2021 7th IEEE Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)

2021 7th IEEE Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS) | 978-1-6654-3927-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/BIGDATASECURITYHPSCIDS52275.2021.00041

A Cloud Data Storage Technology for Alliance Blockchain Technology

Han Deng
Big Data Development and Research Center
Guangzhou College of Technology and Business
Guangzhou, China
aviva_daisy@163.com

Fei Fang
College of Information Science and Engineering
Hunan Normal University
Changsha, China
2811864433@qq.com

Juan Chen
College of Computer Science and Electronic Engineering
Hunan University
Changsha, China
juanchen98@hun.edu.cn

Yazhen Zhang
Big Data Development and Research Center
Guangzhou College of Technology and Business
Guangzhou, China
gzgsyazhen8@163.com

***Abstract*—The rapid development of blockchain application technology promotes continuous exploration in the field of computer application science. Although it is still in the initial stage of development, the technical features of blockchain technology such as decentralization, identity verification, tamper resistance, data integrity, and security are regarded as excellent solutions to today's computer security technical problems. In this paper, we will analyze and compare blockchain data storage and cloud data processing technologies, focusing on the concept and technology of blockchain distributed data storage technology, and analyze and summarize the key issues. The results of this paper will provide a useful reference for the application and research of blockchain technology in cloud storage security.**

Keywords—Blockchain, Cloud Storage Security, Cloud Computing, Distributed, Data Storage, Cloud Data

I. INTRODUCTION

In recent years, cloud storage technology has become an emerging trend due to its efficiency and availability in academia and industry. However, with the rapid development of the computer industry and the surge in data sources, the use and storage of data have become more and more serious, because traditional data management tools cannot manage exponentially increasing data. The traditional cloud storage model has obvious shortcomings, such as easy data loss, small storage capacity, and weak user privacy [1,2]. High attention should be paid to the complex storage and availability issues of cloud storage technology[3].

Cloud computing is a model that can realize universal, convenient, and on-demand network access to shared configurable computing resource pools, where networks, servers, storage, applications, and services. These resources can be quickly configured and released with minimal management work or service provider interaction[4].

Outsourcing computing is an important service provided by cloud computing, so it has also become an important advantage and characteristic of the cloud. It further overcomes the limitations of devices with weak computing power by outsourcing data to the cloud and using computing resources in the cloud [5]. Users can rent and pay for storage services or utility computing with the help of cloud services according to their needs. The cloud is more flexible and elastic compared to traditional storage technologies. The limited storage capacity of user devices causes data to be stored in the cloud, so confidentiality and privacy are critical for data and devices, where service providers are not trusted either. Besides, the issue of heterogeneity is considered a major challenge for researchers while preserving data. The heterogeneity in data storage is often referred to as large-scale data, and cloud environments and blockchain technology are suitable for this availability. Therefore, it is time to combine these two technologies to improve the performance of existing applications. Blockchain is a distributed and secure ledger database network system in which many computers called nodes are stored. Blockchain plays a vital role in storing and transmitting large amounts of data. At the same time, it can also minimize costs and improve security and accuracy [6].

The cloud provides computing advantages for storing user data. Currently, some organizations and Internet resources are adopting cloud storage for individuals and organizational users. One of the cloud computing models is cloud storage, which can store large amounts of data and can be retrieved using the Internet. Cloud storage service providers can control even organized or semi-organized data [7]. And it treats information storage as a service and charges users regularly. It is for this reason that cloud storage enables clients to store and access records of information somewhere in the cloud without knowing where the document is stored. Besides, these records can be stored in a global cloud storage environment. Cloud storage has become an important topic today, benefiting from the rapid growth of cloud customers. However, these customers generally do not trust where their information will be stored and who will access and contact it. Therefore, many customers believe that the cloud should be committed to security work to promise their information ownership. For this reason, authentication, integrity, availability, confidentiality, and privacy issues are the things that users are most concerned about.

Blockchain is one of the most popular technologies today and is an innovative technology widely used in various fields [8], which has gained considerable importance. Blockchain is mainly regarded as an accounting book or digital distributed database. Since 2008, blockchain has been a disruptive development that may change the way we interact with computerized spending, tracking, and monitoring transactions. In the blockchain, other entities are cryptographically marked and confirmed in each transmission that holds a copy of the entire record containing all transactions. This makes the

978-1-6654-3927-5/21/$31.00 ©2021 IEEE
DOI 10.1109/BigDataSecurityHPSCIDS52275.2021.00041

recording impossible to adjust gradually, securely, synchronize and share time.

The major contributions of this paper are summarized as follows:

- This article provides an effective solution for cloud data storage and point-to-point distributed data management .
- The article analyzes the combined technology and characteristics of cloud storage and blockchain, and combines specific case analysis and summary.
- Combine current technology and development to put forward demands and challenges for the development of blockchain and cloud storage in the future.

The rest of the paper is organized as follows. In Section II, we introduced blockchain and cloud computing-related work. Section III introduces the existing blockchain technology for cloud storage. We introduced the characteristics of cloud storage blockchain in Section IV. Section V presents the integration requirements and challenges of blockchain and cloud storage. Then, we conclude the paper and identify future directions in Section VI.

II. Related Works

Many scholars who have a strong interest in blockchain technology have introduced many new technologies and frameworks and published a large number of advantageous results to prove the advantages of blockchain over existing applications. Examples of these studies include blockchain technology for business applications, e-government, healthcare, security, edge computing, etc. Some of the research deals with blockchains' obstacles, prospects, and plans. For example, [9] proposed a data fusion method for collaborative anomaly intrusion detection in a blockchain system. A circuit copyright blockchain is studied in [10], which is used for homomorphic encryption of IP circuit protection. The [11] proposed a fast defogging image recognition algorithm based on bilateral hybrid filtering. The research of [12] provides a detailed overview of privacy and security issues in cloud computing, covering potential threats and detection methods based on blockchain. The [13] deals with secure data storage and recovery in the industrial blockchain network environment. The [14] proposed a data transmission technology based on the secure Fabric blockchain for the industrial Internet of Things. The author solves the problems of the security, security, and transaction processing of cloud exchanges using blockchain in [15]. Besides, [16] is dedicated to the blockchain of edge computing systems and its potential uses. This paper investigates the use of blockchain technology in cloud storage, aiming to introduce the use of blockchain technology in cloud computing in detail.

III. Existing Blockchain Technology for Cloud Storage

A. Cloud Storage Data Deletion Scheme based on Blockchain

The scheme of deleting redundant data is used to eliminate redundant data and optimize storage space in the cloud. This technology retains only one copy of indistinguishable information to optimize storage capacity. Therefore, it can manage data efficiency and save the cost of physical equipment, while there is an opportunity to increase data reliability issues. Use the method of deleting redundant data to distribute files to different servers, and record the storage information on the blockchain. It can realize the protection of system confidentiality and data integrity by combining the scheme of deleting redundant data with blockchain technology. Moreover, it is very suitable for distributed storage systems. Cloud service providers and data owners should join the blockchain network as a node for related services.

The method of deleting redundant data can be divided into redundant data deletion of the data unit, redundant data deletion of location, and redundant data deletion of disk placement according to the data unit, location, and disk placement [17]. The redundant data deletion of the data unit is divided into file-level and block-level redundant data deletion. File-level deletion of redundant data uses a unique hash value to compare two files. If the hash value is the same, only one copy is stored. In deleting data redundancy at the block level, the file is divided into fixed-length or variable-length blocks, and then the duplicate content is checked. Location-based deletion of data redundancy is divided into deletion of source data redundancy and deletion of target data redundancy. After the client transmits the file, the receiver deletes the redundant data of the target and rejects other data. Without affecting the operation of the client, the redundant data deletion process is completed by the storage device. The process of removing data redundancy is hidden from the user. Before transferring the data, the process of deleting the source data redundancy has been completed. This deletion of data redundancy has the advantage of network traffic bandwidth because it utilizes the resources of the client. Disk-level redundant data deletion is divided into two parts: forward reference redundant data deletion and backward redundant data deletion.

