International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8101
***Article Received:** 22 June 2023 **Revised:** 18 August 2023 **Accepted:** 04 September 2023*

DStore: Blockchain-Powered Decentralized Cloud Mesh

Sheetal Atul Phatangare[1], Sangita Maheshwar Jaybhaye[2], Vaishali Savale[3], Aryan Vimal[4], Avish Agrawal[5], Raghav Bajaj[6]
[1]Department of Computer Engineering, Vishwakarma Institute of Technology, Pune,India
sheetal.phatangare@vit.edu
[2]Department of Computer Engineering(Artificial Intelligence), Vishwakarma Institute of Technology
Pune, India
sangita.jaybhaye@vit.edu
[3]Department of Artificial Intelligence and Data Science, Vishwakarma Institute of Technology
Pune, India
vaishali.savale84@gmail.com
[4]Department of Computer Engineering, Vishwakarma Institute of Technology, Pune, India
aryan.vimal2001@gmail.com
[5]Department of Computer Engineering, Vishwakarma Institute of Technology, Pune, India
avishagrawal999@gmail.com
[6]Department of Computer Engineering, Vishwakarma Institute of Technology, Pune, India
bajajraghav487@gmail.com

Abstract— Data is a critical asset for any company, as well as for any individual as well, but it is also vulnerable to attack. In the last few years, we have seen an alarming increase in data breaches that have compromised millions of accounts and resulted in billions of dollars lost. But how do you protect something so sensitive? In response to this, we propose our Project. This project focuses on developing a Decentralized Cloud Storage to store and secure data. You don't access data simply specifying 'where it is' in Decentralised Cloud Storage. Instead, you define 'what it is'. Because data is distributed throughout a global network rather than being stored in a specific location, the concept of location is rendered obsolete in decentralised cloud storage.

Keywords- Blockchain, Decentralized Cloud Storage, Pinata, IPFS,AES, WEB3.

I. INTRODUCTION

The project's goal is to create a Decentralized Cloud Storage to store and safeguard data. Over Decentralized Cloud Storage, you don't access data by declaring 'where it is'. You define 'what it is' instead. Because data is disseminated throughout a worldwide network rather than being stored in a specific area, the concept of location becomes obsolete in decentralized cloud storage.

Decentralized Cloud Storage (DCS) is a groundbreaking concept that transforms the way data is stored and accessed. Unlike traditional cloud storage solutions that rely on specifying the location of data, DCS focuses on defining the content of data, rendering the concept of location obsolete. Through the use of distributed protocols and blockchain technology, data is fragmented and distributed across a global network of nodes, mitigating the risks of data loss and single points of failure. One of the key advantages of DCS is its enhanced security measures. By employing robust cryptographic techniques, data stored in the network remains highly secure against unauthorized access and tampering. This ensures that users have complete control over their data while granting access rights to others through smart contracts. As a result, DCS promotes a decentralized access control system, facilitating secure and automated data sharing between users.

Moreover, DCS ensures censorship resistance, allowing data to remain accessible even in the face of attempts at censorship. The decentralized nature of the storage network promotes data availability for users globally, regardless of any regional restrictions or limitations. Additionally, data transactions within the DCS ecosystem are recorded on an immutable blockchain, ensuring transparency and creating a tamper-proof record of data activity. Technical implementation of DCS involves the integration of blockchain technology and smart contracts. Blockchain serves as a distributed ledger, recording data transactions and access control permissions in a transparent and auditable manner. Smart contracts play a vital role in automating access management, allowing users to securely share their data with others while retaining ownership. Furthermore, DCS embraces a distributed file system protocol that fragments and stores data across various nodes. These nodes are part of a global network that collaborates to provide storage solutions. This inclusive network encourages participation from providers worldwide, fostering a diverse and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8101
***Article Received:** 22 June 2023 **Revised:** 18 August 2023 **Accepted:** 04 September 2023*

resilient storage ecosystem. The security and privacy of data within DCS are paramount. Data stored in the network is encrypted using sophisticated cryptographic algorithms, ensuring confidentiality and protection against unauthorized access. Techniques like zero-knowledge proofs provide evidence of data authenticity without revealing the actual data, reinforcing data privacy.

Hence, Decentralized Cloud Storage is a revolutionary approach to data storage and access, offering enhanced security, privacy, and scalability. By eliminating the reliance on specific data locations, DCS promotes a decentralized, secure, and censorship-resistant ecosystem that empowers users with control over their data. With global collaboration and accessibility, DCS represents a significant step forward in the evolution of cloud storage, fostering a sustainable and secure data storage landscape.

1.1 Centralized Storage System - A centralized storage system is a type of data storage architecture where data is stored and managed in a single, centralized location or server. In this system, all data is stored and accessed through a central server, and clients or users interact with the server to retrieve or store their data. In a centralized storage system, the central server acts as a single point of control and authority. It is responsible for managing and maintaining the storage infrastructure, handling data backups, enforcing access controls, and providing data services to clients. Clients or users typically connect to the central server over a network, such as the internet or a local area network (LAN), to access their data.

Advantages of Centralized Storage System:

(i) Simplicity: Centralized storage systems offer a straightforward and easy-to-manage infrastructure. Data is stored in a single location, making it simple to set up, maintain, and administer.

(ii) Centralized Control: Having a central server allows for centralized control and management of data. Administrators can enforce access controls, data policies, and backup procedures from a single point of control.

(iii) Performance: Centralized storage systems can provide high performance and low latency since all data is stored in one location. This can be beneficial for applications that require fast and direct access to data.

(iv) Centralized Backup and Recovery: With a centralized storage system, it is easier to implement backup and recovery strategies. Administrators can schedule backups, perform data restores, and ensure data integrity more efficiently.

