INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 1118-1125

SECURE FILE STORAGE WITH BLOCKCHAIN TECHNOLOGY

Darshan kadam[1], Tanishq Dhepe[2], Nishant Dhanvi[3],

Nirbhay Kamble[4], Sayali Karmode[5]

[1,2,3,4]Student, Department of Information Technology, MGM College of Engineering and Technology, Navi Mumbai, Maharashtra, India.

[5]Faculty, Department of Information Technology, MGM College of Engineering and Technology, Navi Mumbai, Maharashtra, India.

DOI:https://www.doi.org/10.58257/IJPREMS33366

ABSTRACT

In today's digital era, safeguarding data is crucial, but traditional centralized storage systems are vulnerable to hacking and lack transparency. Enter blockchain technology, a decentralized solution offering immutable file storage. Instead of relying on a single authority, data is spread across a network, enhancing security and resilience. Each file is divided, encrypted, and distributed across multiple nodes, making tampering nearly impossible. Smart contracts automate transactions, reducing costs and increasing efficiency. Blockchain's immutable nature ensures data integrity, crucial for sensitive applications like healthcare and supply chain management. Challenges like scalability and regulation exist but are being addressed. In conclusion, blockchain file storage offers enhanced security, transparency, and trust, poised to revolutionize data management.

Keywords: Blockchain, Blockchain technology File storage, Decentralization, Data security

1. INTRODUCTION

In today's digital world, keeping data safe and organized is super important. Traditional ways of storing data in one central place have some big problems, like being easy targets for hackers and not being very transparent. That's where blockchain comes in. It's a new way of storing files that spreads them out across lots of computers instead of keeping them all in one spot. This makes it much harder for anyone to mess with the data. Blockchain also uses something called "smart contracts" to make transactions super secure and automatic. With smart contracts, people can upload files, control who gets access to them, and do all sorts of things without needing a middleman. This saves time and money.

Overall, blockchain-based file storage is a gamechanger because it's safer, more transparent, and easier to manage. It's like keeping your digital stuff in a super secure, invisible vault that you control.

A. Background

In today's digital world, we need secure and efficient ways to store data. Traditional storage systems, where all data is kept in one place controlled by one authority, have problems like being easy targets for hackers and lacking transparency. But now, there's blockchain technology. It's the tech behind things like Bitcoin, but it's being used for lots of other stuff too, including storing files. Basically, blockchain is a way of storing information across a network of computers in a super secure and transparent way.

With blockchain-based file storage, data isn't kept in one place. Instead, it's divided into tiny pieces and spread out across many computers. This makes it hard for anyone to mess with the data.

One cool thing about blockchain is smart contracts. These are like digital agreements that automatically enforce themselves when certain conditions are met. With blockchain-based file storage, smart contracts help make transactions secure and automated. Users can upload files, manage who gets access to them, and do other stuff without needing a middleman.

B. Motivation

Blockchain-based file storage is driven by the need for safer, clearer, and faster ways to manage data in today's digital world. Traditional storage systems, where all data is controlled in one place, have problems like being easy targets for hackers and not being very transparent.

Blockchain offers a different approach: it spreads data out across lots of computers instead of keeping it all in one spot. This makes it much harder for anyone to mess with the data. With blockchain, each file is broken into pieces, encrypted, and spread out across many computers.

2. LITERATEUR REVIEW

This section provides a comprehensive review of existing literature on this topic, highlighting key approaches, challenges, and opportunities identified in the research. Decentralized and Blockchain Technology

Decentralized and Blockchain Technology: In regular file storage, your stuff is usually kept in one big place controlled by one boss. If something goes wrong there, like a break-in or a computer crash, all your stuff could be lost. Plus, the boss decides who gets to see your stuff, which can lead to problems like someone snooping around or not letting you access your own things. But with decentralized storage, your stuff is spread out across many different places, like hiding your treasures in multiple secret spots. Even if something bad happens to one spot, your stuff is safe in the others. And because there's no single boss in charge, it's harder for anyone to snoop or block you from getting your stuff. This makes your things more secure, dependable, and harder to mess with.

