ISSN No:-2456-2165

IPFS based Solution for Secure File Storage

Akshay Sripriya, Arvinth Ram, Shakthi B and Shanthosh Kumar,
Students, VIT University, Chennai

Abstract:- In today's digital world, the need for safe and dependable file storage is becoming a crucial matter. The traditional means of file storage, like centralized servers, have many drawbacks like accessibility, scalability, and security. This study investigates the application of IPFS, a distributed peer-to-peer file system, as a safe file storing method. In comparison to conventional file storage techniques, we propose an IPFS-based solution for safe information storage using Moralis IPFS API. This study examines its advantages and disadvantages as well.

Keywords:- *InterPlanetary File System (IPFS), Blockchain, peer-to-peer, Moralis, distributed*.

I. INTRODUCTION

THE demand for safe file storage is facilitated by the rising value and sensitivity of digital information. Protecting sensitive data from unauthorized access and alteration is necessary. With the rise in cyber-attacks like hacking, data breaches, etc., a secure storage solution is a requirement of high priority today. This is crucial for businesses and organizations that handle a lot of sensitive data, including but not limited to financial records, personal data, and trade secrets. Secure file storage helps stop data loss, data theft, and other hostile actions that could hurt people or organisations. The adoption of secure file storage solutions is frequently required for compliance with legal and regulatory requirements including GDPR, HIPAA, and PCI-DSS.r .

A. InterPlanetary File Storage

The InterPlanetary File System (IPFS) functions as a decentralized network, protocol, and hypermedia system aimed at facilitating the sharing and exchange of files within a distributed file system. Every file within the interconnected IPFS servers' global namespace is uniquely identified through content-addressing, a fundamental component of the IPFS architecture.

IPFS uses a content-addressable system where files are assigned a unique hash based on their content, which allows for efficient retrieval and verification of files. This is a decentralized approach to file storage. It provides several benefits, like increased security, redundancy, and scalability. IPFS also includes features such as versioning and encryption, making it a flexible and secure file storage solution.

Since its debut, IPFS has undergone a number of notable upgrades and modifications. This demonstrates the need for community and technological landscape evolution and change.

The introduction of IPFS v0.4 in 2018 was one of the most significant developments in IPFS's development. The protocol underwent numerous improvements as a result. These improvements included enhanced performance and reliability, faster and more effective content routing, and greater support for content-addressed data.

The launch of IPFS Cluster in 2018 marked yet another significant turning point in the evolution of IPFS. It offered a method for managing and replicating IPFS material across numerous nodes. Greater fault tolerance and redundancy are made possible by IPFS Cluster. As a result, performance and scalability have increased.

With multiple projects using IPFS for distributed file storage and content distribution, IPFS has recently received a lot of attention in the blockchain world. For instance, the decentralised hosting of websites and other material is made possible through the integration of IPFS into the Ethereum Name Service (ENS).

In general, IPFS development has been characterized by an emphasis on enhancing performance, dependability, and scalability as well as broadening the applications for decentralized file storage and content delivery. IPFS is positioned to keep playing a big role in the decentralized web and the larger technology environment with continued development and acceptance.

B. How IPFS works:

Below is the step-by-step functioning of the IPFS system:

- *Add content to IPFS:*

The IPFS client programme is used to add files or other content to the IPFS network. A unique content identifier (CID) is created for the material using this programme. The CID, which is used to later retrieve the material, is a hash value created depending on the content itself.

- *Distribute content across the network:*

The content is then divided into smaller bits and distributed throughout the IPFS network by the IPFS client software. The CID for the content is used to keep track of where each piece is stored, and each piece of content is encrypted and stored on several network nodes.

ISSN No:-2456-2165

➢ *Obtain content from IPFS:*

To obtain content from IPFS, you must use the IPFS client programme to make a CID-based request for the content. The client programme requests content from network nodes, retrieves it, and then puts it back together to create the original file.

➢ *Use an IPFS gateway:*

You can use an IPFS gateway to access content stored in IPFS using a web browser. The gateway serves as a link between the IPFS network and the web by being a web server that is placed in front of the IPFS network. By utilizing a standard URL, you can access IPFS material through the gateway.

➢ *Update content:*

The IPFS client software creates a new CID for the updated content when you make changes to IPFS-stored content. While the new material is dispersed over the network using the new CID, the old content is still present.