B. Storage Efficiency Technology for Cloud-based Design

With the rapid growth of cloud computing, NoSQL databases are the best choice for storing information in the cloud. NoSQL databases are stored and processed by platforms such as MongoDB, Hadoop, graph databases, column-oriented databases, document databases, and key-value storage. The cloud stores data in a simple text format, so this is a very inefficient way of data storage. This caused some problems in cloud computing and further increased the operating system overhead when storing data. To manage large amounts of data, some people use the MapReduce method, but it is not suitable for relational database management systems [18]. BigchainDB is a masterless, scalable, decentralized database for cloud data storage. BigchainDB is efficient storage of cloud storage, which is incorporated as an additional layer on top of the NoSQL RethinkDB database. It utilizes the underlying database and provides functions similar to the blockchain, such as hash blocks, transactions, voting, and record immutability .

On Cloud Storage Optimization of Blockchain with a Clustering-Based Genetic Algorithm is proposed in [19], which is superior to NSGA-II and NSGA-III in terms of local space occupation. Use the Euclidean distance to calculate the distance between different solutions, as shown in Eq. (1). D represents the number of attributes of the object. Solutions are represented by η_x and η_y, and f is the value of a corresponding objective function.

$$dist(\eta_x, \eta_y) = \sqrt{\sum_{d=1}^{D}(f_{\eta x,d} - f_{\eta y,d})^2} \quad (1)$$

It uses Eq. (2) and Algorithm 1 to calculate the optimal storage plan. P_i means the overall query probability of M_i blocks, and M_i means the number of blocks that should be stored in the cloud for peer N_i. k means the ratio of cloud storage versus local storage cost. Y means the number of peers that are connected to the IoT devices in the system. Q means overall local space occupancy of the system. δ means weight value for the corresponding objective function.

$$sum = \sum_{k=1}^{Y} \delta_k P_k + \delta_Y cost + \delta_{Y+2} Q \quad (2)$$

TABLE I. ALGORITHMS 1

Obtain the most suitable solution from the filtered solution set
1: Input: filtered solution set H_a, weights of objective functions δ_1, δ_2,. . . , δ_{Y+2}
2: Output: the most suitable solution η_r
3: for each solution η in H_a do
4: calculate the weighted sum of objective functions according to (2)
5: select the solution η_r that corresponds to the smallest sum
6: end for

A smaller sum means a better solution. In this way, we can get the most suitable solution in the solution set, thereby improving the utilization of storage space.

C. Blockchain-based Cloud Payment System

Due to the complexity of transactions and the decentralization of service providers, security attacks on the current payment framework are increasing. If customers wish to exchange cash, they will pay the annual participation fee to obtain a card and use the card to purchase goods or use services. The customer's bank and the dealer's bank contact each other to settle the fee, and they expect to use the card obtained from the bank to pay for the fee for purchasing goods and businesses. As more and more people use mobile phones to purchase services or conduct transactions, it is necessary to simplify transactions. Regarding the advantages of using the blockchain as a P2P transaction for customer transactions, since no external personnel is involved, the transaction is not only reliable and unquestionable but also cost-effective. Besides, since the physical distance does not affect transactions, transactions using the blockchain can be completed quickly, while conventional cross-border transactions may be slow. In contrast, traditional centralized management transactions cannot prevent major information leakage during database management because all valuable information is processed in the central server. Since all important information needs to be communicated, it is extremely difficult to attack blockchain-based transactions. The attacker must hack and change 51% of shared P2P. Outsourcing services usually involve Internet security and payment issues, which is an attractive business model for cloud computing. The mistrust between customers and outsourcing providers can seriously hinder people from accepting such popular cloud services. However, some current payment technologies only consider outsourcing providers and rely on trusted third parties. To ensure safe and fair payment services without a trusted party, outsourcing cloud computing services requires blockchain-based online payment parties. As shown in Fig.1, it is a simple blockchain-based cloud payment system.

