iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.83157

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Cost Efficient & Scalable Blockchain Architecture for Cloud Computing Integrity Auditing

Mr. Kunal Mohan Pawar, Ms. Pooja Tupe
Dept. of Information Technology University of Mumbai Mumbai, India

Abstract: ***In today's world, cloud computing has become the primary choice for data storage and management. However, the security of data stored in a distributed environment via the cloud remains a key challenge. The traditional approaches to the verification of integrity rely heavily on the use of centralized architectures, which result in lack of transparency, trust, and vulnerability to failure points. Blockchain technology has been proposed as a decentralized means for securing data integrity in a cloud computing environment due to those limitations. It becomes clear that blockchain technology allows us to improve security and transparency significantly; however, at the moment, all existing solutions tend to consider only certain aspects of the problem such as auditing, optimization of the storage space, etc. Most critical insights obtained in the research include the issues of high cost, large overhead, limited scalability, and complicated architecture. Moreover, most studies do not have adequate cost considerations and practical validation regarding implementation. Based on the above analysis, this paper proposes important areas for further study, such as the development of architectures that are scalable, cost-effective, and feature data integrity schemes. In addition, the research suggests the need for a unified solution that will integrate sharding, off-chaining, and layer-two methods for massive cloud infrastructures.***

I. INTRODUCTION

The use of cloud computing has been a necessary feature of contemporary data storage and processing because of its versatility, scalability, and affordability. With increased dependence on cloud services providers by enterprises, cloud data integrity becomes an important issue because it deals with the protection and maintenance of data consistency and accuracy when it comes to storing, transferring, and retrieving data from cloud storage. The problem is that people do not usually have any control over distant cloud servers; therefore, it may be difficult to verify whether data is changed or deleted by malicious individuals and faulty cloud storage servers.

It seems that traditional solutions for cloud data integrity verification depend on centralization and third-party audits. Such approaches imply using a centralized system, which poses serious risks related to data and network security. Therefore, researchers have tried to apply blockchain technology to increase the level of security of the data verification process by making it more transparent and decentralized.

However, despite its numerous benefits, there are some problems associated with blockchain technology that have not been solved yet. One of the biggest challenges faced by blockchain-based systems is scalability issues, excessive transaction fees, and additional storage overhead, especially in cases where massive amounts of cloud data need to be processed. With the growing use of cloud computing platforms, the development of blockchain infrastructure has also become more widespread. Nonetheless, combining blockchain with cloud infrastructures poses many issues associated with performance efficiency, scalability, and safe cloud data handling. Thus, the creation of scalable blockchain architectures for efficient cloud data integrity becomes a relevant issue for scientific research.

With the growing popularity of blockchain systems and their wide-scale application in conjunction with cloud platforms, scientists have attempted to address this problem and provide viable solutions for further research. There are already multiple studies devoted to various ways of improving blockchain systems' performance and enhancing transaction processing speed while minimizing blockchain storage overhead and ensuring maximum efficiency. Nevertheless, many studies have concentrated only on one aspect of the matter, such as auditing framework design or scalability mechanisms.

There are several classifications for the reviewed literature. First, it can be categorized as either dealing with auditing blockchain, using multiple clouds for integrity assurance, using off-chain solutions, or introducing new Layer-2 scalability methods.

In this paper, a survey of blockchain-based integrity methods in cloud computing will be provided. In this case, recent achievements and developments of blockchain applications to cloud systems, such as scalability, efficiency, and secure data verification will be examined.

For this reason, 40 scholarly articles that have been written since 2014 until 2025 have been identified and analyzed. To identify such works, it was necessary to search for the most relevant articles in reputable journals, conference publications, and online libraries.

The purpose of this paper is to conduct a thorough review of blockchain technology in terms of cloud data integrity.

Contributions of the Paper

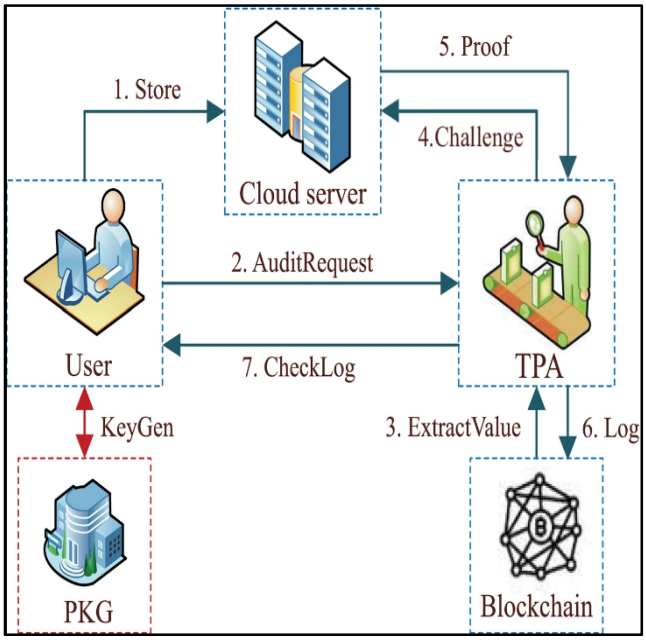
The main contributions of this study are summarized as follows:

- A systematic review of existing research on blockchain-based cloud data integrity frameworks.
- A classification of the literature into key categories including blockchain auditing frameworks, multi-cloud integrity systems, off-chain storage solutions, and Layer-2 scalability mechanisms.
- A comparative analysis of existing approaches based on architecture, scalability methods, cost considerations, and limitations.
- Identification of research gaps and challenges that remain unresolved in current blockchain-based cloud integrity solutions.
- Discussion of future research directions for developing cost-efficient and scalable blockchain architectures for cloud computing environments.

II. BACKGROUND

A. *Cloud Data Integrity*

The development of cloud computing technology has seen it emerge as an important tool used to store huge amounts of data in the modern world. Companies and individuals find themselves having to utilize the services provided by cloud service providers in order to safely store their data, thus creating the need for ensuring data integrity. Data integrity in cloud computing is the maintenance of consistency in data during its storage and transfer processes.

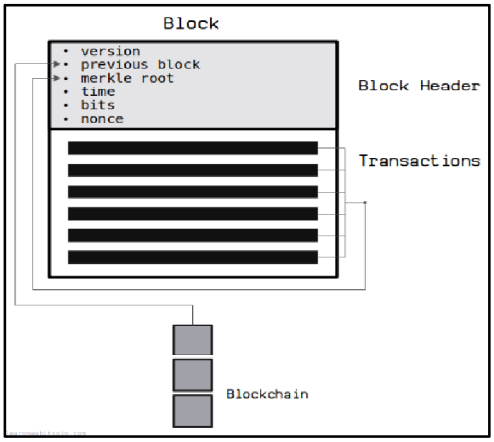


Traditional models used to verify data integrity in clouds usually use centralized audit systems or the services of third-party auditors. Users are not able to monitor the operations of remote servers and hence find it hard to check whether the data in question has been corrupted or changed in any way. Cryptography methods like hash functions, digital signatures, and proof mechanisms have been employed in maintaining data integrity in cloud computing.