Architecture and Protocols: The core of the project is built on a blockchain protocol. Ethereum, Hyperledger, and EOS are some popular choices. These protocols provide the necessary infrastructure for decentralized consensus, immutability, and smart contract execution. Papers by Zhenget al. (2018) and Lietal. (2020) explore P2P architectures tailored for decentralized cloud storage, focusing on aspects such as data distribution, replication strategies, and fault tolerance.

Consensus Mechanisms: Consensus is like making sure everyone agrees on something in a group. In decentralized storage systems, this is super important for keeping everything reliable and trustworthy. A person named Nakamoto came up with Proof-of-Work (PoW) back in 2008, which is like a game that computers play to agree on things in a blockchain. But PoW uses a lot of energy and can't handle too much at once. So, people started looking for other ways to agree. They found Proof-of-Stake (PoS), where people can use their cryptocurrency to help decide what's real. Another one is Delegated Proof-of-Stake (DPoS), where people choose trusted leaders to make decisions for them. Some smart folks like Buterin and Larimer wrote about PoS and DPoS to explain how they work. And recently, other researchers like Wang and Zhang have been inventing new ways for everyone to agree on stuff, especially for storing data in the cloud. They're trying to find ways that are efficient and work well for everyone involved.

Security and Privacy: Ensuring data security and privacy is paramount in decentralized storage systems. Blockchain's cryptographic primitives enable data encryption, access control, and authentication mechanisms to protect user data from unauthorized access and tampering. Research by Bonneau et al. (2015) and Miers et al. (2015) delve into the security and privacy considerations of blockchain-based storage systems, addressing challenges such as key management, data confidentiality, and privacy-preserving computations. Smart people like Bonneau and Miers have looked into how to make sure these systems are as secure and private as possible. They talk about stuff like how to manage secret codes (called keys) that protect your data, keeping your data secret so only you can see it, and doing calculations in a way that keeps your privacy safe. These are all important things to figure out to make sure your data stays safe and private in decentralized storage systems.

Scalability and Performance Optimization: Scalability remains a critical challenge in decentralized storage networks, particularly concerning transaction throughput and data storage capacity. Papers by Buterin (2018) and Wood (2014) propose scalability solutions, including sharding and layer-2 protocols, to improve the performance of blockchain networks. Moreover, research by Dong et al. (2019) and Wang et al. (2020) explores techniques for optimizing storage efficiency and reducing latency in decentralized cloud storage systems.

3. EXITING SYSTEM

The existing system for the project can be a traditional file storage and sharing system. This can include platforms such as Dropbox, Google Drive, OneDrive, and similar cloud storage services. In these systems, users can upload and store files on the cloud, and then share them with other users by granting them access to specific folders or files. This traditional file storage and sharing systems often use centralized servers to store the files, which can pose security risks such as unauthorized access to files or data breaches. Furthermore, these systems may also require users to pay for storage space, which can be expensive for large amounts of data. Another existing system for file sharing is Peer-to-Peer (P2P) file sharing. In this system, users can share files directly with each other without the need for centralized servers. P2P file sharing is often associated with illegal sharing of copyrighted material, but there are also legal P2P file sharing systems such as BitTorrent Sync, which allow users to share files securely. While traditional file storage and sharing systems and P2P file sharing have their own advantages and disadvantages, the proposed blockchain-based file storage and sharing system aims to provide a more secure and decentralized alternative.

Some systems use blockchain to store files in a safe and decentralized way. For example, File coin lets people rent out their extra storage space and earn special tokens. Blockchain ensures that files stay safe and reliable using strong math. Storj and Sia work similarly, using blockchain and peer-to-peer tech to store files across many computers. People pay with specific tokens for storing and getting files. IPFS isn't exactly blockchain-based but uses it to store files in a decentralized way. Arweave makes files permanent on the blockchain, and people pay once for it. These systems have different features and costs, so people can choose what fits their needs best.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 1118-1125

4. PROPOSED WORK

The proposed system is a blockchain-based file sharing platform that allows users to securely store and share files with others. The system leverages the immutability and transparency of blockchain technology to provide a secure and tamper-proof file storage and sharing mechanism. Each user is given a unique public key that is used to encrypt and decrypt their files. The encrypted files are then stored on the blockchain, ensuring that they are resistant to tampering or unauthorized access. To share a file, the user simply grants permission to the intended recipient, and they can access the file using their private key. The system also employs access control mechanisms to ensure that only authorized users can view or modify files. This is done using a permission- based system that is enforced by smart contracts on the blockchain. Each file has a set of permissions associated with it, and only users with the appropriate permission can access it. For example, a user can grant read-only access to a file to a colleague, but only allow them to modify the file if they have specific editing permissions. Users of the suggested system will be able to safely store and exchange files with others on a file sharing platform built on blockchain technology. The system offers a safe and impenetrable method for exchanging and storing files by utilizing the immutability and transparency of blockchain technology. A distinct public key is provided to each user, which they use to encrypt and decode their files. After that, the encrypted files are kept on the blockchain, guaranteeing that no one can alter them or view them without authorization. A file can be shared by just giving permission to the chosen recipient, who can then access it with their private key. Access control measures are also used by the system to guarantee that files can only be viewed or modified by authorized users. To do this, a permission-based

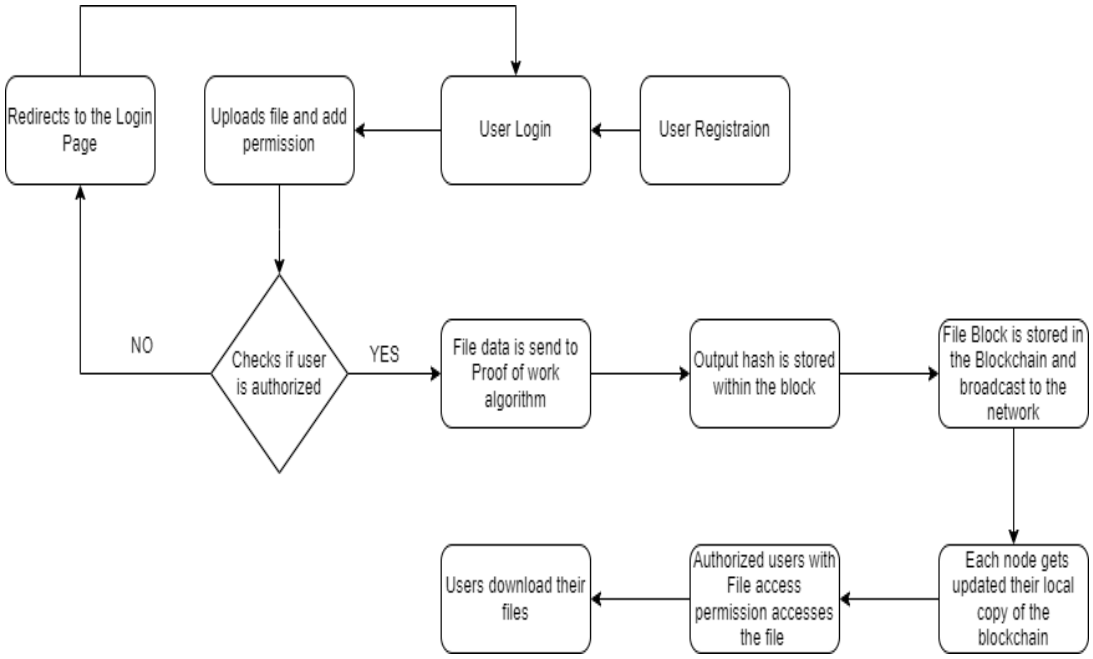

Fig 1: File Sharing System Workflow

Module 1: User Registration

In order for users to create user accounts and utilize the system's capabilities, the User Registration module is essential to the file sharing system. Typically, this module comprises of a user registration form where users fill in their email address, password, and username, among other required information. Through the registration procedure, every user is given a distinct identity within the system, making it possible for them to be identified and set apart from other users. Numerous validations and checks are carried out during the registration process to guarantee the integrity and correctness of the information submitted. The module might, for instance, verify that the email address is entered correctly or see if the username has already been occupied by another user.. Once the user registration form is submitted and the provided information is validated, the module typically stores the user data in a user database or directory. This data includes details like username, email address, password (stored in a hashed format), and other relevant information. The stored user data serves as a reference for authentication and authorization processes throughout the file sharing system. The User Registration module often goes hand in hand with additional functionalities such as account verification. After registration, users may receive a verification email containing a link or a verification code. This step ensures that the provided email address belongs to the user and helps to prevent automated account creation or misuse of the system. By completing the verification process, users confirm their ownership of the email address and activate their user account, allowing them to access the file sharing system.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 1118-1125

