Pegem Journal of Education and Instruction, Vol. 13, No. 4 , 2023 (pp. 746-761)

RESEARCH ARTICLE WWW.PEGEGOG.NET

DATA INTEGRITY AUDIT SCHEME BASED ON BLOCK CHAIN EXPANSION TECHNOLOGY

T. Mounika[1], Challa Sucharitha[2], Saragandla Sai Bindu[3], Vollala Sriha[4]

[1] Assistant Professor, Department of Information Technology, Sridevi Women's Engineering College, Hyderabad

swecmounikait@gmail.com

[2, 3, 4] Department of Information Technology, Sridevi Women's Engineering College, Hyderabad

ABSTRACT: More and more people are moving their data to the cloud, despite the fact that data integrity is a major concern. The immutability and decentralization of block chain are attracting researchers as a potential replacement for third-party auditors. In order to tackle the high maintenance costs of the blockchain network and the fast increase of blocks in the present data integrity audit scheme, this article proposes a data integrity system that is based on blockchain expansion technology. Users and cloud service providers (CSPs) deploy smart contracts on the main chain and its subchains. The sub-chain performs frequent and heavy computations and updates the main chain with its findings at regular intervals or as required to ensure its finality. We offer the idea of non-interactive audit to make sure that communicating with the CSP during the audit doesn't impact the user experience. To ensure data security, a reward pool system is put into place. The plan's correctness is shown by an exhaustive analysis from several viewpoints, such as capacity, clump evaluation, and information consistency. The plan's ability to reduce capacity and processing overhead is shown by investigations into the Ethereum blockchain stage.

Keywords: Blockchain network, Data integrity, Data security, Cloud service providers, Clump evaluation.

1. INTRODUCTION Today, CHUNK-BASED deduplication is often used in backup and main storage systems to significantly reduce space requirements. It keeps just one physical copy of each copy piece and uses small size references to connect all copy lumps to that one physical copy. Research has shown that deduplication may significantly decrease the storage space requirements of main storage by 50% and backup storage by as much as 98%. To save substantial capacity costs, this drives the widespread use of deduplication in various enterprise distributed storage administrations (such as Dropbox, Google Drive, Bitcasa, Mozy, and Memopal). Scrambled deduplication adds an encryption layer to deduplication, so that each piece is deterministically encoded through symmetric-key

How to cite this article: T.Mounika1, Challa Sucharitha2, Saragandla Sai Bindu3, Vollala Sriha4. DATA INTEGRITY AUDIT SCHEME BASED ON BLOCK CHAIN EXPANSION TECHNOLOGY.Pegem Journal of Education and Instruction, Vol. 13, No. 4, 2023, 746-761

Source of support: Nil **Conflicts of Interest:** None.

DOI: 10.47750/pegegog.13.04.83

Received: 12.10.2023

Accepted: 22.11.2023 **Published:** 24.12.2023

encryption by a key obtained from the lump content (e.g., the cryptographic hash of piece content) before being

composed to deduplicated capacity. This ensures classification. Due to the fact that identical chunks retain their information even after encryption, deduplication may be used to encrypted chunks to reduce storage space requirements. Many research efforts have resulted in a variety of encrypted deduplication algorithms for efficient management of data stored in the cloud. In addition to archiving data that has not been duplicated, a deduplication storage system should also keep track of deduplication metadata. There are two types of deduplication metadata. In order to check whether all of the previously recorded chunks' fingerprints are identical, the system maintains a fingerprint index. In the same way, in order for a record to be replicated, the system maintains a document recipe that specifies the relationships between the record's chunks and the references to the related physical copies. Because metadata storage above becomes increasingly prevalent, deduplication metadata is notorious for producing large capacity above, especially for very repeated tasks (e.g., reinforcements). To decrypt individual files, encrypted deduplication maintains crucial information like key recipes that record the chunk-to-key mappings; nevertheless, this leads to an even greater burden on metadata storage, as we explain in this study. Because they include important key information, key recipes must be handled independently of file recipes, encrypted with the master keys of file owners, and kept independently for each file owner. Such a significant metadata storage cost could hinder encrypted deduplication's storage efficiency in real implementation.

