EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Smart Contracts for Ensuring Data Integrity in Cloud Storage with Blockchain

Kashish Bhurani[1], Aashna Dogra[2], Prerna Agarwal[3*], Pranav Shrivastava[4], Thipendra P Singh[5] and Mohit Bhandwal[6]

[1,2,3]School of Computer Science Engineering & Technology, Bennett University, Greater Noida, India
[4,6]Department of Information Technology & Engineering, Amity University Tashkent, Uzbekistan
[5]Department of Information Technology & Engineering, Bennett University, Greater Noida, India

Abstract

INTRODUCTION: Data integrity protection has become a significant priority for both consumers and organizations as cloud storage alternatives have multiplied since they provide scalable solutions for individuals and organizations alike. Traditional cloud storage systems need to find new ways to increase security because they are prone to data modification and unauthorized access thus causing data breaches.
OBJECTIVES: The main objective of this study is to review usage of smart contracts and blockchain technology to ensure data integrity in cloud storage.
METHODS: . Case studies, performance evaluations, and a thorough literature review are all used to demonstrate the effectiveness of the suggested system.
RESULTS: This research has unveiled a revolutionary approach that capitalizes on the fusion of smart contracts and cloud storage, fortified by blockchain technology.
CONCLUSION: This theoretical analysis demonstrate that smart contracts offer a dependable and scalable mechanism for maintaining data integrity in cloud storage, opening up a promising area for further research and practical application.

Keywords: Cloud Storage, Blockchain, Smart Contracts, Data Privacy Enhancement, Decentralisation, Data Access Control, Secure Data Storage

Received on 27 December 2023, accepted on 28 March 2024, published on 04 April 2024

Copyright © 2024 K. Bhurani *et al.*, licensed to EAI. This is an open access article distributed under the terms of the CC BY-NC-SA 4.0, which permits copying, redistributing, remixing, transformation, and building upon the material in any medium so long as the original work is properly cited.

doi: 10.4108/eetsis.5633

1. Introduction

The modern world's pioneering service paradigm of cloud storage has transformed the data management landscape with scalability, cost savings, accessibility, and effectiveness which traditional storage methods failed to do. Users can now store data on distant servers that are controlled by different companies and reachable via internal networks such as VPNs, which securely link users to cloud data centres. Redundancy is ensured through data replication, while data security comes from access control measures. Through secure connections, users upload and control data, expanding their architecture to distant servers for adaptability and scalability [1]. As it does away with actual hardware, boosts productivity, broadens its global reach, and has a smaller negative environmental impact it is growing in popularity. Despite the numerous advantages, the escalating usage of cloud storage brings forth a critical challenge: the paramount importance of protecting data integrity. With the potential for data breaches heightened by the technology's widespread accessibility and scalability, ensuring the integrity of data becomes a top priority.
In the context of this study, several research gaps draw attention:

(i) Smart Contracts and Blockchain Integration

*Prerna Agarwal. Email: prerna.agarwal@bennett.edu.in,

The integration of smart contracts and blockchain technology into cloud storage systems remains an underexplored area. Understanding how these decentralized and tamper-proof technologies can contribute to data integrity in the cloud is a critical research gap.

(ii) Addressing Data Breach Risks:

While the advantages of cloud storage are clear, the associated risks, especially in terms of data breaches, need to be systematically addressed. Investigating how smart contracts and blockchain can act as a robust defence mechanism against potential breaches is an essential research focus.

(iii) Impact on Data Security and Scalability

The potential impact of smart contracts and blockchain on overall data security and the scalability of cloud storage solutions is a key area requiring exploration. Determining how these technologies enhance security measures and adapt to the growing demands of cloud storage is crucial.

This study seeks to bridge the research gaps by investigating the possibilities of smart contracts and blockchain technology as a remedy for data integrity issues in cloud storage. By exploring the integration of these technologies, the aim is to provide insights into how they ensure immutability, decentralization, and enhanced security, thereby mitigating the risks associated with the expanding landscape of cloud storage.