(v) Resource Utilization: Centralized storage systems can efficiently allocate and utilize resources such as storage capacity and network bandwidth. It allows for centralized monitoring and optimization of resource utilization.

Disadvantages of Centralized Storage System:

(i) Single Point of Failure: Since all data is stored in a central server, it becomes a single point of failure. If the server experiences downtime, hardware failures, or other issues, it can lead to data inaccessibility for all users.

(ii) Dependency and Bottlenecks: Users and applications depend on the central server to access and retrieve data. This creates a potential bottleneck if there is a high volume of simultaneous data requests or if the server cannot handle the workload efficiently.

(iii) Scalability Challenges: Centralized storage systems may face challenges in scaling to accommodate growing data volumes or increasing user demands. Upgrading the central server or storage infrastructure can be costly and complex.

(iv) Data Privacy and Security Risks: In a centralized storage system, the central server has access to all the stored data, which raises concerns about data privacy and security. Unauthorized access or breaches to the central server can compromise the security of all data.

(v) Limited Flexibility: Centralized storage systems may lack flexibility in terms of deployment options and adaptability to changing needs. Modifications or reconfigurations typically require updates to the central server, resulting in potential disruptions and downtime.

1.2 Decentralized Storage System - A decentralized storage system is a type of data storage architecture where data is distributed across multiple nodes or devices rather than being stored in a central location. In this system, data is broken down into smaller pieces and stored on different nodes within a network. Each node contributes storage capacity and resources to collectively form a distributed storage network.

Advantages of Decentralized Storage System:

(i) Data Redundancy and Fault Tolerance: Decentralized storage systems distribute data across multiple nodes, ensuring redundancy and fault tolerance. If some nodes fail or go offline, data remains accessible from other available nodes, enhancing data availability and resilience.

(ii) Scalability: Decentralized storage systems can scale more efficiently by adding new nodes to the network. As the number of nodes increases, so does the storage

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8101
***Article Received:** 22 June 2023 **Revised:** 18 August 2023 **Accepted:** 04 September 2023*

capacity and performance of the system, without relying on a central server or infrastructure upgrades.

(iii) Data Privacy and Security: Decentralized storage systems prioritize data privacy and security. Data is often encrypted and distributed across nodes, reducing the risk of a single point of failure or unauthorized access. Users retain control over their encryption keys, enhancing data security.

(iv) Cost Efficiency: Decentralized storage systems can be cost-effective compared to centralized alternatives. Participants in the network contribute their excess storage capacity, eliminating the need for large-scale data centers and associated infrastructure costs.

(v) Data Ownership and Control: Decentralized storage systems empower users with greater control and ownership of their data. Users can determine how their data is stored, who has access to it, and can revoke access at any time, enhancing data sovereignty and user autonomy.

Disadvantages of Decentralized Storage System:

(i) Complexity: Decentralized storage systems can be more complex to set up and manage compared to centralized systems. Coordinating data distribution, node connectivity, and ensuring data integrity across a distributed network can require additional technical expertise.

(ii) Performance Variability: The performance of decentralized storage systems can vary based on factors such as network connectivity, node availability, and data retrieval mechanisms. Accessing data from multiple nodes may introduce higher latency compared to a centralized system.

(iii) Resource Utilization and Efficiency: In decentralized storage systems, not all nodes may contribute equal resources or have the same level of uptime. This can lead to variability in resource utilization and efficiency, requiring mechanisms to ensure balanced resource contributions.

(iv) Network Dependency: Decentralized storage systems rely on the underlying network for data access and retrieval. If the network experiences congestion or disruptions, it can impact the availability and performance of the decentralized storage system.

(v) Data Integrity and Consistency: Ensuring data consistency and integrity across a distributed network can be more challenging in decentralized storage systems. Coordinating updates, maintaining consistency, and resolving conflicts may require additional mechanisms and protocols.

1.3 Blockchain - Blockchain is a distributed digital ledger that is decentralized and distributed across several computers or nodes. It is a technology that enables secure and transparent transactions without the use of middlemen. A blockchain, at its heart, is a chain of blocks, each of which contains a list of transactions. These transactions are confirmed and uploaded to the blockchain using a consensus method that assures all parties agree on the transaction's authenticity. One of the most important characteristics of blockchain is its decentralized nature. Instead of a centralized authority, such as a bank or government, managing transactions, blockchain enables various participants, known as nodes, to keep a copy of the complete blockchain. Because no single party has complete control over the system, it is more resistant to censorship, fraud, and sabotage. Another critical feature of blockchain is its immutability. Once a block is uploaded to the blockchain, it is extremely impossible to change or delete the information contained inside it. Each block carries a unique identification known as a hash, which is produced based on the data contained within it. If the data within a block is changed, the hash of that block and all following blocks are invalidated, alerting the network of the tampering attempt.

1.4 IPFS - IPFS is an acronym that stands for Inter Planetary File System. It is a peer-to-peer distributed file system that intends to revolutionize how files are stored, viewed, and shared over the internet. Unlike typical file systems, IPFS is built on content addressing, which implies that files are recognized by their content rather than their location. Each file and all of its variants in IPFS are allocated a unique hash that is produced depending on the file's content. This hash acts as the file's address, allowing any node in the network to readily discover and retrieve it. When a file is added to IPFS, it is divided into smaller pieces, and each chunk is assigned a unique hash. These chunks are then spread around the network, and nodes can request and retrieve the chunks required to rebuild the file. One of the primary advantages of IPFS is its decentralized nature. Rather than relying on a single server, files in IPFS are stored and served by various network nodes. This not only enhances redundancy and fault tolerance, but also allows for faster and more efficient file retrieval because files can be supplied from the nearest and quickest nodes.