➢ *Content deletion:*

If no one demands it, IPFS content that has been kept there instead remains orphaned. As nodes go down or storage space is required for new material, orphaned content is finally removed from the network over time.

In general, using IPFS entails adding content to the network, dispersing it across various network nodes. It also consists of retrieving content using its CID, gaining access to content using an IPFS gateway, updating content using a new CID, and allowing orphaned content to gradually disappear from the network. Figure 1 shows the process of storing and retrieving a file.

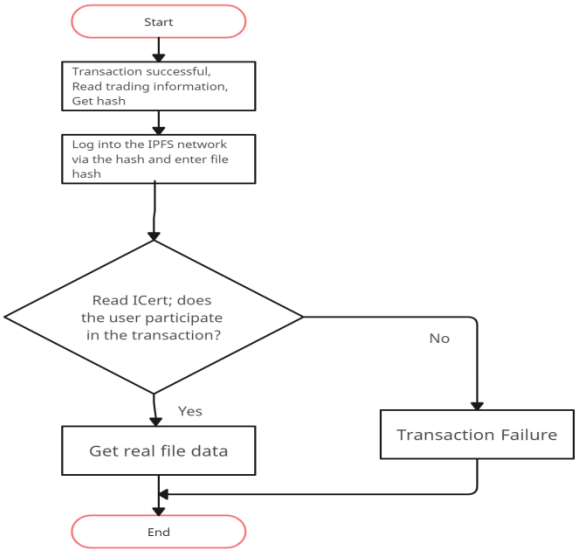

Fig 1: IPFS Network File storage mechanism

C.Moralis IPFS:

Moralis IPFS is an IPFS-based decentralised file storage system. The IPFS solution offered by Moralis is intended to make it simple for developers to store and manage data on the IPFS network. Moralis is a platform that offers a variety of tools and services for developing decentralised apps.

With Moralis IPFS, developers can store files on a decentralized network that is resilient, secure, and censorship-resistant. Moralis IPFS provides features such as content addressing, file replication, and access control, making it a flexible and scalable solution for decentralized file storage.

Moralis IPFS also provides APIs and SDKs for integrating with other applications and services, making it a popular choice among developers building decentralized applications on IPFS. With Moralis IPFS, developers can easily incorporate decentralized file storage into their applications, enabling greater privacy and security for their users.

As it offers a variety of features and functionality for developers, Moralis IPFS is an effective option for secure file storage. With features like end-to-end encryption, access control, and file versioning, Moralis IPFS gives developers the ability to create decentralised, secure, and privacy-focused applications.

II. LITERATURE SURVEY

Paper Details	Abstract
Nizamuddin, Nishara & Hasan, Haya & Salah, Khaled. (2018). IPFS-Blockchain-Based Authenticity of Online Publications. 10.1007/978-3-319-94478-4_14.	The authors of the paper propose a solution to ensure the originality and authenticity of digital content such as books, music, and movies that are published and posted online for free. The solution uses a combination of emerging technologies, including IPFS and blockchain smart contracts.
Q. Zheng, Y. Li, P. Chen and X. Dong, "An Innovative IPFS-Based Storage Model for Blockchain," 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), Santiago, Chile, 2018, pp. 704-708, doi: 10.1109/WI.2018.000-8.	The authors propose a solution to the growing data volume problem in blockchain technology using an IPFS-based storage model. The high storage and bandwidth demand of existing blockchains prevent many nodes from joining the network and limit its development. The solution involves miners depositing transaction data into the IPFS network and incorporating the returned IPFS hash into blocks. This solves the data volume problem and promotes the expansion of the decentralized network.
Haimei Xu et al 2021 IOP Conf. Ser.: Mater. Sci. Eng. 1043 052014 “Content Sharing Network based on IPFS and Blockchain”	The authors propose InnerLight, a mental health content-sharing system using IPFS, blockchain, and ranking algorithms for decentralization and sustainability.
Nizamuddin, Nishara, Haya R. Hasan and Khaled Salah. “IPFS-Blockchain-Based Authenticity of Online Publications.” International Conference on Blockchain (2018).	The authors propose a solution for originality and authenticity of online digital content using IPFS and blockchain smart contracts. IPFS stores the content, while the Ethereum smart contract governs its history, ensuring traceability and visibility.
Kang, Peng, Wenzhong Yang, and Jiong Zheng. 2022. "Blockchain Private File Storage-Sharing Method Based on IPFS" *Sensors* 22, no. 14: 5100. https://doi.org/10.3390/s22145100	The authors propose a knowledge file storage and sharing method combining NDN technology, a distributed blockchain, and IPFS to ensure file safety and efficient sharing while addressing the issues of opaque file management, tampering with intellectual copyright, and inconsistent file management among institutions. The NDN is used for file signature and encryption.

Most existing secure file storage systems that implement Web 3.0 use IPFS only as an underlying platform but do not implement the integration of IPFS with the file storage application.

III. PROPOSED SYSTEM

While most current systems use IPFS with moderation or just as a support framework, the proposed system uses the Moralis API and integrates Blockchain technology in every phase of the process to increase data security. The following are the major functionalities in the proposed system.

A. System Functionalities:

- *Authentication*:

Authentication is performed via the login module. Unlike conventional Login modules used in numerous systems, the proposed system integrates blockchain technology right from the authentication phase. This is done by associating the login credentials with a crypto wallet. In theory, the user will need to have a crypto wallet like MetaMask or BitWallet and can use this wallet to log in to their account.

- *Home Page:*

The user is brought to the system's home page, from which they can access a number of features.

- *Upload File*:

After choosing this option, the user is invited to choose a file from their local drive. The file is then compressed and encrypted to make it smaller.

- *File Chunking*:

Depending on the size of the original file, Moralis API splits the file into numerous chunks that range in size from 256 KB to 1 MB. The IPFS technology is then used to provide each item a distinct content address. Using these addresses, a hash code is generated. This is like a key for retrieval of the file in the future.

- *File Retrieval:*

By supplying the generated hash code, the user can then retrieve it from the IPFS network. For access to the original file, the system reconstructs the file from its multiple chunks and decrypts it.

The entire process is very straightforward and simple. There is negligible deviation from normal/conventional file storage processes in the proposed system. Figure 2 shows the system process flow.

ISSN No:-2456-2165

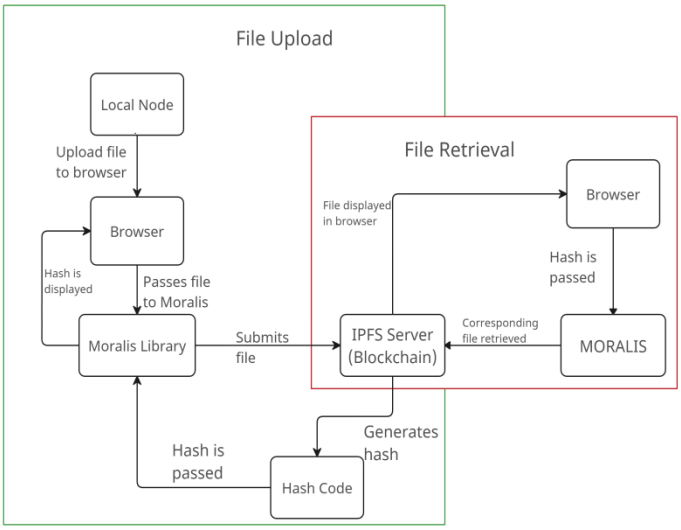

Fig 2: System process flow

IV. IMPLEMENTATION

The back end of the proposed system was implemented successfully with minimalistic front end. The file upload process worked as intended. When the user uploaded the file, the system generated a hash code.

On submitting the hash code back, the system was able to retrieve the correct file. The system is currently limited to handle images alone. However, it can be upgraded to support other formats too.