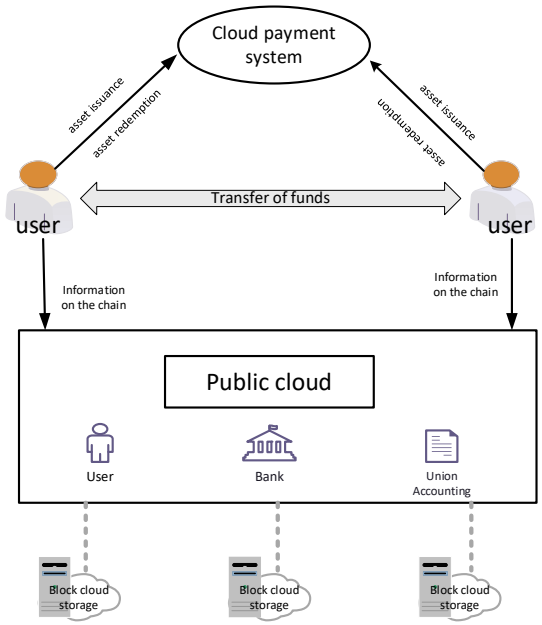

Fig. 1. Blockchain-based cloud payment system

D. Cloud Storage Data Deletion Scheme based on Blockchain

The cloud server maintains user information to reduce the cost of saving, updating, and deleting data. Therefore, we must add security features when deleting, storing, and updating cloud data. Recently, some articles have carried out some research work to safely delete the selected data needed. However, most of the available technologies can use the same "one-bit-return" protocol process to mean: the cloud server deletes the data and reverses the one-bit result. The owner of the information must trust the result because the owner cannot verify the result. Therefore, the blockchain-based deletion scheme can increase the transparency of deletion operations. The data owner can test the deletion result without considering the malicious behavior of the cloud server. Besides, the secure deletion technology can be publicly verified without any third party through the application of the blockchain [20]. It is assumed that the data has been safely deleted, but the proposed scheme still has two characteristic constraints. That is, most schemes with coverage strategies cannot support verification. In such an agreement, the owner of the information must accept the framework for managing the data, because they cannot check the results of the data deletion. Although some programs are verified, they must also introduce a trusted third party. Other inherent constraints are that the proposed convention is not effective in practical applications. For the design of a secure information deletion plan, it is very important to delete information effectively and permanently, and this is also a direction that can continue to be studied.

E. Cloud storage audit scheme based on blockchain

With the rapid development of cloud computing, more and more companies and individuals share and store information on untrusted clouds. Therefore, the audit of shared information has become a major issue in cloud storage, which has aroused public thinking. A publicly audited and shared cloud storage information protocol that uses blockchain and rank-based privacy protection and batch auditing to maintain the protection of the updated blockchain records in the plan.

The main thing TPA needs to check data evidence is the administrator's public key. Besides, community managers cannot change the changed records at will. Performance evaluation shows that the proposed scheme is safe and effective.

[21] proposed an intelligent and decentralized public audit plan for cloud storage. Eliminate the TPA in the framework model by introducing the blockchain framework into the plan. Due to its completely decentralized development, the stability and reliability of cloud storage have been improved. Similarly, they have developed an automatic audit protocol and smart contract that can periodically check the integrity of the data in the cloud, not the owner of the data. Therefore, this can ensure that the data owner is free from the burden of regular verification. The audit results cannot be changed because each smart contract is executed and stored by all nodes in the system. As shown in Fig. 2, it is a blockchain-based cloud storage audit program.

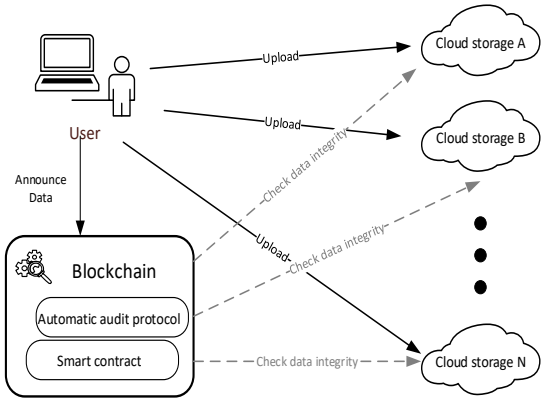

Fig. 2. Cloud storage audit scheme based on blockchain

F. Security and privacy issues in cloud-based cloud storage

The blockchain discards the server to prohibit the association of the central authority and allows members to conduct transactions. These members jointly save the exchange documents and use P2P network technology to confirm the transaction. Blockchain has a shared framework, using peer-to-peer networks and peer-to-peer resource computing. To improve the security of the blockchain, a special assessment was implemented. Although the security of the blockchain has been continuously improving, problems continue to arise, and security assessments are also diverse. The intruder may make various attempts to access the personal key stored on the client device or mobile phone. Investigations into the use of security tokens or secure storage tokens to protect personal keys are ongoing. In [22], a deep learning-based RFID-PUF circuit mutual security authentication method was proposed. [23] Proposed a service-centric identity authentication protocol. The use of blockchain in the cloud computing environment should consider current specific issues. Even now, the blockchain has many problems, such as transaction security, wallets, and programming, and various investigations have been conducted to solve these problems. The anonymity of customer data should be ensured when using the blockchain in a cloud computing environment, and after the software is deleted, the client data should be completely deleted. If the client data is not deleted but some of it remains, the client data can be inferred from the remaining data. Given the environment in which large amounts of data are transmitted, it seems that we still need to conduct efficiency evaluations while protecting data security.

IV. Characteristics of Cloud Storage Blockchain

A. Immutability (tamper-proof and permanent)

Blockchain transactions usually generate permanent records. Therefore, once a block is added, there is no need to modify the block to create trust in the transaction record. The anti-tampering mechanism is a blockchain data structure based on cryptography, which connects the beginning and the end of each block like a chain, increasing the difficulty of tampering. Also, through the consensus mechanism and other means, multi-party nodes verify the information to ensure that the data is more difficult to tamper with.

B. Decentralization

Blockchain technology is a distributed platform that provides a secure distributed ledger for cloud manufacturing. The blockchain is mainly a digital ledger of transactions, which will not cause data loss, and its security is also greatly guaranteed because the computer has a complete copy of the ledger. Blockchain's digital ledger technology retains integrity and confidentiality, reduces computational costs, and improves accuracy. Besides, the transaction process is secure, and no other third party can use blockchain technology to access the transaction.

C. Reliable service

Blockchain is a representative anonymous technology. Combined with the cloud computing environment, the blockchain can be upgraded to a reliable service. The data integrity is guaranteed through the "block + chain" database structure. Constructing the protocol mechanism of the P2P distributed network structure allows any node in the entire network to verify the correctness of the results recorded by other nodes, achieving decentralized reliability. At the same time, every node on the network will have a data backup. Provides data security, any node data error or hacker attack will not affect the stability of the entire system. Blockchain makes it difficult for attackers to obtain and separate network data from the storage process. The information on the blockchain is distributed, encrypted, cross-checked, and verified. These features support the manageability, controllability, reliability, and security of the upper-level business.

Based on practical Byzantine fault tolerance (PBFT), the [24] proposed asynchronous Byzantine fault tolerance (SBFT) algorithm. As shown in Algorithm 2, SBFT has better performance in data consistency, efficiency, and reliability.

D. Fuzzy authorization

Fuzzy authorization is a secure file sharing scheme based on ciphertext policy attributes [25]. Fuzziness means that the scheme has tolerance for differences. Fuzzy authorization provides comprehensive security for outsourced data, including privacy, accuracy, secure access control, high scalability, and flexibility. Public blockchains have gained early functions and approvals to achieve fuzzy authorization, which allows private blockchains to restrict access to specific customers.

TABLE II. Algorithm 2. SBFT.

Require: request messages from each client
Ensure: replies to each request from every node

1: while true do
2: phase 1：
3: client c sends m to n_0, …, n_3
4: phase 2:
5: n_i maps m to <bitarray>n_i
6: n_i sends <bitarray>n_i to others
7: phase 3:
8: n_i calculates <commonbitarray>
9: n_i creates block according to <commonbitarray>
10: n_i sends the created block to others
11: phase 4:
12: n_i votes for each block
13: n_i sends D(n_i)(<vote : value>n_i) to others
14: phase 5:
15: n_i calculates D(n_i)(<vote>n_i)
16: n_i identifies the traitorous node
17: end while

E. Automation through smart contracts

A smart contract is a computer protocol that can be automatically executed and self-verified after its organization and deployment. A smart contract can be regarded as a computer program, which can autonomously execute all or part of the contract-related operations, and generate corresponding verifiable evidence to illustrate the effectiveness of the contract operations. Compared with traditional contracts, smart contracts have more diverse forms, simple processes, and high efficiency. The commitments defined in digital form are used to ensure the safety and reliability of the agreements of contract participants. And based on the encryption of the blockchain, the data cannot be tampered with. One of the most likely results of blockchain technology is the potential for companies and individuals to cut off intermediaries in information monitoring. However, one thing that can improve the way people conduct transactions is smart contracts, which can automate all transactions.

V. INTEGRATION REQUIREMENTS AND CHALLENGES OF BLOCKCHAIN AND CLOUD STORAGE

The combination of blockchain and cloud storage has been used in supply chain finance, trusted deposit certificates, electronic bills, identity management, digital currency, and other fields. There are many existing platforms that support fast and low-cost chains starting in the cloud, such as the self-developed blockchain underlying platform Tencent Cloud Blockchain (TBaaS), and the widely used Hyperledger Fabric underlying chain.

Blockchain and cloud have gathered a large number of virtualized service structures, including hardware and software tools. In this field, these systems are called "infrastructure as a service", "platform as a service" and "software as a service". Large data centers support cloud computing services, sometimes referred to as "data farms." The public cloud provides a wide range of customers with unlimited access to shared information and assets, but cannot guarantee the security of customer information. Access to data and resources in the private cloud is restricted, and a strong authentication and authorization process is required to verify all users. Generally speaking, enterprises are the owners of private cloud clusters and work under clear cloud standards. A hybrid cloud seems to be a perfect model to integrate a large number of private clouds into a combined global framework. This consolidation is done through the upper public layer. The main problem with this model is to reach a consensus among private cloud providers to operate under a unified public cloud standard.

For blockchain systems, the number of transactions can be huge. A large amount of information created requires flexible resources to process. Scalability and flexibility may be the most critical functions in the cloud framework, which can be used to provide on-demand dynamic change activities of cloud attributes. Public clouds have the potential to provide large-scale resource networks that are open to consumers who only pay for the resources they are using. Generally, a private cloud should be configured to accommodate large data sets. From a security perspective, cloud systems can effectively cover the physical domain of knowledge. The adjustment experiment can be performed continuously, and the impact on the deployed application is negligible, which is critical to the successful implementation of most blockchain algorithms. Any blockchain system must accept data sovereignty guidelines and store and process information only in areas permitted by the guidelines. This means that cloud service providers require their customers to control the areas where their information is processed and stored. Another important issue of blockchain systems is the flexibility of the architecture and the ability to respond to failures. This means that even a single failure of the blockchain network will not affect the work of the entire framework. In these cases, cloud services help by copying stored information and using different programming applications.

Finally, the use of blockchain algorithms can enhance the security of the blockchain framework. We can use numerous blockchain features to ensure the privacy, confidentiality, accessibility, and transparency of cloud data, thereby improving efficiency and accuracy. Table 1 is a simple performance comparison of the three cloud storage blockchain systems ChainFS [26], ProvChain [27], and Yugala [28].

VI. CONCLUSIONS

This paper mainly introduces the research of cloud storage security in blockchain and cloud computing, which also conducts a detailed study on the existing cloud storage blockchain technology, the characteristics of cloud storage blockchain technology, the future integration needs, and challenges of blockchain and cloud storage. Blockchain provides a guarantee for the security of cloud storage data. By recording the history of data access and the legal use of information encryption on the blockchain, and according to the requirements of user verification and control access rights, comprehensive design of the storage security of the data on the chain is carried out. Therefore, the trust of blockchain data storage is based on the smart contract design of normal transactions, which eliminates the need for a trusted third party. The summary of the work of this paper can provide effective solutions for cloud data storage, P2P network distributed data management, and storage information. At present, although this technology is still in the initial stage of blockchain development, there are still some challenges in the application of blockchain to cloud data storage and technological innovation. However, the research of this technology will provide new development potential for the fifth-generation network technology.

TABLE III. RELATED CLOUD STORAGE BLOCKCHAIN SYSTEMS AND THE COMPARISON BETWEEN THEIR VARIOUS ATTRIBUTES (⊕:LOW, ⊕⊕:LOWER, ⊕⊕⊕:GENERAL, ⊕⊕⊕⊕:HIGHER, ⊕⊕⊕⊕⊕: HIGH)

System / Performance	ChainFS	ProvChain	Yugala
Decentralization	⊕⊕⊕	⊕⊕⊕⊕	⊕⊕⊕⊕
Safety	⊕⊕⊕⊕⊕	⊕⊕⊕⊕	⊕⊕⊕⊕
Privacy	⊕⊕⊕⊕	⊕⊕⊕⊕⊕	⊕⊕⊕⊕
Reliability	⊕⊕⊕⊕	⊕⊕⊕⊕⊕	⊕⊕⊕⊕
Verifiability	⊕⊕⊕	⊕⊕⊕⊕⊕	⊕⊕⊕
Data Integrity	⊕⊕⊕	⊕⊕⊕	⊕⊕⊕⊕
Overhead	⊕	⊕⊕	⊕⊕
Scalability	⊕⊕⊕	⊕⊕⊕⊕⊕	⊕⊕⊕⊕

REFERENCES

[1] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren. "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Trans. Info. Forensics Secur, 11(11) :2594–2608,2016.

[2] M. Qiu, Z. Ming, J. Wang, L. T. Yang and Y. Xiang, "Enabling Cloud Computing in Emergency Management Systems," IEEE Cloud Computing, 1(4): 60-67, 2014.

[3] K. Gai, M. Qiu, H. Zhao and X. Sun, "Resource Management in Sustainable Cyber-Physical Systems Using Heterogeneous Cloud Computing," IEEE Transactions on Sustainable Computing, 3(2): 60-72, 2018.

[4] W. Dai, L. Qiu, A. Wu and M. Qiu, "Cloud Infrastructure Resource Allocation for Big Data Applications," IEEE Transactions on Big Data, 4(3): 313-324, 2018.

[5] B. Feng, X. Ma, C. Guo, H. Shi, Z. Fu, and T. Qiu, "An efficient protocol with bidirectional verification for storage security in cloud computing," IEEE Access, 4: 7899–7911, 2016.

[6] H. Kaur, M. A Alam, R. Jameel, A. K. Mourya, and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment," Journal of Medicine Systems, 42(8): 156, 2018.

[7] S. R. Patil, "A comparative review on Ceph and Swift open source cloud storage platform, global trends in signal processing," Proceedings of the IEEE International Conference on Information Computing and Communication (ICGTSPICC'16), 213-218, 2016.

[8] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, "Decentralized applications: the blockchain-empowered software system," IEEE Access , 6: 53019–53033, 2018.

[9] W. Liang, L.Xiao, K. Zhang, M. Tang, D. He, K.-C. Li, "Data Fusion Approach for Collaborative Anomaly Intrusion Detection in Blockchain-based Systems," IEEE Internet of Things Journal, 2021.

[10] W. Liang, D. Zhang, X. Lei, M. Tang, K.-C. Li and A.Zomaya, "Circuit Copyright Blockchain: Blockchain-based Homomorphic Encryption for IP Circuit Protection, " IEEE Transactions on Emerging Topics in Computing, 2020.

[11] W. Liang, J. Long, K.-C. Li, J. Xu, N. Ma, X. Lei, "A Fast Defogging Image Recognition Algorithm based on Bilateral Hybrid Filtering," ACM Transactions on Multimedia Computing, Communications, and Applications, 2020.

[12] J. H. Park and J. H. Park, "Blockchain security in cloud computing: Use cases, challenges and solutions," Symmetry, 9(8): 1–13, 2017.

[13] W. Liang, Y. Fan, K. -C. Li, D. Zhang and J. -L. Gaudiot, "Secure Data Storage and Recovery in Industrial Blockchain Network Environments," IEEE Transactions on Industrial Informatics, 16(10): 6543-6552, 2020.

[14] W. Liang, M. Tang, J. Long, X. Peng, J. Xu and K. Li, "A Secure FaBric Blockchain-Based Data Transmission Technique for Industrial Internet-of-Things," IEEE Transactions on Industrial Informatics, 15(6): 3582-3592, 2019.

[15] S. Khezr, M. Moniruzzaman, A. Yassine, and R, Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," Applied Sciences, 9(9):1–28, 2019.

[16] S. Xie, Z. Zheng, W. Chen, J. Wu, H. Dai, and M. Imran, "Blockchain for cloud exchange: A survey," Computers & Electrical Engineering, 81: 1–20, 2019.

[17] S. Supriya and S. Mythili, "Study on data deduplication in cloud computing," INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE, 8(8), 2017.

[18] V. Bhatia and A. Jangra, "SETiNS: Storage efficiency techniques in No-SQL database for Cloud based design," Proceedings of the IEEE International Conference on Advances in Engineering and Technology Research(ICAETR'14):1-5, 2014.

[19] M. Xu, G. Feng, Y. Ren and X. Zhang, "On Cloud Storage Optimization of Blockchain With a Clustering-Based Genetic Algorithm," IEEE Internet of Things Journal, 7(9): 8547-8558, 2020.

[20] S. Pavithra, S. Ramya, and S. Prathibha, "A survey on cloud security issues and blockchains," Proceedings of the 3rd International Conference on Computing and Communication Technologies (ICCCT'19):136–140, 2019.

[21] H Yu and Z Yang, "Decentralized and smart public auditing for cloud Storage," Proceedings of the IEEE 9th International Conference on Software Engineering and Service Science (ICSESS'18):491–494, 2018.

[22] W. Liang, S. Xie, D. Zhang, X. Li, and K. Li, "A mutual security authentication method for RFID-PUF circuit based on deep learning," ACM Transactions on Internet Technology, 2020.

[23] W. Liang, S. Xie, J. Long, K.-C. Li, D. Zhang, and K. Li, "A double PUF-based RFID identity authentication protocol in service-centric internet of things environments," Information Sciences, 503: 129-147, 2019.

[24] Z. Zhu, G. Qi, M.Zheng, J.Sun, C. Yi, "Blockchain based consensus checking in decentralized cloud storage," Simulation Modelling Practice and Theory, 102: 101987,2020.

[25] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," IEEE Symposium on Security and Privacy (SP '07), Berkeley, CA: 321-334, 2007.

[26] Y. Tang , Q. Zou , J. Chen , K. Li , C. A. Kamhoua , K. Kwiat and L. Njilla, "ChainFS: Blockchain-Secured Cloud Storage," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA: 987-990, 2018.

[27] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat and L. Njilla, "ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability," 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Madrid: 468-477, 2017.

[28] S. P. Gochhayat, E. Bandara, S. Shetty and P. Foytik, "Yugala: Blockchain Based Encrypted Cloud Storage for IoT Data," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA: 483-489, 2019.