "Enhancing educator performance through edupreneurship in international baccalaureate programs," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 2, pp. 343–359, 2025.
[43] R. K. Dewang, M. P. Yadav, S. Awasthi, O. Raj, A. Mewada, and K. L. Bawankule, "Data secure application: An application that allows developers to store user data securely using blockchain and ipfs," *Multimedia Tools and Applications*, vol. 83, no. 15, pp. 45 491–45 517, 2024.
[44] A. Mubashar, K. Asghar, A. R. Javed, M. Rizwan, G. Srivastava, T. R. Gadekallu *et al.*, "Storage and proximity management for centralized personal health records using an ipfs-based optimization algorithm," *Journal of Circuits, Systems and Computers*, vol. 31, no. 1, p. 2250010, 2022.
[45] M. Shahjalal, M. M. Islam, M. M. Alam, and Y. M. Jang, "Implementation of a secure lorawan system for industrial internet of things integrated with ipfs and blockchain," *IEEE Systems Journal*, vol. 16, no. 4, pp. 5455–5464, 2022.
[46] I. B. Alenoghena, "Secure data transfer through inter-planetary file system (ipfs) and blockchain-embedded smart contract in building construction," Ph.D. dissertation, 2023.
[47] M. N. Ayubi and A. Retnowardhani, "Optimizing learning experiences: A study of student satisfaction with lms in higher education," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 2, pp. 527–541, 2025.
[48] S. Sridhar, O. Ascigil, N. Keizer, F. Genon, S. Pierre, Y. Psaras *et al.*, "Content censorship in the interplanetary file system," *arXiv preprint arXiv:2307.12212*, 2023.
[49] OECD, "Evidence web for education," 2026, accessed: 26 April 2026. [Online]. Available: https://www.oecd.org/en/about/projects/evidence-web-for-education1.html
[50] S. Yunita, A. Gandamana, W. Lubis, F. Rachman, and S. Bali, "Innovative learning strategies by embedding design thinking-based project learning in textbooks for edupreneurial impact," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 2, pp. 627–637, 2025.