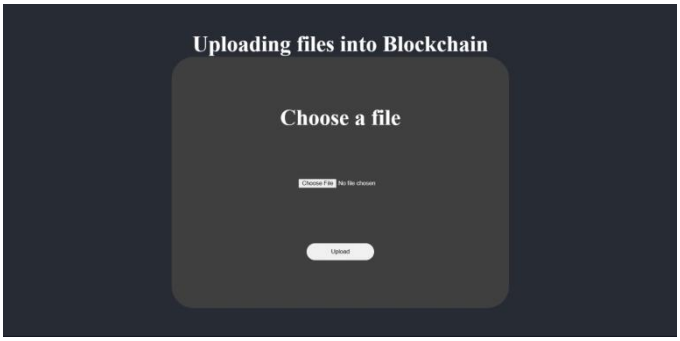

Fig 3: Implementation results

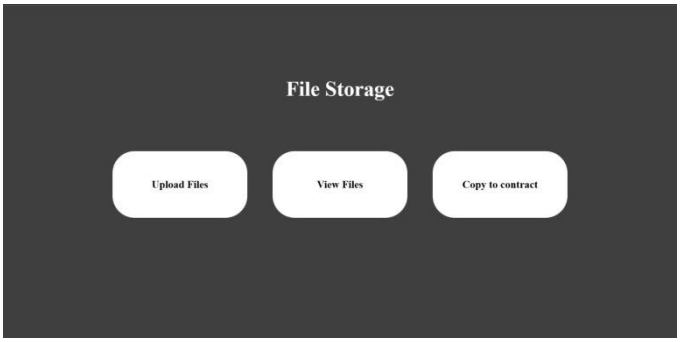

Fig 4: Implementation results

V. CONCLUSION

The IPFS-based solution for secure file storage provides numerous benefits in terms of security, accessibility, and availability. This solution has been successfully implemented in various domains, including healthcare, e-commerce, cloud computing, supply chain management, and smart homes. The combination of IPFS and blockchain technology ensures that the data is stored securely and is easily accessible by authorized users only. Moreover, the decentralized nature of this solution ensures that the data is available even if some of the nodes fail or are taken down. The proposed process flow for uploading a file in the IPFS-based secure file storage system ensures that the file is broken down into multiple pieces and scattered across multiple nodes, ensuring its security and availability. Therefore, the IPFS-based solution for secure file storage has the potential to revolutionize the way we store and share data, especially in domains where security and accessibility are of utmost importance.

REFERENCES

[1]. D. Benet, "IPFS - Content Addressed, Versioned, P2P File System," arXiv preprint arXiv:1407.3561, 2014.
[2]. F. Benhamouda, A. Kate, A. Mohassel, and E. Shi, "On the Security of IPFS-based Decentralized File Storage," Proceedings of the ACM Conference on Computer and Communications Security, pp. 1951-1963, 2018.
[3]. V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2014.
[4]. J. Dimonaco, "Using IPFS as a Secure and Resilient Data Store," Blog post, 2019.
[5]. S. Eyal, G. Sirer, "Bitcoin is Broken," arXiv preprint arXiv:1312.0459, 2013.
[6]. S. Eyal, E. G. Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable," Financial Cryptography and Data Security, pp. 436-454, 2014.
[7]. Filecoin, "The Filecoin Whitepaper," 2017.
[8]. IPFS Cluster, "IPFS Cluster Documentation," 2020.
[9]. IPFS Docs, "IPFS Documentation," 2020.
[10]. IPFS Gateway, "IPFS Gateway Documentation," 2020.
[11]. IPFS Pinning Services, "IPFS Pinning Services," 2020.
[12]. IPFS.io, "IPFS.io," 2020.
[13]. J. Benet, "Protocol Labs: Research and Development," Protocol Labs White Paper, 2018.
[14]. J. Benet, "The InterPlanetary File System: A Peer-to-Peer Hypermedia Protocol," arXiv preprint arXiv:1705.05873, 2017.
[15]. J. Benet, "IPFS: The Permanent Web," arXiv preprint arXiv:1611.01458, 2016.
[16]. J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," GitHub, 2014.
[17]. M. Ferreira, A. Miranda, B. Rocha, "Blockchain-based IPFS Content-Addressed Storage for Distributed Big Data Applications," Proceedings of the IEEE 4th International Conference on Big Data Analysis, pp. 52-59, 2019.
[18]. N. Goel, P. R. Kumar, "An Introduction to Blockchain Technology," IEEE Potentials, vol. 37, no. 2, pp. 18-21, 2018.

