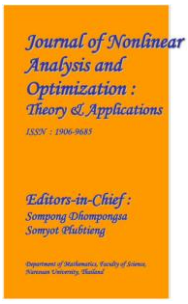
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.15 : 2024
ISSN : **1906-9685**



Paper ID: ICRTEM24_151 **ICRTEM-2024 Conference Paper**

EXPLORING THE ROLE OF BLOCKCHAIN TECHNOLOGY IN ENSURING DATA INTEGRITY AND SECURITY IN CLOUD COMPUTING

[#1]SRIDHAR KONTHAM, ***Research Scholar,***
[#2]Dr. PAWAN KUMAR, ***Associate Professor & Guide,***
Department of Computer Scinece &Engineering,
NIILM UNIVERSITY, KAITHAL, HARYANA, INDIA.

ABSTRACT: Data is becoming an increasingly important resource that influences computer-assisted human activities and all organizational decisions. Threats to data integrity are critical because deliberate data tampering can have serious consequences for business choices. This problem is common in cloud computing systems because data owners have little control over basic data attributes like storage and access control. Blockchain has emerged as a riveting new technology in recent years, offering compelling features such as data integrity and other aspects. Using blockchain to address data integrity concerns is difficult in practice due to the technology's inherent limitations, such as insufficient throughput, excessive latency, and poor stability. This paper focuses on the case study from the European SUNFISH project, which seeks to create a secure cloud federation platform for the public sector. This enables us to clearly specify the research subjects required to create blockchain-based databases, as well as the unique data integrity requirements of cloud computing systems. First, we identify unresolved research issues and hurdles in finding solutions.

Indexed Terms- Block Chain, Cloud Computing

I.INTRODUCTION

Data is becoming one of the most valuable commodities in the modern day. It is critical to evaluate the organization's overall strategy while making decisions for a corporation in disciplines such as public administration, education, or health care. As computer-assisted human activities rely more on data, the ability to trust data becomes increasingly important. Computers can now collect and store data, which is why this happened. Data has become a prime target for attacks due to its vital nature, which requires preserving Availability, Integrity, and Secrecy, the three basic criteria for data reliability. These characteristics include the ability to ensure the confidentiality, integrity, and accessibility of information. Ensuring data confidentiality, integrity, and restricted access is critical. The level of damage done to a user's trust in their data varies depending on which CIA attributes are compromised during different breaches. Reducing availability prevents access to data for a specified amount of time, but processes can resume once the data is available again. The original data is still accessible and usable to the extent that the harm allows. An organization affected by data leaks may face financial consequences. A violation of confidentiality causes the irreversible

revealing of private information. However, compromising the integrity of the data is a highly harmful attack that will cause serious problems with data reliability.

This strategy routinely glosses over serious issues. Data tampering can occur both subtly and actively, such as deleting individual items to remove undesired traces or modifying data sections to influence data consumers' behavior. This can be accomplished by adjusting specific data points or removing individual records. This goal can be achieved by changing or eliminating specific data points. In 2015, Kaspersky Lab discovered a significant cyberattack that stole money from user accounts at over a hundred financial institutions around the world.

The stolen money was estimated to be worth about $1 billion. When data integrity is breached, the previous version of the data cannot be retrieved since it has been irreversibly lost and is irrecoverable. This contrasts the confidentiality and accessibility of the data. This endeavor stresses data integrity over data availability or confidentiality because attacks on data integrity are difficult to detect and have a major impact. The study does not focus on data accessibility or privacy. Cloud computing technologies exacerbate data integrity issues by giving data owners less control over data storage location, access restrictions, and accessibility methods. This complicates verifying the accuracy and dependability of the data. However, an increasing number of companies, both public and private, are opting to outsource data management in order to save money on maintenance and eliminate the need for local data storage.It is critical to address the pressing requirement to ensure the data integrity of cloud computing systems.It is usual practice to protect data integrity by using appropriate data replication mechanisms and cryptographic tools such as digests and asymmetric keys.

This is done to ensure that the data was not tampered with. Existing cryptography algorithms support the signature of individual data items. This is done to speed up the detection of any counterfeiting attempts via cryptographic signature validation. This is done for security purposes. An assault could only happen if the secret keys were successfully broken. This would allow the attacker to modify data signatures and avoid cryptographic integrity checks. Once the technique is mastered, these attacks are tough to execute yet exceedingly difficult to detect. To ensure data integrity in all situations, it is strongly encouraged to use appropriate data replication mechanisms. When data is copied and dispersed across numerous nodes, it becomes substantially more difficult to compromise its integrity since an attacker must discreetly tamper with all of the replicated data to avoid detection. Consequently, compromising data integrity becomes more difficult. This data replication approach has a variety of practical applications, including cloud computing platforms, which provide abundant resources for remote data storage.

Block chain: Data Integrity, Performance, Stability Blockchain is a relatively new technology that is considered cutting-edge. It was recently introduced onto the market. Initially, it served as a public ledger for the digital money bitcoin. It is largely made up of interconnecting bricks that are continuously chained and welded together. It also holds records. Every node in a peer-to-peer network has a copy of the record stored on it.These documents confirm that the aforementioned transactions were carried out using aliases or pseudonyms. Any asset, even cryptocurrencies like Bitcoin, can be used in transactions instead of traditional cash. Miners, or specialized nodes in the network, are in charge of both the decentralized collecting of transactions and the generation of blocks that make up the blockchain.

Miners are accountable for the blockchain's integrity.This operation is referred to as "mining". Miners use defined block creation techniques, known as the mining process, to obtain an agreement on freshly formed blocks. Mining is the mechanism used to accomplish this. Because of the permissionless structure of the Bitcoin blockchain, nodes can participate in the mining process without restrictions. This is due to the blockchain's decentralized structure. If a layer

gives miners authentication and authority, the blockchain is considered permissioned. The initial mining mechanism, which is currently used for Ethereum and Bitcoin blockchains, was based on proof of work (PoW). The basic mining approach is based on Proof of Work. The hashing process is computationally intensive and is governed by blockchain difficulty, which determines the average time miners take to complete such tasks and generate a new block.

The difficulty level is determined by the total number of blocks mined since the blockchain was formed. The key factor influencing this challenge is the total amount of blocks mined since the blockchain's inception. Each miner in the network receives a copy of a newly generated block that was successfully built by a single miner.This method is referred to as "broadcasting." They begin mining further blocks on the idea that this is the most recent link to be added to the chain, allowing the links to be linked to it. Simply said, each time a miner creates a new block, it is added to the chain.

This will help to maintain order. When two miners contribute a block at the same moment, a temporary fork arises; however, this is normally resolved quickly because miners are supposed to prioritize the longer chain. When many miners work on a block at the same time, the blockchain temporarily forks. Proof-of-Work blockchains ensure data integrity by mining and full replication across several nodes, distinguishing them from other blockchain versions. The features are the result of complete copies of the blockchain being held on multiple independent nodes in proof-of-work blockchains. Each miner verifies the contents of a block before adding it to the chain. Every time a new block is added, this happens.

As a result, the block is fundamentally irreversible and unchangeable, until an attacker obtains control of the majority of the miners' hash power and potentially splits the chain. When trustworthy miners control the majority of the hash power, the probability of a fork reaching n depths is O(2n). Users can now wait for a small number of nodes to be added (six blocks in the case of Bitcoin) with complete confidence that their transactions will be permanently included. Users can be confident that their transactions will be permanently merged thanks to this feature. However, blockchains based on proof of work (PoW) have a significant drawback: poor performance.

The majority of this delay is due to the time-consuming PoW procedure and transmission delays when blocks are shared across the network. The longer confirmation times of each transaction limit a blockchain's transaction throughput dramatically. Blockchains were not designed to handle large volumes of transactions. This is caused by the primary source of the issue, which is significantly low transaction throughput. The network can process about seven new transactions per second, but the average wait time for a Bitcoin transaction is ten minutes.

The reliability of blockchain technology is an important consideration for its potential applications. There have been no widely accepted academic studies to explain why this phenomenon occurred, whether it will recur, or how long it will last. A good example of this is the blockchain technology that underpins Bitcoin, which has performed well so far. Currently, the literature lacks adequate methods for evaluating the economic and social assumptions that would ensure Bitcoin's stability. The stability of the PoW-based consensus system continues to be debated. Cryptocurrency-based blockchains that use Proof-of-Work (PoW) are typically extremely vulnerable to market movements. This weakness reduces the blockchain's long-term usefulness.

II.APPLICATION OF THIRD-PARTY AUDITOR

Encryption cannot protect data from damage caused by software flaws or problems during installation. Encryption protects data from external dangers. An audit conducted by an impartial third party is an effective approach to demonstrate that data stored on a remote server has not been modified. If the company requests it, a third party can verify the accuracy of the data. Individuals who participate in the Third-Party

Auditor (TPA) program have the necessary skills to carry out all auditing procedures to assure the integrity of the project's data. Figure 1 shows how the TPA scheme's design protects data integrity and assures data owners that their information is secure. This is demonstrated with a diagram. This solution ensures the accuracy of data for all cloud-stored resources by eliminating human error through the owner's involvement in the auditing process. Zikratov et al. (2017) cited a third-party communication channel requirement and vulnerability to man-in-the-middle attacks as disadvantages of this data integrity protection approach. Third-party engagement in data processing raises the likelihood that hackers will exploit various system vulnerabilities. According to Zhu et al. (2019), a major modern problem is to develop efficient and safe ways for checking and ensuring the data integrity of massive amounts of data stored in clouds. Blockchain technology is supplanting traditional methods of data integrity verification, such as encryption for cloud data storage and Third-Party Auditors. The action is driven by cost savings and increased security. Blockchain-enabled data integrity techniques have the ability to address trust challenges inherent in TPAs. (2019; Wang and Zhang).

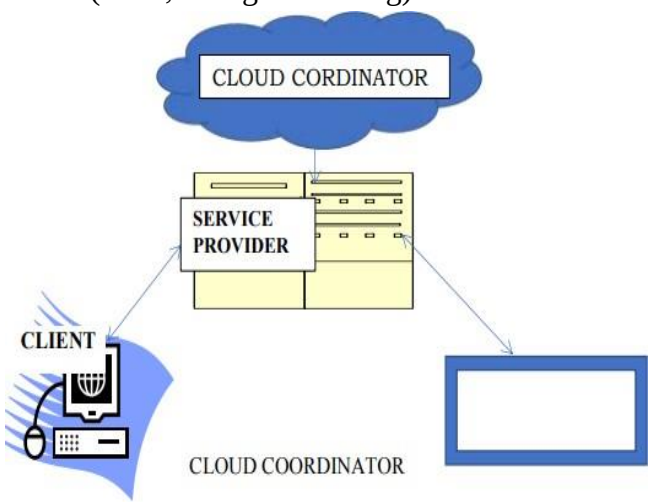


Fig 1. TPA Framework.

III.AN EXAMINATION OF THE SAFETY OF BLOCKCHAIN TECHNOLOGY

The blockchain, a decentralized ledger system, was first created in 2008 for the Bitcoin platform. This technology has the ability to alleviate trust concerns in a variety of scenarios. Enterprises, particularly in the financial industry, are looking into integrating blockchain technology with existing software to establish a more secure and transparent audit trail. These researchers aim to develop an immutable log. Blockchain technology are increasingly being utilized in a variety of service areas, including healthcare, and have sparked renewed interest in recent months. Blockchain technology is offered as a possible solution for managing participant consent, establishing identity, authorizing access to medical records, and managing patients.

Using emerging cryptographic technologies, such as blockchain, may reduce the risk of data manipulation while increasing user confidence in the data. Blockchain is a decentralized database that underpins the Bitcoin currency. It is an extremely significant idea related to the platform. This article defines a blockchain as a succession of data blocks constructed using cryptographic methods, as seen in Figure 2. Each block contains information about a transaction that occurred on the Bitcoin network inside the block's timeframe. This information is required to generate the next block and validate the data contained within it. A blockchain is a sequential data structure that connects data blocks within a specific timeframe.In other terms, it's a distributed ledger. Blockchain records transactions using cryptography, resulting in a distributed ledger that is unchangeable and secure.

Blockchain technology can securely store and validate data on a large scale by utilizing blockchain data structures. This is made possible through the use of blockchain data architecture. The system uses distributed node consensus processes for data creation and updating, encryption for secure data transfer and access, and intelligent contracts made up of automated script code for data programming and modification. It uses smart contracts to ensure safe data access and transmission. Blockchain technology is distinguished by decentralization, traceability, immutability, collaborative maintenance, openness, and transparency. Consider a few of these features. Trustworthy relationships and

partnerships require honesty and openness, which blockchains foster. Several application scenarios rely on blockchain technology's capacity to resolve information asymmetry while also facilitating cooperative trust and coordinated action.

Applications of Blockchain Technology

Blockchain, a distributed ledger technology, was developed in 2008 exclusively for Bitcoin. Our technique effectively addresses trust difficulties in a variety of settings. Blockchain is a secure and immutable distributed ledger and data structure thanks to cryptography. Financial institutions are investigating the integration of blockchain technology into their existing software to address the demand for a more transparent and irreversible audit trail. Blockchain applications in service industries, particularly healthcare, have recently received increased attention.

Blockchain technology can help handle healthcare data, consent, and patient identity. Blockchain technology ensures uniformity. Encryption and consensus are employed to secure data consistency between nodes. The ledger consists of distributed ledger algorithms. Blockchains link records in a chronological order. Cryptography protects this distributed ledger from tampering and counterfeiting. Blockchain participants keep their node information public and available. Publicly available knowledge is unchangeable and permanent. Cloud computing customers can rely on the blockchain's open verification and tamper-proof capabilities. Blockchain technology can improve data security in cloud computing by publishing discoveries to the blockchain for authentication and allowing any user to maintain the blockchain. Blockchain data structures store and validate information. IT uses distributed node consensus to update data.Smart contracts use encryption to automate script code for programming and data updates. Blockchain technology is open source, transparent, decentralized, traceable, and community-managed.

The blockchain's unique properties ensure its integrity and transparency, fostering confidence. The blockchain is a versatile instrument that can address information imbalances, foster mutual trust, and synchronize operations across multiple industries. manufactured ProvChain is a blockchain-based system for collecting, preserving, and verifying provenance information, and it provides a detailed record when asked. Zhu et al. (2019) developed a file management system that employs blockchain technology to prevent project document modification. We presented a blockchain-powered verification method for peer-to-peer cloud storage, which uses Merkle trees to ensure data integrity. In 2019, Wang, Wang, and He created the first secure and efficient blockchain-based PDP model by combining the PDP scheme and the blockchain. Zhu et al. (2019) proposed using blockchain technology to create a certificate-free system as a way to discourage auditors who extend the auditing process.[53] This strategy is only helpful for correcting late auditors and does not address issues such as TPA collaboration.

The blockchain's transparency, openness, and data monitoring qualities make it critical for the IoT, financial, and healthcare industries. Blockchain technology to verify the integrity of cloud data is currently being developed. Traditional data integrity verification protects cloud data with encryption and trusted Third-Party Auditors (TPAs). Using blockchain technology for data integrity plans helps overcome trust issues with third-party administrators (TPAs). Wang and Zhang (2019) developed a Data Integrity Scheme (BB-DIS) for handling large-scale Internet of Things data by combining bilinear mapping with blockchain technology. BB-DIS, a prototype, divides Internet of Things data into shards to generate homomorphic verifiable tags (HVTs) for sample verification. Bilinear mapping can be used in blockchain transactions to assure data integrity, according to the BB-DIS performance research, which takes into account complexity, dynamicity, security, and feasibility. An experiment using Hyperledger Fabric improves integrity verification for large-scale Internet of Things data in the absence of Trusted Third Parties (TPAs). Liu et al. (2017) advocated using blockchain technology for data integrity verification, which might be

beneficial to data storage and blockchain systems. Retricoin uses substantial Proofs of Retrievability (POR) to ensure data integrity and coin transfers. This currency uses POR files instead of PoW.

An examination of the safeguards already in place to guarantee the accuracy of the data

A well-known way for verifying data integrity is to calculate and compare checksum values. Cryptographic techniques serve as the foundation for a variety of approaches to data integrity. These techniques include electronic signatures, key hashing, and keyless hashing. One disadvantage of employing these strategies is that they cannot guarantee their own integrity without relying on a data recovery mechanism.RAID technology, duplication techniques, and redundant coding methodologies can all help to preserve the original data.

RAID technology can be implemented with hardware or software. Another technique for ensuring the validity of the data is to use a range of protections. When using these strategies, a significant amount of unneeded effort is generated. A trial chain was created as a blockchain network to verify the accuracy of massive scientific research trial data. The trial chain was used to create the platform. This was done to improve data visibility and analytical quality. Argues that the first step in the effective operation of an analytical system is the collection of reliable data. The methods used to acquire data have a direct impact on its accuracy. The inquiry involved the creation of a private blockchain utilizing MultiChain technology. The blockchain was then connected with a data science platform housed within a prestigious academic institution. Validating the data and documenting the analysis methodologies are critical for turning the findings into high-quality therapeutic interventions. Conducting validity checks on the data could help increase the reliability of the results.

IV. MODELS TO ENSURE DATA INTEGRITY WITH BLOCKCHAIN

Ensuring data integrity during transmission or storage is a difficult task. When encrypting data, it is recommended to use cryptographic algorithms that require more processing time. This article investigates the use of blockchain technology for data integrity. Vainshtein and Gudes (2021) proposed a new way to use a Proof-of-Work (PoW)-based Blockchain to maintain data integrity in cloud database management systems. This was done to solve issues that arise when databases or data are saved using cloud services. This strategy was developed to solve the issues associated with using cloud platforms. The concept involves connecting a blockchain system to a cloud platform using the proof-of-work method.

This solution uses lightweight software agents and a Distributed Hash Table to track changes made to cloud database storage nodes. This strategy seeks to monitor and document any changes. This is significant because clients do not have a straightforward way to validate the accuracy of data stored in a cloud database. This is hence crucial. Agent interactions will be recorded as Blockchain log/audit transactions once they have been cryptographically and permanently protected by the Blockchain network.

This solution enables the Cloud Provider to efficiently manage metadata in order to detect purposeful or unintentional transaction corruptions and restore transactions in the event of data corruption issues. The study's authors proposed this option. One significant challenge we have is guaranteeing the efficient and safe verification and preservation of data integrity in vast amounts of data stored in the cloud.Blockchain technology is replacing the previous approach of assuring data integrity, which relied on encryption and trusted third-party auditors (TPAs) to safeguard data stored in the cloud. Because of its excellent security features, blockchain technology is gradually replacing traditional methods of confirming data integrity. Blockchain-based data integrity methods can assist address the trust difficulties that exist in TPAs. Wang and Zhang (2019) suggested a Data Integrity Scheme (BB-DIS) that uses Blockchain and Bilinear mapping to handle massive amounts of Internet of Things data while also addressing difficulties with Third Party Auditors. Sharding

IoT data was critical for creating homomorphic verified tags.

The goal of this phase was to authenticate the samples. By incorporating blockchain transactions, the features of bilinear mapping were preserved, ensuring data validity.

V.CONCLUSION

All nodes collaborate to keep data up to date on a blockchain, and some nodes retain backup copies. A typical distributed database stores all of its information on a single central server. Data kept on a single node can be erased, wiped, or updated, but data recorded in the blockchain remains unchanged. Only when more than half of the attacker nodes collaborate can data on the blockchain be updated. This renders the data recorded on the blockchain theoretically immutable, allowing for safekeeping. Blockchain technology reduces the possibility of data theft or corruption by safeguarding it from malicious actors. It also protects against deception. The inclusion of blockchain technology as a third-party authentication system can ensure user privacy while also increasing security and efficiency. The combination of these ingredients could result in these benefits. Blockchain technology can make digital information easier to access, exchange, and store. Furthermore, by encrypting the data with cryptographic methods, it ensures the security of each transaction. Companies that take this step can significantly improve their levels of transparency and safety.

REFERENCES

1. Haug, C. J. (2015). Peer-review fraud—hacking the scientific publication process. New England Journal of Medicine.
2. Rosak-Szyrocka, J., Żywiołek, J., & Shahbaz, M. (Eds.). (2023). Quality Management, Value Creation and the Digital Economy (1st ed.).
3. Dr. Shashi Kant Gupta, Hayath T M., Lack of it Infrastructure for ICT Based Education as an Emerging Issue in Online Education, TTAICTE. 2022 July.
4. Hayath T M., Dr. Shashi Kant Gupta, Pedagogical Principles in Learning and Its Impact on Enhancing Motivation of Students, TTAICTE. 2022 October; 1(2): 19-24. Published online 2022
5. Shaily Malik, Dr. Shashi Kant Gupta, “The Importance of Text Mining for Services Management”,
6. Dr. Shashi Kant Gupta, Shaily Malik, “Application of Predictive Analytics in Agriculture”, TTIDMKD. 2022 November.
7. Dr. Shashi Kant Gupta, Dr. A. S. A. Ferdous Alam, “Concept of E Business Standardization and its Overall Process” TJAEE 2022 August; 1(3): 1–8. Published online 2022 August
8. A. Kishore Kumar, A. Alemran, D. A. Karras, S. Kant Gupta, C. Kumar Dixit and B. Haralayya, "An Enhanced Genetic Algorithm for Solving Trajectory Planning of Autonomous Robots," 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur.
9. S. K. Gupta, V. S. Kumar, A. Khang, B. Hazela, N. T and B. Haralayya, "Detection of Lung Tumor using an efficient Quadratic Discriminant Analysis Model," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC),
10. Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. Proceedings of the 16th ACM conference on Computer and communications security