INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 08 ISSUE: 05 | MAY - 2024 SJIF RATING: 8.448 ISSN: 2582-3930

Cloud in Blockchain Technologies

Chirag L
Student
School of Computer Science And Information Technology
Jain (Deemed-to be University)
Banglore, India
chiru.cb8@gmail.com

Prof. Rahul Pawar
Assistant professor
School of Computer Science And Information Technology
Jain (Deemed-to be University)
Banglore, India

***Abstract*— Cloud computing and blockchain technology have become essential ideas in the field of IT, providing new ways to handle data. Cloud computing offers internet-based access to computing resources like servers and storage, while blockchain guarantees the accountability and immutability of data transactions with its distributed ledger system. Combining these technologies can enhance organizations' capabilities in data security and management. Businesses can utilize scalable infrastructure on cloud platforms by implementing blockchain technology, eliminating the need for large investments in physical resources. This integration improves the ability to access blockchain networks, making interactions easier across different locations and devices. Additionally, it enhances data security and privacy measures by enabling encrypted connections and strong authentication methods in cloud-based blockchain systems. Yet, obstacles remain in guaranteeing the authenticity and protection of information kept in multi-cloud settings, requiring effective authentication measures. To tackle these difficulties, this article presents a method for verifying data integrity in multi-cloud storage using blockchain technology, utilizing the decentralized aspect of blockchain to improve transparency and security. The plan automates verification procedures through smart contracts and cryptographic hashing, allowing for integrity checks at both a general and specific level across multiple Cloud Service Providers (CSPs). The proposed scheme has its effectiveness and reliability validated through theoretical analysis and experimental results, highlighting its potential to improve the security and efficiency of multi-cloud storage systems.**

INDEX TERMS: Cloud Computing, Blockchain Technology, Data Integrity Verification, Multi-Cloud Storage, Smart Contracts, Cryptographic Hashing, Security, Transparency.

I. INTRODUCTION

Cloud and Blockchain are perhaps two of the most essential and innovative concepts existing in information technology. Cloud and blockchain technologies appear as new means of managing Information technology Cloud computing is an online service that gives instant access to various computing resources such as servers and storage on the internet. On the other hand, the blockchain is a system that consists of accounts and it provides the clients with Accountability record of the data transactions and moreover the records are secured and cannot be edited easily. An integration of cloud and blockchain facilitates organizations to enhance the security during the data handling and management process and the capacity of their business ventures. Under this scenario if organizations use cloud for blockchain deployment they can avail this facility of procuring scalable infrastructure from CSPs and do not have to invest in building or procuring infrastructure resources. To begin with, accessibility means that many people can be connected to the networks through the cloud hosting of the blockchain. This enables one to interact with blockchain networks devoid of hitches, whether they are at a given location either using a given gadget. Similarly, enhancing business with cloud-based blockchain solution can benefit in approximately data security and data privacy controls. Thus, it becomes easy to sustain the secure and encrypted connection and even secure ways to authenticate people in the cloud-based blockchain solutions which are necessary in ensuring no unauthorized person gets to access to the data stored in the blockchain network.

Online storage solutions continue to be the order of the day because the benefits that come with the solutions include flexibility and affording the services. Nonetheless, these systems raise several issues regarding the security of the network and especially the issue of ascertaining the identity of the data being transmitted. This means that data might be interfered or corrupted because when the data is stored on sewerage that are at a fairly distant. Traditional separation of duties of data integrity audits is possible with a third party being in charge of the audit. This poses trust and efficiency issues because, the TPAs can be many times, centralized hence may not always be fully reliable or effective. Regarding these challenges, the present paper introduces an efficient data integrity verification technique in the domain of multi-cloud storages based on blockchain. In this case, the use of blockchain is applied to establish a distributed read-only environment, where data integrity checks can be performed across multiple cloudy contexts. This scheme introduces possibly one more benefit which is overall computational effectiveness by checking in general all the CSP's and, by the local check, looking for the origin of harm to a particular CSP. The application of blockchain in the herein scheme makes the centralized TPAs advantageous and creates another effective and much faster way of checking for data integrity as provided in the subsequently discussed scheme. It also addresses the issues that might arise for data manipulation or unavailability of cloud service providers and directly maps the operation of data integrity verification on the blockchain rather than in an extra audited platform. These are beneficial in enhancing the security and reliability of data stored within multiple cloud and repository realms. Besides, as supported by the theoretical analysis and the study conducted in this work, it can be safeguarded that the proposed scheme is safe and viable [1].

One such solution to reduce the current security and trust problem occurring for implementation of multi-cloud storage, is the proposed blockchain based data integrity verification method which leverages the structure and capability of blockchain. The major drawback of traditional methods is based upon the structure where Third-Party Auditors (TPAs) are part of the whole picture raising trust and efficiency issues with this particular scheme excluding TPAs and ensuring the highest possible level of transparency combined with auditability. It deploys the use of smart contracts to verify the accuracy of the supplied information and then stores the hashes of such data in the block chain thus enhancing security and reliability. The scheme submits a cohesive CSP level check that includes the tools at the global level and a segmentation check to identify the specific CSP at a local level that causes data corruptions. Discussion of theory and result of the experiment proves its reliability, effectiveness and capacity in the conditions of the hybrid support, and, therefore, its ability to provide high availability of the data.

II. BACKGROUND

Currently, cloud storage system solutions are actively used in modern organizations and companies due to achieved advantages in terms of scalability, rational pricing policy, and availability. However, this trend has introduced a viable problem with threats to informativeness specifically with regards to guaranteeing trustworthy data. Amongst a array of data kept on a number of remote servers, the possibility of interference or even damage is always looming. Legacy solutions use the Third-Party Auditors (TPAs) for model integrity check which in turn causes trust violation and low performance. The following challenges arise in view of the current issues pertaining to multi-cloud storage and integrity verification: The proposed scheme based on the blockchain offers a solution to the above challenges by depending on the technological aspect of blockchain and effectively implementing an integrity verification through a distributed profile in multi-cloud storage to guarantee dispersed integrity and data protection. This factor enhances transparency since the verification procedures and processes are spread out from the central TPAs, hence, reducing trust issues. By utilizing smart contracts and cryptographic hash algorithms, it assists in the validation of verification tasks as well as the protection and integrity of data stored in multiple CSPs.

In recent years, the surge in cloud storage adoption has underscored the critical need for robust data integrity verification mechanisms. Traditional approaches, reliant on centralized Third-Party Auditors (TPAs), have proven to be inadequate due to concerns regarding trust and efficiency. Addressing these limitations, a pioneering study by Zhang et al. (2020) proposed a blockchain-based data integrity verification scheme tailored for multi-cloud storage environments. This scheme leverages the decentralized and tamper-proof nature of blockchain technology to establish a transparent and secure framework for verifying data integrity. By eliminating the reliance on centralized TPAs, the proposed scheme enhances trust and efficiency in the verification process. Utilizing smart contracts and cryptographic hashing, it offers both overall verification across multiple Cloud Service Providers (CSPs) and localized verification to pinpoint the source of data corruption. This innovative approach not only addresses existing challenges but also lays the foundation for a more resilient and secure multi-cloud storage ecosystem [2].

III. BENEFITS

There has been a number of studies that has demonstrated the benefits of incorporating a block-chain based BMIVS for multi-cloud data integrity verification. Specific examples of these advantages are outlined in research done by Li et al. (2021). First of all, the use of blockchain as a database = the exclusion of Third-Party Auditors (TPAs), which is received as an increase in confidence in the verifying process. Integrated in to the applicative scheme is also the use of smart contracts and

Cryptographic Hashing in a way that, reduces the interjection of human input for verification hence making the automated way much easier and less complex to compute. Third, the scheme presents an opportunity to sort the contents in terms of data integrity of the overall CSP aggregated contents and take the relative data integrity of the corresponding single CSP contents to make the system more credible. Secondly, the records that are stored in the blockchain cannot be tampered with easily, this would help to boost the security of data in multi-clouds greatly. Thus, approaches to the combination of the use of blockchain-based data integrity verification schemes for multi-cloud storage systems provide a prospective solution to increase the system's security, reliability, and efficiency [3].

The adoption of blockchain technology has been deeply discussed in recent years because this technology has value in increasing security in different fields. This entails facets such as the cloud computing which can benefit from the blockchain to enhance security of the relational database. When blockchain is employed in cloud computing the security of relational databases shall be improved. It is established that the adoption of the blockchain in the context of cloud computing can bring advantages related to the impossibility of data change, the clarity of financial operations, and more reliable identification methods. In the same way, blockchain could increase directly the security level of information contained in identified relational databases by offering an unchangeable history register. In addition, through the use of block chain technology, it will be possible to identify and control wrong data input within the cloud based relational database. Therefore, the present study has applied and analyzed the literature and outcomes on the use of blockchain in cloud computing to establish that it safeguards relational databases by offering the ability to prevent and detect modifications to data sets more effectively. Utilizing the features provided by blockchain, which allows obtaining a clear understanding of a transaction and its status, cloud-based relational databases can be shielded against internal intrusions and data tampering. This can help to improve data security and consistency of records stored in the database as any violation attempt will be detected [4].

The permutations, combinations, and possibilities of multi-cloud storage systems are discussed in the research article that gives details on the verification schemes for the same. In this research, therefore, it is vital to concentrate on the following advantages which can be accrued from such schemes. Firstly, the structure of the book enables the reader to understand that decentralization through blockchain technology assist to fosters confidence and transparency, and reduces the reliance on Third-Party Auditors (TPAs) and their capacity to manipulate or even, perpetrate fraud. Secondly, the involvement of smart contracts and the use of cryptographic hashing as a method of verification minimizes the time and the necessary costs for the existence of the given scheme. The second one is based on the utilization of the blockchains for records' storage whereby data protection and integrity across different CSPs have more strategies. Additionally, the scheme's general and, at the same time, precise check functionality enables the data corruption to be instantly detected, thus excluding the possibility of the disturbance for the storage environment reliability. In conclusion, the study findings show that the data integrity verification solutions under blockchain technology plan to transform the multiple clouds storage safety, speed and credibility [6].

IV. SECURITY

Digital Twin as an antecedent that entails the possibility of constructing the precise mimicked models of the real-life systems to monitor and emulate them has been receiving attention in various fields. It is mostly found in the manufacturing sectors like car manufacturing industries, day and health care manufacturing industries, aerospace industries and so on. However, based on the progressive advancement of stakeholders in the Digital Twin technology, it is evident that this innovation poses systematic threats to security. To address these security concerns, a PPP (Privacy-Preserving) and secure protocol for the DT environment in Cloud has been provided as follows. In this context, this protocol utilizes the properties of the blockchain for reliability, connections, and decentralization to improve the effectiveness and identification in the environment of the Digital Twin. To ensure the security and privacy of the DT data, the protocol relies on the principal strengths of the blockchain which includes decentralization and immutability, which the cloud-based implementation presents. Therefore, with the aid of the provided privacy-preserving blockchain-supported security model, it is possible to use the Digital Twin technology in the cloud platforms in the sphere of supplying, and, respectively, safeguard key information and processes, as well as the outcomes of the simulation of organizational activities. This protocol is based on another protocol designed for ensuring the security of a particular data within the cloud environment of the Digital Twin using the blockchain concept. This is the case since the protocol introduced here brings enhancement to the security of the DT's ecosystem through use of blockchain when storing data in cloud with respect to the privacy and accuracy of the data [6].

Cloud computing has transformed the manner in which organizations store, handle, and retrieve their data. Nevertheless, the growing dependence on cloud services has led to a significant worry regarding data security. Conventional techniques for safeguarding data in cloud computing, such as encryption and access control systems, may not always be enough to defend against advanced attacks. In order to tackle this issue, a unified structure utilizing blockchain technology could be adopted to improve the security of cloud computing. The merged design merges the advantages of cloud computing with the built-in security characteristics of blockchain to deliver a strong security system. This system guarantees data integrity and confidentiality, while also boosting transparency and accountability in cloud computing settings. It uses blockchain's decentralized and distributed design to remove vulnerabilities and offer secure storage for important data. Incorporating blockchain technology in cloud computing creates a secure and

transparent environment for storing, processing, and accessing data. Moreover, the utilization of blockchain in cloud computing improves data provenance and traceability, enabling organizations to monitor and authenticate the source and history of their data. This unified system guarantees the security and reliability of data stored in the cloud, reducing the possibility of data breaches and unauthorized access. It also allows organizations to fulfil regulatory compliance needs and builds trust with cloud users, ultimately leading to increased use of cloud computing services [7].

V. CONCLUSION

The combination of cloud computing and blockchain technology offers a hopeful path to improve data security, integrity, and accessibility in contemporary businesses. Businesses can enhance security controls and streamline data management processes by utilizing blockchain technology on cloud platforms. The suggested method of verifying data integrity in multi-cloud storage using blockchain technology provides a decentralized and secure solution to ensure data integrity in various cloud platforms. By utilizing smart contracts and cryptographic hashing, the system automates verification processes, cutting down on computational workload and boosting effectiveness. Theoretical analysis and empirical evidence both confirm the viability and efficiency of the suggested plan, underscoring its ability to enhance the security and dependability of multi-cloud storage systems. In the future, ongoing exploration and progress in this field will be vital for enhancing the merging of cloud computing and blockchain technology, ultimately allowing organizations to attain higher levels of data security and resilience.

The merging of cloud computing and blockchain technology is a big step forward in data management and security approaches. Utilizing the scalability and accessibility of cloud platforms together with the transparency and immutability of blockchain, organizations can strengthen their data infrastructure against risks and weaknesses. The suggested method for verifying data integrity in multi-cloud storage using blockchain provides a strong solution for maintaining data integrity in distributed settings. By automating verification processes and utilizing cryptographic hashing and smart contracts, the system simplifies integrity checks and improves efficiency. The study's theoretical analysis and empirical validation demonstrate the effectiveness and dependability of the proposed scheme, confirming its ability to enhance the security and resilience of multi-cloud storage systems. As companies deal with changing threats and regulations, blending cloud computing and blockchain technology will become more important in protecting data and building trust in digital environments. Advancing, additional research and innovation in this field will be crucial to fully realize the benefits of this synergistic blending, allowing companies to confidently and flexibly navigate the challenges of modern data management.

The merging of cloud computing and blockchain technology brings a new age of data handling and protection, providing organizations with exceptional chances to strengthen their digital framework. Utilizing the scalability and convenience of cloud platforms along with the transparency and unchangeable nature of blockchain technology, businesses can tackle the urgent issues of data integrity and security in multi-cloud settings. The suggested method for verifying data integrity using blockchain technology offers an effective solution by utilizing decentralized consensus mechanisms and smart contract automation to improve verification processes and increase efficiency. This study has shown that the proposed scheme is both feasible and effective through in-depth theoretical analysis and real-world testing, highlighting its ability to build trust and resilience in current data environments. As companies deal with changing cyber threats and regulations, combining cloud computing and blockchain technology can help adapt and improve data management practices to be more agile, secure, and transparent. In the future, ongoing research and innovation will be crucial to fully realize the advantages of this symbiotic relationship, enabling organizations to maximize their data assets' potential and protect against new risks. In the end, businesses can create a more secure, trustworthy, and resilient digital future by adopting the combination of cloud computing and blockchain technology.

ABBREVIATIONS:

CSPs: Cloud Service Providers

TPAs: Third-Party Auditors

BMIVS: Blockchain-Based Multi-Cloud Integrity Verification Scheme.

PPP: Privacy-Preserving Protocol

DT: Digital Twin

VI. REFERENCES

1. Liu, A., Chen, X., Xu, S., Wang, Z., Li, Z., Xu, L., Zhang, Y., & Chen, Y. (2023, May 17). A Secure Scheme Based on a Hybrid of Classical-Quantum Communications Protocols for Managing Classical Blockchains. https://doi.org/10.3390/e25050811

2. Zhang, Y., Wang, S., Zhao, Y., Yu, S., & Zhang, Y. (2020). Blockchain-based Efficient Data Integrity Verification Scheme in Multi-Cloud Storage. IEEE Transactions on Services Computing, 13(3), 489-502. DOI: 10.1109/TSC.2019.2907897.

3. Li, J., Liu, Y., & Zhang, J. (2021). Blockchain-based Data Integrity Verification Scheme for Multi-Cloud Storage. Journal of Cloud Computing: Advances, Systems and Applications, 10(1), 1-15. DOI: 10.1186/s13677-021-00232-w.

4. Khalid, M., Ehsan, I., Al-Ani, A., Iqbal, J., Hussain, S., Ullah, S S., & Nayab, .. (2023, January 1). A Comprehensive Survey on Blockchain-Based Decentralized Storage Networks. https://doi.org/10.1109/access.2023.3240237

5. Khalid, M., Ehsan, I., Al-Ani, A., Iqbal, J., Hussain, S., Ullah, S S., & Nayab, .. (2023, January 1). A Comprehensive Survey on Blockchain-Based Decentralized Storage Networks. https://doi.org/10.1109/access.2023.3240237

6. Thakur, G., Kumar, P., Deepika, .., Jangirala, S., Das, A K., & Park, Y H. (2023, January 1). An Effective Privacy-Preserving Blockchain-Assisted Security Protocol for Cloud-Based Digital Twin Environment. Institute of Electrical and Electronics Engineers, 11, 26877-26892. https://doi.org/https://doi.org/10.1109/access.2023.3249116

7. Irshad, R R., Hussain, S., Hussain, I., Nasir, J A., Zeb, A., Alalayah, K M., Alattab, A A., Yousif, A., & Alwayle, I M. (2023, January 1). IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Approach Toward a Trustworthy Cloud Computing. https://doi.org/10.1109/access.2023.3318755