Module 2: Uploading File

The Uploading File module is a crucial component of the file sharing system that allows users to upload their files to the system's storage infrastructure. This module provides a user-friendly interface where users can select files from their local devices and initiate the upload process. It enables seamless and efficient transfer of files from the user's device to the system's storage. Upon selecting the file(s) for upload, the module performs various tasks to ensure the successful and secure transfer of the files. It may validate the file type, size, and other attributes to ensure compatibility and adherence to system requirements. Additionally, the module may apply data compression or encryption techniques to optimize file size and enhance security during the upload process. To facilitate the upload, the module typically utilizes a file transfer protocol or API to establish a connection between the user's device and the system's storage infrastructure. The files are transmitted over a secure network connection to protect against unauthorized interception or tampering. The module may also implement mechanisms to monitor the upload progress and provide real-time feedback to the user, such as progress bars or status notifications. Once the file upload is completed, the module stores the uploaded file in the designated storage location within the system. It assigns a unique identifier or filename to the file to ensure proper organization and future retrieval. The module may also perform additional tasks such as generating a thumbnail or extracting metadata from the uploaded file to enhance the user experience and facilitate file management. The Uploading File module is designed to simplify and streamline the process of transferring files from the user's device to the file sharing system. It provides a secure and efficient mechanism for users to upload files of various types and sizes, ensuring seamless integration with the system's storage infrastructure. This module is a fundamental component in enabling users to contribute their files to the shared repository, fostering collaboration and information exchange within the file sharing system.

Module 3: Access Control for File Access

The Access Control for File Access module is responsible for managing and enforcing access control policies to regulate the permissions and privileges granted to users for accessing shared files within the file sharing system. This module ensures that only authorized users can view, download, modify, or delete files based on predefined access rules and permissions. One of the primary tasks of this module is user authentication and authorization. Upon user login, the module verifies the user's credentials and checks their access privileges. It may authenticate users using various methods such as username-password authentication, multi-factor authentication, or integration with external identity providers. Once authenticated, the module retrieves the user's access rights and permissions from the system's database or access control lists. The module applies access control mechanisms to determine whether a user has the necessary permissions to access a specific file. It evaluates factors such as the user's role, group membership, or explicitly assigned access rights to determine the level of access granted. For example, some files may be restricted to specific user groups or require higher- level privileges for modification or deletion.

Module 4: Login - Authorization

The Login - Authorization module is a vital component of the file sharing system that handles the authentication and authorization process for users attempting to access the system. It ensures that only legitimate users with valid credentials can log in and perform authorized actions within the system. This module encompasses various security measures to protect user accounts and sensitive information. The first step in the Login - Authorization process is user authentication. Users provide their credentials, such as a username and password, which are then verified against the stored user data. This verification process may involve techniques like hashing and salting to securely store and compare passwords. Additionally, advanced authentication methods such as two-factor authentication or biometric authentication can be implemented for enhanced security. Once the user is authenticated, the Authorization aspect of this module comes into play. Authorization determines what actions and resources a user is permitted to access based on their role, privileges, and access control policies. This module checks the user's permissions and verifies whether they have the necessary rights to perform specific operations within the file sharing system, such as uploading, downloading, or modifying files. It ensures that users are limited to their assigned roles and cannot exceed their authorized boundaries.

Module 5: Proof of Work, Consensus

One essential element of the file sharing system that guarantees the security and integrity of the blockchain network is the Proof of Work (PoW) and Consensus module. It creates a process for approving and validating the insertion of fresh blocks into the blockchain. This module is based on the Proof of Work (PoW) principle, in which network participants must solve intricate computational puzzles to demonstrate their value and obtain the authority to add new blocks. Miners, or members of the network, compete to solve a computational challenge that takes a lot of time and processing power during the Proof of Work (PoW) process. The first miner to find the solution can propose a new block to the network. This solution acts as proof that the miner has dedicated computational resources to secure the network, hence the name

Proof of Work. The consensus mechanism ensures that all participants in the network agree on the validity of the proposed block. This prevents the addition of fraudulent or malicious blocks and maintains the integrity of the blockchain. In most blockchain systems, including the file sharing system, the consensus is achieved through a majority vote or agreement among network participants. Once a proposed block is validated by the consensus mechanism, it is added to the blockchain, becoming a permanent part of the distributed ledger. The PoW and Consensus module brings several benefits to the file sharing system. Firstly, it enhances the security of the network by making it computationally expensive to modify or tamper with existing blocks. The consensus mechanism ensures that a majority of the network participants must agree on the validity of a new block, making it challenging for malicious actors to manipulate the system. Additionally, the PoW mechanism encourages decentralization and fairness by rewarding miners who contribute computational power to secure the network. This helps prevent concentration of power and ensures that no single entity can control the blockchain network.

Module :6 Transaction Storage

The Transaction Storage module is a critical component of the file sharing system that handles the storage and management of all transactions recorded on the blockchain. In the context of the file sharing system, a transaction represents an action performed by users, such as uploading a file, granting file access rights, or revoking access permissions. These transactions are securely stored and organized in the blockchain, forming an immutable record of all file-related activities. The Transaction Storage module is responsible for receiving, validating, and storing incoming transactions on the blockchain. When a user performs an action, such as uploading a file or modifying access permissions, the system generates a corresponding transaction. An essential part of the file sharing system, the Transaction Storage module manages and stores every transaction that is registered on the blockchain. Within the framework of the file sharing system, a transaction denotes an action taken by users, like uploading a file, allowing access to a file, or removing access. The blockchain organizes and safely stores these transactions, creating an unchangeable record of all file-related operations. On the blockchain, incoming transactions are received, validated, and stored by the Transaction Storage module.

The system creates a related transaction whenever a user takes an action, such uploading a file or changing access permissions. This transaction contains relevant information, such as the user's identity, the file involved, and the specific action performed. The module ensures that the transaction is properly formatted, follows predefined rules, and meets the necessary validation criteria before it is added to the blockchain. Once a transaction is validated, it is stored in a block and added to the blockchain. Each block contains a set of transactions, and each block is linked to the previous block, creating a chain of blocks that form the blockchain.

This structure ensures the chronological order and integrity of the transactions. As new transactions are added, they become part of the blockchain's permanent record and cannot be altered or removed, providing an audit trail of all file-related activities. The Transaction Storage module plays a crucial role in ensuring the transparency and accountability of the file sharing system. By recording every transaction on the blockchain, it enables users to trace the history of file activities and verify the legitimacy of actions. This promotes trust among users, as they can easily verify the origin and authenticity of transactions. Furthermore, the decentralized nature of the blockchain ensures that the transaction history is distributed across multiple nodes, making it resilient to tampering or data loss.

Module :7 File Access Rights

In the file sharing system, each file is associated with a set of access rights that define the actions that can be performed on the file. These access rights may include read, write, execute, and delete permissions. The File Access Rights module manages and enforces these access rights by validating user requests and granting or denying access accordingly.

It checks the user's identity, their relationship to the file (e.g., owner, collaborator), and the requested action to determine if the user is authorized to perform the operation. Additionally, the File It enhances the system's security and accountability by providing a comprehensive record of file access and ensuring that any unauthorized or malicious activities can be identified and addressed. The File Access Rights module is like the bouncer at a party, checking if you're allowed to do what you're asking for with a file.

It looks at who you are, how you're related to the file (like if you made it or are just sharing it), and what you want to do. If you're not supposed to do it, it says no. It also keeps a diary of every time someone does something with a file, like opening it or changing it. This diary helps keep an eye on what people are doing and can catch anyone who's up to no good. It's like having a security camera at the party to see if anyone's causing trouble.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 1118-1125

Impact Factor: 5.725

5. RESULTS AND DISCUSSION

This section synthesizes the outcomes of empirical studies, theoretical frameworks, and case analyses, offering a comprehensive understanding of the state-of-the-art and future directions in Secure File storage systems.

Figure 1: Signup page

Figure 1 shows that users can enter their valid credentials to register their information in the DB, so that he/she can login to the game. The SQL commands used here are SELECT and INSERT. The SELECT command is used to check if the user is already present in the database and the INSERT command is used to insert new data into the database.

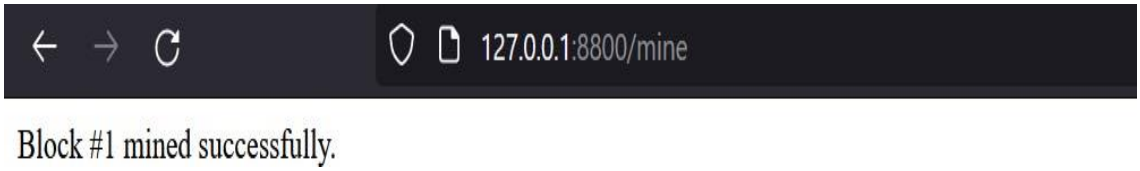

Figure 2: Signup page

Figure 2 shows that Once the user selects the users whom he/she wants to share the file will be stored along with the File Block now as soon as the User clicks the “Request to mine” button in the Navbar the file and file data in the buffer will be sent to the POW algorithm, Here it will generate the hash randomly so that it will stop generating the hash for different values of Nonce, once it finds the hash with leading three digits as zeros. After the POW runs, the successfully mined file block.

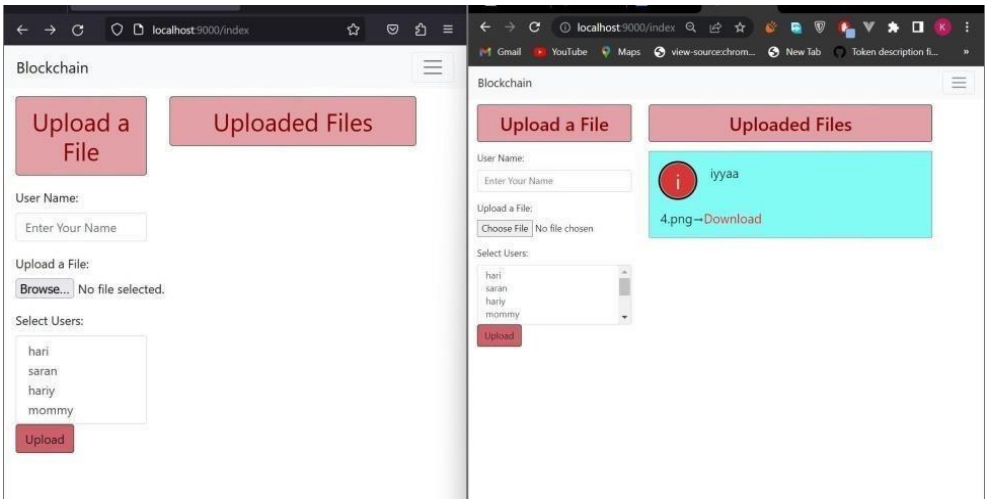

Figure 3: Mining Page

Figure 3 shows that The Mined Block will be Stored in the “127.0.0.1:8800” domain which actually has all the File blocks in a Blockchain format.

Figure 4**:** Download page

After the Successful mining of Block the files will only be available for the users who have permission. Figure 6 shows that Now users can download their files with the Download button in the files which are shown in the Uploaded Files section.

6. CONCLUSION

The implementation of a blockchain-based file storage and sharing system offers a secure and decentralized solution for users to store and share files. The system is designed with the goal of ensuring the privacy and security of user data by using encryption and access control mechanisms. The use of blockchain technology ensures that data is stored in a tamper-proof and decentralized manner, making it resistant to data breaches and other malicious attacks. The integration of REST APIs for file upload and access control allows for seamless integration between the front-end and the blockchain-based storage system. Overall, the implementation of this project demonstrates the potential of blockchain technology in solving real-world problems and offers a glimpse into the future of secure and decentralized data storage and sharing systems.

Using blockchain for storing files is a great way to make storage decentralized, safe, and easy to understand. Systems like Filecoin, Storj, Sia, IPFS, and Arweave all have their own cool ways to store files on a blockchain network. They keep your data safe and private because blockchain is super secure and spread out. These systems make sure your files stay intact and you have more control over them. As more people want safe and good storage, these blockchain systems will become even more important, giving people lots of choices for what they need.