[19]. P. Gupta, R. Bhushan, "Decentralized Content Sharing Platform using IPFS and Ethereum," Proceedings of the 10th International Conference on Cloud Computing, Data Science and Engineering, pp. 231-237, 2020.
[20]. P. Hunt, A. Konar, F. P. Junqueira, "Zookeeper: Wait-free Coordination for Internet-scale Systems," USENIX Annual Technical Conference, pp. 11-25, 2010.
[21]. S. Kshetri, "Blockchain's Roles in Meeting Key Supply Chain Management Objectives," International Journal of Information Management, vol. 39, pp. 80-89, 2018..
[22]. R. Landa, "IPFS: An Introduction to the InterPlanetary File System," Blog post, 2017.
[23]. S. Liang, J. Fok, V. Sekar, "Challenges and Opportunities in Distributed Ledger Technologies," Proceedings of the IEEE International Conference on Communications, pp. 1-7, 2018.
[24]. D. Mazières, M. Waldman, "Tapestry: An Infrastructure for Fault-tolerant Wide-area Location and Routing," Journal of Distributed Computing, vol. 16, no. 2-3, pp. 187-202, 2003.
[25]. E. Nazarov, "Moralis IPFS Integration," Blog post, 2020.
[26]. D. Nikolov, S. Klauser, G. Karame, "Secure Distributed File Storage on IPFS Using Smart Contracts," Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency, pp. 1-6, 2019.
[27]. G. Peters, M. Panitzek, M. Schlecker, and T. Schaber, "IPFS as a Decentralized Storage Solution in Industry 4.0," Proceedings of the IEEE International Conference on Industrial Technology, pp. 1498-1503, 2019.
[28]. J. Qiu, J. Wang, J. Cao, W. Liu, and D. He, "Blockchain and IPFS-Based Secure Sharing Platform for Medical Records," IEEE Access, vol. 7, pp. 43316-43325, 2019.
[29]. M. Vukolić, "The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication," Proceedings of the ACM Symposium on Applied Computing, pp. 213-218, 2015
[30]. M. Waldman, "Tapestry: A Resilient Global-scale Overlay for Service Deployment," Ph.D. dissertation, University of California, Berkeley, 2002.
[31]. H. Wang, "IPFS-based Cloud Storage System," Bachelor's thesis, Zhejiang University, 2018.
[32]. J. Wang, K. Ren, J. Lou, and K. Zeng, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 28, no. 4, pp. 42-47, 2014.
[33]. J. Wang, K. Ren, J. Li, and X. Ma, "Secure and Practical Outsourcing of Linear Programming in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1172-1181, 2013.
[34]. X. Wu, W. Wang, and Y. Shi, "A Hybrid Incentive Mechanism for IPFS-Based Distributed Storage," Proceedings of the IEEE International Conference on Computational Science and Engineering, pp. 747-752, 2019.
[35]. H. Xu, K. Cao, J. Zhu, and J. Lu, "Bao: A Secure and Efficient Public Auditing Scheme for Cloud Data," IEEE Transactions on Cloud Computing, vol. 5, no. 1, pp. 48-59, 2017.
[36]. Y. Yan, X. Zhang, Y. Wang, and X. Su, "An Effective Strategy for Improving the Performance of IPFS Storage System," Proceedings of the IEEE International Conference on Big Data, pp. 1002-1007, 2019.
[37]. Y. Yang, H. Li, and C. Cao, "A Secure Cloud Storage Scheme Based on IPFS and Blockchain," Proceedings of the IEEE International Conference on Big Data and Smart Computing, pp. 367-371, 2019.
[38]. L. Yu, H. Zhang, and X. Li, "A Distributed Ledger System for Supply Chain Traceability Based on IPFS," Proceedings of the IEEE International Conference on Industrial Technology, pp. 1462-1467, 2019.
[39]. Z. Zhang, W. Wang, X. Zhang, and L. Zhao, "Performance Evaluation of IPFS-based Distributed Storage System," Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, pp. 56-60, 2019.
[40]. C. Zheng, Y. Wang, and C. Wu, "A Distributed and Secure File Sharing System Based on IPFS and Blockchain," Proceedings of the IEEE International Conference on Cloud Computing and Security, pp. 87-91, 2019.
[41]. Y. Luo and Y. Yu, "A Secure Data Storage System Based on IPFS and Blockchain for IoT Applications," Proceedings of the IEEE International Conference on Internet of Things and Intelligent Applications, pp. 46-50, 2019.
[42]. Y. Sun, Z. Wang, and Y. Liu, "A Secure and Scalable Decentralized Storage System Based on IPFS and Blockchain," Proceedings of the IEEE International Conference on Networking, Architecture, and Storage, pp. 132-135, 2018.
[43]. L. Li, Y. Li, and H. Li, "A Secure Data Storage and Sharing System Based on IPFS and Blockchain," Proceedings of the IEEE International Conference on Computer, Communication and Control Technology, pp. 99-102, 2020.
[44]. M. Chen, Y. Zhang, and Z. Huang, "An IPFS-based Data Storage System with Privacy Protection," Proceedings of the IEEE International Conference on Information Security and Cryptology, pp. 163-168, 2019.
[45]. J. Li, S. Zhou, and Z. Li, "A Decentralized and Secure File Sharing System Based on IPFS and Blockchain," Proceedings of the IEEE International Conference on Cyber Security and Protection of Digital Services, pp. 1-6, 2019.
[46]. H. Liu, Y. Shen, and Y. Huang, "A Secure and Efficient Data Storage System Based on IPFS and Blockchain for Cloud Computing," Proceedings of the IEEE International Conference on Cloud Computing and Intelligence Systems, pp. 77-81, 2018.
[47]. Q. Wu, L. Zhang, and Y. Sun, "A Secure Data Storage System Based on IPFS and Blockchain for Smart Grid," Proceedings of the IEEE International Conference on Smart Grid and Clean Energy Technologies, pp. 178-182, 2020.

[48]. X. Wang, S. Feng, and S. Yang, "A Distributed Data Storage System Based on IPFS and Blockchain," Proceedings of the IEEE International Conference on Internet of Things and Cloud Computing, pp. 113-117, 2018.
[49]. Z. Xu, S. Wei, and X. Wang, "A Secure and Efficient Data Sharing System Based on IPFS and Blockchain for Vehicular Networks," Proceedings of the IEEE International Conference on Vehicular Electronics and Safety, pp. 157-161, 2020.
[50]. Y. Gu, X. Zhang, and K. Ren, "A Secure Data Storage and Sharing System Based on IPFS and Blockchain for Healthcare Applications," Proceedings of the IEEE International Conference on Healthcare Informatics, pp. 78-82, 2019.
[51]. Y. Li, Z. Liu, and X. Zhang, "A Secure and Decentralized Data Sharing System Based on IPFS and Blockchain for E-Commerce," Proceedings of the IEEE International Conference on E-Commerce and Knowledge Management, pp. 1-5, 2020.
[52]. S. Park, H. Kim, and H. Kim, "A Decentralized and Secure Data Sharing System Based on IPFS and Blockchain for IoT," Proceedings of the IEEE International Conference on Advanced Communication Technology, pp. 170-173, 2018.
[53]. Y. Hu, X. Shen, and W. Yang, "A Secure and Reliable Data Sharing System Based on IPFS and Blockchain for Cloud Computing," Proceedings of the IEEE International Conference on Cloud Computing and Big Data Analysis, pp. 11-15, 2019.
[54]. Y. Wang, X. Wei, and W. Wang, "A Secure and Efficient Data Sharing System Based on IPFS and Blockchain for Supply Chain Management," Proceedings of the IEEE International Conference on Industrial Informatics and Computer Engineering, pp. 234-239, 2020.
[55]. J. Liu, W. Chen, and K. Chen, "A Decentralized and Secure Data Storage System Based on IPFS and Blockchain for Edge Computing," Proceedings of the IEEE International Conference on Edge Computing, pp. 1-6, 2019.
[56]. X. Yang, Y. Liu, and J. Tang, "A Secure and Decentralized Data Sharing System Based on IPFS and Blockchain for Mobile Crowdsourcing," Proceedings of the IEEE International Conference on Mobile Ad-hoc and Sensor Networks, pp. 123-127, 2018.
[57]. C. Wang, W. Huang, and J. Zhu, "A Secure and Reliable Data Storage System Based on IPFS and Blockchain for Data Center Networks," Proceedings of the IEEE International Conference on Data Mining and Big Data, pp. 96-101, 2020.
[58]. Y. Zhang, S. Chen, and C. Xiong, "A Decentralized and Secure Data Storage System Based on IPFS and Blockchain for Intelligent Transportation Systems," Proceedings of the IEEE International Conference on Intelligent Transportation Systems, pp. 88-93, 2019.
[59]. Y. Huang, J. Zou, and J. Wang, "A Secure and Decentralized Data Sharing System Based on IPFS and Blockchain for Smart Home," Proceedings of the IEEE International Conference on Smart Homes and Health Telematics, pp. 30-35, 2018.