Nevertheless, traditional techniques cannot be used successfully in large distributed cloud-based environments. The main reason behind this is that centralized auditing techniques might create performance bottlenecks as well as single points of failure. In addition, achieving trust and transparency between users and service providers is another obstacle faced by cloud computing systems. For this reason, decentralized techniques like blockchain technology have been utilized as potential solutions.

B. Blockchain Fundamentals

Blockchain is a distributed ledger technology that facilitates secure and tamper-proof recording of information without depending on any central authority. Transactions in a blockchain network are collected in blocks that are linked to each other via hash functions, thus forming a chain of blocks of information. All users in the blockchain network keep an identical copy of the distributed ledger for transparency purposes.



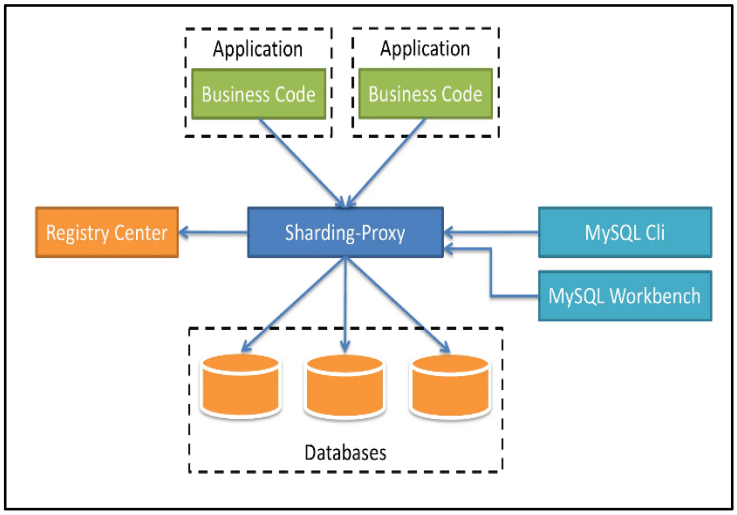
Another important feature of blockchain technology is its decentralized consensus algorithm. Consensus algorithms allow network users to jointly confirm transactions in a blockchain system. Popular consensus algorithms in blockchain technology include Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). Consensus algorithms help prevent any unauthorized changes and record only valid transactions in a blockchain network.

There are many benefits that blockchain technology can provide in cloud computing settings. The immutable nature, transparency, and distributed architecture of blockchain technology makes it an excellent fit for creating reliable logs of the activities performed on any type of data. Blockchain technology also supports smart contracts, which can automatically implement pre-defined policies and rules.

There are several issues associated with blockchain technology, especially when dealing with high transaction volumes from cloud-based applications.

C. Blockchain Scalability Issues

One of the most critical issues facing blockchain technology is scalability. As blockchain networks continue to expand, they become slower since they experience difficulties with scalability due to problems like transaction speed, latency, and transaction costs. This is due to the very structure of the technology as, for each transaction performed in a blockchain, there is a need for several different nodes to verify it.



Many public blockchains have limited the amount of data that can be stored in blocks through their consensus mechanisms, thus placing a cap on the number of transactions they can perform per second. Blockchain technology usually processes far fewer transactions than cloud servers do, especially when used for high transaction volume activities. Moreover, data storage in the blockchain results in very fast-growing ledgers.

Various scalability techniques have been suggested by researchers as possible remedies to tackle these problems, including techniques like sharding, off-chain storage techniques, and Layer-2 protocols. In sharding, the entire blockchain network is partitioned into several partitions which carry out computations in parallel fashion, hence increasing the speed and efficiency of transactions processing while alleviating the network from being congested with a large number of transactions. Off-chain storage techniques enable huge amounts of data to be stored without storing in the blockchain network but still verify integrity using hashes. While these techniques increase scalability in blockchain technologies, the integration of these technologies with cloud-based data integrity schemes is still a topic that requires more research.

III. TAXONOMY AND CLASSIFICATION OF BLOCKCHAIN-BASED INTEGRITY MECHANISMS

Blockchain technology can be considered as a viable means of improving integrity and transparency in cloud computing. Given the characteristics of blockchain technology, a number of scholars have suggested models that combine the use of blockchain technology with cloud storage systems to provide secure verification of stored data. Nevertheless, each existing solution varies greatly in its architecture, scalability techniques, and approach to storing the information. In order to get a better idea about these techniques, the available literature on the subject can be divided into four main groups. These are blockchain audit systems, multi-cloud integrity systems, off-chain storage techniques, and Layer-2 scalability solutions.

A. Blockchain Auditing Frameworks

Auditing frameworks for the blockchain concentrate on offering transparent verification methods that ensure the integrity of the data stored in cloud infrastructure. As a rule, blockchain auditing tools use cryptographic data that is registered on the blockchain to perform data verification while the actual data is stored in the cloud. Due to the inherent immutability of the blockchain, it is possible to prove that the data stored in the cloud has not been altered by unauthorized users.

Many papers discuss the use of blockchain as an effective replacement for third-party auditing services. The use of blockchain in the context of auditing usually requires the application of cryptographic methods such as hash verification, proof of storage, proof of retrievability, and aggregate verification.

However, even if blockchain auditing provides enhanced trust and transparency, these benefits come at the price of added computational burden related to the processing of the verification transactions. Besides, in the case of frequent verification of the integrity of data stored in the cloud, there could be issues of network congestion.

B. Multi-Cloud Integrity Systems

Multi-cloud integrity frameworks involve the deployment of systems where data integrity and availability are achieved by storing and managing data from multiple cloud service providers as opposed to using the centralized cloud framework. The main aspect of these models is the utilization of the blockchain technology to act as a distributed trust layer for storing information on integrity verification.

In such a system, distributed storage approaches are utilized in which data is either replicated or partitioned across various clouds. The blockchain serves as the logging mechanism that ensures integrity and consistency in data operations within all participating clouds.