7. REFERENCES

[1] S. Gore, S. Hamsa, S. Roychowdhury, G. Patil, S. Gore and S. Karmode, "Augmented Intelligence in Machine

[2] Learning for Cybersecurity: Enhancing Threat Detection and Human-Machine Collaboration," 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, 2023, pp. 638-644, DOI: 10.1109/ICAISS58487.2023.10250514.

[3] Layth Almahadeen, Renzon Daniel Cosme Pecho, Murugananth Gopal Raj, Nichenametla Rajesh, Zainab Mohammed Imneef, Sayali Karmode Yelpale, “Digital Investigation Forensic Model with P2P Timestamp Blockchain for Monitoring and Analysis” , Journal of Electrical System, Vol. 1, No 1, (2024): 09-17 (DOI : https://doi.org/10.52783/jes.656)

[4] Sayali Karmode, Security Challenges for IoT Based Applications & Solutions Using Fog Computing: A Survey, Journal of Journal of Cybersecurity and Information Management, Vol. 3 , No. 1 , (2020) : 21-28 (DOI : https://doi.org/10.54216/JCIM.030103)

[5] M. S. K. Yelpale, “Security and privacy challenges in cloud computing: a review,” Journal of Cybersecurity and

[6] Information Management, vol. 4, no. 1, pp. 36–45, 2020. View at: Google Scholar

[7] Sayali Karmode Yelpale, “IOT Technology for Pandemic Situation,” NJITM, vol. 4, no. 2, pp. 25–27, Jan. 2022 https://mbajournals.in/index.php/JoITM/article/view/806.

[8] Karmode, S. S., & Bhagat, V. B. (2017). DETECTION AND BLOCKING SOCIAL MEDIA MALICIOUS POSTS. International journal of modern trends in engineering and research, 4(5).

[9] Kermode, S. S., & Bhagat, V. B. (2016). A Review: Detection and Blocking Social Media Malicious Posts. Int. J. Mod. Trends Eng. Res, 3(11), 130-136. doi: 10.21884/IJMTER.2016.3133.Q4M8O .

[10] Prof. Bhushan B. Thakare, Prof. Sayali Karmode Yelpale, “Smart Home with Edge Computing,” International Journal of Interdisciplinary Innovative Research & Development (IJIIRD), Vol 6, 2021 https://ijiird.com/wpcontent/uploads/CSE016-1.pdf

[11] Sayali Karmode, “Blockchain Technology Security Issues and Concerns : A Review,” International Research

[12] Journal of Modernization in Engineering Technology and Science, Vol 6, Issue 03, March 2024 DOI https://www.doi.org/10.56726/IRJMETS50249

[13] M. Kumar and E. Walia, “Analysis of electronic voting system in various countries,” International Journal on Computer Science and Engineering, vol. 3, pp. 1825–1830, May 2011.

[14] N. Kersting and H. Baldersheim, “Electronic voting and democratic issues: An introduction,” in Electronic Voting and Democracy: A Comparative Analysis, N. Kersting and H. Baldersheim, Eds. London: Palgrave Macmillan UK, 2004, pp. 3–19.

[15] C. E. Corry, “Basic voting principles,” in Vote Fraud and Election Issues. http://www.ejfi.org/Voting/Voting.htm, 2009.

[16] P. Wolf, R. Nackerdien, and D. Tuccinardi, “Introducing electronic voting: Essential considerations,” Policy Paper, International Institute for Democracy and Electoral Assistance (IDEA), December 2011.

[17] C. Cachin and M. Vukolic, “Blockchain consensus protocols in the wild,” CoRR, vol. abs/1707.01873, 2017. [Online]. Available: http://arxiv.org/abs/1707.0187

[18] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf," 2008.

[19] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," National Institute of Standards and Technology (NIST), Internal Report 8202, October 2018. [Online]. Available: https://doi.org/10.6028/NIST.IR.8202

[20] C. Meter, "Design of Distributed Voting Systems," master's thesis, Department of Computer Science, HeinrichHeine-University Dusseldorf, ¨ September 2015.

[21] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," White Paper, 2014. [Online]. Available: https://ethereum.org/en/whitepaper/

[22] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger petersburg version," 2020. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf