Review

Blockchain Based Information Retrieval System: A Survey

Sidrah Kaleem , Humaira Ashraf * , NZ Jhanjhi *

Posted Date: 21 December 2023

doi: 10.20944/preprints202312.1667.v1

Keywords: Blockchain, IPFS, Cloud Computing

Review

Blockchain Based Information Retrieval System: A Survey

Sidrah Kaleem [1], Humaira Ashraf [1,*] and NZ Jhanjhi [2,*]

[1] Departement of computer science and Information Technology, International Islamic University Islamabad; sidrah.mscs1145@iiu.edu.pk
[2] School of Computer Science, SCS, Taylors University, Subang Jaya, Malaysia
* Correspondence: Humaira.ashraf@iiu.edu.pk (H.A.); noorzaman.jhanjhi@taylors.edu.my (N.Z.J.)

Abstract: One of the most popular developments today that potentially address security issues with cloud computing is the use of blockchain. Blockchain is a decentralized data management platform that offers data integrity, security, and anonymity without the involvement of a third party. This work presents a comprehensive study of blockchain-based data storage system and their security concerns with their solutions to address these concerns. We provide a thorough overview of how blockchain is used in the cloud computing model to provide security services, and we examine the research trends of blockchain-related technologies in the current cloud computing models. As we examine, we also quickly look into how cloud computing may impact blockchain, particularly the performance enhancements that cloud computing may offer. This paper performs a review of the cutting-edge investigations of the blockchain-based system with a selfish-mining attack and the primary focus on IPFS. We also note their challenges, open issues, and future directions. The findings demonstrate that blockchain offers a productive platform in this area. However, one of the most significant problems that still need more research is security-related issues. The article offers a platform for future research and action as well.

Keywords: Blockchain; IPFS; Cloud Computing

1. Introduction

One of the most essential needs in the computer age is data storage. Direct-connected storage is being replaced by network-based storage technologies to address the increase in data volume. With time, new technologies are being used to update the storage infrastructure. Technology has evolved as a result of an increase in data volume. Blockchain is frequently used as a secure means to store data, including account information, trading history, and others. Every data that is saved in a blockchain is sealed and cannot be modified once it has been saved.

Blockchain technology has revolutionized the way data is stored and managed. The decentralized and immutable nature of blockchain makes it an ideal solution for secure data storage and sharing. Blockchain-based storage systems are gaining popularity due to their ability to provide secure, decentralized, and cost-effective storage solutions. Blockchain technology is a sophisticated method for storing data in a distributed manner that cannot be changed once it has been saved. This might result in problems including disagreements over governance, network dispersion, and a lack of accountability. In Blockchain, all data copies must be consistent which arises scalability issues in the system. Since the cloud server is centralized, it becomes difficult to access data while maintaining data security using blockchain. If the model fails, the entire cloud server will become unavailable.

As a result, we suggest a decentralized blockchain-based design for the storage system. Each person in decentralized distributed systems is in charge of their data. There is no requirement for a third party while storing or transferring data. Distributed storage systems must include incentives for users to maintain the system to become decentralized. Furthermore, it is even harder to maintain security in these distributed storage systems. Each person is responsible for their data, and the system must guarantee complete user security. Figure 1 demonstrates the blockchain structure.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1667.v1

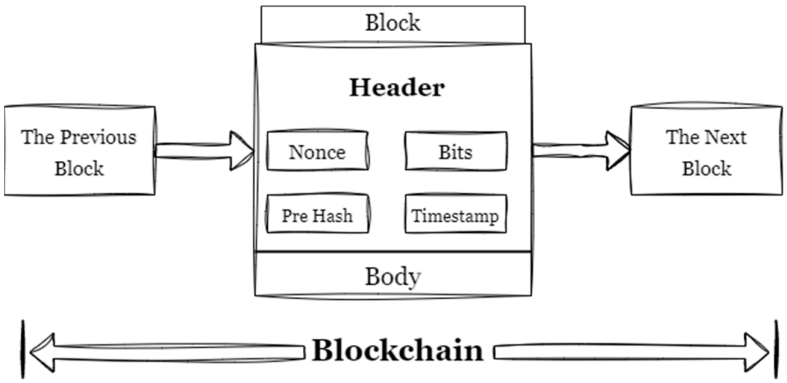

Figure 1. Structure of the Blockchain.

We consider InterPlanetary File System (IPFS) as our storage platform to address this issue. A unique hash is assigned to each stored block via the decentralized storage protocol IPFS, which was created to combat excessive redundancy. The user can then retrieve the relevant block using the hash address. Decentralization makes IPFS immune to zero points of failure. IPFS is a peer-to-peer, distributed file-sharing system, and these qualities set it apart from more established centralized file systems. Using IPFS, it is possible to track versions of a file through time and the file can be moved around the network by the users who are on the network. Data is accessible with IPFS even if the storage site crashes since it employs content-based addressing rather than location-based addressing.

The [1] reviewed different open issues and challenges of blockchain concerning distributed file systems. It includes scalability issues, privacy and security issues, application issues and big data issues. [2] focused on accessibility while maintaining the privacy of the electronic health record stored in the blockchain environment. [3] This study presents a thorough analysis of blockchain-based storage systems and their operational principles and then compares them with cloud-based storage networks. [4] reviews the different applications of blockchain technology for securing cloud storage. The fundamental components of blockchain-based distributed cloud storage solutions are analyzed based on several factors. In the exploration of Blockchain-Based Information Retrieval Systems, our survey draws upon the foundational insights presented in [23–36].

Table 1 presents a summary of the existing surveys of blockchain based storage technologies. The motivation of the current surveys is stated in the brief. Additionally, the contrast between the existing surveys and this research study is also presented.

Table 1 makes it clear that there are several gaps in the current research surveys. The surveys do not offer thorough critical and comparative analysis, nor are they presented in a structured manner. The most robust methods for storing data in blockchain environments such as IPFS and Swarm-based systems are not covered by the surveys provided. To contribute to the field and fill in the gaps in the current surveys, we have created this thorough literature review. The latest techniques and cutting-edge methodologies for saving data in blockchain are presented in this work.

Table 1. Summery of Surveys of Blockchain Storage Technologies.

Year	Main Focus	Major Contribution	Developments in Paper
2020	Focusing on blockchain based distributed file system	[1] reviewed DF systems IPFS and Swarm, the advantages and disadvantages of these systems are listed along. However, the solution of scalability issue and incase of malicious attack is not discussed	Our survey provides a thorough analysis of the literature as well the solution of the gaps identifies in the scheme
2020	Review different blockchain standards for management of storing data of EHRs.	[2] presented the review of the existing models which stores the medical records on blockchain.	Our Research presents the comprehensive critical analysis of all the systems.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1667.v1

		However, the drawbacks of each system not specified.	
2020	Survey on various decentralized storage networks	[3] presented distributed file and storage systems. Furthermore, the solution of the issues of the systems are not discussed. Also, the presented survey was not systematic.	Our survey presents a detailed systematic literature review of all the existing methods of blockchain file systems. Moreover, solutions are specified for future research.
2020	Systematic literature review on blockchain-based cloud storage applications	[4] The pros and cons of existing cloud storage technologies and blockchain-based studies are discussed. However, there was neither a critical analysis of schemes nor a quality assessment of research articles.	A thorough critical analysis of all present systems is provided in our survey. Research limitations and challenges are also mentioned.

The need for Blockchain innovation and the importance of its use have sparked ongoing research in many academic and practical fields. Although it is only currently undergoing initial testing [4]. This Systematic Literature Review goal is to identify gaps in the research on the storage and security of data in the blockchain. To determine the research gap, A protocol for searching was created, and papers published in the last three years (2020, 2021, 2022, and 2023) were chosen for the protocol. Also, four databases (IEEE, Scholar, Springer, and Elsevier) and synonyms for each phrase were searched. White papers and review papers were not included, and repeatedly printed publications in all strings were also omitted. For inclusion, all papers from journals were included, and papers were selected on the bases of title and abstraction. The fundamental components of blockchain-based distributed cloud storage solutions are analyzed based on several factors.

This System literature review explores the concept of blockchain-based storage systems and their potential benefits and drawbacks. It will delve into the technical aspects of how blockchain-based storage systems work and compare them to traditional storage systems. Additionally, several methods will investigate the potential use cases for blockchain-based storage systems and examine the challenges that need to be addressed for wider adoption. This also explained the comprehensive critical analysis of the various existing systems, Later the critical analysis, the SLR presented a detailed performance analysis of the existing methodologies. Lastly, this SLR finalizes that many researchers have presented different techniques based on different objectives. Various methods were presented based on the accessibility, performance, scalability and security of the data. By the end of this paper, the reader will have a comprehensive understanding of blockchain-based storage systems and their potential impact on the future of data storage on blockchain and its management.

The following key topics are discussed in this survey article:

1. An overview of blockchain and IPFS technology is briefly highlighted and analyzed.
2. The benefits and drawbacks of existing cloud storage blockchain-based studies are discussed.
3. The blockchain-based cloud storage applications are explored e.g., IPFS.
4. The fundamental components of blockchain-based distributed cloud storage solutions are analyzed based on a-various factors.

Figure 2 illustrates the organization of the paper in the form of a block diagram.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1667.v1

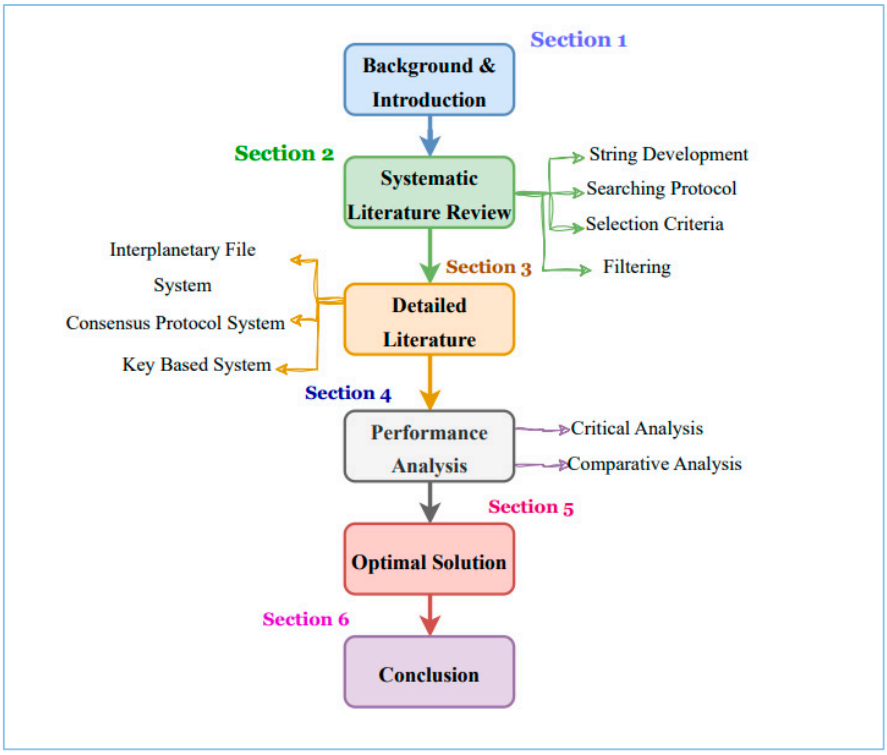

Figure 2. Paper Organization.

The structure of this article is as follows: Section 2 discusses the process for the systematic literature review, Comprehensive literature review is presented in Section 3, and performance analysis is presented in Section 4. Based on the critical analysis and comparison analysis. The final section, Section 6, offers conclusions after Section 5 analyses the ideal options.

2. Systematic Literature Review

The systematic literature review includes data and conclusions from other writers that are analyzed about one or more predetermined research topics. This can be accomplished using a variety of research methodologies, including a systematic literature review. The criteria should be clearly outlined before the review is undertaken and the systematic review should adhere to a clearly defined process or plan.

Initially, a search methodology was created, then systematic searches were carried out by it. These searchers were guided by strings that were created by the determined study question. Afterward, all of the searches were categorized using a search method. Also, research publications were screened based on their title, abstract, and objectives as well as included based on their inclusion criteria.

2.1. String Development

The strings were developed by using the synonyms of each keyword. Research Question is **"How to provide scalability and security in blockchain based information retrieval systems?"**. There will be three strings developed according to the research question using various synonyms of each keyword.

Table 1 displays that the word "Blockchain" and "Information Retrieval" has been used to find the synonyms and made different strings. Furthermore, we also used the string interplanetary file system as this system is closed to our research question.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1667.v1

Table 2. Synonyms of each Strings.

Word	Synonym 1	Synonym 2	Synonym 3
Blockchain	Distributed ledger	Digital ledger	Immutable ledger
Information Retrieval	Information Retrieval	Information Retrieval	Information Retrieval
Storage system of distributed ledger			
Information retrieval system of digital ledger			
Immutable ledger of information retrieval system			
Data storage system of blockchain based technology			
Searching protocol of blockchain based technology			
Blockchain based search engine system			

Table 1 presents the different strings with synonyms used to get the research articles across numerous databases. These databases are Scholar, Elsevier, IEEE and Springer.

2.2. Searching Protocol

A protocol for searching was created, and papers published in the last three years (2020, 2021, 2022, and 2023) were chosen for the protocol. Also, four databases (IEEE, Scholar, Springer, and Elsevier) and synonyms for each phrase were searched.

Figure 1 presents the search strategies. The strings created using research questions and 27 paper was selected from IEEE database, 33 papers selected from scholar, 18 papers from Elsevier, 25 papers from Springer.

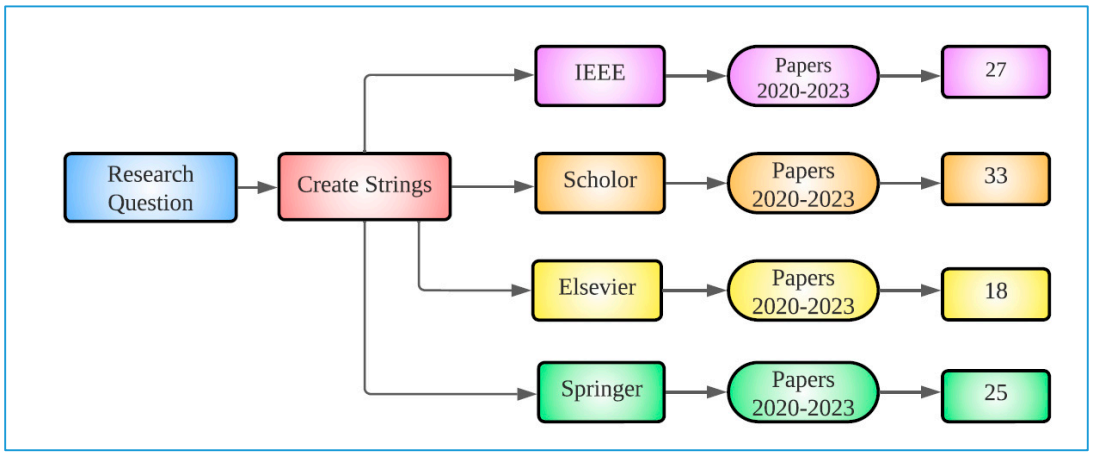

Figure 3. Searching Protocol.

2.3. Selection of Publication

A number of criteria, which are detailed in the various sections below, were used to determine which publications to include in the systematic literature review:

2.3.1. Inclusion Criteria

The qualities or qualifications that potential research subjects must possess in order to be included in the study are known as inclusion criteria. Demographic, clinical, or regional factors are frequently used as inclusion criteria.

An inclusion criterion was made according to which all papers from journals were included. The latest articles over the time span of last three years (2020-2023) are chosen for this study.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1667.v1

2.3.2. Exclusion Criteria

Exclusion criteria are traits used to determine which potential research subjects should not be included in a study. These can also be the factors that cause individuals to leave a study after being first enrolled.

In this research study, the review papers were not included. Those papers which are not yet published are not included.

Notation Table

Following Table 2 explains the Definitions, proper spelling, capitalization, and punctuation of commonly used abbreviations and acronyms.

Table 2. Notation & Definition.

Acronyms.	Definition
PBFT	Practical Byzantine Fault Tolerance
SBFT	Synchronous Byzantine Fault Tolerance
IPFS	Interplanetary File System
MOOCs	Massive Open Online Courses
ELRs	Electronic Learning Records
MIPSA	Multi-Platform Interoperable Scalable Architecture
VANET	Vehicular Ad-Hoc Network

2.4. Filtering

Filtering is the capability to significantly reduced the scope of the search and lesser the number of results returned makes methodological filters interesting. Following are the processes in filtering:

- Title-based Filtering
- Abstract-based Filtering
- Object-based Filtering
- Technique-based Filtering

2.4.1. Title Based Filtering

Title-based filtering was the initial stage of the filtering process. All publications that did not address the issue at hand were removed from the databases that were chosen.

Figure 2 shows the title-based filtering. It clearly shows the number of research papers selected which are related to our research question. Total 34 papers were selected after title-based filtering.

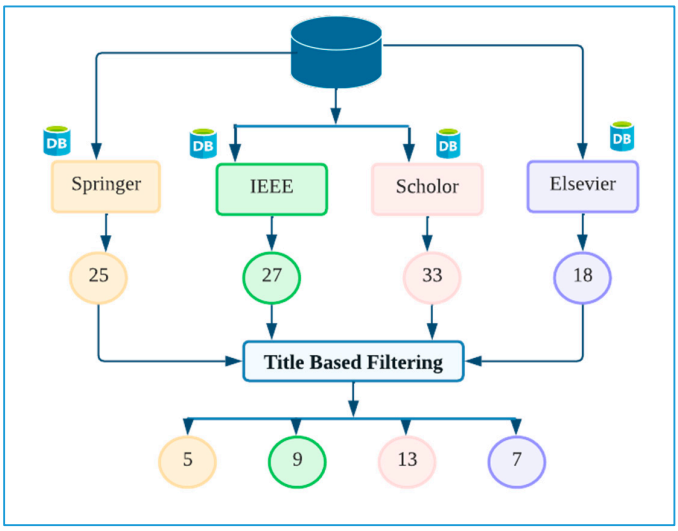

Figure 2. Title-Based Filtering.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1667.v1

2.4.2. Abstract Based Filtering

Abstract-based filtering was done in the second section. All of the chosen databases did not include any papers whose abstracts did not address the issue.

2.4.3. Objective Based Filtering

In the third part of filtering, we performed objective based filtering. All the papers that are irrelevant are filtered according to their objectives.

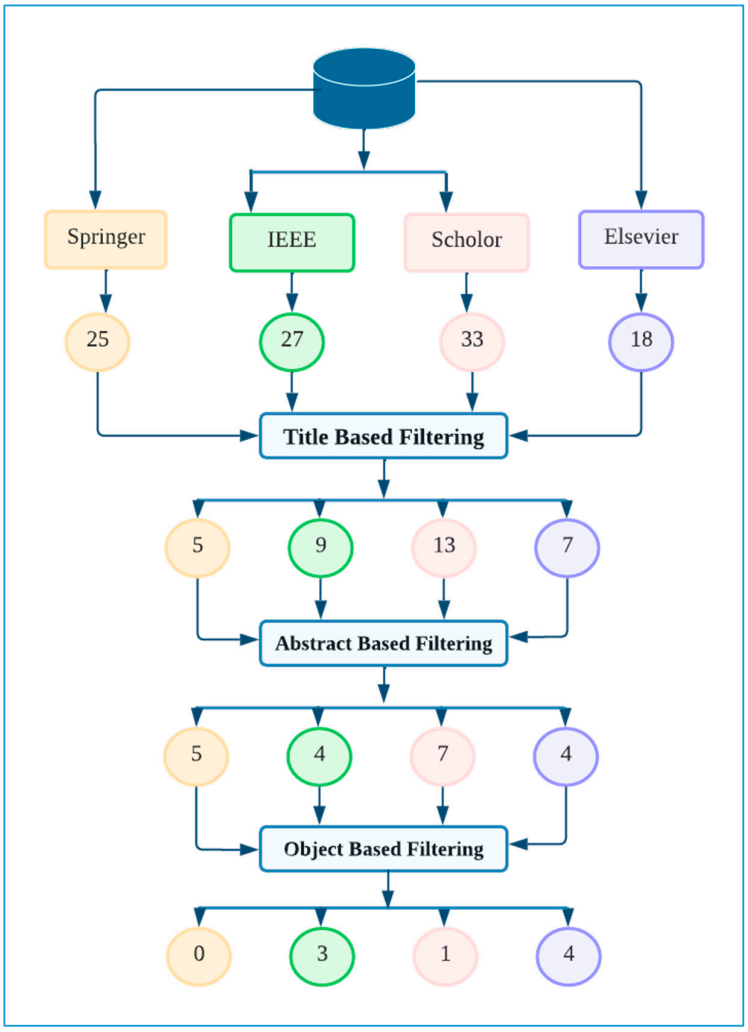

Figure 3. Object-Based Filtering.

Figure 3 shows that the steps of how each phase is done step by step. The paper selected after title-based filtering is 34 afterwards the abstract based filtering was done. In the last the object-based filtering was done, 08 research studies selected as their objectives matched with the research question.

2.4.4. Technique-Based Filtering

In technique-based filtering, it involves using specific techniques or tools to filter, analyze, and interpret research data. It is a systematic and objective approach to analyzing research data, aimed at identifying relevant information and patterns.

The Table 3 is shows about the techniques and different protocols used in the research papers. There are many techniques which are same like consensus algorithm and IPFS because of the blockchain technology.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1667.v1

Table 3. Techniques used in research paper.

Research Papers	Techniques
[4]	Meta-Key protocol, Public-Key and Symmetric-Key Encryption
[5]	IPFS, Advanced Encryption Standards
[6]	Consensus mechanism
[7]	IPFS
[8]	Advanced Encryption Standards Algorithm
[9]	Consensus Protocol
[10]	IPFS, Advanced Encryption Standards
[11]	Consensus Protocol, practical Byzantine fault tolerance (PBFT)

The research work of [4] presents a novel approach to secure data sharing in a decentralized environment. The authors propose a protocol that combines blockchain technology and decentralized storage to achieve secure and efficient data sharing. One of the strengths of the paper is its clear and concise presentation of the proposed Meta-Key protocol. The authors provide a detailed description of the protocol, including its key components, such as the meta-key management mechanism and the data access control mechanism. They also explain how the protocol can be used to ensure secure data sharing in various scenarios, such as data sharing among different organizations.

The [5] focuses on secure storage and access of electronic medical records (EMRs) using blockchain and IPFS (InterPlanetary File System) technology. The authors propose a secure and efficient method of storing and accessing EMRs, which ensures data confidentiality, integrity, and availability. They propose a four-layered architecture consisting of a data layer, a blockchain layer, a storage layer, and an access layer to achieve secure storage and access of EMRs.

The authors then provide a detailed description of each layer of their proposed architecture and the various mechanisms employed to ensure security and efficiency. They also provide a performance evaluation of their proposed system and compare it with existing approaches.

The study [6] provides a comprehensive taxonomy for blockchain-based distributed storage technologies, which is a highly relevant and timely topic given the growing interest and adoption of blockchain technology in various domains. The paper starts by providing an overview of the state-of-the-art in blockchain-based distributed storage technologies, highlighting the different approaches and architectures used by various systems. The authors then propose a taxonomy for categorizing these systems, which consists of six main categories: 1) Data Access Mechanisms, 2) Consensus Mechanisms, 3) Security Mechanisms, 4) Storage Mechanisms, 5) Performance Metrics, and 6) Application Domains.

The [7] presents an interesting study that proposes a novel approach for secure event storage in vehicular ad-hoc networks (VANETs). The authors propose the use of blockchain and interplanetary file system (IPFS) technologies to ensure secure and decentralized storage of event data, while also incorporating an authentication protocol to prevent unauthorized access. It explains the importance of event data in VANETs and the need for secure and reliable storage solutions.

Moreover, the authors then provide a brief overview of blockchain and IPFS technologies, highlighting their benefits and limitations. The proposed system architecture is then presented, which includes the use of blockchain-based smart contracts and IPFS for event storage and retrieval, and an authentication protocol based on digital signatures.

The authors conducted a simulation-based performance evaluation of their proposed system and compared it with a traditional centralized event storage solution. The results demonstrate the effectiveness of the proposed approach in terms of security, reliability, and scalability. The paper also includes a discussion of the limitations and future research directions.

The [8] proposed the decentralized storage systems, such as InterPlanetary File System (IPFS), to store and retrieve data in a decentralized manner. This helps to ensure that data is stored securely and can be accessed by authorized parties only. They also used use consensus mechanisms, such as proof of work or proof of stake, to ensure the validity and consistency of the blockchain-based cloud

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1667.v1

storage system. This helps to prevent malicious attacks and ensures that the data stored in the system is secure and reliable.

The [9] worked on novel blockchain-based solution for secure storage and sharing of Massive Open Online Courses (MOOCs) learning materials. The paper aims to address the security and privacy concerns associated with traditional MOOCs platforms by leveraging blockchain technology using the consensus algorithm.

The paper shows its innovative solution to a pressing problem in the field of MOOCs. The MOOCsChain scheme offers several advantages over traditional MOOCs platforms, such as improved security, privacy, and transparency. The authors provide a detailed description of the architecture and design of the MOOCsChain scheme, highlighting the different components and their functions.

This paper [10] proposes the challenges of centralized cloud storage, such as the risk of data breaches and the high costs of storage and maintenance. The authors then propose their solution of decentralized cloud storage using blockchain and explain how it works. They describe the architecture, which includes a network of nodes that store data in a distributed manner and use blockchain for data authentication and access control.

The authors also provide a detailed analysis of the performance and security of their proposed system through simulations and experiments. The results show that their approach is highly efficient and secure, with low latency and high throughput. The proposed system provides several benefits, including security, privacy, and efficiency, and the performance evaluation demonstrates its effectiveness. With some improvements in the areas mentioned above, this paper has the potential to be a significant reference in the field of decentralized cloud storage using blockchain technology.

In the proposed system of [11] provides an interesting solution for the problem of verifying data consistency in decentralized cloud storage systems. The authors propose the use of a blockchain-based consensus algorithm to verify the consistency of data stored across multiple nodes in a decentralized cloud storage system.

The authors present the proposed solution, which involves the use of a blockchain-based consensus algorithm to verify the consistency of data stored across multiple nodes in a decentralized cloud storage system. The proposed algorithm uses a distributed ledger to store a record of all transactions in the system, which allows for easy verification of data consistency. They provide a detailed description of the proposed algorithm and explain how it can be implemented in a decentralized cloud storage system. The authors also present simulation results that demonstrate the effectiveness of the proposed algorithm in ensuring data consistency.

Table 4 present the objectives of the research papers that were identified and their top priority to achieve these targets. These categories include data consistency, scalability, reliability, efficiency and data security.

Table 4. Objectives of the research articles.

Papers	Consistency	Reliability	Efficiency	Security	Scalability
[4]	✓	✓	✓	-	-
[5]	-	✓	-	✓	-
[6]	-	-	✓	✓	-
[7]	✓	✓	-	-	-
[8]	✓	✓	-	✓	✓
[9]	-	✓	✓	✓	-
[10]	-	-	-	✓	-
[11]	-	✓	✓	-	✓

There are many techniques like IPFS and Consensus protocol which are commonly used is in the research studies. Consensus protocol includes the multiple protocols like proof of work or proof

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1667.v1

of stake were being used. In addition to that there is a hash table used in almost every selected article in order to get the blockchain based secure environment system.

The Table 4.1 also shows the techniques and methods used in these research studies. It clearly defines the common protocols and processes used in different research articles to gain the objectives.

Table 4.1. Common Techniques Table.

Papers	Meta-Key Protocol	AES Algorithm	Consensus Protocol	Identity	Anonymity	IPFS
[4]	✓	-		-		-
[5]	-	✓	-	-		✓
[6]	-	-	✓		✓	-
[7]	-	-	-	-		✓
[8]		✓	-	-		✓
[9]	-	-	✓	-		-
[10]	-	-	✓	-		✓
[11]	-	-	✓	-		

2.5. Detailed Literature

The main aim of all the papers was to store and secure the data in the blockchain based environment.

2.5.1. InterPlanetary File System (IPFS) Based System

The **[5]** use advanced encryption standards (AES) to encrypt the EMRs, which ensures the confidentiality and integrity of the data. It also uses hashing to generate a unique identifier for each EMR. The hash of the EMR is stored on the blockchain, which ensures that the EMR cannot be tampered with. The InterPlanetary File System (IPFS) to provide a decentralized and redundant storage system for the encrypted EMRs. This ensures that the data is available even if some nodes in the network fail.

In **[7]** the blockchain technology used for secure and immutable event storage in VANETs, providing a decentralized and transparent storage solution. The IPFS method for decentralized event sharing in VANETs, enabling efficient and reliable event dissemination among vehicles. Furthermore, the authentication protocol for the proposed technique to ensure security and privacy features such as authentication, confidentiality, and integrity.

The article **[10]** used Advance Encryption Standard (AES) to encrypt the file because it needs to be highly secure. It used for protecting sensitive data in financial transactions, securing communications in networks, and encrypting stored data in databases. The IPFS peer to peer file transfer protocol is used to save the users data. The uploaded data is duplicated on three peers in order to achieve high availability and dependability of the data.

2.5.2. Consensus Protocol Based System

In the article **[6]** the author develops a taxonomy for blockchain-based storage systems, categorizing them based on their storage mechanism, data structure, consensus mechanism, and security and privacy features. They review and analyze various blockchain-based storage systems that have been proposed in the literature, classifying them based on their storage mechanism, data structure, consensus mechanism, and security and privacy features. Also, analyze various

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1667.v1

blockchain-based storage systems based on the classification scheme they developed, providing a detailed comparison of these systems and their strengths and weaknesses.

The **[8]** worked on a blockchain technology to store data in a decentralized and transparent manner, ensuring data security and privacy. Used advanced encryption algorithm for encryption decryption. They proposed the optimization algorithm for data validation, ensuring the integrity of data stored in the blockchain-based distributed ledger. It also uses a smart contract for automating data retrieval, providing an efficient and reliable method for accessing stored data.

The research article **[9]** discusses the components of the proposed scheme, including a blockchain-based distributed ledger, a consensus algorithm for data validation, and a smart contract for automating data sharing. The authors also provide a detailed description of the implementation and evaluation of the proposed scheme, including the use of simulation tools and performance metrics.

In this study the consensus mechanism is summarized as:

1) To complete the PoW (Proof-of-Work) algorithm, a hash must meet a predetermined threshold.
2) PoS (Proof-of-Stake) has been presented as a solution to the problem of energy usage in PoW.
3) Practical Byzantine Fault Tolerance (PBFT) enables quick consensus.

The research article **[11]** main objective is to maintain the data consistency and eliminate the factors which affects the data. It uses the diverse type of blockchain called the practical Byzantine fault tolerance subclass of blockchain. In contrast to existing broad blockchain algorithms, the synchronous Byzantine fault tolerance (SBFT) algorithm proposed in this research offers a significantly higher efficiency. Byzantine fault tolerance (BFT) and PBFT are compared with SBFT in a modest cloud-based system.

2.5.3. Key Based Protocol System

The article **[4]** proposes a secure data-sharing protocol that utilizes a blockchain-based decentralized storage architecture. The protocol combines several techniques and methods to ensure data privacy, security, and efficiency. The Meta-Key protocol uses a combination of public-key and symmetric-key encryption techniques to protect the confidentiality and integrity of the shared data. The protocol uses a distributed key management system that enables secure and efficient management of cryptographic keys for data encryption and decryption.

The Meta-Key protocol utilizes a blockchain-based decentralized storage architecture that ensures data is stored in a secure and tamper-proof manner. The decentralized storage architecture provides a higher level of security and privacy compared to traditional centralized storage systems. Meta-Key employs a distributed data-sharing and retrieval mechanism that enables authorized parties to securely and efficiently access shared data.

The Table 5 presents the summery of methodologies of blockchain based information retrieval system. The schemes or techniques used in the related research studies along their methods and implementations are described.

Table 5. Summery of Methodology.

Ref.	Scheme	Methodology
[4]	Meta-Key Protocol	It uses a combination of public-key and symmetric-key encryption techniques. where the user's private key protects data decryption keys that are kept in a blockchain as part of the metadata.
[5]	Encryption Algorithm with InterPlanetary File System (IPFS)	It uses advanced encryption to encrypt the EMRs. Then the InterPlanetary File System (IPFS) to provide a decentralized storage system for the encrypted EMRs. After that the doctor decrypts the ciphertext with its own secure private key and obtains the original medical records.

[6]	Blockchain-based distributed storage technologies	The aim to provide a taxonomy that can help researchers, developers, and practitioners understand the different types of Blockchain-based distributed storage technologies and their characteristics.
[7]	InterPlanetary File System (IPFS)	In the blockchain mechanism it presents a protocol for securing event information and vehicle authentication. Then to get the information securely from the interplanetary file system (IPFS).
[8]	Advanced Encryption Algorithm and optimization algorithm	For authentication and key generation techniques used AES. Then saves the data in blockchain structure and apply the optimization algorithm to minimize the time complexity.
[9]	Consensus Algorithm	This algorithm uses two sub-methods 1) PoW (Proof-of-Work) algorithm is done by finding a hash that matches a target threshold. 2) PoS (Proof-of- Stake) for the purpose of reduce the energy consumption
[10]	Advanced Encryption Algorithm and IPFS	This scheme is used to encrypt the file because it needs to be highly secure. It used for protecting sensitive data in financial transactions, securing communications in networks, and encrypting stored data in databases. The IPFS peer to peer file transfer protocol is used to save the users data.
[11]	Practical Byzantine Fault Tolerance (PBFT)	This method is the special type of blockchain and it enables quick consensus. The objective of using this is to maintain the data consistency and eliminate the factors which affects the data.

2.6. Critical Review

The paper [4] presents an interesting and innovative approach to secure data sharing in a decentralized environment. The authors use a series of experiments to demonstrate the efficiency and security of the Meta-Key protocol. The experiments show that the protocol can achieve fast data access while ensuring data security and confidentiality.

However, there are also some limitations to the paper. One potential limitation is that the proposed protocol relies heavily on the blockchain technology, which may not be practical in all scenarios. As they rely on secret keys to encrypt and decrypt the data, which can be difficult to manage and secure. If the keys are lost or stolen, the data may become inaccessible or compromised. Additionally, the paper does not address the scalability issues that may arise when using a blockchain-based decentralized storage architecture. [12]

The Meta-Key protocol proposed by the authors shows great potential for practical applications, and the thorough evaluation of the protocol adds credibility to the research. However, further research is needed to address the limitations of the protocol and to explore its potential applications in different scenarios.

The research paper [5] presents a comprehensive and well-structured approach to secure storage and access of EMRs using blockchain and IPFS technology. The proposed architecture appears to be well-designed, with various security mechanisms to ensure confidentiality, integrity, and availability of data. The performance evaluation also indicates that the proposed system is efficient and can handle a large volume of data.

Though, there are some limits of the research paper that need to be addressed. First, the authors do not provide a detailed discussion of the potential challenges associated with the adoption and implementation of their proposed system in real-world healthcare settings. Second, the authors do not provide a thorough discussion of the potential privacy concerns associated with the use of blockchain technology for EMR storage.

The decentralized nature of IPFS can make it challenging to manage and govern the network, which could impact its long-term viability and sustainability. This could potentially lead to issues such as governance disputes, network fragmentation, and lack of accountability. Since IPFS relies on

 doi:10.20944/preprints202312.1667.v1

the availability of network nodes to provide content, there is a risk that content may not be available if nodes hosting the content go offline or become unavailable. This could potentially impact the accessibility of important data or information. [13]

The [6] paper's strengths lie in its comprehensive coverage of the topic and its clear and well-organized taxonomy, which provides a useful framework for researchers and practitioners interested in blockchain-based distributed storage technologies. The taxonomy is well-structured, and the authors provide a detailed description of each category, highlighting the key features and characteristics of each.

But the paper also has some boundaries that need to be addressed. One of the limitations is that the authors do not provide a detailed evaluation of the different systems or technologies discussed in the paper. While the taxonomy is useful, it would have been more beneficial if the authors had included a critical evaluation of the different approaches, highlighting the strengths and weaknesses of each.

Furthermore, the paper does not discuss some of the more recent developments in the field, such as the emergence of decentralized storage networks (DSNs), which represent a promising alternative to traditional blockchain-based distributed storage systems. Including such developments would have provided a more complete picture of the state-of-the-art in blockchain-based distributed storage technologies. As different blockchain-based storage solutions have their own protocols and standards, it can be difficult to transfer data between different systems. This can limit the usefulness of these technologies for applications that require data sharing and collaboration between multiple parties. [14]

Overall, [6] is a valuable contribution to the field of blockchain-based distributed storage technologies. It provides a comprehensive taxonomy that can serve as a useful framework for researchers and practitioners, although it could have been strengthened by providing a more detailed evaluation of the different systems and including more recent developments in the field.

The paper [7] provides a well-researched and well-presented approach for secure event storage in VANETs. The use of blockchain and IPFS technologies is a novel and effective solution to the challenges of secure and decentralized event storage. The authors' simulation-based evaluation provides empirical evidence of the effectiveness of their proposed system. However, the study could benefit from more comprehensive real-world experiments to validate the results further.

One area where the paper could be improved is in its clarity of presentation. Some of the technical details are not adequately explained, making it challenging for readers without an in-depth knowledge of the subject matter to understand fully. Additionally, the paper could benefit from more detailed discussions of the limitations of the proposed system and potential future research directions.

In conclusion, we can say that it is a valuable contribution to the field of secure event storage in VANETs. The proposed approach is innovative, and the simulation-based evaluation provides evidence of its effectiveness. With some improvements in clarity of presentation and more extensive experimentation, this paper has the potential to be a significant reference in this field.

In [8] the author examines the various challenges associated with decentralized storage, including issues related to data privacy, security, and scalability. The author presents a balanced view of the challenges and benefits of decentralized storage solutions and suggests ways to mitigate these challenges.

The article could benefit from more detailed discussion of potential drawbacks or limitations of the proposed architecture. For example, the article briefly mentions that the use of blockchain technology could result in slower processing times and higher energy consumption, but it does not go into detail on how these issues could be addressed. Additionally, the article could provide more information on the potential challenges of implementing such a decentralized architecture in practice. Some consensus protocols, such as proof of work, can be slow and require a lot of computational power to function. This can result in slower transaction times and higher energy consumption. PFS is still a relatively new technology, and its network currently has limited bandwidth. This can result in slow download times and lower performance compared to traditional centralized systems.

 doi:10.20944/preprints202312.1667.v1

Moreover, it provides a comprehensive overview of decentralized storage solutions, their benefits and challenges, and offers insightful analysis and evaluation of each type of solution. The article is a valuable resource for anyone interested in understanding the potential of decentralized storage solutions and their applications.

The paper [9] presents an innovative solution to the security and privacy concerns associated with traditional MOOCs platforms. However, the paper has several limitations that need to be addressed. One of the limitations is the lack of evaluation of the proposed solution. While the authors provide a detailed description of the MOOCsChain scheme, they do not provide any experimental results or performance evaluation of the system. This makes it difficult to assess the practicality and effectiveness of the proposed solution.

Furthermore, the authors do not discuss the potential scalability issues associated with blockchain-based solutions. MOOCs platforms typically serve a large number of users, and blockchain-based solutions may not be able to handle the scale and performance requirements. The authors could have provided more insights into how the MOOCsChain scheme addresses these scalability issues. Nevertheless, the lack of evaluation and discussion on scalability issues limits the practicality and effectiveness of the proposed solution.

The paper [10] presents an innovative solution for decentralized cloud storage using blockchain technology. The authors' approach offers several benefits, including data privacy, security, and efficiency. The performance evaluation demonstrates the effectiveness of the proposed system in terms of scalability, reliability, and security.

However, the paper could be improved in several areas. Firstly, the authors could have provided more detailed information about the challenges of centralized cloud storage and the limitations of existing solutions. Secondly, the paper could benefit from a more comprehensive discussion of the potential limitations and drawbacks of the proposed system, including the scalability and cost of running a large-scale decentralized storage network.

Additionally, the paper could be improved by providing more detailed technical information on the implementation of the proposed system. While the paper provides a good high-level overview of the architecture, it could be difficult for readers without a deep technical background to understand the implementation details.

The paper [11] provides a detailed overview of the proposed blockchain-based consensus checking mechanism, which involves creating a decentralized network of nodes that can validate data and ensure its authenticity. The mechanism employs a combination of smart contracts, cryptographic algorithms, and blockchain technology to achieve consensus among the nodes.

One notable limitation of the paper is that it assumes a certain level of familiarity with blockchain technology, which may be challenging for readers who are not well-versed in the field. It would have been useful for the authors to discuss the scalability of the proposed algorithm and how it might perform in larger, more complex cloud storage systems. Another limitation of consensus protocols is their vulnerability to attacks. For example, in a Proof of Work protocol, an attacker with a significant amount of computational power can perform a 51% attack, which can compromise the integrity of the system. Similarly, in a Proof of Stake protocol, an attacker with a significant amount of stake can perform a similar attack. [15]

Additionally, the paper only focuses on the consensus checking mechanism and does not provide an in-depth analysis of other aspects of cloud storage systems, such as data privacy or security. The author could have explored alternative consensus algorithms and compared their effectiveness to the proposed blockchain-based solution.

Overall, the article presents an interesting solution to the problem of data consistency in decentralized cloud storage systems. While there are some limitations to the paper, the proposed algorithm is well-described and appears to be effective in ensuring data consistency.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1667.v1

Table 6. Critical Analysis Table.

Papers	Year	Technique	Shortcoming
[4]	2019	Meta-Key protocol	It heavily relies on secret keys to encrypt and decrypt the data, which can be difficult to manage and secure. Lack of scalability [4]
[5]	2020	IPFS	It led to issues such as governance disputes, network fragmentation, and lack of accountability [13]
[6]	2021	Key Management & IPFS	It can be difficult to address the scalability and throughput limitations of blockchain. This can limit the usefulness of these technologies for applications that require data sharing and collaboration between multiple parties. [14]
[7]	2021	IPFS	There is a risk that content may not be available if nodes hosting the content go offline or become unavailable. This could potentially impact the accessibility of important data or information. [7]
[8]	2020	IPFS, Consensus Mechanism	IPFS result in slow download times and lower performance compared to traditional centralized systems. Consensus protocols require a lot of computational power to function. [8]
[9]	2022	Proof-of-Stake (PoS) consensus protocol.	PoS requires a high level of participation from validators to maintain network security. If there is low participation, then the network may become vulnerable to attacks and less secure overall. [9]
[10]	2020	IPFS, Consensus Protocol	Retrieving data from a IPFS cloud storage system can be slower than retrieving data from a centralized system. [10]
[11]	2020	Proof-of-Work (PoW) Distributed Consensus Protocol	PoW is vulnerable to 51% attacks, where an attacker with more than 50% of the network's computational power can control the network and potentially double-spend transactions. [15]

5. Identified Challenges

This section outlines the problems and difficulties, Table 7-listed strategies for identifying and avoiding the shortcomings. It briefly outlines all of the limitations. These are the unexplored areas for research that can be explored in the future to resolve the problems and difficulties.

Table 7. Challenges od blockchain-based system.

Issues Type	Challenges
Scalability (Key Management) [4] - [6]	Each user or participant in the blockchain network will typically have their own secret keys for encryption and decryption, and these keys must be stored securely. As the number of users in the network grows, the number of keys that need to be managed also grows. This can lead to issues with key management.
Accessibility (Single Point of Failure) [7]	It is difficult to maintain the server active because the server's capacity to supply the requested information is essential to the scheme's overall operation. Their system won't function if the computer server mysteriously goes down or crashes.
Encryption Algorithms [8]	Encryption algorithms are not perfect, and new weaknesses or vulnerabilities may be discovered over time. The algorithms used in blockchain systems. While encryption is used to protect the privacy of users in blockchain systems, there are concerns about the potential for data leaks and the use of personal information for targeted advertising and other purposes.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1667.v1

Consensus Protocol [9] - [10]	Consensus mechanisms require decision-making around protocol upgrades and changes, which can be challenging in decentralized systems. In addition, retrieving data from centralized system can be slower. It effects the system efficiency.
Proof-of-Work (PoW) Distributed Consensus Protocol [11]	The system uses this type of consensus protocols can be vulnerable to attacks. Moreover, Proof-of-Work (PoW), require significant amounts of energy to validate transactions and add blocks to the blockchain. This energy consumption can be environmentally unsustainable and result in high costs for participants.

5.1. Need to Work with Scalability

Blockchain networks frequently experience scalability issues, which can result in issues like significant delays which ultimately degrades performance. Due to the rising transaction of blockchain, each peer in blockchain networks must periodically validate and store a growing size of transactions.

5.2. Need to Work on Encryption Methods in Blockchain

The cloud servers are not completely trustworthy and can be vulnerable to security breaches, it is important to protect the data by encrypting it before storing it on the cloud. Implementing an effective encryption solution to encrypt outsourced data is crucial since confidential commercial information is shared on cloud servers. Therefore, there is a need to implement a efficient, trustworthy encryption method.

6. Optimal Solutions

The prior section specifies the issues and challenges such as scalability of key management, privacy and security issues of different algorithms and encrypted algorithms.

Problem	Solution
Scalability with Key Management	Consortium Hierarchical Key Management [16]
	Dynamic Consensus Protocol [17]
	Partitioning, Sharding, And Off-Chain Storage [18]
Encryption Strategy	Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) [19]
	Public-Key Cryptography and Homomorphic Encryption [20]
	Multi-Layered Approach [21]

The [16] proposes a solution that involves a consortium blockchain-based system with distributed key management. The system utilizes hierarchical key management, where the root key is held by the consortium manager and each member of the consortium holds a derived key. This allows for secure data sharing and searching, as well as efficient key management. [17] offers a solution that involves a blockchain-based storage system with a dynamic consensus protocol and multi-level sharding. The system is designed to support efficient storage and retrieval of large amounts of IoT data, while also addressing key management and scalability issues. [18] suggest the solution of scalability using partitioning, sharding, and off-chain storage.

The [19] proposes the use of strong encryption algorithms, such as Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC), to protect sensitive data on the blockchain. [20] discusses various encryption techniques that can be used to secure blockchain-based systems, including public-key cryptography and homomorphic encryption. [21] suggest using a multi-layered approach that includes the use of strong encryption algorithms, key management techniques, and regular security audits. The framework consists of three layers:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1667.v1

1. The first layer focuses on the use of strong encryption algorithms, such as AES and ECC, to protect data on the blockchain. This layer also includes the use of secure key management techniques to ensure that keys are properly protected and not vulnerable to attacks.
2. The second layer focuses on the use of regular security audits to identify potential weaknesses in the blockchain encryption. This layer includes the use of both manual and automated techniques to detect vulnerabilities and security issues.
3. The third layer focuses on the use of additional security measures, such as access controls and intrusion detection systems, to further protect the blockchain from attacks.

The framework can help blockchain developers and administrators identify and address weaknesses in the system before they can be exploited by attackers.

Problem Statement:

Existing methods for the security and privacy of data storage have lack of scalability of key management, and complex encryption algorithm.

Research Question:

RQ1: How to provide scalability in blockchain-based information retrieval systems?
RQ2: How to provide security in blockchain-based information retrieval systems?

Aim & Objective:

Aim:

Improve blockchain mechanism by using lightweight algorithms in cloud-based data storage systems

Objective:

To propose an effective technique to avoid the selfish mining attack on blockchain
A lightweight secure consensus algorithm is proposed to reduce delay time and complexity.
Scheme:

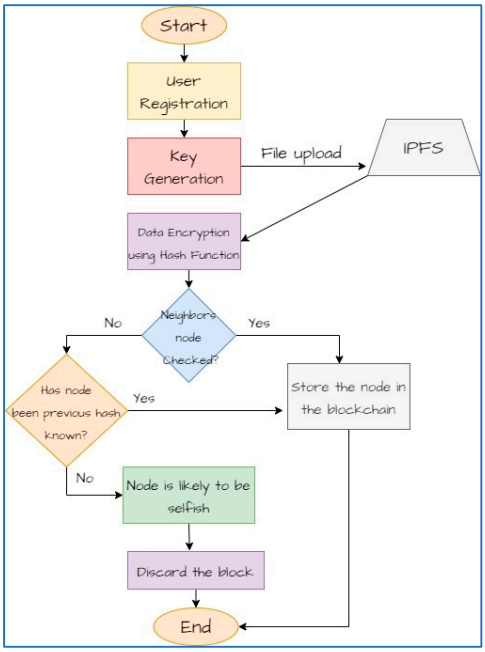

Figure 4. Flow of the System.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1667.v1

Detailed FlowChart of Selfish Mining Attack:

If the public chain becomes longer than the selfish mining group's private chain, the selfish mining group will reveal their private chain to the network. As shown in Figure 5. By doing so, they nullify the work done by other miners, as the revealed private chain becomes the new valid chain.

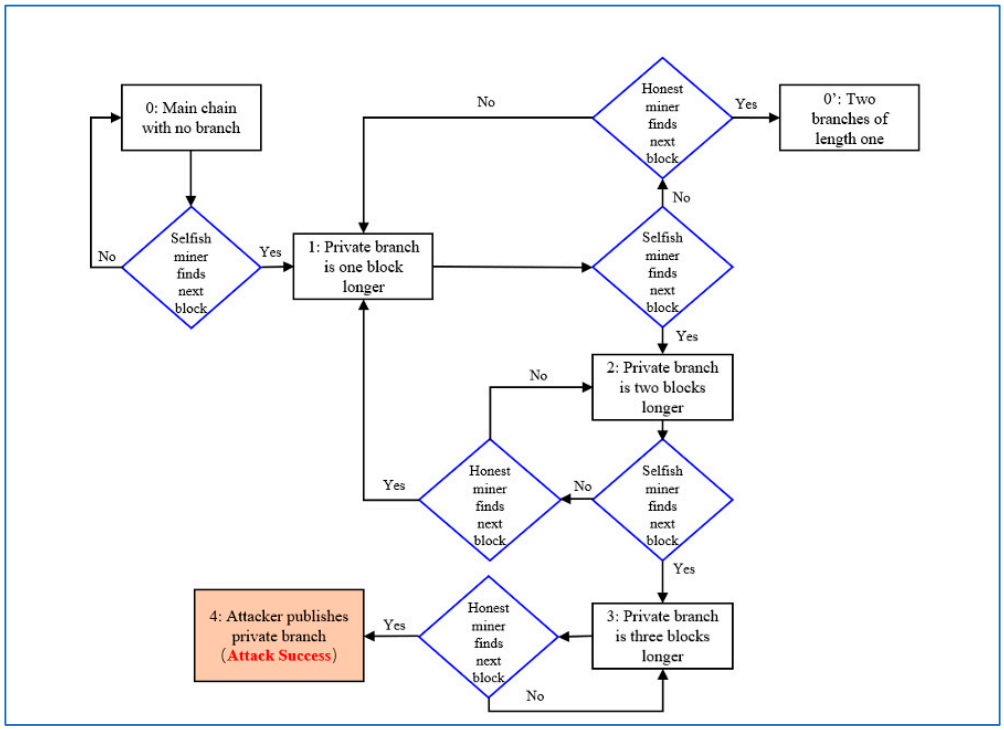

Figure 5. Detailed Flow of Selfish Mining Attack.

Algorithm:

User Registration

Step 1. Start
Step 2. Prompt the user to provide a unique username and password.
Step 3. Verify that the username is not already taken by checking against existing usernames in the database.
Step 4. If the username is taken, display an error message and ask the user to choose a different username.
Step 5. If the username is available, store the username and password securely in the database.
Step 6. Display a success message indicating that the user has been registered.

User Login

Step 1. Prompt the user to enter their username and password.
Step 2. Retrieve the stored username and password from the database for the entered username.
Step 3. If the username does not exist in the database, display an error message indicating that the username is not found.
Step 4. If the username exists, login to the system

Key Generation:

Step 1. Generate a random sequence of bits or bytes as the symmetric key.
Step 2. Drive the corresponding public key from the private key.
Step 3. Create the key pair object with the private and public keys

 doi:10.20944/preprints202312.1667.v1

Step 4. Store the public key.
Step 5. Encrypt the private key.

File Uploading:

Step 1. Prompt the user to select a file for uploading.
Step 2. Read the file.
Step 3. Create an IPFS node connection
Step 4. Add the file to the IPFS network.

Encryption:

Step 1. Apply the hash function to the data, which will produce a fixed-size hash value.
Step 2. Store or transmit the hash value separately from the original data.
Security Check:
Step 1. Retrieve the list of neighboring nodes from the IPFS node
Step 2. IF the neighboring node list is empty THEN retrieve its hash value

a. IF Found THEN store the result in blockchain

ELSE
Step 3. Discard the node
Step 4. Stop

Conclusion:

Blockchain is a disruptive technology that can alter a wide range of sectors thanks to its peer-to-peer and decentralized properties. Data retrieval and storage in cloud storage are two of the most important and contentious problems of the day. Traditional storage systems have several drawbacks and problems that blockchain-based storage systems can address. This survey discusses a novel data storage strategy that aims to improve security and privacy in the blockchain environment.

However, there are still questions about scalability concerns, data access and analysis, and other issues in this field, it is thought that blockchain-based storage is still developing as a mature application of this technology. The lightweight consensus protocols can be combined, changed, or even started from scratch to achieve objectives. For a deeper investigation in this area. we plan to reach an improved algorithm for a high-risk attack on data.

References

1. H. HUAWEI, L. JIANRU and Z. BAICHUAN, "When Blockchain Meets Distributed File Systems:," p. 13, 10 March 2020.
2. S. Ramachandran, O. K. O, A. Ramasamy, V. R and S. Mukherjee, "A Review on Blockchain-Based Strategies for Management of Electronic Health Records (EHRs)," in Proceedings of the International Conference on Smart Electronics and Communication (ICOSEC 2020), 2020.
3. N. Z. B. a, M. A. a and B. Javadi, "Blockchain-based decentralized storage networks: A survey," Journal of Network and Computer Applications, pp. 1084-8045, 13 April 2020.
4. D. Li, R. Du, Y. Fu and M. H. Au, "Meta-Key: A Secure Data-Sharing Protocol Under Blockchain-Based Decentralized Storage Architecture," vol. 1, no. 1, pp. 30-33, 2019.
5. "Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS," Digital Object Identifier, vol. 8, pp. 59389-59401, 2020.
6. H. Van-Hoan, L. Elyes and Y. Ghamri-Doudane, "Privacy-Preserving Blockchain-Based Data Sharing Platform for Decentralized Storage Systems," Information Processing & Management, vol. 58, no. 5, p. 102627, 2021.
7. S. K. Dwivedi, R. Amin and S. Vollala, "Blockchain-Based Secured IPFS-Enable Event Storage Technique With Authentication Protocol in VANET," Journal of Automatica Sinica, vol. 8, no. 12, pp. 1913-1922, 2021.
8. P. Sharma and R. Jindal, "Blockchain-based decentralized architecture for cloud storage system," Journal of Information Security and Applications, vol. 62, p. 102970, 2021.
9. D. Li, D. Han, Z. Zheng and H. Liu, "MOOCsChain: A blockchain-based secure storage and sharing scheme for MOOCs learning," Computer Standards & Interfaces, vol. 81, p. 103597, 2022.
10. M. Shah and M. H. Shaikh , "Decentralized Cloud Storage Using Blockchain," in 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), 2020.

11. Z. Zhu and G. Qi, "Blockchain based consensus checking in decentralized cloud," Simulation Modelling Practice and Theory, vol. 102, p. 101987, 2020.
12. M. Abdollahi, "Simultaneous Sensor and Actuator Fault Detection, Isolation and Estimation of Nonlinear Euler-Lagrange Systems Using Sliding Mode Observers," in IEEE Conference on Control Technology and Applications (CCTA), Copenhagen, 2018.
13. Ivan, "InterPlanetary File System Explained – What is IPFS?," acadmy, 8 April 2021. [Online]. Available: https://academy.moralis.io/blog/interplanetary-file-system-explained-what-is-ipfs#:~:text=All%20files%20in%20the%20IPFS,to%20256%20KBs%20of%20data..
14. L. Yang, "The blockchain: State-of-the-art and research challenges," Journal of Industrial Information Integration, vol. 15, pp. 80-90, 2019.
15. "Consensus Algorithms: Proof of Work," Bitpanda, [Online]. Available: https://www.bitpanda.com/academy/en/lessons/consensus-algorithms-proof-of-work/.
16. L. Zhang, X. Liu, H. Hu, L. Xu and &. Wang, "Secure Data Sharing and Searching for Industrial IoT Networks Based on Consortium Blockchain," Internet of Things, vol. 7, no. 11, pp. 11285-11297, 2020.
17. G. Chen and J. Huang, "A Scalable Blockchain-Based Storage System for IoT Data.," Internet of Things Journal, vol. 6, no. 4, pp. 6611-6621, 2019.
18. Z. H. S. Z. &. Y. M. H. Kardan, "A Survey on Secure Storage Systems in Blockchain," ournal of Information Security and Applications, no. 47, pp. 59-71, 2019.
19. Dorri, Kanhere, S. S., R. Jurdak and P. Gauravaram, "Securing the Internet of Things with Blockchain: Theoretical and Methodological Approaches," IEEE Communications Magazine, vol. 9, no. 57, pp. 68-94, 2019.
20. Bano, Z. S., M. A., J. Arshad and S. Hassan, "Blockchain-based security and privacy solutions: A survey.," Network and Computer Applications, no. 159, p. 102589, 2020.
21. P. S. Basu, D. B. Rawat and S. Jeschke, "A Framework for Identifying and Mitigating Weaknesses in Blockchain Encryption," IEEE Transactions on Industrial Informatics,, vol. 6, no. 17, pp. 4083-4093, 2021.
22. P. Sharma, R. Jindal and M. D. Borah, "Blockchain Technology for Cloud Storage: A Systematic Literature Review," ACM Comput, vol. 4, no. 53, p. 32, 2020
23. Shafiq, M., Ashraf, H., Ullah, A., Masud, M., Azeem, M., Jhanjhi, N. Z., & Humayun, M. (2021). Robust Cluster-Based Routing Protocol for IoT-Assisted Smart Devices in WSN. Computers, Materials & Continua, 67(3).
24. Lim, M., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). Hidden link prediction in criminal networks using the deep reinforcement learning technique. Computers, 8(1), 8.
25. Gouda, W., Sama, N. U., Al-Waakid, G., Humayun, M., & Jhanjhi, N. Z. (2022, June). Detection of skin cancer based on skin lesion images using deep learning. In Healthcare (Vol. 10, No. 7, p. 1183). MDPI.
26. Sennan, S., Somula, R., Luhach, A. K., Deverajan, G. G., Alnumay, W., Jhanjhi, N. Z., ... & Sharma, P. (2021). Energy efficient optimal parent selection based routing protocol for Internet of Things using firefly optimization algorithm. Transactions on Emerging Telecommunications Technologies, 32(8), e4171.
27. Alsaade, F., Zaman, N., Hassan, M. F., and Abdullah, A. 2014. "An Improved Software Development Process for Small and Medium Software Development Enterprises Based on Client's Perspective," Trends in Applied Sciences Research (9:5), pp. 254–261.
28. Humayun, M., Jhanjhi, N. Z., Almufareh, M. F., & Khalil, M. I. (2022). Security threat and vulnerability assessment and measurement in secure software development. Comput. Mater. Contin, 71, 5039-5059.
29. Kaur, R., Verma, S., Jhanjhi, N. Z., & Talib, M. N. (2021, August). A comprehensive survey on load and resources management techniques in the homogeneous and heterogeneous cloud environment. In Journal of Physics: Conference Series (Vol. 1979, No. 1, p. 012036). IOP Publishing.
30. Alotaibi, A. F. (2021). A comprehensive survey on security threats and countermeasures of cloud computing environment. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(9), 1978-1990.
31. Bashir, I. R. A. M., Hamid, B. U. S. H. R. A., Jhanjhi, N. Z., & Humayun, M. A. M. O. O. N. A. (2020). Systematic literature review and empirical study for success factors: client and vendor perspective. J Eng Sci Technol, 15(4), 2781-2808.
32. Lim, M., Abdullah, A., & Jhanjhi, N. Z. (2020). Data fusion-link prediction for evolutionary network with deep reinforcement learning. International Journal of Advanced Computer Science and Applications, 11(6).
33. Alwakid, G., Gouda, W., Humayun, M., & Jhanjhi, N. Z. (2023). Diagnosing Melanomas in Dermoscopy Images Using Deep Learning. Diagnostics, 13(10), 1815.
34. Tayyab, M., Marjani, M., Jhanjhi, N. Z., Hashem, I. A. T., Usmani, R. S. A., & Qamar, F. (2023). A Comprehensive Review on Deep Learning Algorithms: Security and Privacy Issues. Computers & Security, 103297.
35. Pal, S., Jhanjhi, N. Z., Abdulbaqi, A. S., Akila, D., Almazroi, A. A., & Alsubaei, F. S. (2023). A hybrid edge-cloud system for networking service components optimization using the internet of things. Electronics, 12(3), 649.

 doi:10.20944/preprints202312.1667.v1

36. Almuayqil, S. N., Humayun, M., Jhanjhi, N. Z., Almufareh, M. F., & Khan, N. A. (2022). Enhancing sentiment analysis via random majority under-sampling with reduced time complexity for classifying tweet reviews. Electronics, 11(21), 3624.