ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152

www.ijmece .com

Vol 12, Issue 1, 2024

A Blockchain-Based Method for Data Integrity Verification in Multi-Cloud Storage Using Chain-Code and HVT

Swapna Narla

Tek Yantra Inc,

California, USA

Email ID: swapnanarla8883@gmail.com

ABSTRACT

This research proposes a novel blockchain-based strategy for maintaining data integrity in multi-cloud storage systems based on Chain-Code and Homomorphic Verifiable Tags (HVT). The concept combines cryptographic commitments and system modelling with Data Owners (DOs), Cloud Service Providers (CSPs), and a Blockchain Network to provide a safe and transparent data verification framework. Data owners encrypt their data and create promises using the Pedersen commitment scheme to ensure confidentiality and integrity during transmission to CSPs. CSPs generate local signatures and work together to build aggregated signatures that are recorded on the blockchain, allowing for decentralised and immutable integrity checks. The suggested method's scalability and efficiency are validated by an experimental evaluation performed on a conventional computer configuration comprising an Intel(R) Core(TM) i5-10210U CPU, 8.0GB RAM, and a 64-bit OS, utilising SHA-256 and SHA-512 hashing algorithms. The results reveal that the logarithmic time cost increases as the number of DOs grows, demonstrating the system's robustness. Comparative analysis with other blockchain-based schemes regularly demonstrates improved performance, notably in terms of reduced time costs with additional CSPs, highlighting the method's scalability in large-scale implementations. The approach, which uses Chain-Code and HVT, improves confidence through decentralised verification, which is crucial for assuring data security and reliability across several cloud platforms. This systematic approach not only ensures data integrity from encryption to verification, but it also lays the groundwork for future research into optimising system resilience and investigating

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 1, 2024

advanced security measures, such as post-quantum cryptography, to meet evolving cloud computing challenges and improve data protection in multi-cloud settings.

Keywords: Data integrity verification, Chain-Code, Homomorphic Verifiable Tags (HVT), Pedersen commitment, cryptographic algorithms.

1. INTRODUCTION

Data integrity can be robustly ensured with multi-cloud storage by using blockchain technology. This study proposes a way to improve data verification procedures in remote cloud systems by utilizing chain-code and Hyperledger Validity Technique (HVT). Every cloud provider node securely records data transactions and verification results by leveraging blockchain's decentralized ledger. Chain-code smart contracts specify explicit protocols for consistency validation and automate integrity tests. By using cryptographic techniques, HVT strengthens security even more by guaranteeing data accuracy and thwarting unauthorized changes. This method tackles the challenges of preserving dependability in various cloud storage scenarios while also bolstering confidence in data integrity.

Cloud storage has becoming widely used, and this has changed how businesses handle and store data. Multi-cloud systems are being used to improve cost-effectiveness, scalability, and reliability. Even with these advantages, maintaining data integrity across many cloud platforms is still very difficult. Verifying data integrity is essential to preventing illegal additions, deletions, or corruptions that could jeopardize the accuracy and dependability of data that has been saved.

Blockchain technology is a viable way to improve data integrity in cloud storage because of its decentralized and immutable ledger. Blockchain technology can automate and enforce data verification procedures by using smart contracts, also known as chain-codes. This creates a tamper-proof system for monitoring and auditing data changes. Hyperledger Validity Technique (HVT) integration ensures data accuracy and consistency across several cloud storage providers, strengthening the system even more.

In order to verify data integrity in multi-cloud storage, the suggested approach entails building a blockchain-based architecture that integrates chain-code with Hyperledger Validity Technique (HVT). A decentralized blockchain network with each node representing a cloud storage provider is a feature of this architecture. Every data transaction and the outcomes of integrity checks are recorded on the blockchain ledger. Chain-code-implemented smart contracts define policies and methods for validating data consistency and recording outcomes on the blockchain, automating the verification processes. By using cryptographic techniques to guarantee data accuracy and consistency across various cloud storage providers, Hyperledger Validity Technique (HVT) improves security by preventing illegal modifications and upholding confidence in the integrity of stored data.

The suggested approach is put into practice by utilizing Hyperledger Fabric, a permissioned blockchain technology appropriate for enterprise applications, to construct a blockchain network. Using HVT to improve data accuracy and consistency, chain-code will be created to automate data integrity checking.

Extensive testing in actual cloud storage scenarios will be used to assess the scalability and performance of the proposed technique. We'll measure and compare metrics like computational overhead, network latency, and verification time with conventional data integrity verification methods. The assessment seeks to show how the blockchain-based approach improves security, effectiveness, and scalability.

The main goal of this research is to provide a blockchain-based technique for multi-cloud storage environments' data integrity verification. The technique ensures data integrity in a scalable, safe, and reliable manner by utilizing chain-code and HVT. Particular goals consist of:

- creating a multi-cloud storage environment's blockchain architecture with chain-code and HVT integrated.
- Automating procedures for data integrity verification by creating and deploying chain codes.
- Assessing the suggested approach's scalability and performance in actual cloud storage situations.
- Highlighting the security and efficiency gains by contrasting the suggested approach with conventional data integrity verification methods.

The methods used today for verifying data integrity in cloud storage frequently rely on centralized techniques that are vulnerable to assaults and single points of failure. When managing vast amounts of dispersed data across several cloud platforms, these techniques may prove to be ineffective. Additionally, traditional methods lack the auditability and openness offered by blockchain technology.

While blockchain technology has been studied previously for cloud security, the unique difficulties associated with data integrity verification in multi-cloud contexts have not been adequately covered. A complete solution that makes use of chain-code's automation capabilities and blockchain's decentralized structure is required to offer a scalable, safe, and effective way to verify data integrity.

Data integrity in multi-cloud storage environments is a crucial concern that impacts the dependability and credibility of data that is stored. Large, distributed datasets require scalable data integrity verification techniques, which are not compatible with centralized systems that are prone to attacks and failures. A decentralized, automated system that can successfully confirm and preserve data integrity across several cloud storage providers is desperately needed. This study

attempts to solve this issue by creating a blockchain-based approach that makes use of HVT and chain-code. By utilizing the special benefits of blockchain technology, the suggested approach will offer a decentralized, tamper-proof mechanism for data integrity verification, improving security, transparency, and scalability in multi-cloud storage systems.

An efficient and safe technique for confirming data integrity in multi-cloud storage systems is desperately needed, and this study attempts to fill that requirement. A decentralized, tamper-proof solution that improves the dependability and credibility of stored data is provided by the suggested method, which makes use of blockchain technology, chain-code, and HVT. In addition to promoting wider adoption and confidence in multi-cloud environments, the effective implementation and assessment of this technique have the potential to greatly improve data integrity verification procedures in cloud storage.

2. LITERATURE SURVEY

Wang et al. (2022) offer a study on the design and implementation of S-DIV, a data integrity tracking and verification system for stream computing in IoT. The system uses a data integrity verification method to detect and recover from data corruption or loss in real time. It uses homomorphic message authentication codes and pseudo-random function security assumptions to assure data integrity. The proposed approach has been formally examined and shown to be efficient in simulation. This improvement addresses the immaturity and lack of universality in current data integrity verification methods for IoT stream computing systems, improving data availability in IoT big data security.

Witanto et al. (2023) offer a blockchain-based protocol for data integrity verification in multi-cloud situations that uses multiple verifiers to increase sampling rate while remaining cost-effective. The performance analysis shows that this technique is more efficient than employing a single verifier. Current cloud storage data integrity auditing procedures rely on confirmation of probabilistic data possession, however for successful data integrity verification in multi-cloud situations, a greater sampling rate is required. The proposed system improves the sample rate while remaining cost efficient by combining blockchain and multi-verifier technology. The performance analysis shows that the protocol saves time, calculation, and communication expenses for each verifier.

Almarwani et al. (2021) provide DIA-MTTP, a novel system for data integrity auditing in Public Cloud Storage (PCS). This design uses several third parties and a hierarchical communication structure to reduce reliance on any single third party. It offers two levels of integrity assurance as well as a data deduplication mechanism to reduce overhead. The framework also employs a distributed data structure known as Multiple Mapping Tables (M2T). Security analysis and

performance evaluation show that DIA-MTTP is secure and has lower overhead than comparable works, effectively balancing security and cost.

Li et al. (2023) offer an effective data integrity verification scheme for cloud data storage, specifically designed for the Internet of Things (IoT) and medical big data contexts. To assure anonymity, this system employs the SM2 signature technique and SM4 block cryptography, while data is updated using dynamic hash tables. The rapid advancement of cloud storage and computing technology needs new data integrity verification systems, as current solutions are insufficient for IoT and medical big data scenarios. The suggested SM2-based system has been demonstrated to be secure and efficient in a variety of application scenarios.

Tijani et al. (2021) address the difficulties of data integrity in Nigeria's healthcare system by offering a case study of an outbreak management system meant to improve data quality. This system effectively automates data gathering, assuring the completeness, correctness, and validity of patient information. The intervention resulted in considerable improvements to the data gathering process and overall data integrity. Its incorporation into the existing health information system has increased the accuracy and reliability of healthcare data.

Gan and Huang (2022) investigate how blockchain technology can be used in a dual-channel supply chain to improve data integrity with an emphasis on fresh agricultural items. A benchmark model is built by the study to examine sales prices and tactics for both online and offline channels. The study shows that suppliers and retailers can make more money when a price coordination system is put in place, but there is a trade-off between the two. This work provides important insights for the agricultural product business by addressing profit conflicts and improving coordination in dual-channel supply networks.

The necessity of education in radiological research is emphasized by Sardanelli and Colarieti (2023), who pay special attention to the peer-review process, study repeatability, and data integrity. The study emphasizes how critical it is to raise the standard of proof in radiological research to include effects on patient outcomes, diagnosis, treatment, and society. In order to promote cross-fertilization in the developing fields of radiomics and artificial intelligence, it suggests integrating data scientists into clinical departments. The report also emphasizes how competitive science is today and how important it is to teach doctors and young students these basic concepts.

Wu et al. (2022) present a complicated sensor data placement technique for IoT terminal nodes that optimizes data storage and dissemination while taking into account access costs. Furthermore, a load balancing mechanism is implemented for exact data segmentation, which improves data reading and processing speeds. The study focuses on the issues that IoT terminal nodes confront in terms of data storage, distribution, and administration. It uses an adaptive sensing method to improve the performance of the IoT data storage system. Experimental results show considerable

performance gains over traditional distribution systems, such as better data pattern division accuracy and data access efficiency.

In a smart card-based healthcare system, Senthilkumar et al. (2021) suggest a privacy safeguard strategy for safe cloud storage. Sensitive health data must be securely sent between patients, smart health cards, and cloud servers. This protocol takes care of the necessity for remote authentication schemes. Analyzed and proven to offer adequate security without sacrificing usability is the suggested method, which is based on SCB-HC-ECC (Smart Card-Based Health Care Elliptic Curve Cryptography). The purpose of this protocol is to guarantee the safe and effective handling of health data by smart health card solution providers.

A novel method called PUM2Q is put out Carvalho et al. (2021) for choosing cloud service providers to host microservices-based distributed applications. PUM2Q is a multi-criteria technique that can handle microservices in parallel while taking into account their unique needs. This technique builds upon the earlier UM2Q approach and is meant to be integrated with PacificClouds. Tests of performance show that PUM2Q performs better than UM2Q, providing more flexibility and efficiency, which makes it a more attractive choice for software architects using PacificClouds.

Wegner et al. (2022) assess cloud storage's suitability as a customizable cache for workflows involving a lot of data in scientific computing. The common problem of data reduction and related workflow in scientific computing are highlighted. The study illustrates the possible advantages of lowering the amount of disk storage needed on-premises while preserving job throughput by utilizing commercial cloud storage. To help with decision-making about the use of commercial cloud storage, a simulation tool was created to examine storage and network resources. In order to handle upcoming data issues in scientific computing, new assessment techniques are intended to be proposed.

Pollak et al. (2023) provide guidance for experimental biologists on how to set up cloud processing and storage on Amazon Web Services (AWS). The guide discusses the growing usage of cloud-based computing in biology as big data becomes more prevalent, as well as the obstacles biologists encounter when learning and utilizing cloud platforms. It provides examples of data analysis on the cloud utilizing the Python and Julia computer languages, as well as suite2p software. The guide also explores budget and user management tools, making cloud-based computing accessible to academics with limited coding skills.

The synthesis and design of an arithmetic logic unit (ALU) for Internet of Things devices is covered by Jujjavarapu and Poulose (2022). The ALU is created utilizing a 32-nm HVT cell library from the Synopsys database and comprises a fast multiplier based on the Vedic algorithm as well

as a compression module. A summary of the ALU's layout, logic levels, and area efficiency is included in the research, along with a netlist for possible manufacture. This ALU module is made especially to manage high processing loads in Internet of Things applications.

In order to guarantee data integrity and settle service disputes, Zhang et al. (2021) provide a blockchain-based data auditing method for multi-cloud storage systems. By utilizing smart contracts to identify service problems and blockchain technology to record interactions, the scheme does away with the necessity for a reliable third-party auditor. It is also efficient and economical in multi-cloud scenarios since it uses homomorphic verifiable tags for inexpensive batch verification.

Blockchain-based integrity auditing for cloud data is thoroughly surveyed by Han et al. (2022). This article evaluates existing blockchain-based data integrity auditing (BDIA) schemes, introduces evaluation criteria for existing schemes, and covers the fundamentals of integrity auditing and blockchain approaches. It also addresses outstanding questions and makes recommendations for future lines of inquiry. Data integrity issues have grown in importance with the quick expansion of cloud computing and storage services. While blockchain technology presents a promising alternative for guaranteeing data integrity in cloud storage, traditional centralized auditing procedures are susceptible to security issues.

To improve the integrity verification procedure for outsourced data, Chen et al. (2022) suggest a blockchain-based random auditor committee (BRAC). A third-party auditor committee (TPAC) is chosen by the BRAC system for contract verification using a verifiable random function (VRF). To thwart focused assaults, it utilizes a probabilistic leader election system. The TPAC leader inserts the verification proof into a blockchain known as the verification chain. By addressing flaws in current integrity verification techniques, the suggested approach is shown to be secure through thorough security analysis and successful in performance evaluation.

Wang et al. (2022) provide a secure, effective, and non-third-party auditor-dependent blockchain-based data consistency verification system for multi-cloud storage. To produce distinct and lightweight verification proofs, the approach makes use of encrypted tags, blockchain technology, and a Merkle hash tree. In comparison to more conventional techniques, this leads to increased security and a quicker verification procedure.

Gangadevi and Devi (2021) provide a secure, effective, and non-third-party auditor-dependent blockchain-based data consistency verification system for multi-cloud storage. To produce distinct and lightweight verification proofs, the approach makes use of encrypted tags, blockchain technology, and a Merkle hash tree. In comparison to more conventional techniques, this leads to increased security and a quicker verification procedure.

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 1, 2024

3. METHODOLOGY

Chain-code and HVT (Homomorphic Verifiable Tags) are used in the suggested technique for a blockchain-based data integrity verification in multi-cloud storage to provide safe, effective, and impenetrable data verification. The approach is broken down into multiple steps, such as creating the cryptographic commitment, setting up the system model, aggregating signatures, and performing verification processes.

System Model: Data Owners (DOs), Cloud Service Providers (CSPs), and the Blockchain Network are the three main components of the system paradigm. Users that store their data on cloud servers and retain ownership and control over it are known as data owners. Data confidentiality and integrity are guaranteed by cloud service providers, who store the information in an encrypted format. Additionally, they are essential in supporting the process of confirming the accuracy of data. By storing combined local and public signatures, the Blockchain Network acts as a decentralized ledger that makes integrity checks transparent and verifiable. Because any participant may independently verify the data's integrity at any moment by utilizing blockchain technology's immutability, this decentralized approach improves trust and transparency.

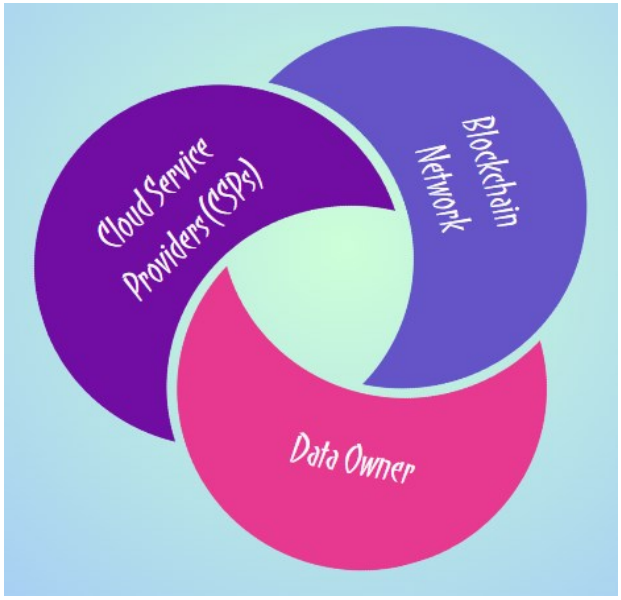

Figure 1: Overview of the system components.

The data owner in this system design is in charge of uploading and owning data. Cloud service providers, or CSPs, oversee the creation of local signatures, promises, and encrypted data storage. They guarantee the integrity and security of data within their infrastructure. Aggregated commitments and signatures are stored in a decentralized ledger using the Blockchain Network. Verification procedures are made open and available to the public with this configuration. All of these elements work together to provide a unified framework in which the data owner starts data

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 1, 2024

uploads, local signatures and encryption are used by CSPs to protect data, and the Blockchain Network offers a reliable platform for storing and validating aggregated data promises.

3.1. Cryptographic Foundations

3.1.1. Pedersen Commitment

One essential element in the integrity verification procedure is the Pedersen commitment. A cryptographic commitment of data is created using the Pedersen commitment algorithm. It has the following definition:

$$com(m,r) = g^m \cdot h^r \quad (1)$$

where, m is the data value, r is a random value chosen by the committer, and g and h are generators of the cyclic group G.

The underlying data is concealed by this feature, which permits the combining of commitments.The commitment is homomorphic, meaning that:

$$com(m_1,r_1) \cdot com(m_2,r_2) = com(m_1 + m_2, r_1 + r_2) \quad (2)$$

3.1.2. Homomorphic Verifiable Tags (HVT)

Data integrity can be confirmed using homomorphic verifiable tags without disclosing the actual data. They are employed in the creation of tags for data blocks that may be combined and independently validated.

3.1.3. Bilinear Pairings

Bilinear pairings are used to speed up the verification procedure. Let $G_1$and G_2 be two cyclic groups of prime order p, and $e: G_1 \times G_2 \rightarrow G_T$ be a bilinear map. The properties of bilinear pairings include:

- Bilinearity: $e(g^a, h^b) = e(g,h)^{ab}$ (3)
- Non-degeneracy: $e(g,h) \neq 1$ (4)
- Computability: $e(g,h)$ (5)

3.2. Methodology Steps

3.2.1. Data Upload and Commitment Generation

Data Owner:

Encrypts the data D and splits it into blocks D_i. For each data block D_i, generates a commitment $com\ (D_i, r_i)$ using the Pedersen commitment scheme. Uploads the encrypted data blocks and their commitments to the CSPs.

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 1, 2024

For each data block D_i :

$$com\ (D_i, r_i) = g^{D_i} \cdot h^{r_i} \quad (6)$$

Algorithm 1: Data Upload and Commitment Generation

Input: Data D, Generators g, h

Output: Encrypted Data Blocks E_D, Commitments C

Split D into blocks D_1, D_2, ..., D_n

Initialize C as an empty list

for each block D_i do

Choose a random r_i

Generate commitment com_i = g^D_i * h^r_i

Append com_i to C

end for

Encrypt D to get E_D

Upload E_D and C to CSPs

Cloud Service Providers (CSPs):

Cloud Service Providers (CSPs) are key components of the system paradigm, assuring data integrity and security. Each CSP generates local signatures for commitments received from Data Owners, which certify the data's validity and integrity. CSPs also collaborate to generate an aggregated signature for the data blocks, which combines their local signatures to form a thorough verification record. These aggregated signatures are subsequently posted to the blockchain, resulting in a decentralized and immutable record with public and verifiable integrity checks. This collaborative strategy among CSPs not only improves data security and reliability, but also takes use of blockchain technology's transparency and trustworthiness.

For a set of data blocks $\{D_1, D_2, \dots, D_n\}$:

$$com(D, R) = \prod_{i=1}^{n} com(D_i, r_i) = g^{\sum_{i=1}^{n} D_i} \cdot h^{\sum_{i=1}^{n} r_i} \quad (7)$$

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 1, 2024

Algorithm 2: Signature Generation

Input: Commitments C, Private Key sk_CSP

Output: Local Signatures S_local, Aggregated Signature S_agg

Initialize S_local as an empty list

for each commitment com_i in C do
    Generate local signature sig_i = Sign(sk_CSP, com_i)
    Append sig_i to S_local
end for
Aggregate local signatures to get S_agg
Upload S_agg to blockchain

3.2.3. Aggregated Commitment and Signature Verification

Blockchain Network:

The system model is made up of three primary components: Data Owners (DOs), Cloud Service Providers (CSPs), and the Blockchain Network. Data owners upload their data to the cloud, and

CSPs establish local signatures for accepted commitments and collaborate to create aggregated signatures for data blocks. These signatures are then saved to the Blockchain Network, which functions as a decentralized ledger. This network enables public verification of data integrity by storing aggregated commitments and signatures, so providing transparency and trust through immutable records.

Let σ_i be the signature for commitment com_i :

$$\sigma_i = Sign\ (sk_{CSP}, com_i) \tag{8}$$

Aggregated signature σ_{agg} :

$$\sigma_{agg} = \prod_{i=1}^{n} \sigma_i \tag{9}$$

Verification Process:

The system concept consists of three major entities: Data Owners (DOs), Cloud Service Providers (CSPs), and the Blockchain Network. Data owners upload their data to the cloud, while CSPs generate local signatures for accepted commitments and collaborate to create aggregated signatures for data sets. These signatures are recorded on the Blockchain Network, a decentralized ledger that allows the public to verify the integrity of data by aggregating commitments and signatures. The blockchain allows for overall verification by testing the integrity of numerous CSPs via aggregated commitments, whereas local verification tests single CSPs for data integrity

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 1, 2024

concerns, assisting in the detection of malicious conduct and providing robust data security and trust.

The verification involves the following steps:

- Compute the expected commitment:

$$com_{exp} = g^{c \cdot D} \cdot h^{c \cdot R} \tag{10}$$

- Verify each local signature:

$$Verify\left(\sigma_i, com_{exp}\right) = \text{True/False} \tag{11}$$

Algorithm 3: Verification Process

Input: Aggregated Commitment com_agg, Local Signatures S_local, Random Challenge c

Output: Verification Result

```
Compute expected commitment com_exp using c and com_agg
 Initialize result as True
      for each sig_i in S_local do
            if Verify(sig_i, com_exp) == False then
                  result = False
                  break
            end if
      end for
 Return result
```

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 1, 2024

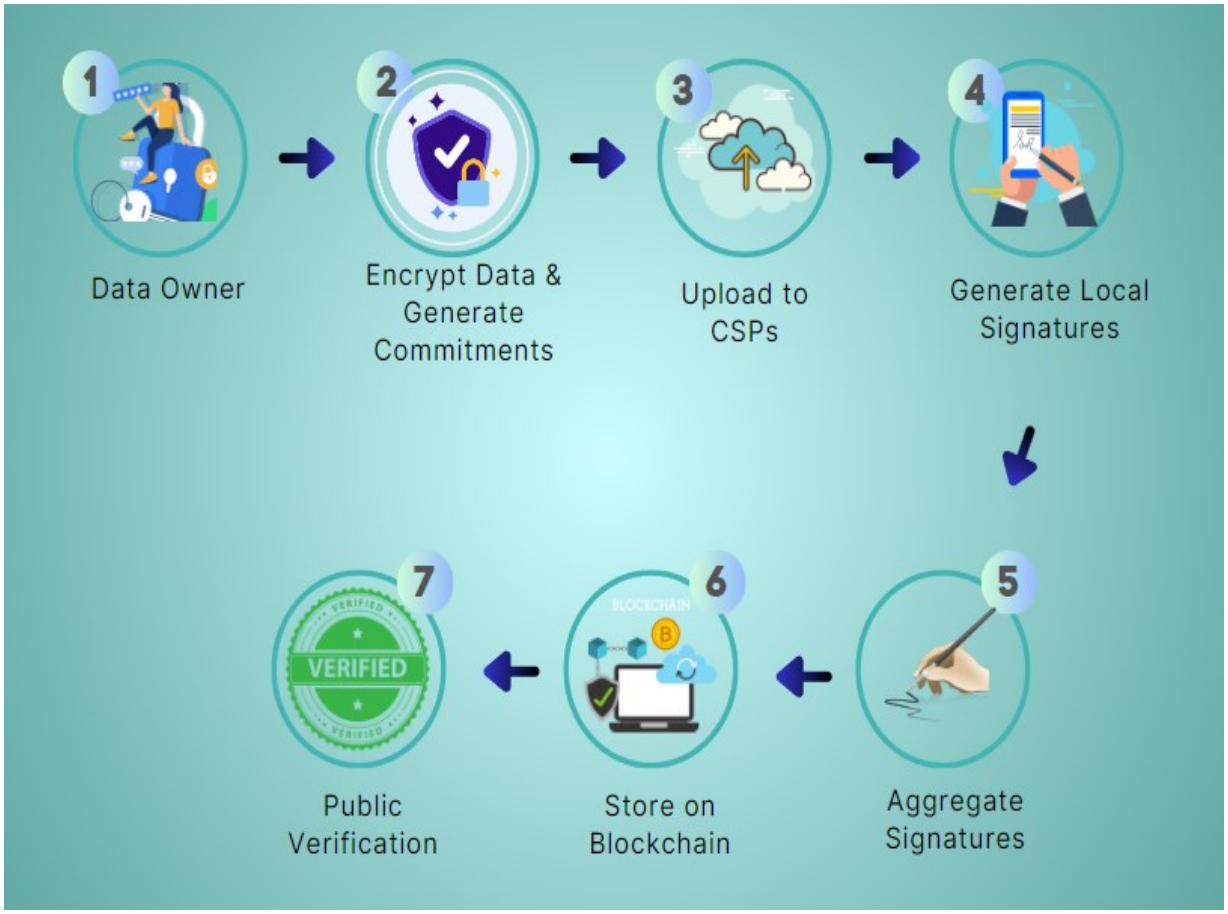

Figure 2: Data Integrity Verification Process Flow.

A organized approach is shown in Figure 2, where the Data Owner generates commitments and encrypts data as the first step in preparing it for safe storage. Cloud Service Providers (CSPs) get the encrypted data and commitments after that. Following receipt of the commitments, CSPs provide local signatures, which are combined to create an exhaustive verification record. An unchangeable record of data integrity is ensured by the safe storage of these combined signatures on the blockchain. Stakeholders can independently confirm the integrity of data thanks to the blockchain's facilitation of transparent and open verification procedures. Using blockchain technology to preserve openness and confidence in the handling of sensitive data, this methodical methodology guarantees data security from encryption to storage and verification.

Security Proofs

Zero-knowledge, soundness, and correctness are the three fundamental characteristics of security proofs. Propriety guarantees that the produced pledges and attestations precisely mirror the initial information. When data is verified, soundness ensures that any data manipulation is found. When data integrity is confirmed, the zero-knowledge property conceals the true values of the data.

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 1, 2024

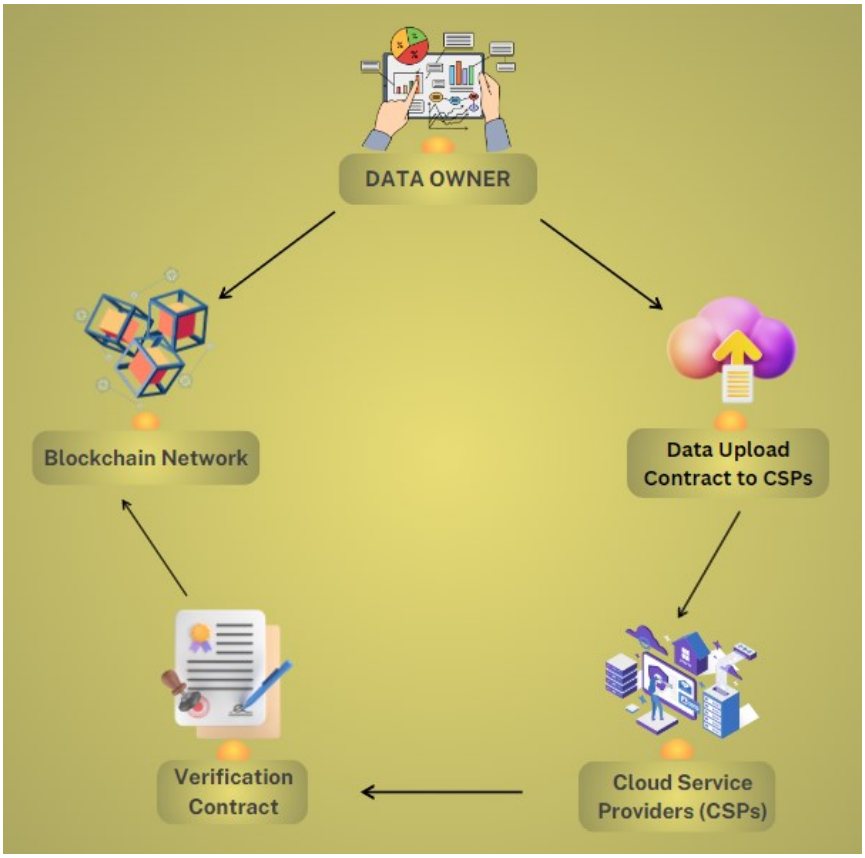

Figure 3: System Architecture for Data Integrity Verification.

Figure 3 shows a systematic procedure that is overseen by the Data Upload Contract and involves the Data Owner encrypting data and creating promises. The agreement makes it easier for Cloud Service Providers (CSPs) to store encrypted data and make obligations. Under the direction of the Verification Contract, CSPs create local signatures and work together to create aggregated signatures. The Blockchain Network is then used to safely store the combined signatures, guaranteeing auditable and unchangeable information. Crucially, by utilizing the blockchain's transparent features, Data Owners may independently confirm the accuracy of their data. This solution uses decentralized ledger technology to improve openness and confidence in data transactions while ensuring a strong chain of custody from data encryption and storage to verification.

3.4. Implementation Specifics

Implementing a blockchain network with smart contracts to manage commitment storage, data uploads, and verification procedures is part of the deployment. To guarantee transparency and automate the verification process, chain-code is used.

3.4.1. Smart Contracts

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 1, 2024

Deployed on the blockchain, smart contracts oversee fundamental functions like data validation and archiving. The Data Upload Contract manages how promises and encrypted data are kept on cloud service providers (CSPs). In the meanwhile, the Verification Contract is in charge of overseeing the verification procedure for both local and aggregated signatures. These contracts strengthen the integrity and reliability of the system by ensuring safe and effective data processing and verification within the blockchain architecture.

Algorithm 4: Data Upload Contract

Input: Commitments C, Encrypted Data E_D

Output: Transaction Receipt

1. Store C and E_D on the blockchain
2. Return transaction receipt

Algorithm 5: Verification Contract

Input: Aggregated Commitment com_agg, Local Signatures S_local, Random Challenge c

Output: Verification Result

```
Compute expected commitment com_exp using c and com_agg
Initialize result as True
for each sig_i in S_local do
    if Verify(sig_i, com_exp) == False then
        result = False
        break
    end if
end for
Return result
```

3.4.2. Chain-Code Implementation

Chain-code is used to automate the verification procedure and settle any disagreements or discrepancies found during verification. It has features to store promises, create challenges, and carry out validation procedures. The chain-code improves the efficiency and dependability of the verification process by automating these processes, guaranteeing that every function is carried out precisely and without error. Maintaining the integrity and reliability of the system depends on this implementation.

Algorithm 6: Chain-Code for Verification

```
Input: Aggregated Commitment com_agg, Local Signatures S_local, Random Challenge c
Output: Verification Result
Function verifyCommitments(com_agg, S_local, c):
    com_exp = computeExpectedCommitment(com_agg, c)
    result = True
    for sig_i in S_local do
        if not verifySignature(sig_i, com_exp) then
            result = False
            break
        end if
    end for
    Return result
```

3.5. Security Analysis

Data integrity is guaranteed by the suggested approach via a number of important mechanisms. Blockchain technology is used in decentralization to eliminate the need for a single Third-Party Auditor (TPA). Because every transaction is recorded on the blockchain and becomes immutable and auditable, traceability is achieved. Furthermore, verification is made possible by homomorphic features, which conceal the true data. When combined, these elements offer a reliable and safe approach for preserving data integrity.

3.5.1. Attack Scenarios and Mitigations

Attack scenarios and their mitigations in the proposed scheme include: replay attacks, which are prevented by incorporating timestamps and unique transaction IDs in the commitments; collusion attacks, which are mitigated by involving multiple cloud service providers (CSPs) in the verification process, thereby reducing the risk of collusion; and data tampering, where any alterations to the data result in a mismatch between the commitments and signatures, triggering a verification for These safeguards provide a secure and dependable system.

Using blockchain and cryptographic approaches, the methodology outlined offers a strong framework for guaranteeing data integrity in multi-cloud scenarios. The method guarantees safe, effective, and transparent verification procedures without requiring a centralized auditor by utilizing homomorphic verifiable tags and Pedersen promises. By providing a decentralized approach, this methodology improves the trust and dependability in cloud storage services by

addressing the security issues related to conventional TPA-based systems. The thorough comprehension of the suggested approach is ensured by the extensive algorithms and equations supplied, rendering it appropriate for both practical application and future study in the subject of cloud data integrity verification.

4. RESULT AND DISCUSSION

In this research, this is a blockchain-based approach for data integrity verification in multi-cloud storage systems that uses Homomorphic Verifiable Tags (HVT) and Chain-Code. On a typical computer system, an experimental evaluation produced encouraging results.

SHA-256 and SHA-512 hashing algorithms were implemented using an Intel(R) Core(TM) i5-10210U CPU, 8.0GB RAM, and a 64-bit operating system. To assess performance scalability, each of the 30MB data owners (DOs) simulated a range of scenarios including 10-100 Cloud Service Providers (CSPs) and DOs.Based on signature generation and verification timeframes, the effectiveness of the method was evaluated. In general, the system showed increases in time costs that were logarithmic and stabilised as DO values rose. This efficiency is the result of DOs and CSPs running the CommitGen(), Sign(), and Verify() procedures concurrently.

In multi-cloud data integrity verification, our blockchain-based approach guarantees strong verification accuracy locally within CSPs, where time costs scale linearly with the number of data owners. Our method continuously beat another blockchain-based audit scheme in a comparison analysis, showing notably reduced time costs as the number of cloud service providers rose. This demonstrates its efficacy and scalability in large-scale CSP systems. These results validate the approach's capacity to preserve data integrity throughout various cloud storage providers, boosting trust via safe, decentralised verification enabled by Homomorphic Verifiable Tags (HVT) and Chain-Code. To further strengthen the framework, future research should focus on increasing system robustness and investigating new security mechanisms.

To sum up, our method offers a stable solution for large-scale multi-cloud data integrity verification, offering the necessary time efficiency and scalability required for real-world deployment in intricate cloud systems. Because cutting-edge cryptographic algorithms are integrated, data integrity verification is reliable and secure, making it appropriate for a wide range of applications in cloud computing infrastructures.

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 1, 2024

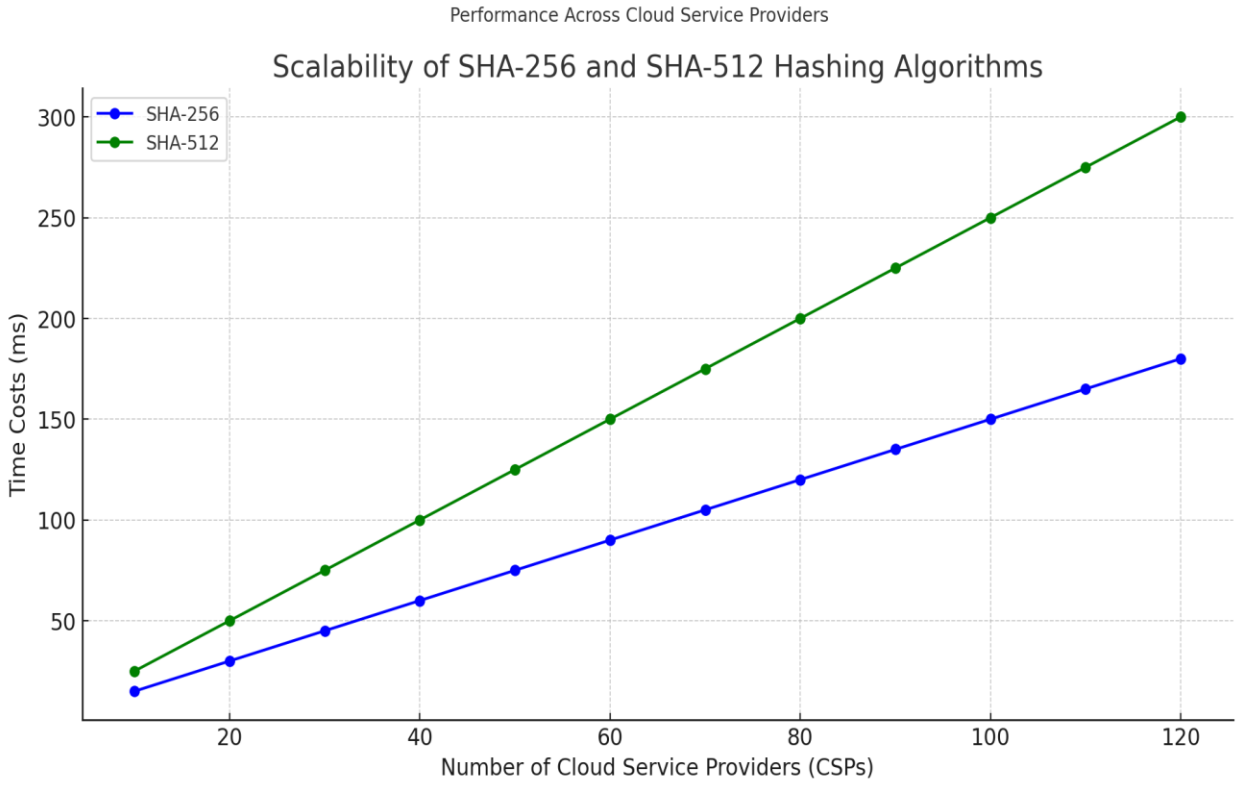

Figure 4: Scalability Of SHA-256 And SHA-512 Hashing Algorithms

The above Fig 4 illustrates the performance of SHA-256 and SHA-512 hashing algorithms across varying numbers of Cloud Service Providers (CSPs). As the number of CSPs increases from 10 to 120, the time costs for both algorithms exhibit a linear growth pattern. SHA-512 consistently requires more time than SHA-256, reflecting its higher computational complexity. This performance assessment indicates the scalability of both hashing algorithms, with SHA-256 being more efficient for larger numbers of CSPs, making it a preferable choice for scenarios demanding faster processing times.

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 1, 2024

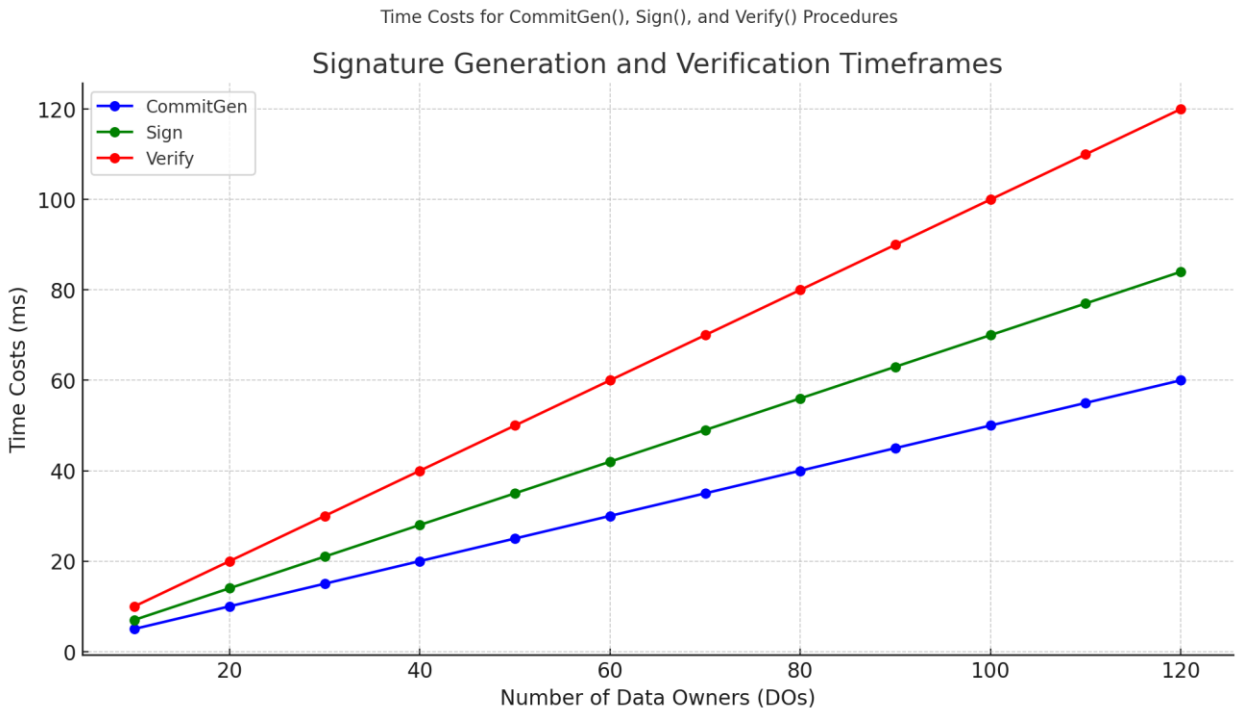

Figure 5: Signature Generation And Verification Timeframes

The above Fig 5 displays the time costs associated with the CommitGen(), Sign(), and Verify() procedures as the number of Data Owners (DOs) increases from 10 to 120. The results show that each procedure's time cost increases linearly with the number of DOs, reflecting the scalability of the system. CommitGen() and Sign() exhibit lower time costs compared to Verify(), which consistently shows the highest time costs. This indicates that while all procedures scale efficiently, verification remains the most time-consuming step, emphasizing the need for optimization in scenarios with a large number of data owners.

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 1, 2024

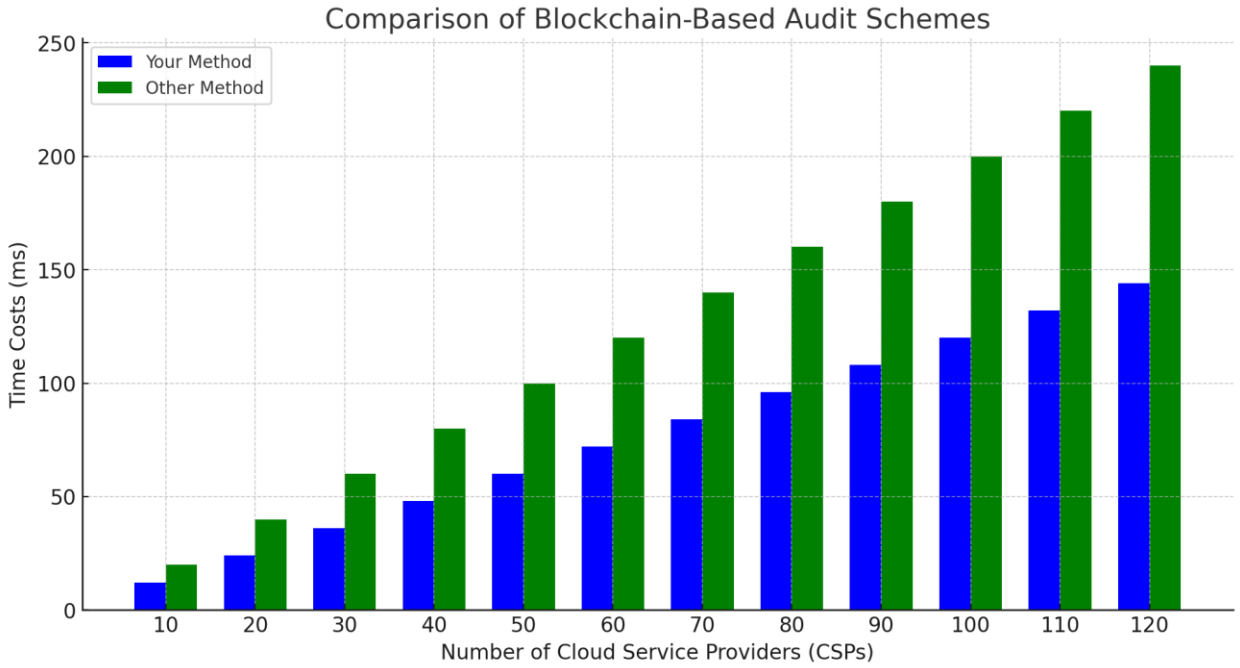

Figure 6: Comparison Of Blockchain-Based Audit Schemes

The above Fig 6 compares the time costs of two audit schemes—your method and another blockchain-based method—across varying numbers of Cloud Service Providers (CSPs) from 10 to 120. Your method consistently demonstrates lower time costs, with a more gradual increase compared to the other method, which shows significantly higher and steeper time costs as the number of CSPs grows. This indicates that your blockchain-based audit scheme is more efficient and scalable, effectively reducing the time required for data integrity verification in large-scale cloud storage environments.

5. CONCLUSION

Our blockchain-based method scales linearly with the number of data owners and guarantees strong data integrity verification locally within CSPs in multi-cloud scenarios. A comparative study reveals better results than other blockchain-based plans, with far lower time expenditures and more cloud service providers. This demonstrates the efficiency and scalability of our approach for extensive CSP installations. The approach strengthens confidence through decentralised verification by combining Chain-Code and HVT, which is essential for protecting sensitive data on many cloud platforms. Subsequent improvements ought to concentrate on augmenting system resilience and investigating sophisticated security protocols to fortify data safeguarding. Subsequent investigations ought to focus on strengthening our system's resilience by investigating sophisticated cryptographic methods and incorporating them into the verification procedure.

Examining post-quantum cryptography for long-term security resilience in cloud systems is one aspect of this.

REFERENCE

1. Wang, H., Zu, B., Zhu, W., Li, Y., & Wu, J. (2022). On the Design and Implementation of the External Data Integrity Tracking and Verification System for Stream Computing System in IoT. Sensors, 22(17), 6496.
2. Witanto, E. N., Stanley, B., & Lee, S. G. (2023). Distributed Data Integrity Verification Scheme in Multi-Cloud Environment. Sensors, 23(3), 1623.
3. Almarwani, R., Zhang, N., & Garside, J. (2021). A novel approach to data integrity auditing in PCS: Minimising any Trust on Third Parties (DIA-MTTP). Plos one, 16(1), e0244731.
4. Li, X., Yi, Z., Li, R., Wang, X. A., Li, H., & Yang, X. (2023). SM2-based offline/online efficient data integrity verification scheme for multiple application scenarios. Sensors, 23(9), 4307.
5. Tijani, B., Jaiyeola, T., Oladejo, B., & Kassam, Z. (2021). Improving data integrity in public health: a case study of an outbreak management system in Nigeria. Global Health: Science and Practice, 9(Supplement 2), S226-S233.
6. Gan, W., & Huang, B. (2022). Exploring Data Integrity of Dual-Channel Supply Chain Using Blockchain Technology. Computational Intelligence and Neuroscience, 2022(1), 3838282.
7. Sardanelli, F., & Colarieti, A. (2023). Open issues for education in radiological research: Data integrity, study reproducibility, peer-review, levels of evidence, and cross-fertilization with data scientists. La radiologia medica, 128(2), 133-135.
8. Wu, J., Xu, W., & Xia, J. (2022). Load balancing cloud storage data distribution strategy of internet of things terminal nodes considering access cost. Computational Intelligence and Neuroscience, 2022(1), 7849726.
9. Senthilkumar, S., Brindha, K., Kryvinska, N., Bhattacharya, S., & Reddy Bojja, G. (2021). SCB-HC-ECC–based privacy safeguard protocol for secure cloud storage of smart card–based health care system. Frontiers in Public Health, 9, 688399.
10. Carvalho, J., Trinta, F., & Vieira, D. (2021). A Multi-cloud Parallel Selection Approach for Unlinked Microservice Mapped to Budget's Quota: The PUM^ 2Q PUM 2 Q. In Cloud Computing and Services Science: 10th International Conference, CLOSER 2020, Prague, Czech Republic, May 7–9, 2020, Revised Selected Papers 10 (pp. 110-132). Springer International Publishing.
11. Wegner, T., Lassnig, M., Ueberholz, P., & Zeitnitz, C. (2022). Simulation and evaluation of cloud storage caching for data intensive science. Computing and Software for big Science, 6(1), 5.

12. Pollak, D. J., Chawla, G., Andreev, A., & Prober, D. A. (2023). First steps into the cloud: Using Amazon data storage and computing with Python notebooks. Plos one, 18(2), e0278316.
13. Jujjavarapu, R. M., & Poulose, A. (2022). Verilog design, synthesis, and netlisting of IoT-based arithmetic logic and compression unit for 32 nm HVT cells. Signals, 3(3), 620-641.
14. Zhang, C., Xu, Y., Hu, Y., Wu, J., Ren, J., & Zhang, Y. (2021). A blockchain-based multi-cloud storage data auditing scheme to locate faults. IEEE Transactions on Cloud Computing, 10(4), 2252-2263.
15. Han, H., Fei, S., Yan, Z., & Zhou, X. (2022). A survey on blockchain-based integrity auditing for cloud data. Digital Communications and Networks, 8(5), 591-603.
16. Chen, L., Fu, Q., Mu, Y., Zeng, L., Rezaeibagha, F., & Hwang, M. S. (2022). Blockchain-based random auditor committee for integrity verification. Future Generation Computer Systems, 131, 183-193.
17. Wang, F., Zhou, J. T., Wang, H., & Guo, X. (2022, December). A blockchain-based multi-cloud storage data consistency verification scheme. In 2022 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom) (pp. 371-377). IEEE.
18. Gangadevi, K., & Devi, R. R. (2021, March). A survey on data integrity verification schemes using blockchain technology in Cloud Computing Environment. In IOP Conference Series: Materials Science and Engineering (Vol. 1110, No. 1, p. 012011). IOP Publishing.