2. MATERIALS AND METHODS:

"Provable data possession with outsourced data transfer," by H. Wang, D. He, A. Fu, Q. Li, and Q. Wang et al. "IEEE Transactions on Services Computing," volume 14, issue 6, pages 1929–1939, November 20, 2021. More and more businesses are interested in storing data on the public cloud as cloud computing continues to grow rapidly. It is common practice for one company to send all relevant data to another when one company sells off its divisions. In a typical scenario, how might one go about outsourcing the computational cost of cloud data transfer? How can I verify that the data I bought online is authentic? Because of this, research on DT-PDP, or proven data possession with outsourced data transport, is crucial. Our groundbreaking idea, DT-PDP, is introduced in this work. Utilizing DT-PDP satisfies three security requirements: (1) protecting the acquired enterprise's other unpurchased data; (2)

guaranteeing the integrity and privacy of purchased data; and (3) offloading the computation of data transferability to public cloud servers. We provide the DT-PDP security concept's

rationale, system model, and security model. After that, we use the bilinear pairings as the basis for DT-PDP scheme design. The concrete DT-PDP scheme's security, efficiency, and adaptability are finally examined. It demonstrates the efficiency and verifiability of our method.

2. "Efficient network coding using secure proof of retrievability," by J. Chang, B. Shao, Y. Ji, M. Xu, and R. Xue Vol. 64, no. 12, Dec. 2021, Art. no. 229301, Science China Industrial Science. Streamlined infrastructure setup, reduced maintenance burden, and ubiquitous data access from any device, anywhere has led to storage-as-a-service's rise as a viable business option to users' local data storage in recent years [5]. Nevertheless, there are a number of security concerns. Protecting the authenticity of users' data is a top priority. Specifically, a user (or data owner) will give up local ownership of the file when storing it to a cloud service provider (CSP) and will instead erase it from their local devices. To make more room and money, CSP may delete certain users' seldom used data. The CSP, meantime, is free to fabricate the truth. Needless to say, it's not great for consumers. "Remotely and reliably checking data's integrity without downloading the whole data file" was an early goal of several protocols, one of which being the Proof of Retrievability (PoR) protocol. Encryption based on identity using the Diffie-Hellman assumption, 3. N. Döttling and S. Garg Publication date: March 20, 2021, volume 68, issue 3, pages 1–46. The first implementations of identity-based encryption and hierarchical identity-based encryption were built around the (Computational) Diffie-Hellman Problem's difficulty, either by factoring or without the usage of groups with pairings. Our design accomplishes the conventional idea of identity-based encryption as proposed by Boneh and Franklin [CRYPTO 2001]. We sidestep known infeasibility findings by use of garbled circuits that utilize the cryptographic primitives in a non-black-box manner.Cloud computing is a novel kind of information technology that users can enjoy sundry cloud services from the shared configurable computing resources. Compared with traditional local storage, cloud storage is a more economical choice because the remote data center can replace users for data management and maintenance, which can save time and money on the series of work. However, delivering data to an unknown Cloud Service Provider (CSP) makes the integrity of data become a potential vulnerability. To solve this problem, we propose a secure identity based aggregate signatures (SIBAS) as the data integrity checking scheme which resorts Trusted Execution Environment (TEE) as the auditor to check the outsourced data in the local side. SIBAS can not only check the integrity of outsourced data, but also achieve the secure key management in TEE through Shamir's (t,n) threshold scheme. To prove the security, security analysis in the random oracle