1.5 Pinata - Pinata is a cloud platform and service that provides decentralized file hosting and content management for projects that use the Inter Planetary File System (IPFS). It makes uploading, pinning, and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8101
***Article Received:** 22 June 2023 **Revised:** 18 August 2023 **Accepted:** 04 September 2023*

maintaining files on IPFS easier by providing a user-friendly interface and additional capabilities. Pinata enables users to upload files to IPFS while also ensuring that the files are accessible on the IPFS network. When a file is "pinned" on Pinata, it is stored and copied across numerous IPFS nodes, increasing its availability and dependability. Pinning prevents a file from being automatically deleted from the IPFS network due to a lack of popularity or brief node outage. Pinata makes dealing with IPFS easier by providing a user-friendly interface, powerful file management functions, and improved accessibility for files hosted on the IPFS network. It's popular among developers and projects looking for decentralized and distributed file hosting solutions.

1.6 P2P - P2P is an abbreviation for Peer-to-Peer. It refers to a network architecture in which computers, gadgets, or nodes communicate and interact with one another without the use of a particular server or intermediary. Each node in a P2P network has equal capabilities and can act as both a client and a server, exchanging resources and data with other nodes in the network. This permits node-to-node communication and data transfer without the requirement for a centralized authority or infrastructure. P2P networks are distinguished by their dispersed nature, in which tasks and responsibilities are spread among participating nodes. Each node contributes to the network by supplying resources like processing power, storage, or bandwidth that other nodes in the network can use.

1.7 MetaMask - It is a crypto wallet that allows users to use with Ethereum apps that are decentralized. It offers a simple interface for managing Ethereum accounts, storing cryptocurrency, and securely carrying out transactions inside the Ethereum ecosystem. MetaMask serves as a connection point between web browsers and the Ethereum network. When installed as a browser extension, it generates a user-friendly interface that allows users to establish and import Ethereum accounts, examine account balances, and transfer and receive Ethereum and ERC-20 tokens. MetaMask holds private keys securely and allows users to sign transactions and messages, assuring the security and integrity of Ethereum transactions. It offers a simple interface for confirming and approving transactions, giving users control over the movement of dollars and data inside the Ethereum ecosystem. MetaMask is critical to the adoption and use of decentralized applications on the Ethereum network. It allows users to maintain their Ethereum accounts, connect with dApps, and safely conduct transactions inside the Ethereum ecosystem in an easy and secure manner.

1.8 Ethereum - Ethereum is a platform for developers to create smart contracts, they are self driven with the conditions of the agreement put directly into the program. These smart contracts execute automatically when predefined criteria are satisfied, eliminating the need for middlemen or centralized control. The Ethereum network enables developers to create and deploy smart contracts using the Solidity programming language. Ether (ETH) is the Ethereum network's native coin. It is utilized as a means of exchange on the platform for conducting transactions and communicating with smart contracts. Users pay gas fees in Ether to compensate the network for the computational resources needed to process their transactions and execute smart contracts.

1.9 Solidity -Solidity is a programming language used exclusively for creating smart contracts on blockchain platforms, most notably the Ethereum network. Smart contracts are self-driven agreements in which the terms of the agreement are in the program itself. When certain triggers or events occur, they automatically enforce and execute the agreed-upon conditions.

1.10 Smart Contract - A smart contract is a digitalized contract that is self-driven and is stored and implemented on a blockchain. It is a computer program that implements predefined acts or provisions of an agreement automatically when certain predetermined criteria are met. Because the blockchain network enforces the terms of the contract, smart contracts eliminate the need for middlemen or trusted third parties.

1.11 AES Algorithm -AES (Advanced Encryption Standard) can be used as a cryptographic algorithm in the context of blockchain to offer safe and private transactions or data storage on the blockchain network. Blockchain technology employs encryption techniques to safeguard sensitive data and preserve data confidentiality and integrity.

1.12 ReactJS -ReactJS, sometimes known as React, is an open-source JS library for creating user interfaces. It was created and is still maintained by Facebook. React is a popular framework for developing dynamic, responsive, and interactive online applications.

II. LITERATURE SURVEY

Authors Parminder Pal Kaur, Dr. Rini Saxena, and Rohini Mahajan delve into the advantages of Decentralized storage systems and explore the practical implementation of various technologies over a network. They primarily focus on the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8101
***Article Received:** 22 June 2023 **Revised:** 18 August 2023 **Accepted:** 04 September 2023*

InterPlanetary File System (IPFS) while examining the integration and functionalities of other decentralized cloud storage technologies, including FileCoin, SiaCoin, SWARM, and Storj. Demonstrating the transformative potential of these technologies, the study showcases how a decentralized cloud storage ecosystem can revolutionize data management by enabling efficient and secure storage and sharing of data through a peer-to-peer service. This approach eliminates the need for a central authority, ensuring data integrity, accessibility, and privacy while promoting scalability and cost-effectiveness. With their research, the authors shed light on the promising future of decentralized cloud storage, empowering users with greater data control and contributing to a more resilient and secure data storage landscape across various industries and applications [1].

Authors G. Richa Shalom and Ganesh Rohit Nirogi present an innovative objective to develop a decentralized storage system using blockchain technology. The study aims to enhance data security by leveraging the AES 256-bit encryption algorithm, in conjunction with prominent technologies such as IPFS (InterPlanetary File System), Metamask, Ethereum, and DHT (Distributed Hash Table). By adopting a multi-layered approach to data security, the authors' solution ensures the privacy and integrity of user data throughout the decentralized storage ecosystem. In their implementation, the authors employ the AES 256-bit encryption technique to encrypt and share data among multiple peers within the system. This encryption process guarantees the utmost privacy and protection of sensitive information, safeguarding it from unauthorized access or tampering. The integration of IPFS enables efficient and distributed storage of data, where files are divided into smaller chunks and distributed across a global network of nodes. This approach eliminates the reliance on a central server, mitigating the risk of single points of failure and enhancing data availability[2].