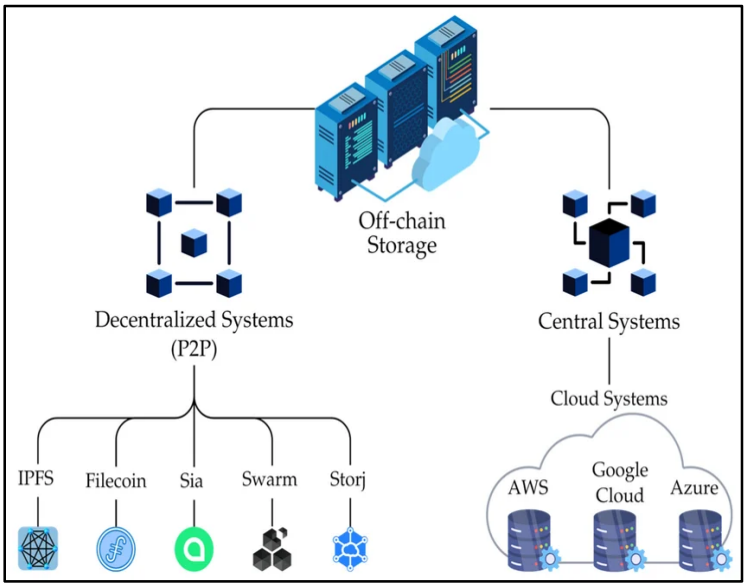
However, there are also several challenges associated with these frameworks, particularly those related to coordination and communications. Maintaining consistency and synchronization between multiple cloud systems can be challenging.

C. Off-Chain Storage Solutions

The rapid expansion of blockchain storage as more large amounts of data are added to the network constitutes one of the main limitations of blockchain technology. Many scientists and engineers suggested several ways to overcome the problem by implementing off-chain storage schemes, where large files are stored offline but have some kind of cryptographic representation within the blockchain.

Such an architecture is characterized by the use of external and usually decentralized storage solutions, such as InterPlanetary File System (IPFS). The actual content of the file can be stored offline in the distributed storage solution and will be referenced via the blockchain through its cryptographic representation – the hash value of the file or any metadata.

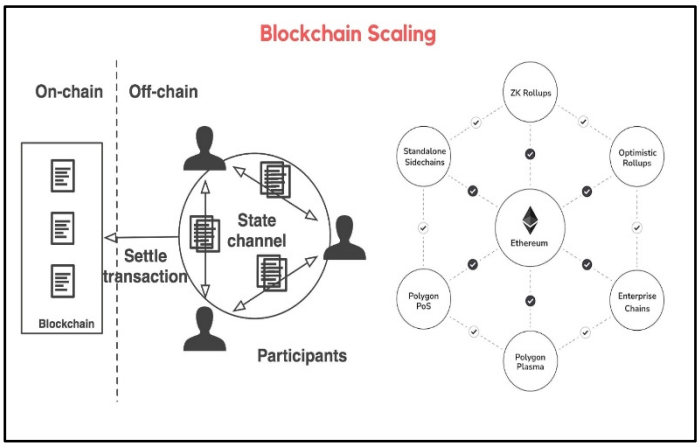
Off-chain storage solutions help reduce blockchain storage and increase system scalability. On the other hand, they may pose a threat to the integrity of the data due to their nature. Therefore, it is necessary to establish constant communication between off-chain and on-chain environments to ensure reliable information storage.



D. Layer-2 Scalability Mechanisms

Nevertheless, scalability is another problem that exists within blockchain systems, especially those that have been integrated into cloud computing environments. Layer 2 scalability systems refer to technologies employed in increasing blockchain efficiency by conducting particular operations or transactions outside the blockchain system and using cryptography to maintain security.

Typical layer 2 technologies include sidechains, state channels, roll-ups, and batch transactions. These methods allow a reduction in the number of transactions conducted on the main blockchain network and increase efficiency. The use of Layer 2 systems can greatly increase the efficiency of blockchain cloud integrity systems.



However, the implementation of these technologies involves complexities that must be considered for effective operation. Specifically, off-chain transactions should be secured and the verification process must be consistent with the main blockchain ledger. Moreover, integration of Layer 2 systems with cloud-based auditing systems presents architectural complexities.

Summary of the Taxonomy

As can be observed from the taxonomy described above, the blockchain cloud integrity schemes can be grouped into four main categories, namely auditing methods, multi-cloud integrity schemes, off-chain storage strategies, and Layer-2 scalability techniques. All these methods are used to overcome the problems related to blockchain cloud integrity issues in their own unique ways. Although all these methods are very helpful, combining them in a coherent manner is another important issue that needs to be addressed. This will be discussed in detail in the next section.

IV. LITERATURE REVIEW

A. Blockchain Auditing Frameworks

Many auditing architectures that employ blockchain technology have been developed over time due to the disadvantages experienced in the use of conventional cloud auditing methods such as dependence on trusted third-party auditors. This is achieved through the use of blockchain technology that facilitates data integrity validation via its immutability and cryptography.

Zhang et al. [1] suggested an integrity verification technique based on blockchain technology tailored for multi-cloud data storage systems. The process involves separating storage from data verification whereby the hash function values of the data stored in the clouds are recorded in a blockchain database. Users can verify the data integrity without the need to access the full data set, increasing auditing efficiency. However, there are extra costs associated with using blockchain in data verification processes.

In a similar vein, Zhou et al. [2] presented a scalable scheme based on blockchains to minimize the cost of verification by aggregating proofs. This solution reduces the amount of communication required for exchanging messages between the cloud server and the blockchain node. Though the scheme is more scalable compared with the conventional auditing system, it is based on the mechanism of aggregation, and some trustable elements can be needed for proof generation.

Han [3] performed a comprehensive analysis of blockchain-integrated integrity auditing methods for cloud data. This study provides insights into several cryptographic audit models with proof-of-storage and proof-of-retrievability mechanisms implemented in blockchain technology. In addition to revealing the benefits of decentralization in blockchain-enabled audits, the work reveals the drawbacks, such as computational and storage overheads associated with blockchain networks.

In their paper, Islam et al. [5] presented a new auditing model based on an optimized version of B-tree structures used to enhance efficiency in cloud auditing. The proposed scheme represents metadata in a hierarchical manner, which helps perform searches and verification processes faster. Even though this solution ensures high speed, it does not fully utilize decentralization features of blockchain solutions.

The Block-secure framework was presented by Li et al. [13] as a means of securing P2P cloud storage using blockchain technology. The framework involves the use of blockchain in the management of authentication and access control to enable decentralized storage between peer nodes. This approach enhances trust in the system through the use of blockchain-based identification. Nevertheless, the framework might be less efficient in managing data of high volume due to blockchain computation.

The immutability auditing framework developed by Bappy et al. [16] is one that uses blockchain to enhance transparency in terms of file version control within cloud storage services. Auditing of files and record keeping of the versions of files are done through blockchain. This ensures audit trails of files that are traceable and non-manipulative but results in increased metadata storage costs and transactions.

Storage-level integrity verification frameworks that could be considered in cloud computing are analyzed by Goswami et al. [26]. Existing methods have been classified based on the type of security involved. The paper offers a detailed analysis of storage-level integrity verification techniques but does not propose an integrity verification framework using blockchain technology.

Kumar and Bhatia [27] undertook a systematic review of cloud security mechanisms by emphasizing the core principles of confidentiality, integrity, and availability. The methodology adopted by the authors focused on studying existing security frameworks and the gaps in current cloud security mechanisms. However, despite the important findings made by Kumar and Bhatia [27], they do not offer any blockchain auditing solutions for cloud computing.

Ismail and Materwala [25] studied the architecture and consensus mechanisms in blockchain in order to explore the potential use cases for decentralized networks and secure applications. The authors explored several consensus mechanisms and their effects on security and performance. Nevertheless, while presenting an in-depth analysis of various aspects of the technology, Ismail and Materwala [25] fail to develop an auditing solution.

Zyskind et al. [33] developed a data management platform for the decentralized network based on the blockchain technology. According to the methodology suggested by the authors, access to the data is controlled by blockchain-based smart contracts whereas data is kept outside the blockchain for cost efficiency and improved performance.

Overall, while blockchain auditing frameworks significantly improve transparency and integrity verification in cloud environments, many of these systems still suffer from high verification overhead, scalability limitations, and increased transaction costs, particularly when dealing with large-scale cloud data.

B. Multi-Cloud Integrity Systems

The multi-cloud integrity approach is intended to overcome the limitations of the traditional infrastructure by decentralizing data across several clouds. The multi-cloud approach will enhance reliability, security, and fault tolerance in cloud systems. Introducing the use of blockchain within the multi-cloud approach facilitates decentralized validation and creates an environment of trust.

Huang and Yi [4] designed a new blockchain-based cryptographic key management technique enhanced with digital twin technology. In their methodology, blockchain technology is used to store key information, whereas digital twins mimic behavior to discover any anomalous activities within the cloud storage platform. Despite the fact that the model improves traceability, integrating the digital twin infrastructure makes the entire system complex.

Hemalatha [6] suggested an innovative decentralized trust management architecture that could be employed in a cloud computing environment. According to the author, decentralizing trust would facilitate the improvement of cloud systems in terms of security and scalability. However, the suggested framework is still largely theoretical and requires more empirical research.

Watane [7] studied secure multi-cloud storage solutions utilizing redundancy and distributed verification processes to achieve data integrity. In the methodology, data redundancy is implemented through replication using multiple cloud environments while cryptographic verification techniques are used to verify consistency of the data. The use of the approach entails additional communication and synchronization between cloud systems.

The work of Murthy et al. [9] suggested a blockchain-powered cloud computing architecture that incorporates distributed ledger technologies in cloud computing services. The research aims to address challenges related to security, trust and transparency in cloud environments by using a blockchain architecture. Although the methodology shows promise for improved data integrity, more evaluation is needed.

The study by Li et al. [23] suggested blockchain architecture designed for the IoT environment. The blockchain-powered system is intended to enhance secure data sharing and device authentication in IoT networks. Despite having several merits, the system incurs computational overhead.

Ali et al. [28] created a blockchain-enabled data management framework for healthcare using hybrid deep learning. The proposed framework protects patient information and provides safe information exchange between different healthcare service providers. However, implementing AI algorithms within blockchain systems requires more computational power.

Xu et al. [38] carried out a review on blockchain applications in cloud computing infrastructures by examining how the blockchain technology improves trustworthiness and transparency in cloud services. This paper illustrated the capabilities of blockchain in solving cloud security problems; however, scalability and interoperability are still major concerns.

In general, multi-cloud integrity frameworks increase data reliability and decentralized trust, but they cause communication costs, coordination difficulties, and scalability issues.

C. Off-Chain Storage Solutions

Storage scalability is among the major challenges faced by blockchains. The inability to scale storage becomes apparent when large databases are stored within the blockchain. Off-chain storage techniques have thus been developed to overcome this limitation.

Jayabalan& Jeyanthi [12] proposed a blockchain design that incorporates IPFS to enable off-chain storage of health information. Using this approach, large files are stored within IPFS whereas references in the form of cryptographic hashes are stored within the blockchain for verification purposes. This combination provides a solution to scalability issues, although dependency on IPFS nodes and latency in retrieving data become key drawbacks.

Benet [34] designed IPFS (InterPlanetary File System) as a decentralized storage technique that allows for file retrieval using a unique hash function alongside a distributed hash table. IPFS supports peer-to-peer sharing of data. It also provides an effective solution to scalability. Data persistence in IPFS, however, still relies on incentive-based schemes.

Liu et al. [32] introduced the concept of an elastic data carrier architecture for the purpose of optimizing smart contracts in blockchains. Liu et al.'s [32] methodology reduces storage overhead by isolating large components of the data from the blockchain transaction while preserving hash referencing for authentication purposes. Although the methodology is able to optimize storage in blockchains, it presents extra issues related to synchronization between the blockchain network and outside storage.

In their study, Ochôa et al. [31] discuss the cost-effectiveness of designing sidechain-based blockchain architecture within smart grid applications. The study shows that off-chain sidechains are cost-effective and secure due to anchoring to the main chain at fixed intervals. Nevertheless, sidechains have added complexities and need cross-chain communication mechanisms.
In general, off-chain storage methods minimize blockchain storage overhead, but they present additional challenges.

D. Layer-2 Scalability Mechanisms

Scalability has been another crucial problem faced by the blockchain technology industry. With the growth of blockchain systems, transaction speeds and latencies have become vital issues. The main objective of the Layer-2 scalability solution is to perform off-chain calculations and maintain security in the process.
In their review of Layer-2 proving schemes for off-chain computing and proof verification, Tortola et al. [8] investigated methods such as rollups and zero-knowledge proofs which help carry out several transactions off the main chain and verify those transactions on the main blockchain.
A bibliometric review of the blockchain literature trends done by Kandpal et al. [10] recognized scalability among the important research challenges in the field. On the other hand, Gong et al. [11] reviewed the problem of scalability in blockchain storage and suggested ways of improving scalability using data pruning and sharding.
Scalability problems in blockchain were also reviewed by Khan et al. [14] and Xie et al. [15]. They mainly considered the challenges involved in consensus protocols, transaction speeds, and network latency. Additionally, Leonardos et al. [17] reviewed the Ethereum fee market introduced in EIP-1559.
Sriman and Ganesh Kumar [18] suggested a transaction validation technique with an objective to enhance efficiency with reduced transaction cost in Ethereum-based networks. Likewise, He et al. [19] studied the inefficiency of gas in actual world smart contract implementations and offered ways for minimizing transaction cost.
Scalability measures such as sharding and consensus algorithm optimization techniques have been highlighted by Chauhan et al. [20] and Kaur and Gandhi [21]. Furthermore, Rao et al. [22] reviewed blockchain scalability technologies along with the scope for future studies.
Mohamed et al. [24] developed an efficient blockchain mining framework to optimize energy expenditure by utilizing renewable energy sources in mining activities.
The foundational research work has also been instrumental in developing blockchain scalability solutions. In this regard, Gervais et al. [35] studied the performance and security tradeoffs in proof-of-work blockchains. Buterin [36] created the Ethereum platform, which enables programmable smart contracts but is challenged by scalability issues. Furthermore, Croman et al. [37] examined scaling issues associated with decentralized blockchain architectures and provided enhancements to the network architecture.
Zheng et al. [39] and Casino et al. [40] performed extensive reviews on blockchain technology, pinpointing scalability, privacy, and interoperability as key research issues.
While Layer-2 solutions provide significant benefits such as improved transaction rate and cost reduction, the deployment of such solutions in cloud-enabled blockchain architecture is an arduous task.

Comparison Table

Paper	Approach	Blockchain Type	Scalability Method	Cost Analysis	Limitations
Zhang 2022 [1]	Multi-cloud integrity verification	Permissioned	Optimized verification	No	Coordination overhead
Zhou 2022 [2]	Aggregated proof auditing system	Blockchain	Proof aggregation	No	Trust assumptions
Han 2022 [3]	Survey of blockchain auditing models	N/A	Conceptual analysis	No	No implementation
Huang 2024 [4]	Blockchain + digital twin key management	Hybrid	Distributed verification	Partial	System complexity
Islam 2024 [5]	Enhanced B-tree auditing scheme	Blockchain	Efficient indexing	No	Limited decentralization
Hemalatha	Decentralized trust	Blockchain	Distributed trust	No	Conceptual

2025 [6]	architecture		nodes		framework
Watane 2025 [7]	Secure multi-cloud storage	Hybrid	Redundant storage	No	Communication overhead
Tortola 2024 [8]	Layer-2 proving mechanisms	Blockchain	Rollups / proof systems	Partial	Integration complexity
Murthy 2020 [9]	Blockchain-based cloud architecture	Permissioned	Distributed architecture	No	Performance evaluation limited
Kandpal 2023 [10]	Bibliometric analysis of blockchain storage	N/A	Analytical study	No	No technical implementation
Gong 2023 [11]	Blockchain storage scalability review	N/A	Data pruning / partitioning	No	Lack of experiments
Jayabalan 2022 [12]	Blockchain + IPFS healthcare system	Hybrid	Off-chain storage	Partial	IPFS dependency
Li 2018 [13]	Blockchain-based P2P cloud storage	Public blockchain	Distributed storage	No	Computation overhead
Khan 2021 [14]	Scalability challenges review	N/A	Sharding / Layer-2 review	No	Conceptual analysis
Xie 2019 [15]	Blockchain scalability survey	N/A	Consensus optimization	No	No architecture proposal
Bappy 2023 [16]	Blockchain auditing framework with version control	Blockchain	Efficient verification	Partial	Metadata overhead
Leonardos 2021 [17]	Ethereum fee market analysis	Public blockchain	Fee optimization	Yes	Limited scalability focus
Sriman 2022 [18]	Gas-efficient transaction confirmation	Ethereum	Transaction optimization	Yes	Protocol compatibility
He 2024 [19]	Smart contract gas optimization	Ethereum	Code optimization	Yes	Limited system scalability
Chauhan 2018 [20]	Blockchain scalability analysis	N/A	Sharding discussion	No	Conceptual study
Kaur 2020 [21]	Scalability challenges and solutions	N/A	Consensus redesign	No	Lack of experiments
Rao 2024 [22]	Blockchain scalability review	N/A	Layer-2 techniques	No	Conceptual analysis
Li 2023 [23]	Blockchain framework for IIoT	Hybrid	Distributed nodes	Partial	Resource constraints
Mohamed 2021 [24]	Energy-efficient mining architecture	Blockchain	Resource optimization	Yes	Domain-specific
Ismail 2019 [25]	Blockchain architecture review	N/A	Consensus comparison	No	No system model
Goswami 2024 [26]	Cloud data integrity classification	N/A	Integrity mechanisms	No	No implementation
Kumar 2020 [27]	Cloud security review	N/A	Security frameworks	No	Limited blockchain focus
Ali 2023 [28]	Blockchain healthcare system	Hybrid	Distributed ledger security	Partial	System complexity
Butt 2020 [29]	Machine learning for cloud security	N/A	AI-based detection	No	No blockchain model

Basu 2018 [30]	Cloud security survey	N/A	Cryptographic protection	No	Outdated techniques
Ochôa 2020 [31]	Blockchain with sidechains	Blockchain	Sidechain scaling	Yes	Integration complexity
Liu 2019 [32]	Cost-efficient smart contract storage	Blockchain	Data separation	Yes	Synchronization overhead
Zyskind 2015 [33]	Decentralized data management	Blockchain	Off-chain data storage	Partial	Scalability issues
Benet 2014 [34]	IPFS decentralized storage	Distributed system	Content-addressed storage	No	Data availability concerns
Gervais 2016 [35]	Blockchain performance analysis	Public blockchain	Network optimization	No	Limited cloud context
Buterin 2014 [36]	Ethereum smart contract platform	Public blockchain	Programmable blockchain	No	Scalability limitations
Croman 2016 [37]	Blockchain scaling study	Public blockchain	Layer-2 concepts	No	Conceptual
Xu 2021 [38]	Blockchain for cloud survey	N/A	Architectural review	No	No implementation
Zheng 2018 [39]	Blockchain opportunities survey	N/A	Technology analysis	No	Broad overview
Casino 2019 [40]	Blockchain research review	N/A	Literature classification	No	No technical model

E. Research Gaps Identified from the Literature

However, after reviewing the analysed works in terms of four main themes, namely the auditing framework for blockchain, multi-cloud integrity, off-chain storage system, and Layer-2 scalability framework, one can conclude that several research opportunities could be considered in future. While most existing literature makes considerable contributions in addressing cloud data integrity issues and improving blockchain scalability, very few works discuss a comprehensive approach applicable in cloud environments.

1) Lack of Integrated Integrity and Scalability Frameworks

A number of studies have explored how blockchain could serve as an effective tool to improve auditing in the cloud storage system. To be more precise, Zhang et al. [1], Zhou et al. [2], and Islam et al. [5] were concerned about enhancing auditing efficiency by adopting an efficient mechanism of verifying data integrity, e.g., through aggregating proofs or designing hierarchical index structures. At the same time, Bappy et al. [16] proposed the concept of immutable auditing framework that would ensure version control in the cloud computing environment. Nevertheless, none of the discussed models addresses scalability and other concerns related to blockchain-based networks.

2) Limited Scalability Solutions for Multi-Cloud Environments

There is existing research that has considered using blockchain architectures in multi-cloud systems in order to provide higher levels of trust and security. Several approaches suggested by Murthy et al. [9], Hemalatha [6], and Watane [7] consider decentralized architectures that share the responsibility for verification among various nodes. In addition, Huang and Yi [4] used digital twins in order to improve the level of monitoring and security. Although such architectures increase the levels of reliability and distributed trust, there might be significant problems associated with high levels of coordination and communication delays. In addition, there are few proposals considering blockchain scalability techniques such as sharding or Layer-2 solutions.

3) Insufficient Cost Optimization in Blockchain-Based Cloud Systems

Transaction fees, computational costs, and other related problems remain essential for blockchain systems. The works of Leonardos et al. [17], Sriman and Ganesh Kumar [18], and He et al. [19] considered the problem of transaction fee schemes and optimizations in terms of gas efficiency in the blockchain network.

Mohamed et al. [24] developed energy-efficient mining architectures that allow lowering operation expenses. Nonetheless, none of the works focuses specifically on cost issues related to blockchain cloud architectures.

4) Dependence on Off-Chain Storage Without Strong Integrity Integration

The usage of off-chain storage technologies, like IPFS, has become widespread among blockchain researchers in order to overcome the inefficiency related to data storage on the chain. In particular, Jayabalan and Jeyanthi [12] combined blockchain and IPFS for protecting the integrity of healthcare information. Moreover, the works of Liu et al. [32] and Ochôa et al. [31] discussed designs where the big data sets could be stored in off-chain storages and the blockchain transactions would operate with metadata only. While these proposals reduce the storage burden on blockchain, they pose several concerns related to availability and synchronization issues, as well as security of off-chain elements.

5) Fragmented Research on Layer-2 Scalability Mechanisms

Many researchers addressed the scalability problems in blockchain networks. The contributions by Tortola et al. [8], Khan et al. [14], and Xie et al. [15] discussed existing limitations and proposed various improvements, including Layer-2 protocols, sharding, and off-chain computing. Furthermore, the seminal research performed by Buterin [36], Gervais et al. [35], and Croman et al. [37] stressed some fundamental scalability issues of blockchain technology. Nevertheless, those solutions usually were not considered in combination with cloud data integrity systems.

6) Lack of Unified Architecture for Cloud Data Integrity

The initial reviews of Zheng et al. [39], Casino et al. [40], Xu et al. [38], and Goswami et al. [26] highlight the vast opportunities that blockchain technology offers in increasing the security and transparency levels in distributed systems. However, it is evident that there is no unification framework in the existing literature, which addresses the issues of data integrity, scalability, efficiency, and cost in cloud computing.

Summary of Research Gap

From the reviewed literature, it is evident that previous research efforts focus on addressing particular features when implementing blockchain technologies in cloud computing. The current research gap lies in the absence of a cost-efficient, scalable architecture, which combines sharding, Layer-2 scalability methods, and off-chain storage mechanisms to provide efficient verification of cloud data integrity.

F. Future Research Directions

Expanding upon the gaps and limitations noted in the literature review, this paper proposes several future directions in order to optimize and refine the use of blockchain technology in cloud computing for improving system integrity.

1) Integration of Sharding for Scalable Blockchain-Based Cloud Systems

It would be beneficial for future studies to examine how sharding can be applied in order to ensure the scalability of cloud computing systems based on blockchain technology. By dividing the blockchain network into small shards, multiple transactions can be processed concurrently by different shards. However, further research needs to be done to ensure that there are secure cross-shard communication protocols.

2) Development of Efficient Layer-2 Techniques for Cloud Data Integrity Verification

The Layer-2 techniques, such as rollups, sidechains, and state channels, have shown promise in terms of reducing blockchain costs and improving scalability. Future work should focus on combining Layer-2 technologies with cloud data integrity systems, aiming to decrease the volume of transactions that occur within the blockchain. More research needs to be done to determine whether these techniques are able to provide security assurances under heavy loads of cloud data integrity verification.

3) Hybrid Blockchain and Off-Chain Storage Architectures

Off-chain storage techniques like IPFS and decentralization storage can significantly decrease the amount of storage space required by blockchain. Future research can focus on creating hybrid architectures where blockchain technology is combined with decentralized storage in order to address efficient management of cloud data storage space. The creation of efficient synchronization methods that help verify data integrity can be helpful in achieving that goal.

4) Cost-Efficient Blockchain Architectures for Cloud Computing

Energy consumption and fees are the key problems of existing blockchain architectures. Future studies should focus on developing cost-effective architectures in order to minimize expenses in such systems and ensure high level of system security at the same time. That can be achieved through adaptive batching of transactions and effective energy-efficient consensus algorithms.

5) Intelligent Resource Management Using Artificial Intelligence

Techniques such as artificial intelligence and machine learning can be used along with the blockchain technology for improving resource allocation and workload management in cloud computing environments. These approaches will help in improving network conditions, processing transactions, allocation of shards, and scheduling of verification in a blockchain-powered cloud platform.

6) Security and Privacy Enhancements in Blockchain-Based Cloud Systems

Although the blockchain technology has the potential to increase transparency and integrity, securing information is still an issue when using the cloud computing environment. In future studies, researchers can look into the application of zero-knowledge proof systems, homomorphic encryption, and secure multi-party computation in the blockchain technology.

7) Real-World Deployment and Performance Evaluation

In most cases, current blockchain-enabled cloud computing systems have been studied using simulation and theoretical approaches. In future research, there is a need to conduct practical experiments with large datasets from cloud computing environments.

Summary on future scope

Overall, future research should focus on developing integrated blockchain architectures that combine sharding, Layer-2 scalability mechanisms, and off-chain storage solutions to address the limitations of existing cloud integrity frameworks. Such approaches have the potential to significantly improve the scalability, cost efficiency, and security of blockchain-based cloud computing systems.

V. CONCLUSION

The current study reviewed the available literature to present an overview of the existing blockchain solutions that have been developed to maintain data integrity in the cloud. The literature was thoroughly classified based on the following four themes: blockchain auditing systems, multi-cloud integrity, off-chain solutions, and layer 2 scalabilities. Each category represents unique ways in which blockchain technology has been utilized to tackle various security, efficiency, and cost issues in the cloud.

Examples of blockchain auditing mechanisms include Zhang et al. [1], Zhou et al. [2], and Bappy et al. [16]. These blockchain auditing techniques allow enhanced transparency and avoid the need for third parties' involvement to ensure auditability. In addition, there are also several cases of multi-cloud integrity systems in the literature, such as those proposed by Murthy et al. [9], Huang and Yi [4], and Hemalatha [6]. Furthermore, off-chain solutions including those based on IPFS architecture suggested by Jayabalan& Jeyanthi [12], Benet [34], and Liu et al. [32] provide effective ways to overcome blockchain storage constraints in that they keep large volumes of data off the blockchain while ensuring integrity through hash links. Lastly, Layer-2 scaling approaches and optimization strategies mentioned in literature including Tortola et al. [8], Khan et al. [14], Xie et al. [15], and Croman et al. [37] offer some possible ways to increase efficiency and reduce transaction costs.

Although there has been considerable advancement in these regards, it is still clear from the literature that most existing solutions tackle separate concerns such as auditing process efficiency, blockchain storage, or scalability in a disconnected way. There are very few works in this field that can serve as an integrated solution tackling data integrity, system scalability, and cost-efficiency together at a large scale. Besides, problems such as transaction overhead in blockchain, synchronization between off and on-chain storage layer, and multi-cloud coordination are yet to be resolved.

Thus, the findings from the above review call for the development of blockchains that will involve the integration of scalability methods, auditing capabilities, and distributed data storage.

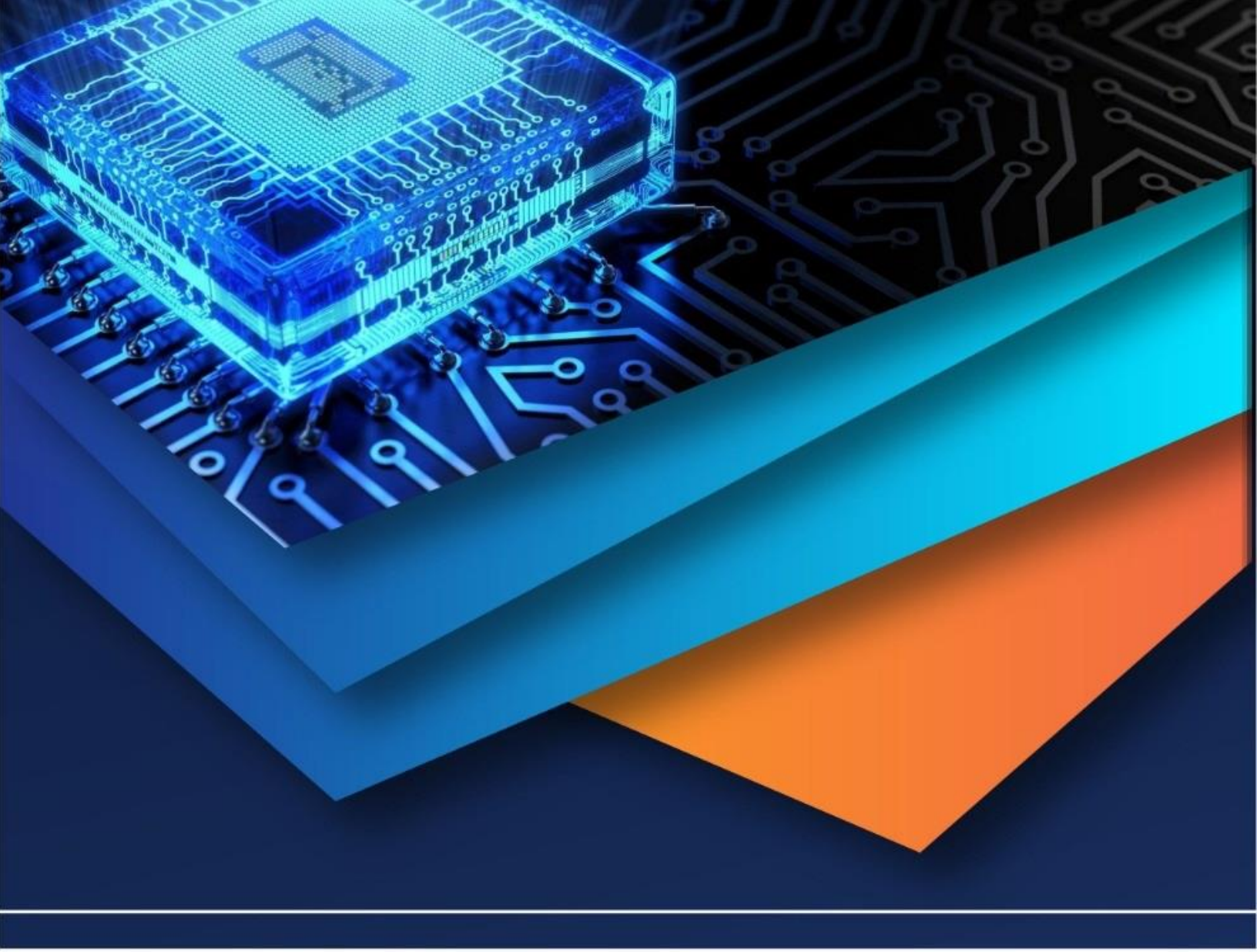
This is likely to improve the efficiency and effectiveness of blockchains while still retaining their high levels of security. The future studies should therefore focus on the creation of highly cost-effective and scalable architectures of blockchains that include such components as sharding, Layer-2 operations, and off-chain storage for verifying cloud data integrity.

REFERENCES

[1] Y. Zhang, H. Geng, L. Su, and L. Lu, “A blockchain-based efficient data integrity verification scheme in multi-cloud storage,” *IEEE Access*, vol. 10, pp. 105920–105929, 2022.

[2] Z. Zhou, X. Luo, Y. Bai, X. Wang, F. Liu, G. Liu, and Y. Xu, "A scalable blockchain-based integrity verification scheme," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 7830508, 13 pages, 10 May 2022.
[3] X. Han, "A survey on blockchain-based integrity auditing for cloud data," 2022.
[4] J. Huang and J. Yi, "The key security management scheme of cloud storage based on blockchain and digital twins," *Journal of Cloud Computing*, vol. 13, art. no. 15, 2024.
[5] T. Islam, F. H. Bappy, M. N. U. H. Shifat, F. Ahmad, K. Hasan, and T. S. Zaman, "An efficient and scalable auditing scheme for cloud data storage using an enhanced B-tree," *arXiv*, Jan. 17, 2024.
[6] R. Hemalatha, "Decentralized trust architecture for enhancing security and scalability in cloud computing," 2025.
[7] S. Watane, "Secure multi-cloud storage systems techniques for data integrity and availability," 2025.
[8] D. Tortola, A. Lisi, P. Mori, and L. Ricci, "Tethering Layer 2 solutions to the blockchain: A survey on proving schemes," *Computer Communications*, vol. 225, pp. 289–310, Jul. 2024.
[9] Ch. V. N. U. B. Murthy, M. L. Shri, S. Kadry, and S. Lim, "Blockchain based cloud computing: Architecture and research challenges," IEEE Access, vol. 8, pp. 205190–205205, 2020, doi: 10.1109/ACCESS.2020.3037703.
[10] M. Kandpal, V. Goswami, R. Priyadarshini, and R. K. Barik, "Towards data storage, scalability, and availability in blockchain systems: A bibliometric analysis," in Proc. Int. Conf. Data Technologies and Applications (ICDTA), 2023.
[11] F. Gong, L. Kong, Y. Lu, J. Qian, and X. Min, "An overview of blockchain scalability for storage," in Proc. Int. Conf. Computer Supported Cooperative Work in Design (CSCWD), 2023.
[12] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," J. Parallel Distrib. Comput., vol. 165, pp. 102–113, 2022, doi: 10.1016/j.jpdc.2022.03.006.
[13] J. Li, J. Wang, and L. Chen, "Block-secure: Blockchain-based scheme for secure P2P cloud storage," Information Sciences, vol. 465, pp. 219–231, 2018, doi: 10.1016/j.ins.2018.07.043.
[14] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic literature review of challenges in blockchain scalability," Applied Sciences, vol. 11, no. 20, art. no. 9370, 2021, doi: 10.3390/app11209370.
[15] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems," IEEE Network, vol. 33, no. 6, pp. 166–173, Nov.–Dec. 2019, doi:10.1109/MNET.2019.1800401.
[16] F. H. Bappy, S. Zaman, T. Islam, R. A. Rizvee, J. S. Park, and K. Hasan, "Towards immutability: A secure and efficient auditing framework for cloud supporting data integrity and file version control," arXiv, 2023.
[17] S. Leonardos, B. Monnot, D. Reijsbergen, S. Skoulakis, and G. Piliouras, "Dynamical analysis of the EIP-1559 Ethereum fee market," in Proc. Conf. Advances Financial Technologies, 2021.
[18] B. Sriman and S. Ganesh Kumar, "Enhanced transaction confirmation performances without gas by using Ethereum blockchain," Webology, vol. 19, no. 1, pp. 5310–5329, 2022, doi: 10.14704/WEB/V19I1/WEB19357.
[19] M. He, S. Xia, B. Qin, N. Yoshida, T. Yu, L. Song, and Y. Zhang, "How to save my gas fees: Understanding and detecting real-world gas issues in Solidity programs," arXiv, 2024.
[20] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, "Blockchain and scalability," in Proc. IEEE Int. Conf. Software Quality, Reliability and Security Companion, 2018.
[21] G. Kaur and C. Gandhi, "Scalability in blockchain: Challenges and solutions," Elsevier, 2020.
[22] I. S. Rao, M. L. M. Kiah, M. M. Hameed, and Z. A. Memon, "Scalability of blockchain: A comprehensive review and future research direction," Cluster Computing, 2024.
[23] R. Li, Y. Qin, C. Wang, M. Li, and X. Chu, "A blockchain-enabled framework for enhancing scalability and security in IIoT," IEEE Transactions on Industrial Informatics, 2023.
[24] M. A. Mohamed, S. Mirjalili, U. Dampage, S. H. Salmen, S. Al Obaid, and A. Annuk, "A cost-efficient-based cooperative allocation of mining devices and renewable resources enhancing blockchain architecture," Sustainability, vol. 13, no. 18, Art. no. 10382, 2021, doi: 10.3390/su131810382.
[25] L. Ismail and H. Materwala, "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions," Symmetry, vol. 11, no. 10, Art. no. 1198, 2019, doi: 10.3390/sym11101198.
[26] P. Goswami, N. Faujdar, S. Debnath, A. K. Khan, and G. Singh, "Investigation on storage level data integrity strategies in cloud computing: Classification, security obstructions, challenges and vulnerability," Journal of Cloud Computing: Advances, Systems and Applications, vol. 13, no. 1, Art. no. 45, 2024, doi: 10.1186/s13677-024-00605-z.
[27] R. Kumar and M. P. S. Bhatia, "A systematic review of the security in cloud computing: Data integrity, confidentiality and availability," in Proc. 2020 IEEE Int. Conf. Computing, Power and Communication Technologies (GUCON), 2020, pp. 1–6, doi: 10.1109/GUCON48875.2020.9231185.
[28] A. Ali, H. Ali, A. Saeed, A. Ahmed, T. T. Tin, M. Assam, Y. Y. Ghadi, and H. G. Mohamed, "Blockchain-powered healthcare systems: Enhancing scalability and security with hybrid deep learning," in Proc. Italian Nat. Conf. Sensors, 2023.
[29] U. A. Butt, M. Mehmood, S. B. H. Shah, R. Amin, M. W. Shaukat, S. M. Raza, D. Y. Suh, and M. J. Piran, "A review of machine learning algorithms for cloud computing security," Electronics, vol. 9, no. 9, Art. no. 1379, 2020, doi: 10.3390/electronics9091379.
[30] S. Basu, A. Bardhan, K. Gupta, P. Saha, M. Pal, M. Bose, K. Basu, S. Chaudhury, and P. Sarkar, "Cloud computing security challenges & solutions—A survey," in Proc. 2018 IEEE 8th Annu. Computing and Communication Workshop and Conf. (CCWC), 2018, pp. 347–356, doi: 10.1109/CCWC.2018.8301630.
[31] I. S. Ochôa, L. A. Silva, G. de Mello, N. M. García, J. F. De Paz, and V. R. Q. Leithardt, "A cost analysis of implementing a blockchain architecture in a smart grid scenario using sidechains," Sensors, vol. 20, no. 3, Art. no. 843, 2020, doi: 10.3390/s20030843.
[32] X. Liu, K. Muhammad, J. Lloret, Y.-W. Chen, and S.-M. Yuan, "Elastic and cost-effective data carrier architecture for smart contract in blockchain," Future Generation Computer Systems, vol. 100, pp. 590–599, 2019, doi: 10.1016/j.future.2019.05.056.
[33] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE Security and Privacy Workshops (SPW), 2015, pp. 180–184, doi: 10.1109/SPW.2015.27.
[34] J. Benet, "IPFS—Content addressed, versioned, peer-to-peer file system," arXiv preprint arXiv:1407.3561, 2014.

[35] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "On the security and performance of proof-of-work blockchains," in Proc. ACM SIGSAC Conf. Computer and Communications Security (CCS), 2016, pp. 3–16, doi: 10.1145/2976749.2978341.
[36] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," 2014. [Online]. Available: https://ethereum.org/en/whitepaper/
[37] K. Croman et al., "On scaling decentralized blockchains," in Proc. Int. Conf. Financial Cryptography and Data Security, 2016, pp. 106–125, doi: 10.1007/978-3-662-53357-4_8.
[38] X. Xu, I. Weber, and M. Staples, "Architecture for blockchain applications in cloud computing: A survey," IEEE Cloud Computing, vol. 8, no. 1, pp. 27–34, Jan.–Feb. 2021, doi: 10.1109/MCC.2021.3051217.
[39] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," Int. J. Web Grid Services, vol. 14, no. 4, pp. 352–375, 2018, doi: 10.1504/IJWGS.2018.095647.
[40] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telematics and Informatics, vol. 36, pp. 55–81, 2019, doi: 10.1016/j.tele.2018.11.006.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY