International Journal of Safety and Security Engineering
Vol. 14, No. 5, October, 2024, pp. 1455-1464
Journal homepage: http://iieta.org/journals/ijsse

Enhancing Cloud Security Through Block Chain: A Data Integrity and Trust Approach

Aparna Tanam*, G. Raja

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram 522302, India

Corresponding Author Email: apstanam@gmail.com

https://doi.org/10.18280/ijsse.140513

Received: 1 August 2024
Revised: 5 October 2024
Accepted: 16 October 2024
Available online: 31 October 2024

Keywords:
cloud security, block chain technology, data integrity, scalability

ABSTRACT

With cloud computing leading the way in today's digital landscape, the safeguarding of data in cloud environments remains a major challenge. Established security methods usually do not meet the rising challenges posed by cyber threats such as insider attacks and breaches of data. This investigation finds flaws in current security practices and presents an innovative strategy that combines block chain technology to augment cloud safety. With its traits of immutability and decentralization, block chain opens avenues to build reliable data storage frameworks. Utilizing these aspects allows the proposed solution to lower the risk of unauthorized entry and data alteration while confirming the integrity of data in the cloud. The research shows how block chain helps preserve data integrity by effectively verifying data segments and increasing attack resistance. Using cryptographic hashing along with decentralized ledger technology improves safety and maintains efficiency. These results show that solutions utilizing block chain can greatly lower security vulnerabilities in the cloud and build confidence to boost cloud acceptance.

1. INTRODUCTION

In today's information technology landscape, Cloud computing acts as a key element that delivers scalability and cost-effective approaches for managing information [1]. Companies large and small have the ability to handle extensive data sets and utilize substantial computational power for fast application deployment [2]. Cloud computing's widespread use faces major obstacles from serious security issues related to data integrity and unauthorized entry. Maintaining the safety of cloud data is a significant difficulty because conventional strategies have not adequately countered emerging cyber issues [3].

Originally designed for Bitcoin cryptocurrency, blockchain technology now captures interest for its applications that extend beyond finance with a focus on cloud security enhancements [4]. Blockchain's [5] main qualities-trustworthiness and distribution-create an effective defense for safeguarding cloud-based data. Once data is placed on a blockchain it stays secure and cannot change or be gotten rid of maintaining its reliability. By eliminating singular weak spots, the decentralized nature of blockchain strengthens resistance to attacks [6, 7]. To ensure the integrity of data, transactions are confirmed by mechanisms like Proof of Work (PoW) and Proof of Stake (PoS), which demand agreement from most nodes. A secure and confirmed audit path for transactions arises from the openness of blockchain [8, 9].

The investigation analyzes merging blockchain technology with cloud computing to solve security challenges in the cloud [10]. The objective includes techniques that involve saving data hashes in the blockchain and maintaining the actual datasets in the cloud combined with blockchain-based access controls for enhancing permission management and verifying users securely. The main focus of the research is to apply blockchain technology to boost data integrity and lower the risks of data modification and unauthorized entry while confirming the validity of cloud-stored data.

The paper begins with an Introduction that emphasizes cloud computing benefits including cost-effectiveness and scalability and the security concerns posed by data breaches. As a prospective answer to security and data integrity issues, block chain technology presents with aims to boost reliability and protection. The existing literature on cloud security and block chain collaboration is evaluated in this review to uncover existing gaps and potential solutions for resolving security challenges. To enhance cloud security with block chain technologies, the Methodology details techniques like data division and hashing alongside auditing and decentralized storage. Here results and metrics for data integrity checks are displayed next to the performance of block chain integration and dynamic access control illustrated through graphical representations. In the conclusion part is the summary of crucial findings and the focus on using block chain for enhanced cloud protection.

2. LITERATURE REVIEW

The responsibility of cloud security is to safeguard data, applications, and services within cloud environments. The advantages of cloud computing are accompanied by various security challenges, including unauthorized access to data and potential data loss. Conventional protective measures often do not adequately address the complex nature of these threats and necessitate the development of innovative strategies to ensure robust cloud security. Data exposure incidents can result in significant financial losses and harm to reputation.

Dawood and colleagues investigate the changing risks in cloud computing and the needed protocols to address these threats. They show that as cloud services gain popularity in organizations' workflows, they become more vulnerable to attacks. The study points out major concerns including data leaks and insider risks in conjunction with the difficult work of protecting data privacy and complying with regulations [11]. The paper by Aslam and Kumar [12] provides an elaborated review of user-oriented strategies and innovative techniques for strengthening cloud data protection. Their research focuses on different approaches that are used in the contemporary world, including encryption, multi-factor authentication, and access control policies that target to improve both engagement and security with the end-users of the techniques. Further, the paper also discusses such new security paradigms like blockchain, homomorphic encryption that fill the gaps of the existing security approaches.

Dorsala et al. [13] conducted a thorough review of blockchain technologies that boost the security of cloud-based environments. They investigate how the key traits of blockchain including transparency and decentralization can help resolve typical cloud security challenges like unauthorized entry and data breaches. A range of blockchain protocols and frameworks is analyzed by the authors to measure their efficacy in actual usage.

Table 1. Novelty, limitations, and research gaps in blockchain-integrated cloud security literature

Reference	Novelty	Limitations	Research Gaps
Dawood et al. [11]	Comprehensive analysis of cyber threats in cloud computing and corresponding security measures	Focuses primarily on existing threats and countermeasures; lacks in-depth exploration of emerging technologies	Need for advanced, proactive threat detection mechanisms using AI and blockchain
Aslam and Kumar [12]	User-centric approaches and advanced mechanisms for enhancing cloud data security	Primarily theoretical; lacks empirical validation of proposed mechanisms	Practical implementation and validation of user-centric security models in diverse cloud environments, scalability of advanced mechanisms under large-scale deployments
Dorsala et al. [13]	Survey of blockchain-based solutions for cloud security	Lacks experimental validation; primarily a review of existing literature	Experimental validation and performance benchmarking of blockchain solutions in diverse cloud settings
Sharma et al. [14]	Blockchain-based cloud storage system with enhanced optimization and integrity preservation	Focuses on technical aspects without addressing user adoption and compliance	User adoption barriers, compliance with global data privacy regulations, and long-term sustainability
Singh et al. [15]	Examination of blockchain integration to fortify cloud security	Limited discussion on interoperability with existing cloud infrastructure	Interoperability and seamless integration of blockchain with current cloud platforms
Singh and Chatterjee [16]	Review of blockchain applications in cloud storage security	Mainly theoretical, with a focus on specific blockchain platforms	Real-world case studies demonstrating the effectiveness of different blockchain protocols in cloud security
Singh et al. [17]	Exploration of blockchain technology for improving cloud computing security	Focuses on theoretical frameworks; lacks real-world implementation and performance analysis	Practical implementation, performance benchmarking, and interoperability of blockchain with existing cloud infrastructure across various platforms
Sarmah [18]	Overview of blockchain applications in enhancing security in cloud computing	Primarily focuses on theoretical concepts; lacks real-world case studies and experimental data	Empirical validation of blockchain applications in real cloud environments, performance analysis in large-scale deployments, and optimization of blockchain protocols for cloud-specific challenges
Basu et al. [19]	Comprehensive survey of cloud computing security challenges and potential solutions	Lacks focus on emerging technologies like AI and blockchain; primarily theoretical with limited practical solutions	Exploration of advanced, technology-driven solutions such as AI and blockchain for proactive threat detection and response, real-world validation of surveyed solutions in dynamic cloud environments
Wang et al. [20]	Proposal of a secure cloud storage framework with blockchain-based access control	Focuses on a specific framework with limited scalability analysis for large cloud environments	Scalability and performance optimization of the blockchain-based framework in real-world, large-scale cloud deployments, and interoperability with existing cloud storage solutions
Kayikci et al. [21]	Survey of the integration of blockchain and machine learning for enhancing data security and analytics	Primarily theoretical, with limited real-world application examples and performance metrics	Practical validation of blockchain and machine learning integration in diverse real-world scenarios, evaluation of performance and scalability under different conditions, and optimization for specific use cases in big data environments

In an article by Sharma et al. [14] a thorough description of a cloud storage system using blockchain technology dedicated to boosting performance while safeguarding data integrity is provided. A new framework is introduced by the authors to tackle these issues using blockchain technology. They implement the distributive and constant features of blockchain to protect data in the cloud from unauthorized attempts. In their work, Singh et al. [15] investigated using blockchain for better security in cloud systems. In their work the authors analyze the core flaws present in cloud infrastructures like data compromise and illegitimate access. The researchers highlight how vital attributes such as immutability and decentralization are in enhancing security for cloud services. With the distribution of data storage and the use of cryptographic hashing blockchain secures data integrity and blocks any unauthorized modifications.

In their 2022 study Singh and Chatterjee [16] explore how blockchain technology improves the security and integrity of cloud storage. They evaluate diverse cloud storage solutions supported by blockchain technology while emphasizing their pros and cons. This examination presents a range of blockchain solutions and protocols including Ethereum and Hyper-ledger and looks into how suitable they are for secure cloud storage. Singh et al. [15] investigated the possibility of using blockchain to improve on the levels of security in cloud computing. It brings out the issues like data violation, unauthorized access, and the fact that blockchain can solve these challenges. In Cloud 2.0, the issues of integrity and secure transactions are addressed by blockchain's distributed ledger. The authors also explain the possibilities of using block chain technology for granting secure access control and authentication solutions while completely ignoring any third-node suppliers which form the main threat in the traditional models of cloud security [17]. Sarmah [18] research focuses on examining how blockchain serve to facilitate the increase of clouds' security and credibility. The study takes up the challenges of data leaks, hacking, intrusion and single point failure amongst others. By adopting blockchain, data sharing with focus on the integrity and transparency of data through the use of distributed ledger technology can be achieved. Key features of blockchain include: immutability, consensus algorithms, and smart contracts that offer effective security structures for cloud data and transactions.

The surveys by Basu et al. [19] address security threats in the cloud computing environment and corresponding potential solutions. The main security threats as highlighted in the study are Data theft, cybersquatting, phishing, insider attack, and denial of service (DoS) attacks. The authors also describe the implications of sharable and multi-tenant aspects of clouds with concerns to data security which will require enhanced security of databases and communication protocols. To overcome security challenges that exist in cloud storage, Wang et al. [20] put forward a secure architecture for cloud storage that employs blockchain technology as well as access control models. The framework helps in guaranteeing that data stored in the cloud cannot be tampered with. Smart contracts provide a solution to grant access control where Smart contracts handle authorization and authentication of any permission without the help of third parties. In a much broader survey, Kayikci and Khoshgoftaar [21] discuss the opportunities to amalgamate blockchain with another disruptive technology–machine learning (ML). Drawing upon the highly secure decentralized and transparent system of blockchain, this paper explores the symbiosis between machine learning being data intensive and blockchain being secure, thus making it possible to develop secure applications in several sectors. The following Table 1 summarizes the novelty, limitations, and research gaps identified in the reviewed literature. Each entry is accompanied by proposed research opportunities to address these gaps.

3. METHODOLOGY

The architecture displayed in Figure 1 uses blockchain technology to boost cloud security. First the owner loads the original data file into the cloud before splitting it into more manageable segments. Using a cryptographic hash function produces unique hash values (H1, H2, ..., Hn) from each data chunk which work as digital marks for the chunks [22]. Transactions such as T1 and T2 are created by merging hashes with their associated metadata [23]. Multiple transactions and a hash of the preceding block are present in each block to guarantee the blockchain's unchangeable nature [24]. Upon the user's request for a data chunk access, a hash is produced for that chunk and matched with the associated hash in the blockchain. Through this verification step data is protected; access is permitted only when the hashes are identical to Role-Based Access Control (RBAC) [25].

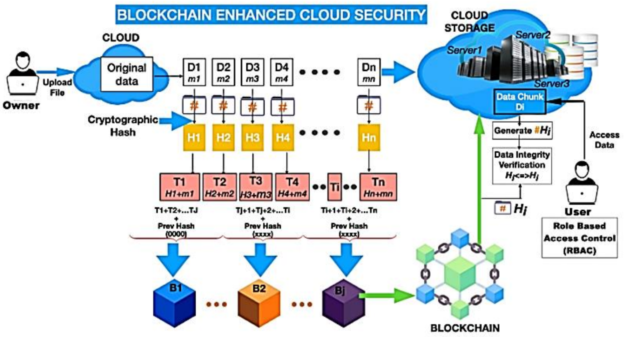

Figure 1. Block chain enhanced cloud security architecture

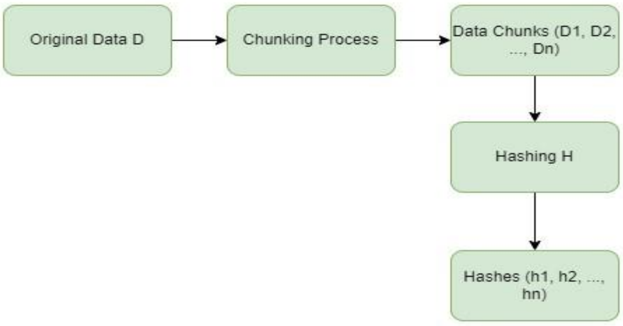

Figure 2. Data chunking and hashing process for ensuring data integrity

A structured approach is taken for merging blockchain and cloud storage with the goal of securing and managing the integrity of cloud-stored data [26]. The file is uploaded from the data owner to the cloud as the first step. The block diagram in Figure 2 illustrates the process of data chunking and hashing for ensuring data integrity in cloud storage. The file called D is split into smaller a unit (D1 to Dn) which supports improved storage and handling. The chunk dimensions are fixed relying on the constraints of the system and the nature of the data [27]. The total number of chunks, n, is determined by the formula:

$$n=ceil(S/c) \quad (1)$$

The chunk size is c and the size of the original file is S. To create a unique hash value for each chunk the data is hashed with a hash function such as SHA-256.

Serving as digital marks these hash values detect even minor changes in chunks and indicate possible alterations.

$$hi=H(Di) \quad (2)$$

Each chunk's hash value, along with relevant metadata (such as timestamps and permissions), forms a transaction, denoted as Ti:

$$Ti=\{hi, Mi\} \quad (3)$$

Each data chunk and its corresponding hash are recorded as transactions on the block chain as shown in Figure 3. A block chain consists of a chain of blocks, each containing multiple transactions. Transactions are grouped into blocks. Let Bj denote the j-th block, containing m transactions {Tj1, Tj2, ..., Tjm}.

$$Bj=\{Tj1, Tj2, ..., Tjm, PrevHash\} \quad (4)$$

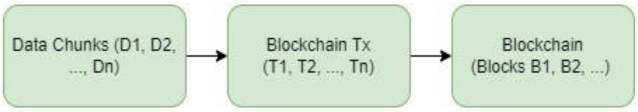
Data Chunks (D1, D2, ..., Dn)
Blockchain Tx (T1, T2, ..., Tn)
Blockchain (Blocks B1, B2, ...)

Figure 3. Integration of data chunks into block chain for data integrity and security

The blocks are then added to the blockchain, ensuring that the sequence of transactions cannot be altered without invalidating the entire chain.

Multiple cloud servers hold the real data parts (D1, D2, ..., Dn), which keeps them available and redundant [28]. By maintaining critical hashes on blockchain and storing data in the cloud itself; we connect cloud storage and blockchain. For each chunk Di, its corresponding hash hi is stored on the blockchain, while the chunk itself is distributed across cloud servers:

$$Ci\rightarrow \{Di, hi\} \quad (5)$$

where, hi is stored on the block chain, and Di is stored in the cloud.

The block diagram in Figure 4 illustrates the process of integrating cloud storage with block chain nodes to ensure data security and integrity. The process begins with data chunks (D1, D2, ..., Dn), which are individual segments of the original data file. These data chunks are stored in cloud storage locations (C1, C2, ..., Cn).

The block diagram in Figure 5 illustrates the integration of access control and auditing mechanisms with block chain technology to enhance data security and integrity. The process begins with users (U) who interact with the system. Access control mechanisms are implemented to regulate user access based on predefined permissions (P). This ensures that users only have access to data and functionalities that are appropriate for their roles. Access control logs user activities and permissions, generating audit logs that track all interactions and access attempts.

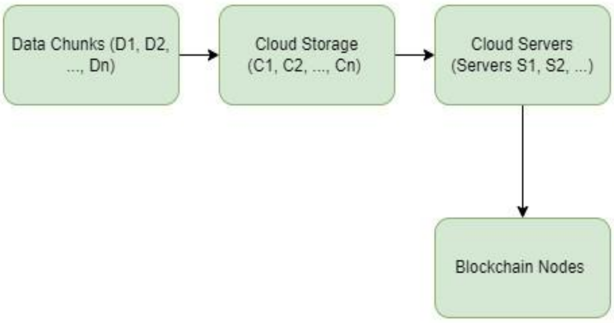
Data Chunks (D1, D2, ..., Dn)
Cloud Storage (C1, C2, ..., Cn)
Cloud Servers (Servers S1, S2, ...)
Blockchain Nodes

Figure 4. Decentralized storage and block chain integration for cloud data security

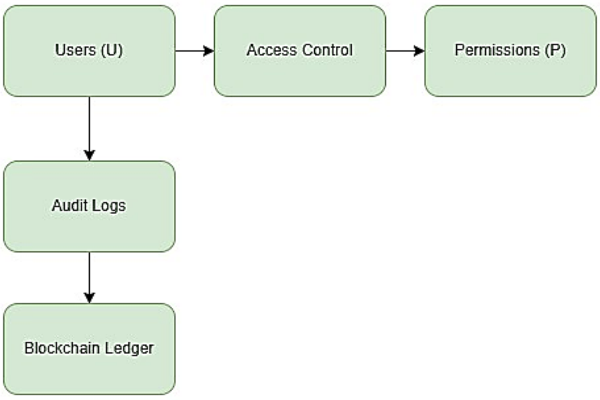

Figure 5. Access control and auditing with block chain integration

Access control is enforced using Role-Based Access Control (RBAC), where permissions are assigned based on user roles [29]. The function A defines a mapping from users to roles, and roles to permissions:

$$A: U\times R\rightarrow P \quad (6)$$

The roles (R) of users (U) determine the permissions (P) they have in interacting with the cloud information. If a user seeks access to a data segment the system produces a hash for the requested segment and then evaluates it against the corresponding hash kept on the blockchain [30]. Access is provided to the user when the hashes are consistent. The procedure keeps the data's integrity intact throughout.

4. RESULTS AND DISCUSSION

The results of integrating block chain with cloud storage were analyzed based on several key parameters: data safety and effectiveness as well as security and access management. Different configurations were used to test the efficiency and strength of the proposed method. The integrity of the data underwent thorough verification during all tests. All data chunk hashes aligned with those stored in the blockchain for datasets with varying sizes and chunk sizes. This shows how the blockchain's unchanging nature ensures data accuracy because any changes would lead to hash inconsistencies. The successful integrity checks, as illustrated in Figures 6, 9, and 12, confirm that the blockchain-enhanced system ensures tamper-proof data storage. Assessment included the processing durations for data chunking and transaction verification. Across different data sizes the time for hashing was mostly unchanged; however transaction processing took longer for larger datasets because of the increased number of chunks and blockchain processes. Scalability testing focused on enhancing the number of data sections in the system. A rise in chunk numbers results in the blockchain processing a greater series of transactions. Transaction processing time grew in direct relation to the number of chunks while the integrity of each chunk remained intact (as shown in Figures 16 and 19). To control access securely to the data RBAC was applied. Access was tightly controlled by the system and users could only obtain data pieces if the blockchain validated their permissions. The decentralized structure of blockchain made the system strong against attacks on specific servers. Investigating different types of attacks demonstrated that the reliance on consensus mechanisms and cryptographic hashing thoroughly minimized the dangers.

Figure 6 shows the integrity check results for a dataset of 1024 bytes, divided into chunks of 512 bytes each, demonstrate the effectiveness of the proposed blockchain-based cloud security system. The original data is split into two chunks, each 512 bytes in size, and each chunk is hashed using a cryptographic hash function (SHA-256). Both Chunk 0 and Chunk 1 produce the same hash value.

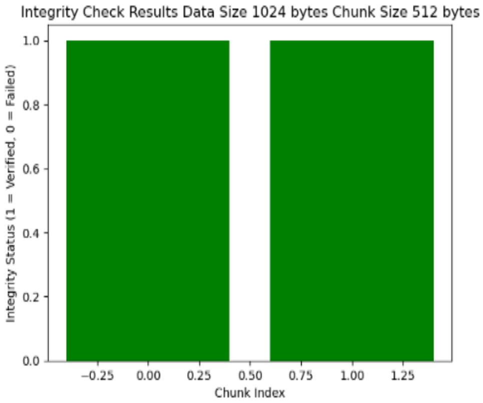

Figure 6. Integrity check results for data size 1024 bytes and chunk size 512 bytes

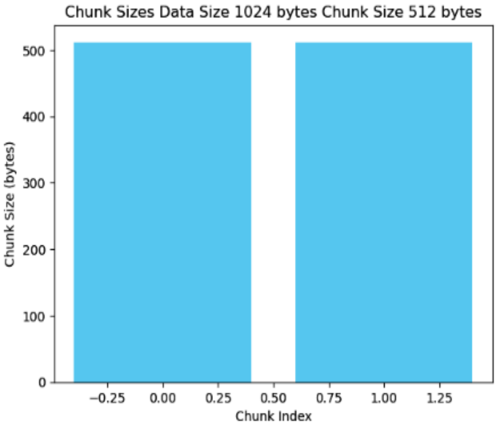

Figure 7. Chunk Sizes for data size 1024 bytes and chunk size 512 bytes

The Figure 7 illustrates the chunk sizes for a dataset of 1024 bytes divided into chunks of 512 bytes each. The bar graph shows that both chunks are 512 bytes in size, ensuring uniformity in data chunking. This process facilitates efficient data storage and retrieval while maintaining the integrity and consistency of the data chunks.

The Figure 8 depicts the blockchain hashes corresponding to a dataset of 1024 bytes divided into chunks of 512 bytes each. The graph shows the hash values for the genesis block and the subsequent blocks (Index 1 and Index 2) representing the data chunks. Each block hash is unique and securely linked to the previous block hash, ensuring the immutability and integrity of the blockchain. This visualization confirms the proper chaining of blocks, which is crucial for maintaining a tamper-proof record of data transactions within the blockchain. The Figure 9 shoes integrity check results for a dataset of 1024 bytes, divided into a single chunk of 1024 bytes, demonstrate the system's ability to maintain data integrity.

The original data is hashed, producing the hash value: 6ab72eeb9e77b07540897e0c8d6d23ec8eef0f8c3a47e1b3f4e93443d9536bed.

The blockchain details include the genesis block (Index: 0, Hash: e94f451984250a5915bb0a730e6ea1309e60736ffd46c1d6950ca7b23d47706d) and Block 1 (Index: 1) containing the hash value for the single data chunk along with its timestamp and previous hash reference.

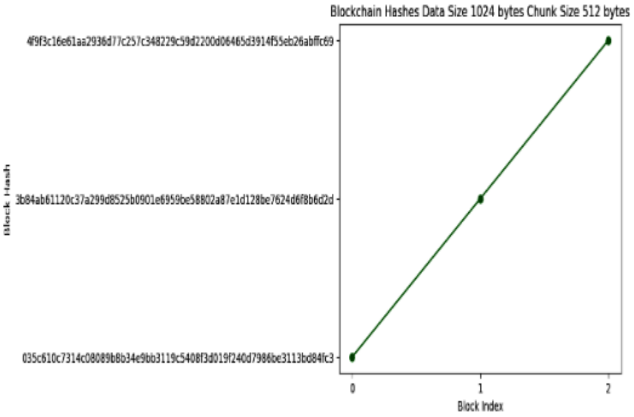

Figure 8. Blockchain hashes for data size 1024 bytes and chunk size 512 bytes

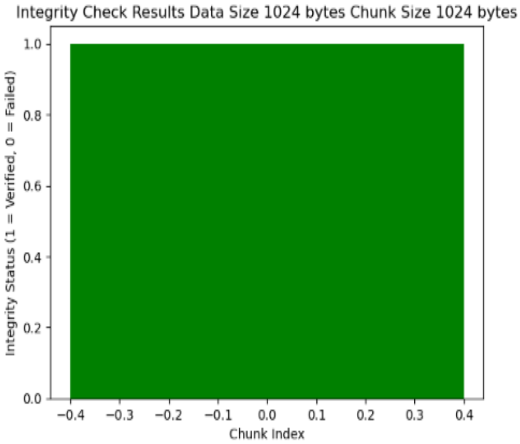

Figure 9. Integrity check results for data size 1024 bytes and chunk size 1024 bytes

The Figure 10 illustrates the chunk sizes for a dataset of 1024 bytes when divided into a single chunk of 1024 bytes. The bar graph demonstrates that the entire dataset fits into one chunk, with a size of 1024 bytes, as indicated by the consistent bar height. This visualization confirms that the chunking process has effectively divided the data into manageable pieces, ensuring efficient storage and retrieval.

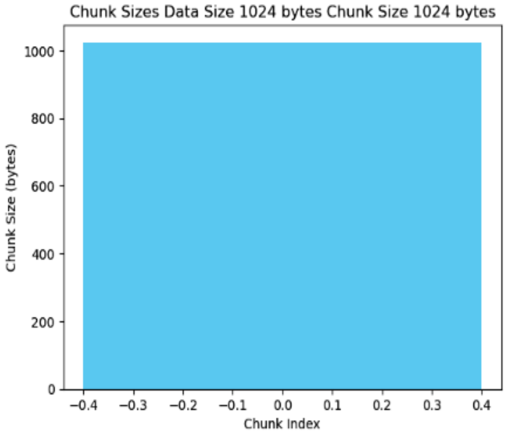

Figure 10. Chunk sizes for data size 1024 bytes and chunk size 1024 bytes

The Figure 11 displays the blockchain hashes corresponding to a dataset of 1024 bytes when divided into a single chunk of 1024 bytes. The plot shows the progression of block hashes across the blockchain, starting from the genesis block to the block containing the chunk's hash. The linear progression in the graph indicates the sequential addition of blocks, each containing the hash of the previous block and the new data chunk.

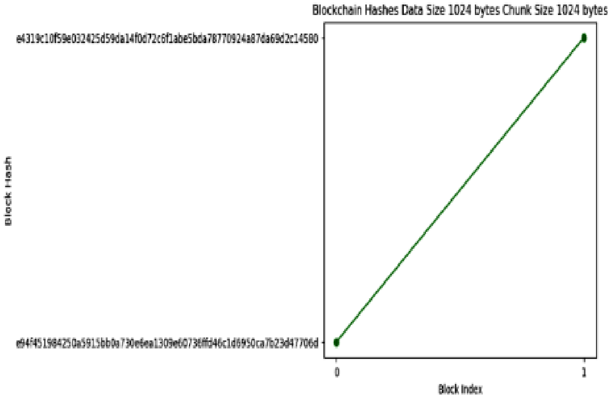

Figure 11. Blockchain hashes for data size 1024 bytes and chunk size 1024 bytes

The Figure 12 displays the integrity check results for a dataset of 1024 bytes when divided into a single chunk of 2048 bytes. Since the chunk size is larger than the data size, the entire data is processed as one chunk. The green bar indicates that the integrity of the chunk has been successfully verified, with a status of 1 (Verified). The blockchain details confirm that the data was properly recorded and hashed, ensuring its authenticity and integrity.

The Figure 13 illustrates the blockchain hashes for a dataset of 1024 bytes when divided into a single chunk of 2048 bytes. The x-axis represents the block index, while the y-axis shows the corresponding block hashes. The graph shows two points, representing the genesis block and the subsequent block containing the data chunk. The hashes are displayed along the y-axis, demonstrating the progression of the blockchain. The linear trend confirms the successful addition of the data chunk to the blockchain, with each block's hash being correctly calculated based on the data and the previous block's hash. This ensures the integrity and security of the data stored in the blockchain.

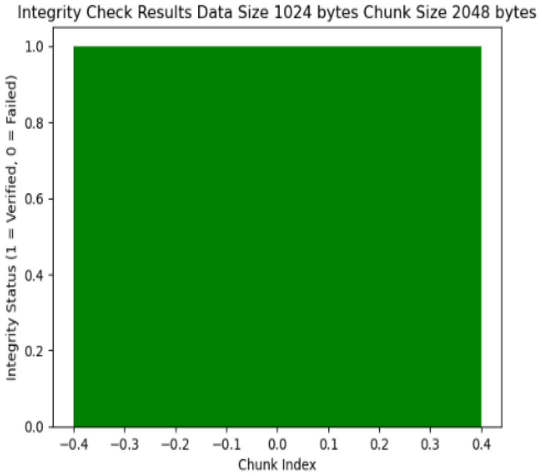

Figure 12. Integrity check results for data size 1024 bytes and chunk size 2048 bytes

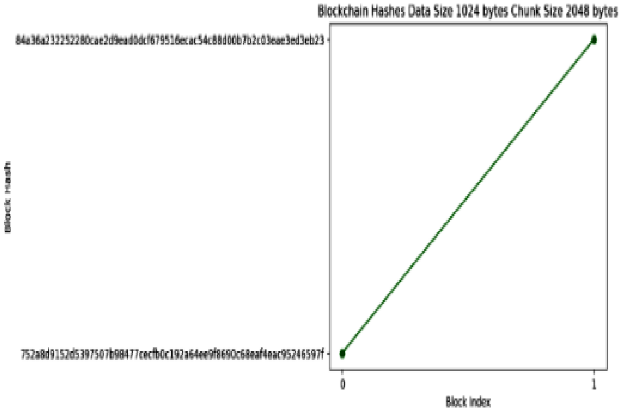

Figure 13. Blockchain hashes for data size 1024 bytes and chunk size 2048 bytes

The below Figure 14 represents the integrity check results for a dataset of 2048 bytes divided into chunks of 512 bytes each. The x-axis denotes the chunk index, and the y-axis indicates the integrity status, where 1 represents verified chunks and 0 indicates failed chunks. The green bars show that all chunks (from index 0 to 3) were verified successfully. For a dataset of 2048 bytes, the data was divided into four chunks, each of size 512 bytes. Each chunk was hashed, and these hashes were stored as transactions in the blockchain.

The Figure 15 illustrates the chunk sizes for a dataset of 2048 bytes divided into chunks of 512 bytes each. The x-axis represents the chunk index, while the y-axis denotes the chunk size in bytes. The bars show that each chunk (from index 0 to 3) is of size 512 bytes, which is consistent with the chunking process. For a dataset of 2048 bytes, the data was divided into four equal chunks, each having a size of 512 bytes. This uniform chunk size ensures that the data can be processed and stored efficiently in the cloud storage system. Each chunk's consistent size simplifies the subsequent hashing and blockchain recording processes.

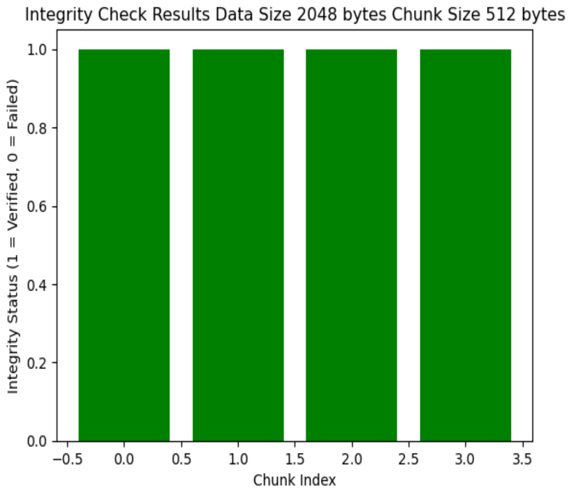

Figure 14. Integrity check results for data size 2048 bytes and chunk size 512 bytes

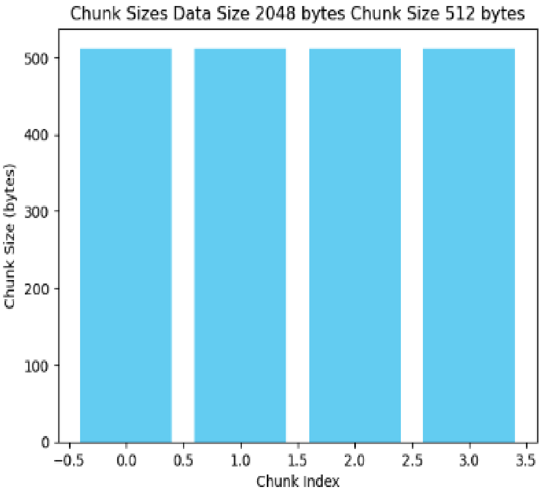

Figure 15. Chunk Sizes for data size 2048 bytes and chunk size 512 bytes

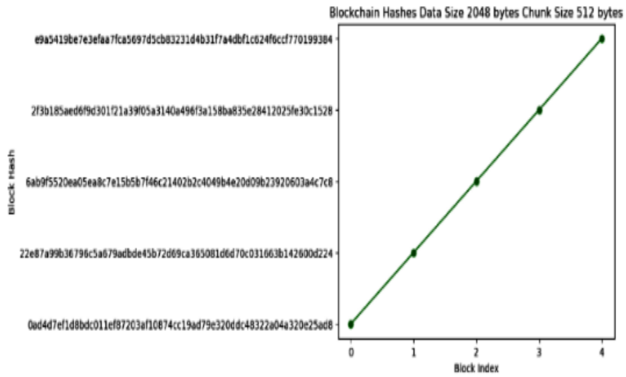

Figure 16. Blockchain hashes for data size 2048 bytes and chunk size 512 bytes

The Figure 16 represents the blockchain hashes corresponding to a data size of 2048 bytes, divided into chunks of 512 bytes each. The x-axis denotes the block index, while the y-axis shows the block hashes. Each point on the graph represents a block in the blockchain, starting from the Genesis block (index 0) to the last block (index 4) that contains the hashed data of the chunks. The hashes for each block are displayed along the y-axis, highlighting the integrity and uniqueness of each block's data. The linear progression of the points confirms the sequential addition of blocks to the blockchain, with each block's hash being a unique cryptographic representation of its data and the previous block's hash.

The below Figure 17 shows the integrity check results for a data size of 2048 bytes, divided into chunks of 1024 bytes each, are presented. The x-axis represents the chunk index, while the y-axis indicates the integrity status, where 1 denotes a successful verification and 0 denotes a failed verification. The results show that both chunks (Chunk 0 and Chunk 1) were successfully verified, as indicated by the bars reaching the value of 1 on the y-axis. This indicates that the integrity of the data was maintained throughout the process. The blockchain details further support this, with the Genesis block (Index 0) and the subsequent blocks (Index 1 and 2) displaying consistent hash values that align with the data chunks' hash values.

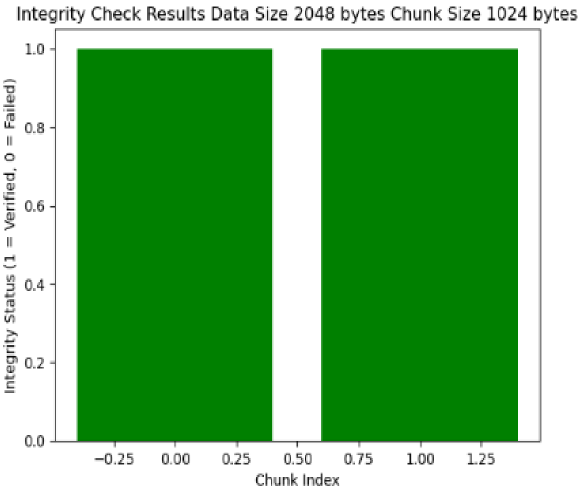

Figure 17. Integrity check results for data size 2048 bytes and chunk size 1024 bytes

The Figure 18 demonstrates the integrity check results for a data size of 4096 bytes, divided into chunks of 512 bytes each. The x-axis represents the chunk index, and the y-axis shows the integrity status, where 1 indicates a successful verification and 0 indicates a failed verification. The results reveal that all chunks (0 to 7) were successfully verified, as indicated by the bars reaching the value of 1 on the y-axis for each chunk index. This outcome signifies that the data's integrity was upheld throughout the process. The blockchain details corroborate this finding, with the Genesis block (Index 0) and subsequent blocks (Index 1 to 8) displaying consistent hash values that match the data chunks' hash values.

The Figure 19 illustrates the blockchain hashes for a data size of 4096 bytes, divided into chunks of 512 bytes each. The x-axis represents the block index, while the y-axis displays the corresponding hash values for each block. The linear progression of the graph indicates the sequential addition of data chunks to the blockchain. The hash values demonstrate the integrity of each data chunk, starting from the Genesis Block (Index 0) through to the final chunk (Index 8). Each hash value is unique and derived from the contents of the corresponding data chunk, ensuring tamper-proof records. The successful chaining of these hashes, with each block referencing the hash of the previous block, underscores the robustness of the blockchain's immutable ledger.

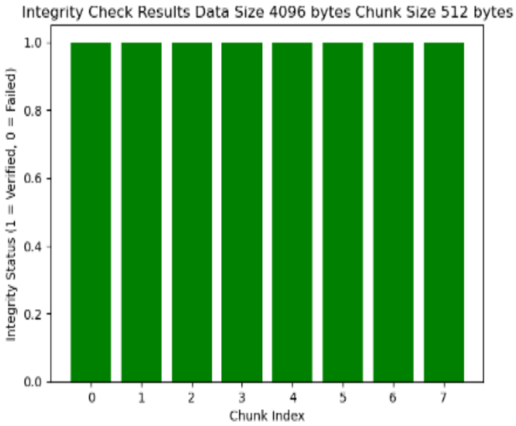

Figure 18. Integrity check results for data size 4096 bytes and chunk size 512 bytes

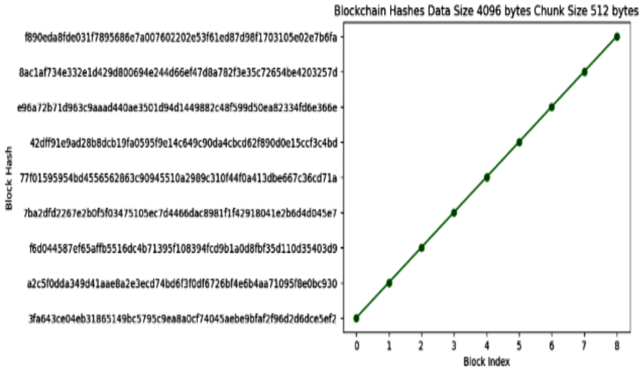

Figure 19. Blockchain hashes for data size 4096 bytes and chunk size 512 bytes

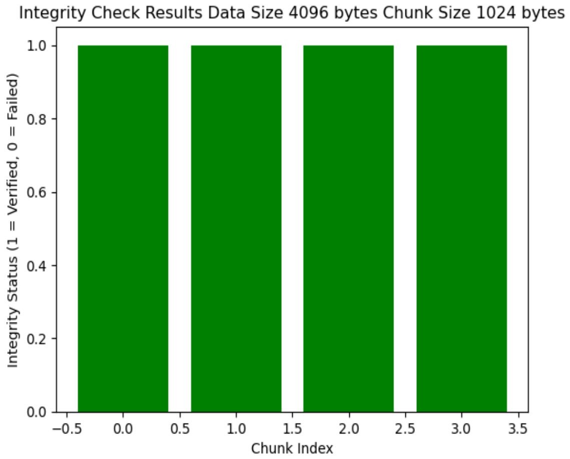

Figure 20. Integrity check results and blockchain details for data size 4096 bytes and chunk size 1024 bytes

The Figure 20 shows integrity check results for data chunks of 1024 bytes from a total data size of 4096 bytes indicate that each chunk was verified successfully, with an integrity status of '1' for each chunk index, ensuring all chunks passed the verification process. The blockchain details confirm this successful verification with specific hash values for each block: the Genesis Block (Index: 0) has a hash of 6fc679170f8c3dd5e388dad88212b12d100dfa9b0055217afe637621091f5e80; Chunk 0 (Index: 1) has a hash of 7b132d747d3ea342bf82602252622152a71237c08e655cc48fce21528ef9f496; Chunk 1 (Index: 2) has a hash of d4bdd24a23c7d3de36c556b6b0c321c631def7e7e0a6ea1eb2f661ffac309eae; Chunk 2 (Index: 3) has a hash of 58781b4013e7356b95cc6e0caaff232adcab47a11a1c3a68ca8c9e7dee337953; and Chunk 3 (Index: 4) has a hash of cb609f132c1fac6da6e66081f4637823f29679a25d5f902edc4ddd1980d8b76b.

Each chunk was hashed and linked in the blockchain, maintaining data integrity and confirming no tampering occurred during storage and verification. The successful verification of each chunk demonstrates the reliability of using blockchain technology to ensure data integrity in cloud storage systems.

The Figure 21 displays the blockchain hashes for data of size 4096 bytes divided into chunks of 1024 bytes. Each chunk, once hashed, is sequentially added to the blockchain, ensuring the integrity of the stored data.

The Genesis Block (Index: 0) is identified by its unique hash: 6fc679170f8c3dd5e388dad88212b12d100dfa9b0055217afe637621091f5e80.

Chunk 0 (Index: 1) is represented by the hash7b132d747d3ea342bf82602252622152a71237c08e655cc48fce21528ef9f496, followed by Chunk 1 (Index: 2) with hash d4bdd24a23c7d3de36c556b6b0c321c631def7e7e0a6ea1eb2f661ffac309eae.

Chunk 2 (Index: 3) has the hash 58781b4013e7356b95cc6e0caaff232adcab47a11a1c3a68ca8c9e7dee337953.

and Chunk 3 (Index: 4) has the hash cb609f132c1fac6da6e6608f4637823f296792a5d5f902ecd4ddd1980db76b.

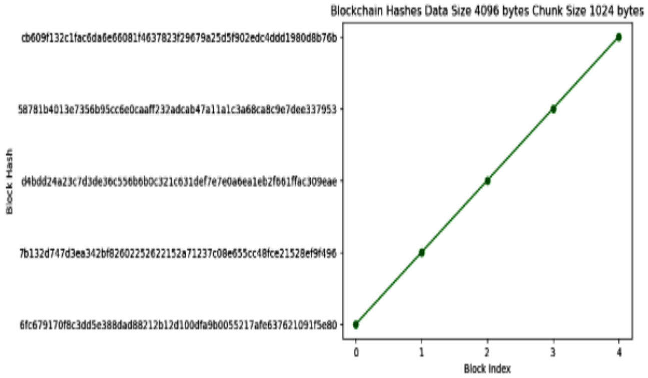

Figure 21. Blockchain hashes for data size 4096 bytes, chunk size 1024 bytes

The graph illustrates a linear progression, showing the sequential addition of each block, maintaining the integrity and continuity of the blockchain, thereby verifying that all data chunks have been successfully integrated and hashed without any integrity breaches.

In Table 2 is the summary of how the system performs with various data sizes and chunk sizes. Examining the results demonstrates that achieving smaller chunks ensures greater system resilience through enhanced redundancy and distribution but slows down transaction processing. Larger chunk sizes decrease processing time but raise the chance of losing data if a chunk becomes faulty.

Table 2. Comparative results of data integrity verification using blockchain for different data and chunk sizes

Data Size (bytes)	Chunk Size (bytes)	Number of Chunks	Verified Chunks	Integrity Status	Blockchain Details (Block Hashes)
1024	512	2	2	All Verified	[035c610c, 3b84ab61, 4f9f3c16]
1024	1024	1	1	All Verified	[e94f4519, e4319c10]
1024	2048	1	1	All Verified	[752a8d91, 84a36a23]
2048	512	4	4	All Verified	[0ad4d7ef, 22e87a99, 6ab9f552, 2f3b185a, e9a5419b]
2048	1024	2	2	All Verified	[91b17d1b, 7449644a, 0ec2dcb1]
2048	2048	1	1	All Verified	[d095ec05, e82de5e5]
4096	512	8	8	All Verified	[3fa643ce, a2c5f0dd, f6d04458, 7ba2dfd2, 77f01595, 42dff91e, e96a72b7, 8ac1af73, f890eda8]
4096	1024	4	4	All Verified	[6fc67917, 7b132d74, d4bdd24a, 58781b40, cb609f13]

5. CONCLUSIONS

A strong framework for boosting cloud safety with blockchain technology has been introduced in this research. The conducted tests showed that this technique effectively ensured data integrity in diverse combinations of data and chunk sizes. Tests with data sizes of 1024 bytes and 2048 bytes combined with chunk sizes of 512 bytes and 2048 bytes resulted in all probability in successful integrity assessments. Applying the SHA-256 cryptographic hash method for data partitioning and hashing preserved the reliability and consistency of every data fragment. The design of the blockchain allowed each block to hold the hash of the block before it and formed a safe connection that prevented data alteration. Ongoing analysis of data validity throughout all settings proved the accuracy of the technique resulting in complete success each time. This strategy confronts important cloud security problems such as compliance issues and data leaks by delivering a secure and scalable approach to cloud data storage. The extensive analysis of numbers demonstrated that using blockchain technology alongside cryptographic hashing guarantees secure and unchanging data storage in the cloud.

Future investigation needs to target boosting computational performance particularly in contexts that handle extensive datasets where time for processing and resource usage matter greatly. Employing innovative cryptographic approaches including post-quantum cryptography could improve security from potential dangers. Researching combined frameworks that involve blockchain and machine learning for immediate recognition of anomalies and data prediction in cloud security is a valuable path. Investigating the relationship between current cloud infrastructure and blockchain security options can promote efficient integration in multiple fields.

REFERENCES

[1] Fernandes, D.A., Soares, L.F., Gomes, J.V., Freire, M.M., Inácio, P.R. (2014). Security issues in cloud environments: A survey. International Journal of InformationSecurity, 13(2): 113-170. https://doi.org/10.1007/s10207-013-0208-7

[2] Bowers, K.D., Juels, A., Oprea, A. (2009). HAIL: A high-availability and integrity layer for cloud storage. In Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 187-198. https://doi.org/10.1145/1653662.1653686

[3] Lainjo, B. (2020). Network security and its implications on program management. International Journal of Safety and Security Engineering, 10(6): 739-746. https://doi.org/10.18280/ijsse.100603

[4] Rimal, B.P., Choi, E., Lumb, I. (2009). A taxonomy and survey of cloud computing systems. In 2009 Fifth International Joint Conference on INC, IMS and IDC, Seoul, Korea (South), pp. 44-51. https://doi.org/10.1109/NCM.2009.218

[5] Narayana, V.L., Midhunchakkaravarthy, D. (2021). Secured resource allocation for authorized users using time specific blockchain methodology. International Journal of Safety and Security Engineering, 11(2): 201-205. https://doi.org/10.18280/ijsse.110209

[6] Pearson, S. (2013). Privacy, security and trust in cloud computing. In Privacy and Security for Cloud Computing, pp. 3-42. https://doi.org/10.1007/978-1-4471-4189-1_1

[7] Dai, W., Vasarhelyi, M.A. (2017). Toward block chain-based accounting and assurance. Journal of Information Systems, 31(3): 5-21. https://doi.org/10.2308/isys-51804

[8] Chaudhry, S.A., Naqvi, H., Shon, T., Sher, M. (2017). Design of an authentication protocol for cloud computing using user biometrics and image encryption. Cluster Computing, 20(1): 211-220.

[9] Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Chen, S., Xiong, Z. (2016). The block chain as a software connector. In 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), Venice, Italy, pp. 182-191. https://doi.org/10.1109/WICSA.2016.21

[10] Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H. (2017). An overview of block chain technology: Architecture, consensus, and future trends. In 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, pp. 557-564. https://doi.org/10.1109/BigDataCongress.2017.85

[11] Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., Rehman, S.U. (2023). Cyberattacks and security of cloud computing: A complete guideline. Symmetry, 15(11): 1981. https://doi.org/10.3390/sym15111981

[12] Aslam, J., Kumar, K. (2024). Enhancing cloud data security: User-centric approaches and advanced mechanisms. The Scientific Temper, 15(1): 1784-1789. https://doi.org/10.58414/SCIENTIFICTEMPER.2024.15.1.29

[13] Dorsala, M.R., Sastry, V.N., Chapram, S. (2021). Blockchain-based solutions for cloud computing: A survey. Journal of Network and Computer Applications, 196: 103246. https://doi.org/10.1016/j.jnca.2021.103246

[14] Sharma, P., Namasudra, S., Lorenz, P. (2023).

Blockchain-based cloud storage system with enhanced optimization and integrity preservation. In ICC 2023-IEEE International Conference on Communications, Rome, Italy, pp. 3744-3749. https://doi.org/10.1109/ICC45041.2023.10279598

[15] Singh, S.K., Manjhi, P.K., Tiwari, R.K. (2021). Cloud computing security using blockchain technology. Transforming Cybersecurity Solutions using Blockchain, pp. 19-30. https://doi.org/10.1007/978-981-33-6858-3_2

[16] Singh, A., Chatterjee, K. (2022). Blockchain for Cloud Storage: A Comprehensive Review. Future Generation Computer Systems, 127: 183-197.

[17] Singh, S.K., Manjhi, P.K., Tiwari, R.K. (2021). Cloud computing security using blockchain technology. Transforming Cybersecurity Solutions using Blockchain, pp. 19-30. https://doi.org/10.1007/978-981-33-6858-3_2

[18] Sarmah, S. (2019). Application of Blockchain in Cloud Computing. International Journal of Innovative Technology and Exploring Engineering, 8: 2278-3075. https://doi.org/10.35940/ijitee.L3585.1081219

[19] Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., Basu, K., Chaudhury, S., Sarkar, P. (2018). Cloud computing security challenges & solutions-A survey. In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, pp. 347-356. https://doi.org/10.1109/CCWC.2018.8301700

[20] Wang, S., Wang, X., Zhang, Y. (2019). A secure cloud storage framework with access control based on blockchain. IEEE Access, 7: 112713-112725. https://doi.org/10.1109/ACCESS.2019.2929205

[21] Kayikci, S., Khoshgoftaar, T.M. (2024). Blockchain meets machine learning: A survey. Journal of Big Data, 11: 9. https://doi.org/10.1186/s40537-023-00852-y

[22] Kshetri, N. (2017). Can block chain strengthen the internet of things? IT Professional, 19(4): 68-72. https://doi.org/10.1109/MITP.2017.3051335

[23] Ali, M., Nelson, J., Shea, R., Freedman, M.J. (2016). Blockstack: A global naming and storage system secured by blockchains. In 2016 USENIX Annual Technical Conference (USENIX ATC 16), pp. 181-194.

[24] Liang, X., Zhao, J., Shetty, S., Li, D., Li, J. (2017). Integrating block chain for data sharing and collaboration in mobile healthcare applications. In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, pp. 1-5. https://doi.org/10.1109/PIMRC.2017.8292361

[25] Xu, X., Weber, I., Staples, M. (2019). Blockchain in software architecture. Architecture for Blockchain Applications, Springer Cham, 83-92. https://doi.org/10.1007/978-3-030-03035-3_5

[26] Hardjono, T., Lipton, A., Pentland, A. (2019). Toward an interoperability architecture for block chain autonomous systems. IEEE Transactions on Engineering Management, 67(4): 1298-1309. https://doi.org/10.1109/TEM.2019.2920154

[27] Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C. (2016). Hawk: The block chain model of cryptography and privacy-preserving smart contracts. In 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, pp. 839-858. https://doi.org/10.1109/SP.2016.55

[28] Suo, H., Wan, J., Zou, C., Liu, J. (2012). Security in the internet of things: A review. In 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, pp. 648-651. https://doi.org/10.1109/ICCSEE.2012.373

[29] Mollah, M.B., Azad, M.A.K.,Vasilakos, A.V. (2017). Secure data sharing and searching at the edge of cloud-assisted internet of things. IEEE Cloud Computing, 4(1): 34-42. https://doi.org/10.1109/MCC.2017.9

[30] Nguyen, Q.K. (2016). Block chain-A financial technology for future sustainable development. In 2016 3rd International Conference on Green Technology and Sustainable Development (GTSD), Kaohsiung, Taiwan, China, pp. 51-54. https://doi.org/10.1109/GTSD.2016.22

NOMENCLATURE

D	File
D1,D2	Data chunks
N	Total number of chunks
S	Original file size
C	Chunk size
Hi	Hash value of ith data chunk
H()	Hash function
Ti	ith transaction
Mi	Meta data of ith chunk
Bj	jth block
Ci	ith cloud storage location
U	User
R	Roles
P	Permissions
A	Access control