1.1. Data integrity challenges in Cloud storage

Data accuracy, consistency, and dependability throughout a piece of data's lifecycle are referred to as data integrity. Data integrity assurance is made more difficult by cloud systems' dynamic and elastic nature. Inconsistencies could arise from the possibility of data transfer, replication, and synchronisation among different cloud instances [1]. However, a mix of technical solutions and strong rules is required to ensure data integrity completely.

There are many different sorts of data integrity issues, including breaches brought on by insufficient access controls, malware and viruses, data interception brought on by unauthorised data interruption during transmission, and data breaches brought on by hackers. Moreover, data integrity can also be affected by software defects and hardware malfunctions. To effectively tackle these challenges, a robust strategy involves employing encryption, setting access restrictions, and consistent monitoring. This approach safeguards against evolving threats as cloud storage gains broader adoption [2].

Additionally, data integrity may be compromised during both storage and transmission. Attacks known as "man-in-the-middle," in which an attacker intercepts and changes data in transit, present a significant and huge risk. Additionally, data stored on centralised systems is vulnerable to tampering and manipulation by undesirable actors, including insider threats and much more. Table 1 given below lists some cloud storage models and their vulnerabilities.

Table 1. Cloud Storage Models and their Vulnerabilities

Cloud Storage Models	Vulnerabilities
Public Cloud	Risk of unauthorized access due to shared infrastructure
Private Cloud	Incorrect configurations can lead to data exposure during transmission of data.
Community Cloud	Preserving data integrity across various settings becomes difficult
Hybrid Cloud	Shared resources increase risks

1.2. Introduction to Blockchain Technology and Smart Contracts

Blockchain is a distributed ledger system that manages an ever-growing database of data called blocks that are linked together and secured by encryption. Blockchain's decentralised architecture makes it resistant to hacking and single points of failure, making it an attractive solution for secure data storage and management.

Smart contracts are agreements that execute according to their terms automatically and are written in code. These contracts automatically take effect without the involvement of any middlemen if certain requirements are met. Smart contracts can be used to enforce data access and storage limitations in the context of cloud storage, maintaining the security and integrity of the data [3].

1.3. Explanation of blockchain architecture and key components

Blockchain architecture is a decentralized and tamper-resistant structure that underpins cryptocurrencies and various applications beyond. It is made up of interconnecting data chunks that are connected by cryptographic hashes to create an immutable chain. Data integrity is guaranteed by this setup, making it reliable and impervious to tampering. Blocks for storing data, cryptographic hashing for linking, consensus methods for agreement, and distributed nodes for decentralisation are important components. Figure 1 given below gives an overview of Blockchain Architecture.

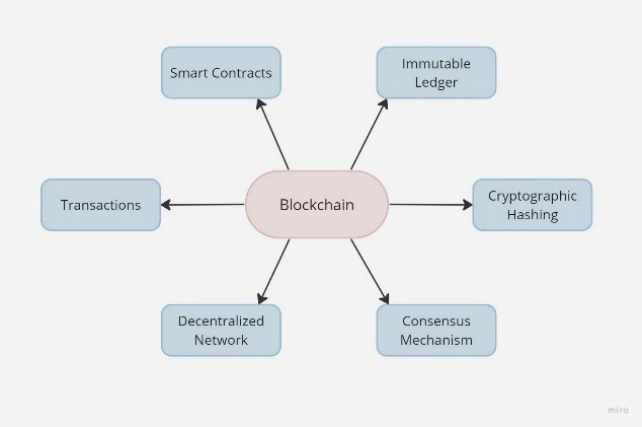

Figure 1. Blockchain Architecture

2. Literature Review

2.1 Data integrity issues in traditional cloud storage systems

Data integrity issues in traditional cloud storage systems are critical concerns that impact the reliability and security of stored data. The following table highlights some common data integrity challenges faced in traditional cloud storage. Table 2 given below lists major data integrity issues.

Table 2. Data Integrity Issues

Data Integrity Issue	Description
Data Tampering	Data corruption caused by unauthorized data alteration during transport or storage [1].
Data Loss	Deletion of data that is either accidental or deliberate and results in information loss [4].
Man-in-the-Middle Attacks	When data is being transmitted from the user to the cloud server, an attacker intercepts it and changes it [5].
Insider Threats	Individuals with access to the cloud storage infrastructure engaging in malicious activity [6].
Hardware Failures	Physical malfunctions in servers or storage devices that result in data loss or corruption [7].
Lack of Transparency	Limited understanding of the data management procedures and security measures employed by the cloud provider [8].

2.2 Blockchain and its role in enhancing data integrity.

A remarkable innovation, blockchain, an independent and irreversible digital ledger system, has emerged with the potential to alter a variety of industries, including data management.

A critical review on 'Smart Contracts in Blockchain Technology' explains how blockchain works. Each new block in the blockchain's architecture seamlessly incorporates a cryptographic hash derived from the block before it, creating a continuous web of connected data. This interdependence suggests an immutable chain, where attempts to change a single block inevitably have an impact on succeeding blocks, creating an impossible barrier against unauthorized data tampering. Real-time data verification becomes a fundamental aspect of the world as a result of the blockchain network's orchestration, where all stakeholders are given access to the same version of the ledger [9].

Additionally, data verification processes are automated by smart contracts built into the blockchain, increasing openness and reducing the need for middlemen [10]. Users are empowered by this transparency to rigorously evaluate the fidelity, accuracy, and untarnished state of the data, which is suitably authenticated by comparing the current data to historical cryptographic hashes.

This combination of automated validation and decentralized trust enhances data integrity while also revolutionizing how different businesses approach secure and open data management.

2.3 Smart contracts and their applications in cloud storage

Smart contracts ensure that transactions only occur upon the satisfaction of predetermined criteria by enacting established rules and conditions. They can automate procedures like data retrieval, sharing, and backup in cloud storage. In a decentralized network, smart contracts can be used to distribute and manage files. A decentralized cloud storage system that ensures data availability and dependability utilizing blockchain and smart contracts [11].

The use of smart contracts to enable exact access control has been looked into in the context of cloud-based data sharing. This method effectively maintains data security by ensuring that only authorized parties are permitted access to data.

Granular access control is also incorporated into smart contracts, creating a transparent audit trail that improves accountability and ensures a verifiable record of data access actions. A smart contract-based strategy was put up by Wang et al. to guarantee data integrity and provenance in cloud storage. Users may track changes and have a reliable history

of their data thanks to the smart contract's data integrity verification [12].

2.4 Using smart contracts for data integrity in cloud storage.

The viability and security implications of using smart contracts ensure data integrity in cloud storage have been examined in several studies. A blockchain-based cloud storage system with smart contracts can be used to improve data integrity and access control. The decentralized nature of blockchain combined with smart contracts can effectively address security challenges in cloud storage, such as data tampering and unauthorized access [13].

Comparing various smart contract systems for data integrity in cloud storage it was evaluated that the performance and security features of various blockchain frameworks and emphasized the potential advantages of utilizing smart contracts to guarantee data integrity in cloud storage systems [14].

As a result, the security and integrity of data in cloud storage systems could be considerably enhanced by smart contracts and blockchain technology. Smart contracts simplify data management processes and provide a solid way to set access controls, while blockchain's immutability and transparency guarantee that data is kept unaltered and verifiable. As this field of study develops, we might expect even more innovative applications of blockchain and smart contract technologies to alter data integrity and security in cloud storage.

2.5 Previous research on issues with Blockchain and Smart Contracts.

The table 3 outlines some major issues and vulnerabilities in smart contracts summarised from various studies and reviews.

Table 3: Comparisons of issues and solutions from current literature

Current Issues	Solutions Proposed
Different blockchains employ different protocols and technology, which might make communicating with one another challenging.	Smart contracts can assist to improve interoperability by offering a common platform for developers to construct apps that can operate on many blockchains [15].
Blockchains can only handle a certain amount of transactions at a time, due to which congestion and expensive transaction fees occur [16].	By allowing batch processing of transactions and outsourcing certain work to off-chain devices, smart contracts can help in increasing scalability [16].
Attacks on Smart Contracts due to liability issues, for example, The DAO which caused a major loss of 60 million US dollars [17].	Before being deployed on the blockchain, smart contracts must be thoroughly examined for security flaws.
Vulnerabilities in security, logic and privacy are a major weak point of Smart Contracts [18].	Static analysis, dynamic analysis, and fuzz testing techniques combined with AI can help improve the discovery of smart contract security flaws [19].

3. Methodology

3.1 Selection of blockchain platform and cloud storage provider

With a focus on data integrity, choosing the best blockchain platform and cloud storage provider requires a thorough evaluation of important variables. Aligning the platform with the particular use case is crucial in the blockchain scenario. For instance, Ethereum's decentralised and open architecture makes it excellent at executing tamper-proof smart contracts and preserving data integrity [20].

The success of a project depends on choosing the best blockchain platform and cloud storage provider. Scalability, consensus procedures, and a responsive community are critical components of blockchain technology. Smart contracts increase functionality, and vigilant security monitoring reduces risks. Securing data security, improving performance, scalability, and redundancy are crucial when it comes to cloud storage. Cohesion is ensured by matching storage with the blockchain architecture of choice.

Compliance with data protection laws, dependable assistance, and easy integration are essential. A successful outcome is built on a thorough evaluation that is sensitive to project specifics.

3.2 Designing Smart Controls

It takes a lot of work to create a smart contract that is efficient for blockchain-based data integrity verification. The main goal is to create a transparent, uncorruptible system that guarantees the integrity and immutability of data. This entails using cryptographic methods like hashing and digital signatures to establish verifiable records and validate the accuracy of stored data [21].

In order to guarantee the validity of data throughout the network, a well-designed smart contract should use consensus techniques like Proof of Authority (PoA) or Proof of Stake (PoS). The capacity of the contract to connect with

outside data sources may be improved using oracles, providing real-time validation and verification [22].

All the techniques used will then be incorporated into the smart contract's code, enabling it to automatically verify data and guarantee its immutability. Figure 2 given below explains the entire process and components to keep in mind when designing Smart Contracts and improving data integrity in cloud storage.

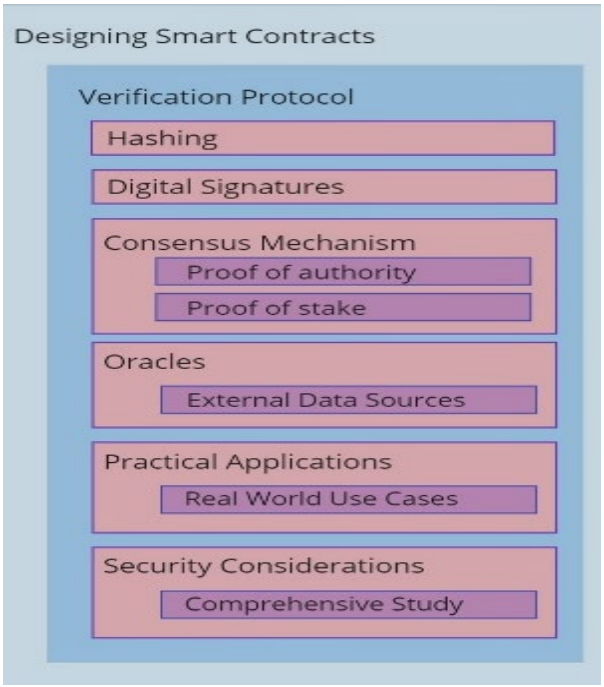

Figure 2. Components used for designing smart contracts. [23]

3.3 Integration of smart contracts with cloud storage infrastructure

Data management and automation will undergo a revolutionary change because of the integration of smart contracts with cloud storage infrastructure. The use of self-executing code known as "smart contracts" on blockchain networks is typically connected to decentralised transactions. Their incorporation with cloud storage, however, brings about unique capabilities. Without the aid of middlemen, these contracts can independently regulate data-related operations including access restriction, sharing, and validation.

Smart contracts in this environment can enable easy and secure data sharing between authorised parties. If a payment is made or a document is digitally signed, for instance, a contract might automatically provide access to particular data kept in the cloud once those circumstances are satisfied. By minimising human interference, such automation not only speeds up procedures but also improves data security.