model under the computational Diffie–Hellman assumption shows that SIBAS can resist attacks from the adversary that chooses its messages and target identities, experimental results also show that our solution is viable and efficient in practice. Achieving data integrity verification for large-scale IoT data in cloud storage safely and efficiently has become one of the hot topics with further applications of Internet of Things. Traditional data integrity verification methods generally use encryption techniques to protect data in the cloud, relying on trusted Third Party Auditors (TPAs). Blockchain based data integrity schemes can successfully avoid the trust problem of TPAs, however, they have to face the problems of large computational and communication overhead. To address the issues above, we propose a Blockchain and Bilinear mapping based Data Integrity Scheme (BB-DIS) for large-scale IoT data. In our BB-DIS, IoT data is sliced into shards and homomorphic verifiable tags (HVTs) are generated for sampling verification. Data integrity can be achieved according to the characteristics of bilinear mapping in the form of blockchain transactions. Performance analysis of BBDIS including feasibility, security, dynamicity and complexity is also discussed in detail. A prototype system of BB-DIS is then presented to illustrate how to implement our verification scheme. Experimental results based on Hyperledger Fabric demonstrate that the proposed verifica tion scheme significantly improves the efficiency of integrity verification for large-scale IoT data with no need of TPAS Data integrity, a core security issue in reliable cloud storage, has received much attention. Data auditing protocols enable a verifier to efficiently check the integrity of the outsourced data without downloading the data. A key research challenge associated with existing designs of data auditing protocols is the complexity in key management. In this paper, we seek to address the complex key management challenge in cloud data integrity checking by introducing fuzzy identity-based auditing, the first in such an approach, to the best of our knowledge. More specifically, we present the primitive of fuzzy identity-based data auditing, where a user’s identity can be viewed as a set of descriptive attributes. We formalize the system model and the security model for this new primitive. We then present a concrete construction of fuzzy identity-based auditing protocol by utilizing biometrics as the fuzzy identity. The new protocol offers the property of error-tolerance, namely, it binds with private key to one identity which can be used to verify the correctness of a response generated with another identity, if and only if both identities are sufficiently close. We prove the security of our protocol based on the computational Diffie-Hellman assumption and the discrete logarithm assumption in the selective-ID security model. Finally, we develop a prototype implementation of the protocol which demonstrates the practicality of the proposal

Blockchain-based decentralized cryptocurrencies have drawn much attention and been widely-deployed in recent years. Bitcoin, the first application of blockchain, achieves great success and promotes more development in this field. However, Bitcoin encounters performance problems of low throughput and high transaction latency. Other cryptocurrencies based on proof-of-work also inherit the flaws, leading to more concerns about the scalability of blockchain. This paper attempts to cover the existing scaling solutions for blockchain and classify them by level. In addition, we make comparisons between different methods and list some potential directions for solving the scalability problem of blockchain.The idea of big data has gained extensive attention from governments and academia all over the world. It is especially relevant for the establishment of a smart city environment combining complex heterogeneous data with data analytics and artificial intelligence (AI) technology. Big data is generated from many facilities and sensor networks in smart cities and often streamed and stored in the cloud storage platform. Ensuring the integrity and subsequent auditability of such big data is essential for the performance of AI-driven data analysis. Recent years has witnessed the emergence of many big data auditing schemes that are often characterized by third party auditors (TPAs). However, the TPA is a centralized entity, which is vulnerable to many security threats from both inside and outside the cloud. To avoid this centralized dependency, we propose a decentralized big data auditing scheme for smart city environments featuring blockchain capabilities supporting improved reliability and stability without the need for a centralized TPA in auditing schemes. To support this, we have designed an optimized blockchain instantiation and conducted a comprehensive comparison between the existing schemes and the proposed scheme through both theoretical analysis and experimental evaluation. The comparison shows that lower communication and computation costs are incurred with our scheme than with existing schemes.

The maturity of network storage technology drives users to outsource local data to remote servers. Since storage service providers are not reliable enough for keeping users' data, remote data auditing mechanisms are studied for mitigating the threat to data integrity. However, many traditional schemes achieve verifiable data integrity for users only without resolutions to data possession disputes, while others depend on centralized third-party auditors (TPAs) for credible arbitrations. Recently, the emergence of blockchain technology promotes inspiring countermeasures. In this paper, we propose a decentralized arbitrable remote data auditing scheme for network storage services based on blockchain techniques.

We use a smart contract to notarize integrity metadata of outsourced data recognized by users and service providers on the blockchain, and also utilize the blockchain network as the self-recording channel for achieving non-repudiation verification interactions. We also propose a fairly arbitrable data auditing protocol with the support of the commutative hash technique, defending against dishonest provers and verifiers. Additionally, a decentralized adjudication mechanism is implemented by using the smart contract technique for creditably resolving data possession disputes without TPAs. The theoretical analysis and experimental evaluation reveal its effectiveness in undisputable data auditing, and the limited requirement of costs.

Despite the rapid development of cloud computing for many years, data security and trusted computing are still the main challenges in current cloud computing applications. In order to solve this problem, many scholars have carried out a lot of research on this, and proposed many models including data integrity test and secure multi-party calculation. However, most of these solutions face problems such as excessive computational complexity or lack of scalability. This paper studies the use of blockchain techniques to improve this situation. Blockchain is a decentralized new distributed computing paradigm. Applying blockchain technology to cloud computing, using the security mechanism of the former to improve the performance of the latter's secure storage and secure computing is a promising research topic. In this paper, the distributed virtual machine agent model is deployed in the cloud by using mobile agent technology. The virtual machine agent enables multi-tenants to cooperate with each other to ensure data trust verification. The tasks of reliable data storage, monitoring and verification are completed by virtual machine agent mechanism. This is also a necessary condition for building a blockchain integrity protection mechanism. The blockchain-based integrity protection framework is built by the virtual machine proxy model, and the unique hash hash value corresponding to the file generated by the Merkel hash tree is used to monitor the data change by means of the smart contract on the blockchain, and the data is owned in time. The user issues a warning message for data tampering; in addition, a "block-and-response" mode is used to construct a blockchain-based cloud data integrity verification scheme.In the new generation of information technology, blockchain technology will be the key to breaking the problem [1]. At present, blockchain technology is becoming a frontier field of high value with its unique technological advantages, innovative value concepts and wide application scenarios [2, 3]. Many experts even believe that blockchain technology is expected to become the technology that has the potential to trigger the next wave of disruptive revolutions after steam engine, power, information and Internet technology [4].

Blockchain can solve the problem of trust mechanism. Trust is a key element of blockchain technology. It is more like a public account book that everyone can record, view, and maintain. Any record has a permanent time stamp and cannot be tampered with [5]. It is precisely because the blockchain technology has broken the centralization characteristics of the traditional Internet that the crisis of trust that plagues the modern economy has been solved to some extent. When the transaction is executed and resolved on the ledger, the parties themselves do not need to establish a trust relationship, but only need to trust the blockchain itself to achieve this goal. Blockchain can solve the problem of data authenticity. Blockchain can effectively promote data circulation and sharing[6]. Blockchain can effectively promote data production convergence. The blockchain led us to open the door to the "value Internet." The emergence of the Internet has made the means of information dissemination leap, and information can flow efficiently on a global scale without third-party and peer-to-peer implementation. The efficiency of value transfer has not been improved simultaneously. The birth of the blockchain is the beginning of human beings building the Internet worth equal to the information Internet. The value of the Internet will lay the foundation for the entire human society to enter a transparent and reliable credit society. Since the emergence of the concept of big data, data science and technology has developed rapidly. At the same time, the big data field is also facing certain problems [7-9]. Especially in the collaborative sharing of data, data transactions and data privacy protection. In the face of these problems, there are currently some solutions, but these solutions are centralized, that is, through some trusted third-party organizations to deal with the problems faced in data processing. However, there are other problems. The so-called trusted third-party organization is really credible. Once a trusted third-party organization is doing evil, it will cause huge losses to users and data owners involved in data processing. The tripartite organization has enormous rights. Once the third-party trusted organization is controlled by the hacker, it will undoubtedly cause some losses to the user. The combination of blockchain and big data will provide solutions to the problems faced by the current big data field, and at the same time avoid the existing centralization problems [10]

The World Economic Forum report pointed out that there are currently more than 20 countries investing in blockchain-related technology areas, 80% of banks began to implement some blockchain distributed ledger-related projects in 2017, and the blockchain has become the Internet A technology that has received much attention around the world [11]. From the perspective of development trend, with the continuous maturity of blockchain technology and

the increasing investment in blockchain technology research in hot industries around the world, people will explore the practical application of this technology in three stages [12]. Phase 1.0: Blockchain technology is mainly used to support digital currency represented by Bitcoin. By supporting transaction transactions such as transfer and payment between accounts, sellers and buyers can realize digital currency security without the help of third-party guarantees. Letter trading [13-15]. Phase 2.0: Combine digital currency with smart contracts, use blockchain technology to optimize a wider range of scenarios and processes in the financial sector, replace the contract with an algorithmic trading program, and trigger the network to automatically execute the contract through external conditions. In the financial industry, products such as bonds and derivatives are supported in asset trading, fund clearing, and intelligent agreements [16-19]. Stage 3.0: Blockchain technology extends from the economic field to social management, charity, culture and entertainment, medical health, science and culture and other social fields, challenging traditional centralized IT application systems, and may change our production in the future. , life and social rules [20]. The block chain was first proposed by Nakamoto in 2008 and became known and familiar with the popularity of digital currencies such as Bit coin [21]. In recent years, blockchain technology and application have attracted extensive attention in academia and industry in China. Major technology companies represented by BAT and financial institutions such as banks have carried out related technical research and application research and development. In July 2016, Alibaba's Ant Financial Service developed a blockchain-based donation platform. In September 2016, Tencent's Weizhong Bank first launched the bank blockchain business in China. In July 2017, Baidu launched Commercial-grade blockchain cloud application platform and more. Blockchain has a very broad application prospect in many fields such as Internet of Things, financial technology, digital forensics, and e-government [22]. However, the blockchain technology was first proposed in 2008, and its theoretical research and application in various fields are still not mature and reliable. In the future, more new technology research and development is needed to further expand the usability and reliability of the blockchain. Many scholars have made efforts and contributions. Herlihy M et al. proposed a distributed computing platform based on blockchain, which uses external blockchain as a network controller to implement access control and privacy protection [23]. In the same year, Aniello L, Baldoni R, Gaetani E and others proposed a distributed personal data management system based on blockchain, which enables users to better control their own data and achieve privacy protection [24]. Kiayias et al. proposed the first blockchain protocol based on the verifiable security-based equity proof mechanism, and compared the

corresponding security attributes in the Bitcoin blockchain protocol [25, 26]. In this paper, the distributed agent model is deployed in the cloud by using the mobile agent technology. The virtual machine agent enables multi-tenants to cooperate with each other to ensure data trust verification, and complete the tasks of reliable data storage, monitoring and verification through the virtual machine agent mechanism. This is also a necessary condition for building a blockchain integrity protection mechanism. The blockchain-based integrity protection framework is built by the virtual machine proxy model, and the unique hash hash value corresponding to the file generated by the Merkel hash tree is used to monitor the data change by means of the smart contract on the blockchain, and the data is owned in time. The user issues a warning message for data tampering; in addition, a "block-and-response" mode is used to construct a blockchain-based cloud data integrity verification scheme.

3. DISCUSSION

1) Based on plasma brilliant agreements, the suggested framework suggests an information uprightness review convention. It is possible that this protocol's implementation of plasma subchains, smart contracts, and smart contracts on both the main chain and sub-chains will minimize the storage burden on the main chain and slow down the growth pace. 2) The suggested system is designed to be audited in batches. Several audit jobs may be processed in parallel using this approach. There is little communication and processing overhead while executing the TPA audit protocol. We propose nonintuitive review as a means to mitigate, to the extent possible, the impact of contact with the CSP on the client experience throughout the review cycle. By using the reward pool method, we can ensure that the review is accurate and provide reasonable awards to the confirmation hub. Examining the plan's security in the suggested framework reveals how it may achieve the usual security aims. Multiple ether block chain studies further demonstrated the plan's efficacy and feasibility.

Owner of Data This component allows the data owner to upload encrypted data to a server in the cloud. Before storing the data file on the server, the data owner encrypts it for security reasons. It is possible for the data owner to do the following actions on the encrypted data file: File uploading, viewing, updating, and blocking verification are all part of the registration and login process (Data Integrity Auditing). Cloud computing When it comes to storing data, the Data Owners may rely on the Cloud. Before storing their data files on the server, data owners encrypt them so that data consumers may access and use them. Data consumers access the shared data files by downloading encrypted data files from the server,

which are subsequently decrypted by the server. In the event that a user logs in, views and authorizes users, or views and authorizes owners, and then asks file permission to access, the server will produce the aggregate key. See All Transactions, Search Requests, Download Requests, and Block Chain Files; See All Attackers Check out the Rank of Files, Results of Time Delay, and Results of Throughput. User The data file in this module can only be accessed with the secret key. Filtering the file according to a user-specified keyword is possible. The following activities will be carried out when the data that matches a certain keyword has been indexed in the cloud server: responding to the end user You may sign up and log in, search, download, view files, and submit requests to search and download. The processing unit (CPU) speed, file viewing, meta data viewing, and secret key generation are all responsibilities of the TPA.

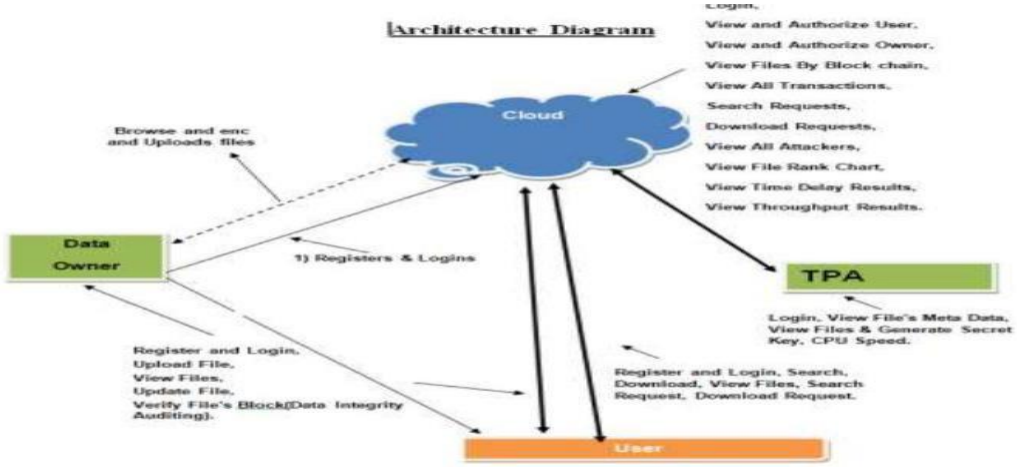
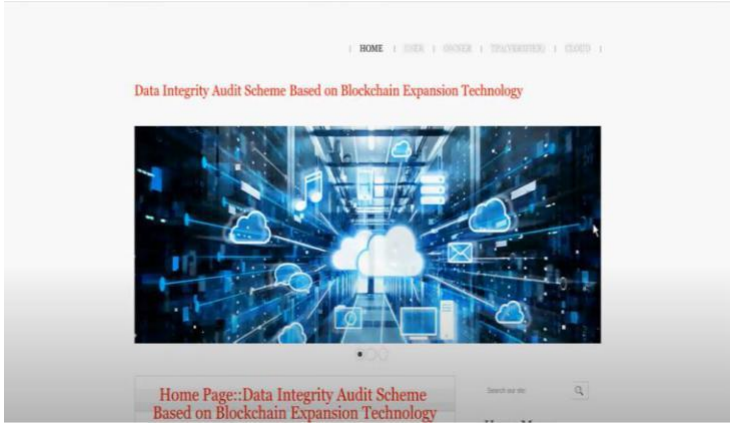


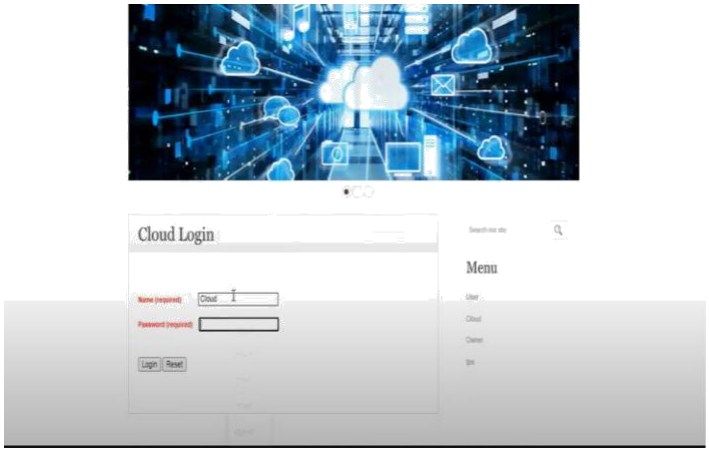
Fig 1: Architecture

4. RESULTS

HOME PAGE



CLOUD LOGIN PAGE



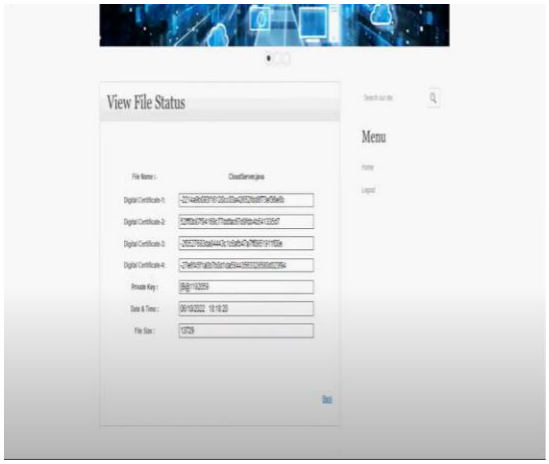
VIEW FILES BY BLOCK CHAIN

DISPLAY UPLOAD & DOWNLOAD TRANSCATIONS

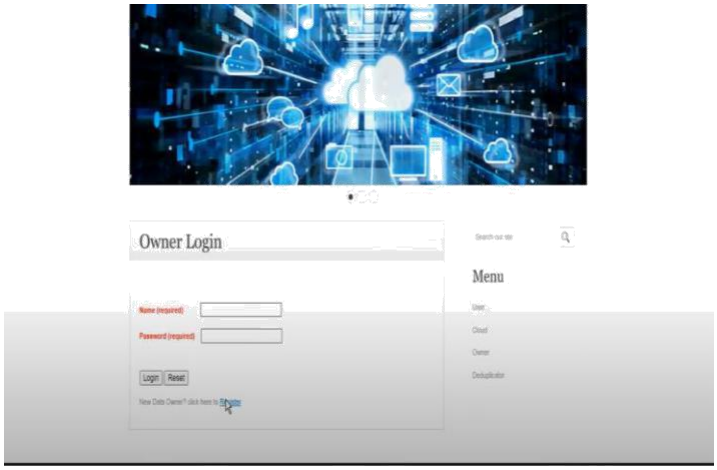
FILE RANKS

TRUSTED USER

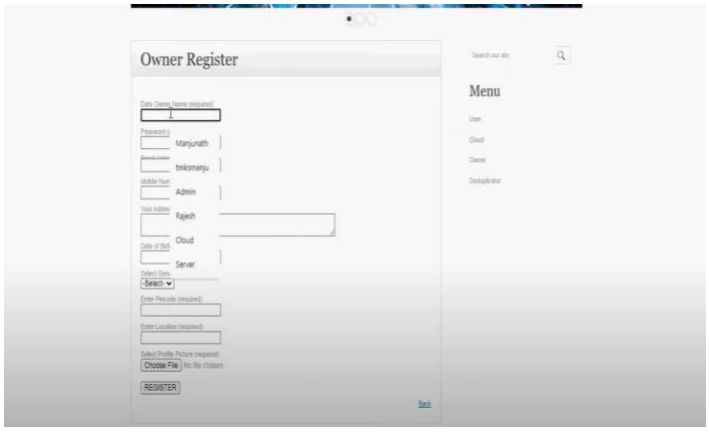
VIEW FILE STATUS



USER LOGIN PAGE



USER REGISTRATION PAGE



Pass All the Required Values in the fields for registration

5. CONCLUSION

With the exponential growth of cloud computing and storage technologies and the subsequent explosion in the amount of data saved in the cloud, how can we guarantee that users can access all of their data stored on cloud servers? Using blockchain expansion technology as its foundation, this paper proposes a data integrity strategy. In our scheme, we use the blockchain network to circumvent several issues with conventional audits, therefore enhancing the program's efficiency and security. The main chain and the plasma sub-chain both have smart contracts implemented. This convention allows for a large reduction in the main chain's capacity strain, a slowing of development, a reduction in capacity and computational overhead, and an improvement in framework execution. Concurrently, the non-interactive audit concept and the reward pool mechanism are included to ensure the correctness of the audit and to prohibit any interaction between the smart contract platform

and the CSP while the contract is being executed. Consequently, the approach accomplishes the desired security objectives.

6. REFERENCES AND CITATATION:

[1] K. Hao, J. Xin, Z. Wang, and G. Wang, ``Outsourced data integrity veri_cation based on blockchain in untrusted environment," World Wide Web, vol. 23, no. 4, pp. 2215_2238, Jul. 2020.

[2] Y. Fan, X. Lin, G. Tan, Y. Zhang, W. Dong, and J. Lei, ``One secure data integrityveri_cation scheme for cloud storage," Future Gener. Comput. Syst., vol. 96, pp. 376_385, Jul. 2019.

[3] H. Wang and J. Zhang, ``Blockchain based data integrity veri_cation for large-scaleIoT data," IEEE Access, vol. 7, pp. 164996_165006, 2019.

[4] Z. Miao, C. Ye, P. Yang, R. Liu, B. Liu, and Y. Chen, ``A scheme for electronic evidence sharing based on blockchain and proxy re-encryption," inProc. 4th Int. Conf. Blockchain Technol. Appl., Dec. 2021, pp. 11_16.

[5] F. Kefeng, L. Fei, Y. Haiyang, and Y. Zhen, ``A blockchain-based _exible data auditing scheme for the cloud service," Chin. J. Electron., vol. 30, no. 6, pp. 1159_1166, Nov. 2021.

[6] K. He, J. Shi, C. Huang, and X. Hu, ``Blockchain based data integrity veri_cation for cloud storage with T-Merkle tree," in Proc. Int. Conf. Algorithms Archit. Parallel Process. Cham, Switzerland: Springer, Oct. 2020, pp. 65_80.

[7] Y. Lei, Z. Jia, Y. Yang, Y. Cheng, and J. Fu, ``A cloud data access authorization update scheme based on Volume : 52, Issue 7, July : 2023 UGC CARE Group-1, 303 blockchain," in Proc. 3rd Int. Conf. Smart BlockChain (SmartBlock), Oct. 2020, pp. 33_38.

[8] Y. Yuan, J. Zhang, W. Xu, and Z. Li, ``Identity-based public data integrityveri_cation scheme in cloud storage system via blockchain," J. Supercomput., vol. 78, pp. 8509_8530, Jan. 2022.

[9] S. Wang, D. Zhang, and Y. Zhang, ``Blockchain-based personal health records sharing scheme with data integrity veri_able," IEEE Access, vol. 7, pp. 102887_102901, 2019.

[10] A. Liu, Y. Wang, and X. Wang, ``Blockchain-based data-driven smart customization," in Data-Driven Engineering Design. Cham, Switzerland: Springer, 2022, pp. 89_107.

[11] H. Wang and J. Zhang, "Blockchain based data integrity verification for large-scale IoT data", *IEEE Access*, vol. 7, pp. 164996-165006, 2019.

[12] Z. Miao, C. Ye, P. Yang, R. Liu, B. Liu and Y. Chen, "A scheme for electronic evidence sharing based on blockchain and proxy re-encryption", *Proc. 4th Int. Conf. Blockchain Technol. Appl.*, pp. 11-16, Dec. 2021.