In research paper titled "Proposed Model for Secured Data Storage in Decentralized Cloud by Blockchain Ethereum," authors present a comprehensive and innovative model to address the critical issue of secure data storage in a decentralized cloud environment using the Ethereum blockchain. Recognizing the growing importance of data security in today's digital landscape, the authors propose an integrated approach that harnesses the inherent features of blockchain technology to enhance data security, integrity, and accessibility. The proposed model capitalizes on the transparency and immutability of the Ethereum blockchain to create a tamper-proof and auditable ledger for storing data transactions. This ensures data integrity, as any changes to the stored information are recorded, making it resistant to unauthorized alterations. By leveraging Ethereum's smart contract functionality, the model introduces robust access control mechanisms, empowering users to securely share and manage their data while retaining full control over their privacy and ownership rights[3].

In paper titled "Blockchain-Based Decentralized Cloud Solutions for Data Transfer," authors propose a pioneering approach to address data transfer challenges in cloud environments using blockchain technology. The paper explores the potential of blockchain in creating decentralized cloud solutions that enhance data security, efficiency, and transparency during data transfer processes. The authors emphasize the significance of blockchain's inherent features, such as transparency, immutability, and decentralization, to create a tamper-proof and auditable ledger for data transfer transactions. By leveraging blockchain's consensus mechanisms, the proposed model ensures data integrity and prevents unauthorized alterations during data transfer operations. The paper introduces innovative solutions that utilize smart contracts to automate and enforce data transfer rules, enabling secure and efficient data sharing between parties. Smart contracts streamline the data transfer process, reducing the need for intermediaries and ensuring transparent and traceable data exchange. Furthermore, the authors explore the integration of decentralized cloud technologies to optimize data transfer performance. By distributing data across a global network of nodes, the proposed model enhances data availability, resilience, and redundancy, providing a robust and reliable data transfer ecosystem. In conclusion, the paper presents a comprehensive exploration of blockchain-based decentralized cloud solutions for data transfer. The proposed model harnesses the capabilities of blockchain technology, smart contracts, and decentralized cloud networks to create a secure, transparent, and efficient data transfer framework. The authors' work contributes valuable insights to the evolving landscape of data transfer solutions, paving the way for more secure and efficient data sharing in cloud environments[4].

In their paper titled "Blockchain-Based Decentralized Cloud Storage," authors G. Abinaya, Preksha Kothari, Alex Pavithran KP, Manasi Biswas, and Farheen Khan propose a novel approach to cloud storage using blockchain technology. The paper explores the potential of blockchain to create a decentralized cloud storage system that enhances data security, accessibility, and availability. The authors emphasize the key features of blockchain, including transparency, immutability, and decentralization, as the foundation of their proposed decentralized cloud storage solution. By leveraging blockchain's tamper-proof and auditable ledger, the model ensures data integrity, preventing unauthorized modifications or deletions. Smart contracts play a pivotal role in the proposed system, enabling secure data sharing and access control. The authors use smart contracts to automate and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8101
***Article Received:** 22 June 2023 **Revised:** 18 August 2023 **Accepted:** 04 September 2023*

enforce data transfer rules, ensuring transparent and efficient data exchange between users [5].

In their paper "Decentralized Cloud Storage Using Blockchain," authors M. Shah, M. Shaikh, V. Mishra, and G. Tuscano propose a groundbreaking methodology that revolutionizes data storage and access. Introducing Decentralized Cloud Storage (DCS), the approach distributes data across a global network of nodes, rendering single points of failure obsolete, while ensuring enhanced data availability and resistance to censorship attempts. By integrating blockchain technology, the methodology ensures transparency and tamper-proof data records, fortified by advanced cryptographic techniques that safeguard data security and privacy. Smart contracts automate access management, enabling secure data sharing while granting users complete ownership control. The methodology's scalability ensures seamless handling of increasing data demands, promoting a sustainable storage solution that empowers users with a decentralized and secure alternative to traditional centralized cloud storage models [6].

The paper "BlockStore: A Secure Decentralized Storage Framework on Blockchain" introduces the BlockStore framework, a novel decentralized storage approach built on blockchain technology by S. Ruj, M. S. Rahman, A. Basu, and S. Kiyomoto. Leveraging blockchain's transparency and immutability, the framework ensures data security, privacy, and availability through tamper-proof records of data transactions. By eliminating single points of failure and distributing data across a global network of nodes, BlockStore enhances data reliability and censorship resistance. Advanced cryptographic techniques protect data integrity, while smart contracts automate access management, granting users ownership control during secure data sharing. The framework's scalability and empowering potential make it promising for various applications, contributing valuable insights into decentralized storage systems, and revolutionizing data storage paradigms [7].

In their paper titled "Enhancing Security of Data in Cloud Storage using Decentralized Blockchain," R. Pise and S. Patil propose a method to bolster data security in cloud storage by leveraging decentralized blockchain technology. The authors present an innovative approach that enhances data protection, privacy, and integrity through the use of blockchain's transparency and immutability. By eliminating single points of failure and distributing data across a decentralized network, their method ensures greater resilience against potential security breaches. Advanced cryptographic techniques are employed to safeguard data integrity and protect sensitive information, while smart contracts facilitate access management, allowing users to maintain ownership control during secure data sharing. The authors' work contributes valuable insights into enhancing cloud storage security and presents a promising step towards a more robust and trustworthy data storage infrastructure [8]. In their paper titled "Decentralized Storage System based on Blockchain Technology," authors Yan Zhu, ChunliLv, Zichuan Zeng, Jingfu Wang, and Bei Pei propose an innovative approach to decentralized storage using blockchain technology. The paper explores the potential of blockchain in creating a secure and resilient decentralized storage system that addresses the challenges of data security, availability, and ownership. The authors emphasize the fundamental features of blockchain, including its transparency, immutability, and distributed nature, as the foundation of their proposed decentralized storage solution. By leveraging blockchain's tamper-proof and transparent ledger, the model ensures data integrity and cuts the need for a central governing authority, enhancing data ownership and control for users. The study focuses on the use of smart contracts in the decentralized storage system to automate access management and data sharing. Smart contracts enable secure and efficient data transactions, facilitating seamless data sharing between users while maintaining data privacy. Moreover, the paper discusses the benefits of decentralized storage in terms of data availability and resilience. By distributing data across a network of nodes, the model minimizes the risk of data loss and improves data accessibility, even in the face of network disruptions. In conclusion, the paper presents a promising blockchain-based approach to decentralized storage, offering a secure, transparent, and efficient storage system. By harnessing blockchain's features, smart contracts, and decentralized architecture, the authors' work contributes valuable insights to the field of decentralized storage solutions. The research offers a potential path to addressing data security and ownership concerns, paving the way for more robust and user-centric data storage solutions in the future [9].

The authors of the paper "Securing Resources in Decentralised Cloud Storage," E. Bacis, S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, M. Rosa, and P. Samarati, give a detailed analysis on strengthening resource security in decentralized cloud storage systems. The study investigates the difficulties and potential vulnerabilities in decentralized cloud storage environments and suggests unique ways to maintain resource confidentiality, integrity, and availability. The authors stress the significance of safeguarding resources in decentralized cloud storage, where data is dispersed across a network of nodes, which introduces new security challenges. They go over how to use cryptographic techniques like encryption and digital signatures to properly protect data and manage access. The study describes a secure data transfer and retrievecontrol technique based on attribute-based encryption that allows for fine-grained resource access management. This

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8101
***Article Received:** 22 June 2023 **Revised:** 18 August 2023 **Accepted:** 04 September 2023*

method ensures that only authorized individuals with certain attributes have access to specific data, boosting data privacy and reducing data exposure to unauthorized entities. Furthermore, the authors investigate the use of blockchain tech. to enhance resource safety. The proposed system provides an immutable record of data transactions and access control policies by using blockchain's tamper-proof and transparent characteristics, assuring transparency and accountability. The study describes a strong method for safeguarding resources in decentralized cloud storage systems. The authors' work presents a possible answer to the security difficulties faced in decentralized cloud environments by merging cryptographic techniques with attribute-based encryption and blockchain technology. The study adds to the realm of information forensics and security by establishing the framework for more safe and trustworthy decentralized cloud storage systems in the future [10].

III. METHODOLOGY

Blockchain:

We investigate the scenario in which a certain someone tries to establish an alternate chain quicker than the original chain. Even if this is achieved, it does not permit the attacker to make modifications to the system, such as stealing money that did not belong to the person. Nodes will not allow illegitimate transactions as payment and correct nodes will never accept a block that has them. A certain someone can only attempt to modify one of his own transactions in order to get value that he has spent. A BRW can be used to represent the race between the original chain and an attacker chain. The original chain expands by 1 block, extending its lead by 1, and the attacker's chain grows by 1 block, reducing the gap by -1. The potential of an attacker emerging from a certain less is akin to the problem of the Gambler's Ruin. Assume a backer with unlimited credit begins with a deficit and attempts an endless number of trials to break even. The chance that he will ever reach breakeven, or that an attacker will ever catch up to the honest chain, can be calculated as follows:

x = chance an original node discovers the next block.
y = the certain someone's chances of discovering the next block
p = the possibility of the attacker catching up from z blocks behind

$$p = \begin{cases} 1, & if x \le y \\ \left(\frac{y}{x}\right)^2, & if x > y \end{cases} \quad (1)$$

Given that y > x, the likelihood decreases exponentially as the attacker clears more barriers. The odds are stacked against him, and unless he makes a fortuitous surge front beforehand, his chances will dwindle as he falls evenlate. We now check the durationof a new agreement'sreceiver must wait before being satisfied that the sender cannot change the agreement. We assume the sender is a certain someone who wants to trick the receiver into thinking he paid him for the time being before switching it back . If this occurs, the receiver will be notified, but the sender wants it to be very late. Shortly before signing, the receiver generates a new value-pair and sends the key to the sender. This prohibits the sender from building a chain of blocks beforehand by working on it indefinitely until he get far enough ahead to complete the transaction. Following the transaction's transmission, the dishonest sender secretly begins working on a rival chain with a different type of his transaction. The beneficiary must wait until the agreement is assigned to a block and linked to z blocks. He doesn't know how far a certain someone has gotten, but assuming the true blocks take the mean expected time per block, the certain someone's progress will be a Poisson distribution with the expected value:

$$\lambda = z\frac{y}{x} \quad (2)$$

To calculate the likelihood of the certain someone catching up presently, multiply the Poisson density for every value of advance he could have made by the chance of catching up from that moment:

$$\sum_{i=0}^{\infty} \frac{\lambda^i e^{-\lambda}}{i!} \cdot \begin{cases} \left(\frac{y}{x}\right)^{z-i} & if i \le z \\ 1 & if i > z \end{cases} \quad (3)$$

Rearranging according to our need...

$$1 - \sum_{i=0}^{z} \frac{\lambda^i e^{-\lambda}}{i!} \cdot \left(1 - \left(\frac{y}{x}\right)^{z-k}\right) \quad (4)$$

With increasing *i*, the likelihood decreases exponentially.

Advanced Encryption Standard (AES):

AES is an electronic data encryption specification developed in 2001 by the NIST. Despite being more harder to create, AES is widely utilized today due to its superior strength than DES and triple DES.

The algorithm employs polynomials from the field G.F.(2^8) modulo the polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. The complete intricacies are beyond of this class, but a way for sorting out all of the processes required to execute AES will be provided, along with some fundamental mathematical explanations. The algorithm does 10 loops for 128-bit AES. It does 12 loops of 192-bit AES encryption. It does 14 loops for 256-bit AES. Only the 128-bit will be covered in depth.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8101
***Article Received:** 22 June 2023 **Revised:** 18 August 2023 **Accepted:** 04 September 2023*

Consider having a 128-bit node divided into 16 bytes, labeled $l_{0,0}$, $l_{1,0}$, $l_{2,0}$, $l_{3,0}$, $l_{0,1}$, $l_{1,1}$, $l_{2,1}$, $l_{3,1}$, $l_{0,2}$, $l_{1,2}$, $l_{2,2}$, $l_{3,2}$, $l_{0,3}$, $l_{1,3}$, $l_{2,3}$, and $l_{3,3}$. These 16 bytes can be represented as four four-byte columns, with the 1st 4 elements in column 1, the 2nd4 elements in column 2, and so on.

$l_{0,0}$	$l_{0,1}$	$l_{0,2}$	$l_{0,3}$
$l_{1,0}$	$l_{1,1}$	$l_{1,2}$	$l_{1,3}$
$l_{2,0}$	$l_{2,1}$	$l_{2,2}$	$l_{2,3}$
$l_{3,0}$	$l_{3,1}$	$l_{3,2}$	$l_{3,3}$

Fig 1. (a)

Repeat what follows for 10 loops:

1) Replacement bytes:
Look up the substitute for each of the sixteen bytes in the s-box replacement diagram, making the new state matrix$l_{0,0}$, $l_{1,0}$, $l_{2,0}$, $l_{3,0}$, $l_{0,1}$, $l_{1,1}$, $l_{2,1}$, $l_{3,1}$, $l_{0,2}$, $l_{1,2}$, $l_{2,2}$, $l_{3,2}$, $l_{0,3}$, $l_{1,3}$, $l_{2,3}$, and $l_{3,3}$.This s-box was built by combining math inverses mod g(x) in the G.F.(2^8). We will just search up each substitute value for our purposes.
2) Move rows:
Do a periodic left shift of i bytes for the rows. This results in the matrix displayed below.

$l_{0,0}$	$l_{0,1}$	$l_{0,2}$	$l_{0,3}$
$l_{1,1}$	$l_{1,2}$	$l_{1,3}$	$l_{1,0}$
$l_{2,2}$	$l_{2,3}$	$l_{2,0}$	$l_{2,1}$
$l_{3,3}$	$l_{3,0}$	$l_{3,1}$	$l_{3,2}$

Fig 1. (b)

3) Combine columns:
Accumulate the state matrix by the matrix shown below:

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

Fig 1. (c)

4) This is not ordinary multiplication; it is multiplication in the previously specified field. Furthermore, instead of adding the 4items in each functioning, they are ⊕ together. Multiplying by 01 results in the identity, but accumulating by 03 results in the identical result as multiplying by 01 and 02 and ⊕ the two outputs. Finally, the thing that is to be done is multiplying by 02: To multiply a byte by 02, follow these steps: 1) Make a one-bit shift to the left. 2) If the original value's left-most bit was a 1, delete it and ⊕ the remaining 8 bits from step 1 with 00011011.

5) Add Cycle Key:
At the end of each loop, the state matrix is simply⊕ with the key for that round.

The Methodology consists of four major components:

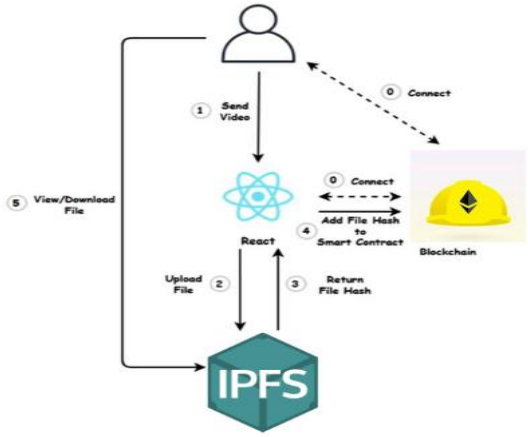

Fig 2. System Architecture

1. Smart Contract Backend: The project's foundation is a smart contract, developed in Solidity language, acting as the backend for storing user and image addresses. Smart contracts are similar to classes in Java, but they execute under specific conditions and agreements. The smart contract enables secure access to uploaded files by authorizing users with permission to access the data. Through the contract, users are assigned specific privileges, ensuring controlled and secure access to the stored images.
2. Ethereum Network and MetaMask Integration: To execute the smart contracts, the project utilizes the Ethereum network, which employs its native cryptocurrency, Ether, to carry out the contract operations. When an image is uploaded, an Ethereum transaction takes place, and the details of these transactions are tracked. Users interact with the Ethereum network through their MetaMask wallets, which play a pivotal role in confirming payment in Ether during image upload. The MetaMask wallet maintains a ledger of all transactions, allowing for efficient tracking of file uploads and monitoring of users with access to the files.
3. Pinata Cloud and IPFS Protocol: After the transactions are executed, the uploaded images are stored on the Pinata cloud. Pinata is an NFT management service that facilitates the implementation of the IPFS (InterPlanetary File System) protocol. IPFS is used for storing the images over

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8101
***Article Received:** 22 June 2023 **Revised:** 18 August 2023 **Accepted:** 04 September 2023*

a P2P-network. In this network, multiple users, known as peers, hold parts of the uploaded file. The pinata returns a unique hash-value representing the address of the image, ensuring efficient and decentralized storage of data.

To begin our project, we must first go to the Pinata website and create a Pinata account. After we've made an account, we can access our dashboard and find our API key and secret API key. Because these credentials are required for authenticating our queries to the Pinata API, we must keep them secure and avoid disclosing them publicly. We've decided to employ Node.js on the backend and React.js on the frontend as part of our project configuration. On the server side, Node.js will enable us interact with the Pinata API, while React.js will be in charge of providing a user-friendly interface to engage with the IPFS features. Because we picked Node.js for our backend, we utilize the axios or package to make HTTP queries to the Pinata API. React.js does not require any extra libraries for API connectivity on the frontend because we can use the native fetch API.

We can now make HTTP queries to the Pinata API endpoints using Node.js on the backend and React.js on the frontend. We will authenticate these queries by including our API key and secret API key in the Authorization header of our HTTP requests. On the server side (Node.js), we will use the pinFileToIPFS endpoint with a POST request and include the file data in the request body to upload files. We may develop a form on the frontend (React.js) where users can select files to upload. We will utilise the pinByHash endpoint with a POST request and supply the IPFS hash of the content we want to pin to pin content both on the server-side and frontend.To maintain a pleasant user experience and proper application functionality, manage API replies and failures on both the server-side and frontend. When dealing with the Pinata API, we handle both successful and unsuccessful answers on the frontend (React.js). Displaying suitable messages to users will assist them in understanding the consequences of their actions.

4. As a user initiates the upload of an image, the system will immediately initiate the AES encryption process. Before the image data leaves the user's device, it undergoes encryption using a unique encryption key, which may be derived from the user's account credentials or a temporary session key. The AES encryption process transforms the raw image data into an unintelligible ciphertext, rendering it indecipherable without the corresponding decryption key. This ensures that even if a malicious actor attempts to intercept or eavesdrop on the data transmission, they would only encounter the encrypted ciphertext, making it practically impossible to extract any meaningful information.The use of AES encryption during transmission provides an additional layer of protection, bolstering the safety of the system. It mitigates the risk of data interception and unauthorized access during transit, safeguarding the privacy of the user's images. As the encrypted data travels across the network to the decentralized cloud storage platform, it remains secure and immune to potential attacks.Upon reaching the cloud storage platform, the encrypted image is stored in its secure and immutable state, thanks to the underlying blockchain technology and IPFS protocol. The combination of AES encryption, blockchain, and IPFS ensures that the user's data is guarded at every stage of the process, from the point of initiation to its secure storage in the decentralized network.In the user-friendly web interface, the user's encrypted images can be seamlessly retrieved and decrypted when accessed by authorized users. Only those with the appropriate decryption key will be able to view the images in their original form, further reinforcing data privacy and user control over their stored content.
5. Web Interface with React.js: To implement all the functionalities mentioned above, the project incorporates a user-friendly web interface. The web interface is built using React.js, providing a seamless and interactive platform for users to interact with the decentralized cloud storage system. Through this interface, users can upload and manage their images securely, access authorized files, and monitor transaction history, all while enjoying a smooth and intuitive user experience.

IV. RESULTS AND DISCUSSION

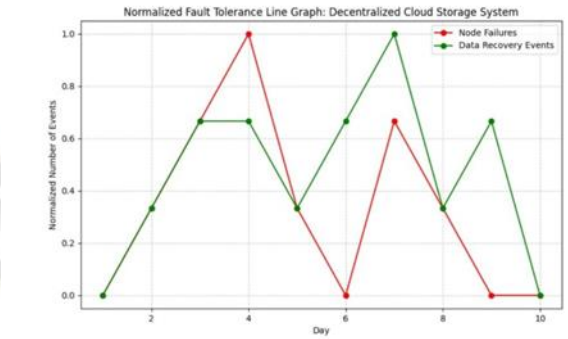

Fig. 3 Normalized Fault Tolerance Graph

The fault tolerance graph showed above tracks the behavior of nodes in our decentralized system. It detects node failures, allowing administrators to respond swiftly and mitigate their impact. The graph also assesses data recovery time after node failures, offering insights into system resilience and efficiency in restoring data access. The data has been normalized to eliminate the impact of different scales of measurement for each parameter, making it easier to compare and interpret the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8101
***Article Received:** 22 June 2023 **Revised:** 18 August 2023 **Accepted:** 04 September 2023*

data accurately. By understanding node health and recovery patterns, we were able to strategically plan maintenance and upgrades without disrupting critical operations.

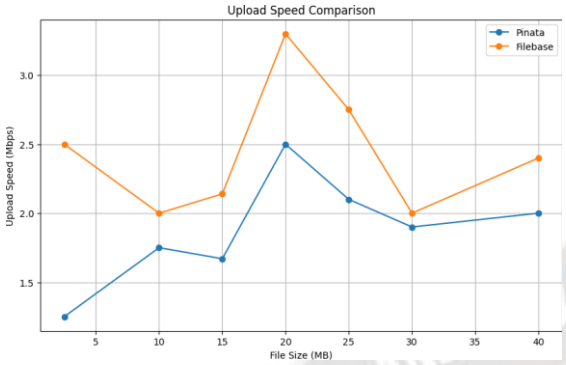

Fig. 4 Comparison of IPFS based storage system

The above graph is a comparison between Pinata(made use in our project) and Filebase, both IPFS-based decentralized storage systems on the basis of upload speed (mbps).The time taken for uploading was calculated manually and divided by the file size to normalize the data since upload speeds vary according to internet speed. While neither system follows a consistent pattern, our system tends to exhibit decreasing upload speeds with larger file sizes, whereas Filebase displays a mix of speed increases and decreases varying across file sizes. These variations stem from the complex interplay of network conditions, optimization strategies and the decentralized nature of IPFS networks. The graph underscores the importance of considering factors beyond mere upload speed, such as data redundancy, retrieval speed, and overall user experience, when selecting a storage system. We have made the use of Pinata in our project. Pinata stood out with its high data redundancy, cost-effectiveness, and low to moderate latency compared to Filebase. Pinata's fine-grained user access control enhances security, while its high scalability and global accessibility make it a versatile choice. Notably, Pinata's utilization of blockchain technology bolsters security measures and makes our system far superior than Filebase.

Attributes	Our System	Filebase
Data Redundancy	Low	High
User Access Control	Fine-grained	Limited
Accessibility	High	Moderate
Scalability	Global Reach	Limited
Security(Blockchain)	Utilizes Blockchain for enhanced security.	Not Utilized

Fig. 5 Parametric comparison between Filebase and our system

V. CONCLUSION

The project aimed to implement blockchain technology to create a decentralized storage system, moving away from centralized solutions. By leveraging Blockchain's security features, such as immutability and cryptography, the project seeks to enhance data security and protect against breaches. Transparency was prioritized by recording all transactions on the blockchain, fostering trust and accountability. Our platform's objective is to enable data sharing exclusively with authorized individuals or entities through access controls, emphasizing user privacy and control. Overall, the project aims to provide a safer, more secure, transparent, and user-centric approach to data storage and sharing. By harnessing blockchain's capabilities, the platform ensures that data remains tamper-proof, transparent, and resilient. It empowers users with greater control over their information, minimizing the risk of data breaches and unauthorized access. The user-centric approach enhances trust and confidence in the system, making it an attractive alternative to traditional centralized storage solutions. As the project materializes, it has the potential to offer a transformative and future-proof solution to the challenges of data security and privacy in the digital age. In addition to bolstering data security, the project aims to foster a sense of trust and transparency among users. With all transactions and data modifications recorded on an immutable blockchain, users can easily verify the history of data changes and track the origin of shared information. This transparency not only enhances accountability but also facilitates auditability and compliance with regulatory requirements.

REFERENCES

[1] Parminder Pal Kaur, Dr. Rini Saxena and Rohini Mahajan: A Comprehensive Study of Decentralized Cloud Storage Platforms-A Review.

[2] G. Richa Shalom, Ganesh Rohit Nirogi: Decentralized Cloud Storage Using Blockchain.

[3] Nabeel Khan, Hanan Aljoaey, Mujahid Tabassum, Ali Farzamnia, Tripti Sharma and Yew Hoe Tung: Proposed Model for Secured Data Storage in Decentralized Cloud by Blockchain Ethereum.

[4] Rajit Nair, Syed Nasrullah Zafrullah, P. Vinayasree, Prabhdeep Singh, Musaddak Maher Abdul Zahra, Tripti Sharma, and Fardin Ahmadi: Blockchain-Based Decentralized Cloud Solutions for Data Transfer.

[5] G. Abinaya, Preksha Kothari, Alex Pavithran KP, Manasi Biswas, Farheen Khan: Block Chain Based Decentralized Cloud Storage.

[6] Kumar P., P. ., Amala Bai, V. M. ., & Prasad Krishnamoorthy, R. . (2023). State-Of-The-Art Techniques for Classification of Breast Cancer Using Machine Learning and Deep Learning Methods: A Review. International Journal of Intelligent Systems and Applications in Engineering, 11(4s), 222–241.

Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2649

[7] M. Shah, M. Shaikh, V. Mishra and G. Tuscano, "Decentralized Cloud Storage Using Blockchain," 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), Tirunelveli, India, 2020, pp. 384-389, doi: 10.1109/ICOEI48184.2020.9143004.

[8] S. Ruj, M. S. Rahman, A. Basu and S. Kiyomoto, "BlockStore: A Secure Decentralized Storage Framework on Blockchain," 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), Krakow, Poland, 2018, pp. 1096-1103, doi: 10.1109/AINA.2018.00157.

[9] R. Pise and S. Patil, "Enhancing Security of Data in Cloud Storage using Decentralized Blockchain," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 161-167, doi: 10.1109/ICICV50876.2021.9388521.

[10] Yan Zhu, ChunliLv, Zichuan Zeng, Jingfu Wang, Bei Pei: Decentralized Storage System based on Blockchain Technology.

[11] Prof. Romi Morzelona. (2017). Evaluation and Examination of Aperture Oriented Antennas. International Journal of New Practices in Management and Engineering, 6(01), 01 - 07. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/49.

[12] E. Bacis, S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, M. Rosa and P. Samarati, "Securing Resources in Decentralized Cloud Storage," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 286-298, 2020, doi: 10.1109/TIFS.2019.2916673.

[13] Juan Benet: IPFS - a comprehensive case study.

[14] Benjamin Johnson: Decentralized Social Networks.

[15] John Smith, Emily Johnsons, Michael Lee: Enhancing Security of Data in Cloud Storage using Decentralized Approach and Blockchain Technology.