Moreover, they can also ensure data integrity by keeping track of modifications to files stored in the cloud and launching responses when tampering is discovered. Critical information's accuracy and dependability are preserved as a result. The privacy of private information must be protected in the open blockchain environment, and scalability issues must be resolved.

4. Smart Contracts for Data Integrity in Cloud Storage

The primary foundation for building trustworthiness, known as data integrity, is to maintain data accuracy, unaltered content, and continuous coherence throughout its existence. Data integrity faces a variety of problems within the constraints of conventional cloud storage architectures, ranging from transmission flaws during upload and download operations to the constant danger of unwanted data modification.

4.1 Verifying data integrity using blockchain and smart contracts.

A blockchain essentially serves as a distributed and immutable data architecture that stores data across a contributor network. Because of the cryptographic linkage, it is ensured that every change to a single block requires consent from most participants, creating a significant barrier to unwanted data tampering.

Verification techniques are included in smart contracts to guarantee data integrity. The contract hashes the input data and compares it to the original hash that is kept on the blockchain. The data is unmodified if the hashes match; a mismatch suggests tampering. Due to the execution of contractual requirements being closely linked to the underlying code rather than being dependent on human comprehension, this automation brings about a level of transparency and confidence that is unmatched. Digital signatures may be used for additional verification. The contract verifies the signatures against the matching public keys before the data owners sign their inputs with private keys. This improves accountability and sincerity.

4.2 Implementation details of the smart contract for data integrity

A combination of technical factors, coding standards, and deployment procedures go into implementing a smart contract for data integrity verification. When developing smart contracts, it is critical to keep a number of crucial factors in mind, including upgradability, thorough event logging, gas efficiency, and transparency.

Table 4. Technical Factors and Coding Standards while implementing smart contracts.

Factors	Description
Contract Structure	Entails defining the functions for data retrieval, updates, verification, granularity of data storage, metadata inclusion for provenance, and the type of cryptographic hashes used for verification.
Data storage and Hashing	Data is hashed before storage using techniques like SHA-256 or Keccak which guarantees that every alteration to the data, no matter how slight, produces an entirely new hash. And this storage is either done off-chain (scalable) or on-chain (tamper-proof).
Consensus Protocols	Proof-of-Work - PoW (computational power), Proof-of-Stake - PoS (stake ownership), Practical Byzantine Fault Tolerance - PBFT (faster) are some protocols that offer security.
Gas Efficiency	Gas refers to the extra cost associated with completing a smart contract or transaction on the blockchain network. Efficiency measures include reduced storage operations and optimizing code execution with effective data structures [24].
Transparency and Testing	Event logs are stored on-chain and can be monitored by external systems. Risks related to coding flaws, vulnerabilities, and potential exploits are reduced via vulnerability assessments, code reviews, and third-party audits.

Transparency and Testing Event logs are stored on-chain and can be monitored by external systems. Risks related to coding flaws, vulnerabilities, and potential exploits are reduced via vulnerability assessments, code reviews, and third-party audits.

4.3 Ensuring tamper-proof data storage and retrieval

The created smart contract has a thorough structure that includes a mapping of various data IDs connected to the associated data hashes. To enable efficient iteration, an array containing all identifiers is also included. The validation function methodically compares these inputs with their stored counterparts using an identity and its associated hash, creating a strong assurance of data fidelity.

In contrast to the method described in a US Patent application [25]; a new, distinctive identification for the new versions of the data can be introduced to the smart contract. This enables the simultaneous validation of several data versions. Blockchain-based hash validation requires the availability of the data in some fashion because the data are not kept in the blockchain itself. This means that when original data is destroyed or its integrity is compromised, blockchain-based hash validation cannot recover it. Therefore, the use of this method should always be accompanied with a mechanism to recover lost data, such as a sufficiently robust backup protocol and periodical data validations. This makes it possible to identify changes in this data quickly and restore the accurate data.

4.4 Security considerations and potential vulnerabilities

Data security has undergone a paradigm shift with the use of blockchain technology and smart contracts, but this change is not without its own set of security concerns and vulnerabilities. While the tamper-proof, decentralized structure of blockchains increases security, they can complicate network attacks and consensus procedures [26]. While automating procedures and increasing transparency, smart contracts are nevertheless prone to coding mistakes and logic errors that could have disastrous results [27]. The irrevocable nature of blockchain transactions can also increase the effect of any security failure. Organizations must carefully evaluate and fix these vulnerabilities, implementing strong security controls, and carrying out rigorous audits to prevent exploitation and maintain the integrity of their systems.

5. Evaluation

5.1 Metrics for evaluating the effectiveness of the proposed system.

(i) Tamper Detection Rate: This metric measures how well smart contracts spot unauthorised changes to data that have been stored. The detection rate can be determined by including simulated tampering situations in the dataset and calculating it as the proportion of accurately identified tampered cases to all tampered instances [28].

(ii) Response Time: Simulating tampering situations allows for the measurement of how quickly smart contracts can recognise and react to breaches. A more effective data integrity validation method is indicated by faster response time.

(iii) Data Consistency: The percentage of consistent data can be calculated by comparing the initial dataset with the version protected by smart contracts, demonstrating the efficiency of the smart contract in keeping synchronised and unaltered data.

(iv) Scalability: By enlarging the dataset, it is possible to assess the smart contract's capacity to maintain

quick validation times and guarantee data integrity as the system grows.

(v) Security Resilience: Security testing and analysis can be used to determine how well smart contracts protect data from flaws, attacks, and unauthorised access.

5.2 Tamper Detection Rate of the approach

Using blockchain technology, an immutable, transparent ledger may be used to store and verify data. The decentralised and distributed structure of blockchain allows for the simple detection and flagging of tampering efforts. A key component of guaranteeing data security and integrity in smart contracts used for cloud storage is the tamper detection rate. The system can spot any unauthorised alterations or attempts at tampering with the stored data by utilising tamper detection methods such as Digital Signatures, Merkle Trees and Intrusion detection system [29]. These methods rely on digital signatures or cryptographic hashes to confirm the accuracy of the data. Any modifications to the data will cause a mismatch, which will reveal manipulation.

5.3 Response Time

The time it takes for a smart contract to carry out its operations and deliver a result is referred to as the response time of smart contracts. The complexity of the contract, network congestion, and the blockchain's consensus mechanism are some of the variables that can affect this [30].

In the context of smart contracts, "Response Time" refers to gauging how quickly these automated contracts can spot and react to instances of tampering or breaches. Researchers and professionals can evaluate how responsive smart contracts are to detecting unauthorized alterations or attempts to manipulate its logic or data by simulating tampering situations. A key proposition is that faster response times imply a more efficient way of ensuring data integrity within smart contracts. In other words, the ability of a smart contract, to identify violations and take appropriate action quickly shows the availability of strong safeguards for validating and ensuring the execution of the contract's integrity.

5.4 Data Consistency

Data consistency is the guarantee that data stays synchronized and coherent across several cloud providers in the context of multi-cloud applications and smart contract orchestration. A multi-cloud architecture might make it difficult to achieve data consistency because of things like network latency, variable data replication techniques, and potential conflicts across multiple cloud platforms [31].

Quantifying the effectiveness of the contract in retaining synced and unaltered data can be done by comparing the original dataset with the one that is protected by smart contracts. It illustrates the contract's capacity to fulfil its stated goals of guaranteeing data transparency and integrity. However, there are a number of challenges along the way to reaching this quantified assurance. The methodology needs to take into account the dynamic nature of the data and recognize allowed changes while highlighting illegal ones. The accuracy of the initial dataset used as the baseline must also be carefully checked; any flaws or imperfections in this dataset could affect the derived measure of consistency.

5.5 Scalability analysis of the blockchain based approach.

The system's capacity to manage rising workloads while retaining performance and efficiency is evaluated as part of the scalability analysis of a blockchain-based solution leveraging smart contracts for data integrity. Blockchain networks have difficulties with transaction performance, latency, and resource consumption as data quantities increase.

Bitcoin-NG is a blockchain technology that aims to increase scalability by accelerating transaction processing. In contrast to conventional proof-of-work consensus systems, it does this by electing a leader for a brief period of time, allowing for a greater rate of transaction inclusion. This strategy shortens the gap between blocks and boosts throughput as a whole.

A survey that analyses several approaches to deal with scalability challenges in blockchain networks [32]. For instance, sharding divides the network into separate sections (shards) to enable transaction processing in parallel. By allowing transactions to take place on distinct chains connected to the primary blockchain, sidechains help to further reduce congestion. Figure 3 compares the execution time of two scalability schemes [33].

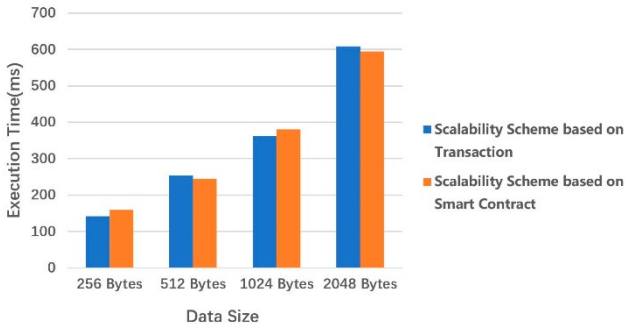

Figure 3. Execution Time of Two Scalability Schemes [33]

5.6 Security Resilience

Security testing and analysis plays a vital role in assessing the resilience of smart contracts in shielding data from errors, attacks, and unauthorized access. By exposing smart contracts to rigorous testing and analysis, potential vulnerabilities can be recognized and addressed, ensuring the integrity and security of the data stored within them. Numerous techniques, such as code review, penetration testing, and formal verification, can be employed to evaluate the robustness of smart contracts and identify any weaknesses that could be subjugated by malicious actor [33].

In addition to this, mathematical proofs of the accuracy and security of smart contracts can be made using formal verification techniques like theorem proving and model checking [34]. Organisations can increase their confidence in the dependability and security of their data storage methods by rigorously analysing smart contracts.

6. Conclusion

In conclusion, the persistent data integrity challenges arising from decentralization, potential unauthorized access, and data corruption necessitate innovative solutions in the realm of cloud storage. This research has unveiled a revolutionary approach that capitalizes on the fusion of smart contracts and cloud storage, fortified by blockchain technology. These self-executing contracts, orchestrated by the secure framework of blockchain, introduce significant enhancements in both automation and data security within cloud storage environments.

This research underscores the transformative potential of smart contracts and blockchain technology in resolving data integrity challenges. The symbiotic alliance of these innovations not only promises elevated data security but also lays a robust foundation for more efficient and secure data management practices across diverse domains.

The scrutiny of pertinent evaluation metrics, including tamper detection rate, false positive rate, data integrity, reaction time, auditability, cost-effectiveness, scalability, and security resilience, has highlighted their paramount role in assessing the effectiveness of this integration. These metrics collectively gauge the proficiency of tamper detection mechanisms, precision in triggering alerts, synchronization of data, responsiveness, transparency in actions, economic viability, adaptability to heightened data loads, and resilience to potential security breaches.

As technology continues to evolve, the implementation of smart contracts and blockchain integration stands poised to reshape data management paradigms, inspiring innovation and instilling confidence in data-driven operations. In an era where data integrity is paramount, this research paves the way for a future marked by resilient and accountable data management practices, setting new standards for security and efficiency in the digital age.

References

[1] Mell P, Grance T, “The NIST Definition of Cloud Computing,” p. 7, 2011.

[2] Ristenpart, T., Tromer, E., Shacham, H., & Savage, S., “Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds,” ACM Transactions on Information and System Security, 2009.

[3] Swan. M., Blockchain: Blueprint for a new economy, O"Reilly Media, Inc, 2015.

[4] Sun Y, Zhang J, Xiong Y, Zhu G. Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks*. 2014;10(7).

[5] A. Menezes, P. van Oorschot and S. Vanstone, Handbook of applied crytography, 1997.

[6] Rizwana Shaikh, M. Sasikumar . Security Issues in Cloud Computing: A survey. International Journal of Computer Applications. 44, 19 (April 2012), 4-10.

[7] Shroff G. &. Melhem R., “Cloud computing: Challenges & opportunities.,” in IEEE International Conference on Advanced Information Networking and Applications, 2010.

[8] Pearson, S. (2009) "Taking account of privacy when designing cloud computing services", Workshop on Software Engineering Challenges of Cloud Computing (CLOUD'09), 44- 52.

[9] H. Taherdoost, Smart Contracts in Blockchain Technology: A Critical Review, 2023.

[10] Mougayar. W., The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology., 2016.

[11] Li X., Cao J.,Chen S., Yu L. & Kim H.K., A secure and efficient cloud storage system using a consortium blockchain. Information Sciences, 2020.

[12] Wan X., Li Z., Cao J., & Ren K., “Verifiable fine-grained data integrity and provenance control in cloud storage.,” IEEE Transactions on Dependable and Secure Computing , 2019.

[13] Kwak J., Lee H., & Kim S., “A Blockchain-Based Secure Cloud Storage System with Auditing and Revoking,” IEEE Access, 2019.

[14] Li H., Xiong H., Wang M. & Li Y., “A Comparative Study of Blockchain-Based Smart Contract Platforms for Cloud Data Integrity,” IEEE Transactions on Services Computing, 2020.

[15] Huang Y., Wang B., Wang Y., “Research and Application of Smart Contract Based on Ethereum Blockchain,” Journal of Physics, 2021.

[16] Vacca A., Sorbo A., Vissagio C., Canfora G., “A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges,” Journal of Systems and Software, vol. 174, p. 110891, 2020.

[17] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur and H. -N. Lee, "Ethereum Smart Contract Analysis Tools: A Systematic Review," in *IEEE Access*, vol. 10, pp. 57037-57062, 2022, doi: 10.1109/ACCESS.2022.3169902.

[18] M. Krichen, Strengthening the Security of Smart Contracts through the Power of Artificial Intelligence, 2023.

[19] D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, 2017.

[20] J. Newsome, Smart Contracts: 12 Use Cases for Business & Beyond, 2015.

[21] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly Media, 2014.
[22] Liu Z, Feng W, Zhang Y, Zhu C. Research on the Architecture of Transactional Smart Contracts Based on Blockchains. *Electronics*. 2023; 12(18):3923. https://doi.org/10.3390/electronics12183923
[23] "Web3 University," [Online]. Available: https://www.web3.university/tracks/create-a-smart-contract/what-is-gas-and-how-is-it-used.
[24] Barinov I., Lysenko V., Beloussov S. Shmulevich M., Protasov S., "System and method for verifying data integrity using blockchain network". Patent 20180025181, 2018.
[25] Dinh T., Wang J., Chen G., Liu R., & Ooi B.C., "Blockchain-Based Data Management and Analytics for Microservices.," in IEEE Transactions on Services Computing, 2018.
[26] Atzei N., Bartoletti M.,Cimoli T., "A Survey of Attacks on Ethereum Smart Contracts (SoK)," in 6th International Conference on Principles of Security and Trust (POST), 2017.
[27] Gupta et al, Enhancing Data Integrity in Cloud Storage Using Tamper Detection Techniques, 2021.
[28] Wang et al, Tamper Detection Rate Evaluation of Blockchain-Based Cloud Storage Systems, 2023.
[29] Wang J. et al, Evaluating the Response Time of Smart Contracts in Public Blockchains, 2021.
[30] Bessani A. et al, Smart Contact Orchestration for Multi-Cloud Applications, 2022.
[31] Wang et al, Blockchain enabled smart contracts, 2019.
[32] Bhattacharya et al, Security Analysis of Smart Contracts: A Comprehensive Study, 2022.
[33] Yu C, Mei N, Du C, Luo H. Blockchain Data Scalability and Retrieval Scheme Based on On-Chain Storage Medium for Internet of Things Data. *Electronics*. 2023;12(6):1454. https://doi.org/10.3390/electronics12061454