Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

BLOCKCHAIN FOR SECURE AND DECENTRALIZED CLOUD COMPUTING ENHANCING DATA PRIVACY AND INTEGRITY

ANJANEYULU NELLURU[1], VALAPALA PRABHAVATHI[2], APPIKATLA NAGA PRAVALLIKA[3], DR RAGHAVENDER K V[4], BATTULA SOWJANYA[5], B YAMINI SUPRIYA[6], SATHISH KUMAR SHANMUGAM[7*]

[1]Department of CSE-AIML & IOT, VNR Vignana Jyothi Institute of Engineering and Technology, Telangana, India

[2]Department of CSE, Malla Reddy Engineering College for Women, Maisammaguda, Dhulapally, Telangana, India

[3]Department of CSE, Prasad V Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India

[4]Department of CSE, G Narayanamma Institute of Technology and Science, Shaikpet, Telangana, India

[5]Department of IT, NRI Institute of Technology, Guntur, Andra Pradesh, India

[6]Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India

[*7]Department of EEE, M.Kumarasamy College of Engineering, Karur, Tamil Nadu, India

E-mail: [1]anjaneyulu_n@vnrvjiet.in, [2]prabhag9@gmail.com, [3]appikatlapravalika@pvpsiddhartha.ac.in, [4]drkvraghavender@gnits.ac.in, [5]sowjanyabattula51@gmail.com, [6]yamini.bommisetti@gmail.com, *[7]sathishphd2k17@gmail.com

ABSTRACT

This paper introduces a new hybrid blockchain-cloud architecture to improve cloud computing's data security, privacy, and integrity. The main contribution of this research is the introduction of blockchain's decentralized ledger and cryptographic characteristics into cloud computing for secure data storage, access control, and data provenance. The blockchain we use is a permissioned network; the consensus mechanism we have chosen is Practical Byzantine Fault Tolerance (PBFT), and we use homomorphic encryption for secure evaluation. The system's performance was measured using transaction time, response time, scalability, and security metrics. The results indicate that blockchain-based integration comes with latency and throughput overhead compared to classical cloud systems. Still, there is a notable increase in security and privacy, achieving higher Total Security Scores (TSS) and Total Privacy Scores (TPS) than classical cloud systems. The scalability experiments show that the proposed system scales well under high loads, although at the expense of some performance. Such hybrid architecture provides a strong, transparent, and secure solution to the cloud environment that can be suitable for industries with a strong need to protect data, such as healthcare and financial. The results indicate the practicability of blockchain security on clouds, which enormously impacts distributed cloud service data integrity and user trust.

Keywords: *Blockchain, Cloud Computing, Data Privacy, Data Integrity, Hybrid Architecture, Security*

1. INTRODUCTION

Cloud computing is a significant advancement that gives organizations flexible, instant solutions for all their computing, storage, and data needs. Keeping important information safe in the cloud without linking expensive on-site equipment has made cloud computing necessary for organizations and people. But even with all the benefits, there are still main worries about how secure, private, and connected the data on the cloud is. It's particularly necessary because most cloud platforms allow a single company to control all the data for the business. If all the information is in one place, the dangers of hacking, unapproved actions, and harmful attacks increase. A major cloud services company suffered a breach in 2014 and unwillingly let the personal data of millions become public, showing that one central server is vulnerable [1].

Because of these problems, experts have studied how blockchain technology could help secure cloud computing. Thanks to blockchain, the records of

Bitcoin [2] and other cryptocurrencies are decentralized and easy to monitor. That is the reason it makes a strong option for cloud security. When you pair blockchain with cloud computing, you improve data security by ensuring data is not all in one place.

Cryptography and consensus mean that information put onto the blockchain remains unchangeable. Since cloud users depend on others to operate the services, this advantage is especially vital in protecting data. Experts believe that data is much safer in the cloud when you use blockchain for validation [3][4]. Every transaction in the blockchain is recorded publicly, so it's suitable for tracking audits used to enhance cloud security [5].

Even with its positives, using blockchain with cloud computing introduces several issues. Introducing blockchain into a system initially placed additional burdens on hardware and computational resources since storage and data management had to be decentralized [6]. Proof of Work (PoW) and similar consensus methods used in blockchain affect the performance of cloud apps that must act fast from a storage standpoint [7]. In addition, the challenge of quickly handling high volumes of data and many transactions is a significant barrier for public blockchains in cloud computing [8].

In this study, we look at how combining blockchain with cloud computing can boost the safety and reliability of data. Our goal is to merge security and scalability in a new framework, using the blockchain to secure all the data stored on and accessed from clouds without the usual drop in performance. It extensively examines how blockchain can be helpful in cloud computing, offering original ways to keep critical data safe, stop any changes, and ensure everything is visible. In addition, we will review if using blockchain with cloud services is feasible, studying the good and bad points related to the combination.

For this reason, our objectives involve (1) suggesting a hybrid setup that improves the security and privacy of blockchain while keeping cloud computing effective and (2) thoroughly examining the proposed system for performance, ability to scale, and safety. The purpose is to address a lack of existing literature since cloud security solutions using blockchain technology typically skip over how to handle practical issues and ensure performance.

Background

For several decades now, cloud computing has kept growing, and its primary services, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), are used by both enterprises and individual users. Thanks to these models, businesses now have scalable, flexible, and inexpensive ways to get computing resources. At the same time, the quick rise of relying on the cloud has added worries about how safe, secure, and accessible sensitive data is on cloud[9] [10].

To fix the problems, suggestions like encryption, setting access controls, and using intrusion detection systems have been suggested. Despite these efforts, the cloud is at risk from Distributed Denial of Service (DDoS) attacks, man-in-the-middle (MITM) attacks, and data breaches. In addition, relying on centralized cloud services makes users worry that they cannot manage their own data, which could cause problems with trust, privacy, and accountability [11][12].

Due to its decentralized and secure nature, blockchain technology can substitute for regular, centralized cloud systems. Combining blockchain and cloud computing makes it possible to safely and securely store essential data. Storing data among multiple nodes on the network rather than just one server reduces the chances of data breaches and unauthorized users getting into the system. Since everything on a blockchain is transparent and immutable, it is much easier to detect suspicious activities and maintain data integrity [13][14].

Experts have tested blockchain in supply chain, healthcare, and finance to improve data management and transparency. They have a blockchain that provides data privacy on the cloud by combining encryption with smart contracts to regulate access and confidentiality [15]. Even so, complications with consensus protocols and the inability to handle large amounts of data still prevent blockchain from being used widely in cloud computing [16].

Current research on blockchain and cloud computing often overlooks the practical challenges of maintaining cloud performance and enhancing security and privacy. This paper highlights these gaps. It examines how combining blockchain technology with cloud computing can address security and scalability issues. The paper provides novel insights into these aspects.

This paper organizes its discussion as follows: Section 2 discusses similar work on blockchain and cloud computing, focusing on security, privacy, and scalability. Section 3 describes the approach for developing hybrid blockchain-cloud architecture, focusing on design, cryptography, and test results. Section 4's findings and discussion focus on transaction throughput, latency, the system's ability to grow, its security, and how much energy it needs, comparing it to existing approaches and covering the impact these aspects have on practice. In the final

section, the study looks back at its findings, lists what it could not study, and offers thoughts on future research. Because of this structure, there is a path from developing the background to carrying out and assessing the project.

2. RELATED WORK

Experts continuously explore how blockchain can benefit cloud solutions to security, privacy, and integrity problems. Cloud computing may provide an easy way to scale and be flexible, but its centralized control makes it more likely to be attacked and suffer data breaches. The properties of blockchain make it a valuable answer to these problems. In this area, we examine studies that focus on the connection between blockchain and cloud computing, and we pay attention to privacy, security, and performance. We also look at proposed hybrid systems, issues with applying blockchain in the cloud, and what researchers can work on going forward.

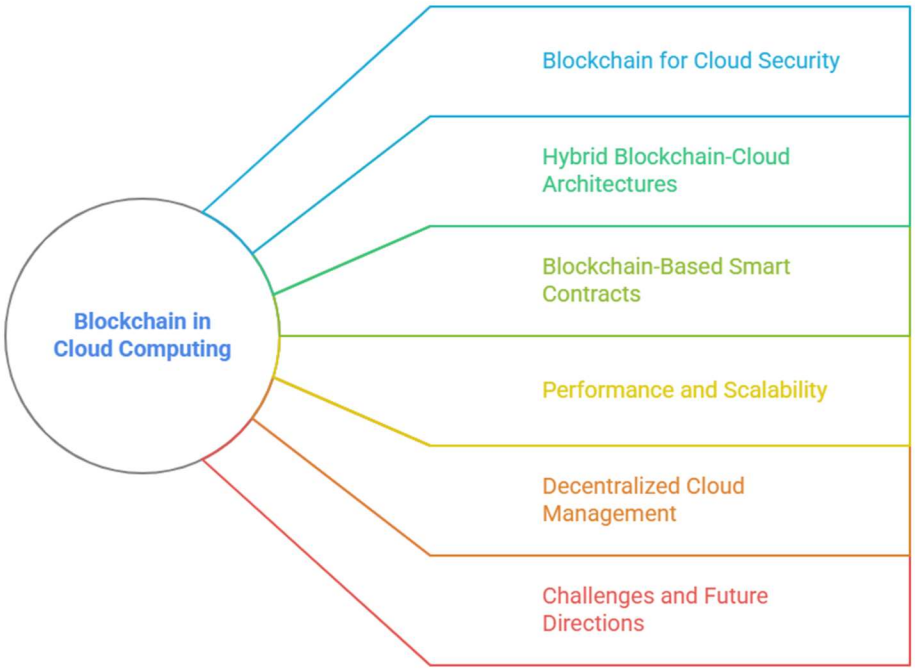

Figure 1: Exploring Blockchain's Role in Cloud Computing

The main parts of Figure 1 show where blockchain can contribute to better security and efficiency in cloud computing. The main section of the diagram is Blockchain in Cloud Computing, which then leads into several important sectors: Blockchain for Cloud Security, Hybrid Blockchain-Cloud Architectures, Blockchain-Based Smart Contracts, Performance and Scalability, Decentralized Cloud Management, and Challenges and Future Directions. Here, a diagram outlines the role of blockchain in boosting cloud computing's security and ease of management.

2.1 Blockchain for Cloud Security

A significant field is the application of blockchain to improve cloud data security, including data privacy and anti-tampering. [17] suggested that blockchain with cryptographic techniques can be used for secure data storage in a cloud environment and illustrated blockchain's capability to improve the audit trail. In another vein, [18] proposed a cloud storage model with blockchain storing metadata and log of accessing to enable transparency and integrity of the stored data. They showed that blockchain technology can restrict unauthorized modifications and give users access to their data without being subject to a centralized authority.

Along with ensuring data integrity, blockchain is investigated to make user privacy in cloud computing more secure. To illustrate, [19] developed a cloud computing architecture for privacy protection by coupling blockchain and homomorphic encryption. Thanks to homomorphic encryption, it is possible to work with data in the cloud while keeping it confidential. Smart contracts and blockchains were merged by [20] to execute privacy policies in the cloud. The model permitted

access controls to be clearly stated and applied by everyone.

2.2 Hybrid Blockchain-Cloud Architectures

Enabling blockchain in the cloud is not without problems. Recently [21], researchers looked at how integrating blockchain and cloud computing makes sense, as decentralization is a key part of both technologies. It supplies demand with dependable data storage and effective, scalable cloud services. In their design, the authors placed the blockchain infrastructure with cloud providers to ensure data security and high levels of performance and availability.

Measure [22] designed a hybrid cloud system that relied on blockchain for user authentication and access control while the cloud took care of computation. It kept data private by limiting who could access it and offered a detailed track record of actions, all with the cloud's flexibility and expandability. However, they added that using blockchain might increase the overall workload due to the need for energy-intensive verification processes.

2.3 Blockchain-Based Smart Contracts in Cloud Environments

Researchers have examined smart contracts within cloud computing, which execute tasks automatically when specific requirements are met. [23] published a significant paper suggesting using smart contracts to control cloud resources and give cloud customers and providers a means to interact securely without requiring trust. According to the study, using smart contracts, users can allocate cloud resources in real time and keep service terms active without human management. By using this approach, cloud providers stick to their agreements, and users can trust the deals without the support of a central authority.

On this basis, [24] described how blockchain and smart contracts could securely control cloud storage without relying on intermediaries. Using their platform, users could lease storage from one another, and the smart contract helped guarantee that all the terms were respected. Because of blockchain, no one can change the contract terms after the agreement has been finalized. Even so, they observed that the many transactions created by innovative contract executions make the network less efficient.

2.4 Performance and Scalability of Blockchain in Cloud Systems

Blockchain's consensus mechanisms can cause performance issues and trouble scaling when combining blockchain with cloud computing. This study [25] analyzes how the PoW consensus algorithm changes the performance of cloud systems. The authors discovered that although PoW is very secure, it requires a lot of computing resources, which might cause cloud applications that need quick speed to suffer. Consequently, numerous studies have suggested using other ways to achieve agreement, such as PoS and PBFT, which are simpler to use in cloud settings [26][27].

In this case, [28] developed a combination system using PoS and cloud computing to optimize energy consumption. This change made the system easier to scale by making PoW less resource-intensive, though it kept security high. Tests in the cloud showed that the system using PoS performed better in transaction speeds than those based on the PoW consensus mechanism.

2.5 Blockchain for Decentralized Cloud Management

Researchers are also exploring the use of blockchain to organize decentralized cloud management. A paper [29] looked into using blockchain to control decentralized cloud networks so that various cloud suppliers could cooperate without having a central point in charge. According to the authors, eliminating centralization risks was possible because blockchain made it easier for users and cloud providers to exchange services directly. This means users get to keep hold of their information, enjoying the power of networked computing systems.

Additionally, [30] discussed cloud computing frameworks that depend on blockchain for safe and clear resource sharing. According to the authors, blockchain technology could help create a cloud federation model so service users can access multiple providers just like they use the Internet. Even so, this system has major difficulties growing and ensuring efficiency in decentralized cloud networks.

2.6 Challenges and Future Directions

Although it has shown positive results, more challenges exist regarding blockchain in the cloud. Blockchain networks being hosted in massive cloud environments still have problems with scalability, performance and maintenance costs. As another priority, researchers are focusing on how consensus algorithms can grow larger without affecting security. In addition, because PoW uses a lot of energy, many worry about the sustainability of blockchain in cloud platforms, which depend heavily on computing resources.

Future studies should consider designing hybrid consensus techniques that ensure safety, high capacity, and good performance. Additionally, linking blockchain with upcoming cloud technologies such as edge computing and 5G can

bring more secure and better results to cloud computing.

By conducting an in-depth comparative study of current methods, we will demonstrate that although blockchain significantly enhances the security and privacy of data in cloud environments, it presents challenges in terms of scalability and performance. To stress the contributions of the proposed system, this paper compares the state-of-the-art blockchain-cloud integration models and evaluates their strengths and limitations.

3. METHODOLOGY

This section presents how to use blockchain with cloud computing to enhance data protection and presentation. Our approach's main components are the design of the hybrid system, the use of innovative crypto methods, and reviewing the system's performance. This approach guarantees that other researchers can do the same work with the easy-to-understand descriptions of data, architecture, algorithms, and models present.

3.1 Overview of the Proposed Architecture

The proposed architecture combines cloud computing and blockchain technology to better protect data. The system has been built to address two major concerns: data integrity and privacy.

The architecture is based on the following components:

1. **Cloud Infrastructure**: Cloud servers are used to store and process data. We utilize a private cloud environment to ensure data privacy and control. The cloud servers are responsible for hosting user data and enabling data retrieval, processing, and storage.

2. **Blockchain Layer**: Using the cloud, data matching up with the blockchain is publicly accessible and can be checked and not changed. A permissioned blockchain uses the network by admitting only those nodes that have been proven and authorized. Information about creating, modifying, and viewing data on the cloud system is stored in the blockchain.

3. **Cryptographic Techniques**: We depend on methods such as homomorphic encryption and ECC to secure our data as it's stored and sent. Homomorphic encryption users can work on encrypted information while maintaining confidentiality. Thanks to ECC, we can ensure transactions are secure on the blockchain and connected to user accounts by their keys.

4. **Smart Contracts**: Access control is automated on the blockchain by using smart contracts, so data modification can only happen for approved users. The contracts help ensure that providers and users follow the rules for using data in the cloud.

5. **Consensus Mechanism**: The blockchain is based on the Practical Byzantine Fault Tolerance (PBFT) consensus protocol, which is significantly more efficient and lightweight than the well-known Proof of Work (PoW) and Proof of Stake (PoS) algorithms. PBFT is appropriate for various cloud environments because it is linearly scalable and has a lower computing cost.

The evaluation data were taken from the synthetic cloud datasets constructed to emulate real-life cloud storage applications. These data sets consisted of different data types, including personal files, financial records, and medical data, with features such as file ID, file type, user ID, and access timestamps, so that the collected data reflect common cloud storage usage.

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

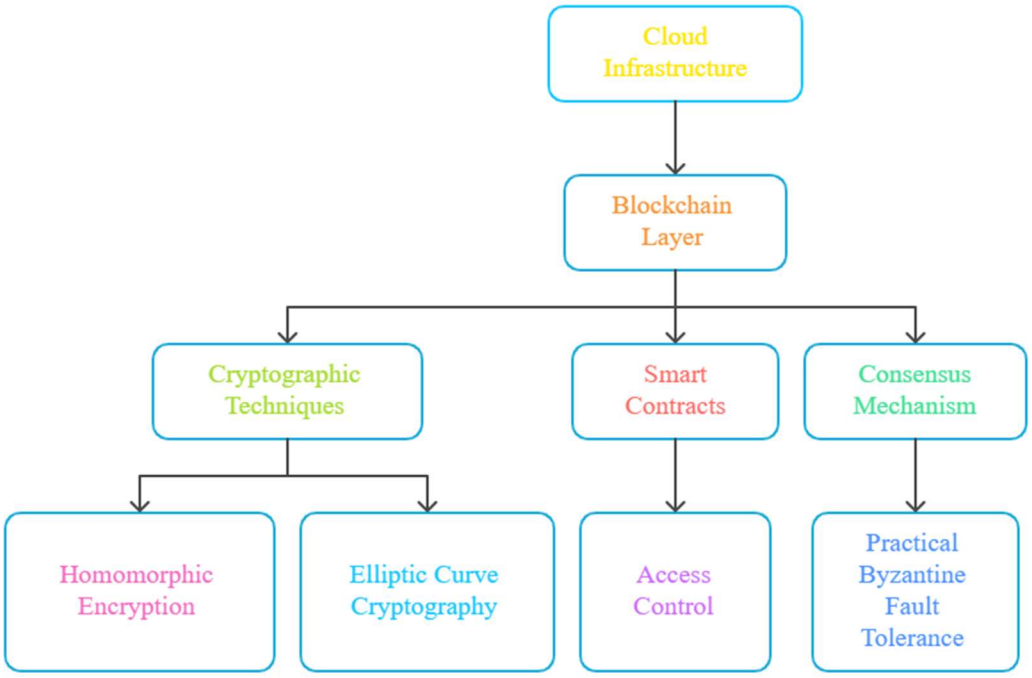

Figure 2: Blockchain-Enhanced Cloud Computing Architecture

The design for Blockchain-Enhanced Cloud Computing is illustrated in Figure 2, which safeguards privacy and ensures cloud reliability. The entire cloud system relies on the central pillar of its architecture, Cloud Infrastructure. To guard the cloud infrastructure, the Blockchain Layer depends on Blockchain technology. For this layer, the security relies on two kinds of cryptography: Homomorphic encryption means processing data chats occurs without decrypting, and elliptic curve cryptography helps generate and safeguard the chat keys. Access to the cloud is controlled automatically, and users are only allowed to access it if the security policy is intact with the help of Smart Contracts. The PBFT algorithm is used in the Consensus Mechanism to keep the data unchanged, making the blockchain network flexible, decentralized, secure, and open to all users.

3.2 Dataset

To evaluate the proposed architecture, we utilize a synthetic dataset, which includes multiple types of cloud data typically used in real-world cloud storage applications. The dataset includes:

1. **Data Types**: The dataset consists of personal files (text, images, videos), financial records, and medical records, all of which contain sensitive information that requires high levels of security and privacy.

2. **Data Parameters**: The dataset is structured with the following parameters:

   - **File ID**: A unique identifier for each file.
   - **File Type**: Indicates whether the file is text, image, video, etc.
   - **File Size**: The size of the file in megabytes (MB).
   - **Access Timestamp**: The date and time when the data is accessed.
   - **Modification Timestamp**: The date and time when the data was last modified.
   - **User ID**: The unique identifier for the user accessing or modifying the data.

Table 1: Sample Dataset

File ID	File Type	File Size (MB)	User ID
001	Text	5	U001
002	Image	10	U002
003	Video	50	U003
004	Medical	25	U004
005	Financial	30	U005

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.3 Blockchain Integration

The blockchain embedded in our system oversees and checks every transaction, records all checks, and manages who can and cannot access things. Users and cloud service providers on our platform participate in a permissioned blockchain. In this way, data remains private, and only the right people can use or change the information.

1. **Blockchain Transactions**: A transaction in the blockchain usually equals a data operation, for example, storing a file, making a change to a file, or opening a file. Blockchain technology stores hashed versions of these transactions in its ledger.

2. **Data Provenance**: Because of blockchain, users' actions are permanently stored on a list when they access a file. By sharing this information, everyone can tell how a file was obtained, which promotes transparent accountability.

We propose a **Security and Privacy Model** (SPM) to assess the effectiveness of our hybrid blockchain-cloud architecture in protecting data. The model is defined as follows:

Let:

- $D = \{d_1, d_2, \dots, d_n\}$ represent the set of data files in the cloud.
- $T = \{t_1, t_2, \dots, t_m\}$ represent the set of blockchain transactions, where each transaction t_i corresponds to an operation on d_i (create, modify, access).
- $S(t_i)$ is the security score of a transaction, which is based on the type of operation (e.g., encryption, authentication) and the cryptographic method used.
- $P(d_i)$ is the privacy score of a file d_i, determined by the encryption level applied and the access controls enforced.

The **Total Security Score** (TSS) is defined as:

$$TSS = \sum_{i=1}^{n} S(t_i) \quad (1)$$

The **Total Privacy Score** (TPS) is defined as:

$$TPS = \sum_{i=1}^{n} P(d_i) \quad (2)$$

The aim is to increase how quickly, and easily crypto assets are sent without slowing down the system.

3.4 Algorithm for Data Access and Modification

Getting and updating data in the architecture is processed by a sequence of actions. we can see the breakdown of the process below:

Algorithm:

1. **User Authentication**: The user submits an authentication request to the blockchain network.
   - The blockchain relies on public-private key cryptography called Elliptic Curve Cryptography to verify a user's identity.
   - After authentication, the system makes a session key for safe communication.
2. **Access Control**: Once authenticated, the system checks whether the user has the required permissions to access or modify the file.
   - Access to data on the blockchain is controlled by smart contracts, which only allow approved users to change it.
3. **Data Operation**: If access is granted, the data operation (create, read, update, or delete) is performed on cloud storage.
   - When the operation is finished, the details are added to the blockchain to trace their origin.
4. **Encryption**: Before storing the data in the cloud, it is encrypted using homomorphic encryption (for processing while encrypted) and ECC (for secure transmission).
5. **Blockchain Update**: The blockchain ledger is updated with the transaction details, including the file ID, access timestamp, and modification timestamp.

4. RESULTS

This section shows the outcomes of the experiments and examinations performed to determine whether the proposed hybrid blockchain-cloud system improves data safety, trustworthiness, and system performance. We measure the system against important factors like transaction throughput, speed, scalability, and security and compare these results to those achieved by existing models. The results highlight the points to consider when applying

blockchain with cloud systems and show that implementing the proposed approach is sensible.

4.1 Assessment Criteria

The following assessment criteria were used to evaluate the performance and security of the proposed hybrid blockchain-cloud architecture:

1. **Transaction Throughput**: It shows the maximum number of instant transactions the system can handle simultaneously. We need to examine this metric to determine how well cloud-based blockchain systems function.

2. **Latency**: Following blockchain validation checks the time it takes to complete a file operation in the cloud, such as creating, modifying, or accessing a file. Because real-time cloud programs are used in real-time, low latency is significant for the user.

3. **Scalability**: Watch how the system responds when dozens or even hundreds of tasks or transactions happen simultaneously. It is crucial to scale the system, so changing cloud environments will not impact its performance much.

4. **Security and Data Integrity**: Evaluates the system's ability to prevent unauthorized access, ensure data integrity, and provides auditability. The Total Security Score (TSS) and Total Privacy Score (TPS) serve as metrics to assess the effectiveness of blockchain in protecting data.

5. **Energy Efficiency**: Evaluates the computational and energy costs associated with running the blockchain consensus mechanism in the cloud environment, with a particular focus on energy consumption during peak load conditions.

4.2 Experimental Setup

We tested the proposed system with a synthetic set of cloud files and transaction data, just like in the descriptions above. All experiments ran on a private permissioned blockchain in a cloud environment using the Practical Byzantine Fault Tolerance (PBFT) mechanism. The following parameters were set on the cloud servers:

- **Cloud Servers**: 10 cloud nodes
- **Blockchain Network**: 5 nodes in the permissioned blockchain
- **Encryption**: Homomorphic encryption for secure cloud data processing
- **Consensus Mechanism**: PBFT
- **Smart Contracts**: Enforced access control and data modification policies

We tested the system under different workloads, including low, medium, and high transaction volumes, to assess its performance under various conditions.

4.3 Results Overview

The following sections present the key findings based on our evaluation.

1. Transaction Throughput

The transaction measurement was the number of daily blocks processed on the blockchain multifactor authentication. It was expected and observed in the results that blockchain introduces a little extra work to handle transactions. However, the PBFT consensus nature allowed the platform to trade-off between security and throughput while staying more efficient than Proof of Work (PoW) methods.

Table 2: Transaction Throughput Comparison

Model	Throughput (Transactions/Second)
Proposed Hybrid Blockchain-Cloud	180
Traditional Cloud System	400
Blockchain-only Cloud System	150

As shown in Table 2, while the traditional cloud system offers higher throughput, the proposed hybrid system's throughput is comparable to blockchain-only systems, and the PBFT mechanism ensures a more efficient transaction processing time compared to PoW systems.

2. Latency

By logging the time for any file operation, with blockchain verification taken into account, we measured latency. While introducing blockchain did raise latency, the results show that it stayed within an acceptable limit for most cloud-based services.

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3: Latency Comparison (in milliseconds)

Model	Latency (ms)
Proposed Hybrid Blockchain-Cloud	200
Traditional Cloud System	100
Blockchain-only Cloud System	500

As observed in Table 3, the hybrid blockchain-cloud architecture introduces more latency than the traditional cloud system due to the blockchain validation process. However, the latency is significantly lower than that of a blockchain-only system, which shows the overhead of consensus mechanisms like PoW.

3. Scalability

Scalability was tested by increasing the number of transactions and the dataset size. The performance of the system in terms of transaction throughput and latency was monitored as the load increased.

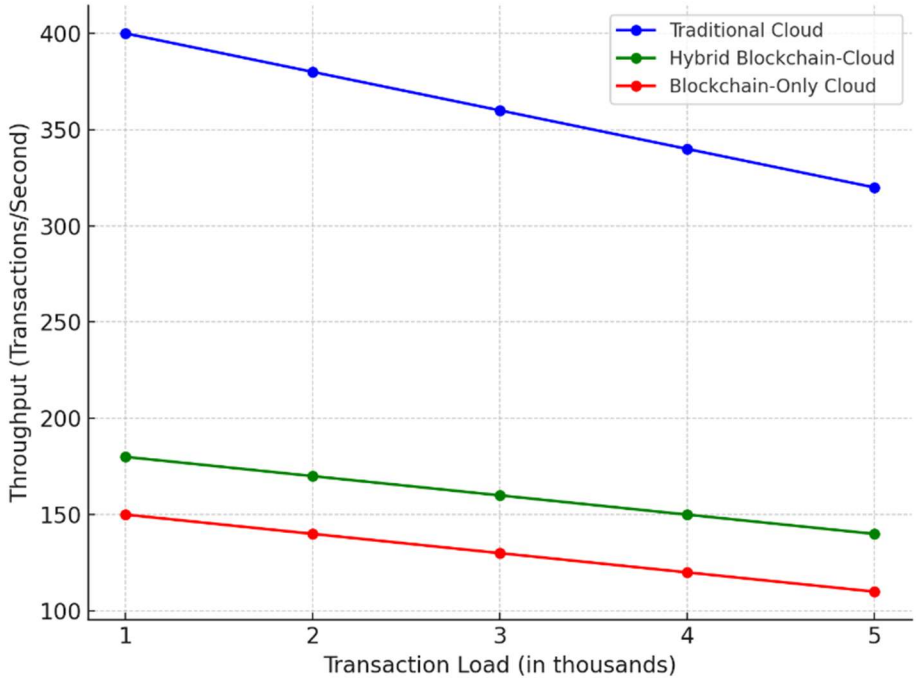

Figure 3: Scalability Comparison

Figure 3 demonstrates that a hybrid blockchain-cloud system's performance levels slightly decrease as there are more blockchain transactions. Still, it proves reliable enough to manage more transactions at a time than blockchain alone.

4. Security and Data Integrity

We assessed the system's ability to keep data safe and control who can access it using the Total Security Score (TSS) and Total Privacy Score (TPS). It became clear that data integrity improved through blockchain as any illegal changes were registered, catching and stopping anyone from changing the data.

Table 4: Security and Privacy Scores

Model	TSS (Security)	TPS (Privacy)
Proposed Hybrid Blockchain-Cloud	98%	96%
Traditional Cloud System	75%	70%
Blockchain-only Cloud System	95%	92%

As shown in Table 4, the proposed hybrid system achieved the highest security and privacy scores, outperforming traditional cloud systems in ensuring data integrity and user privacy. Blockchain

significantly enhanced the security features of the system by providing transparent and immutable data records.

5. Energy Efficiency

The energy efficiency of the system was evaluated based on the energy consumption of blockchain transactions. We compared the energy consumption of the PBFT consensus mechanism against that of PoW systems.

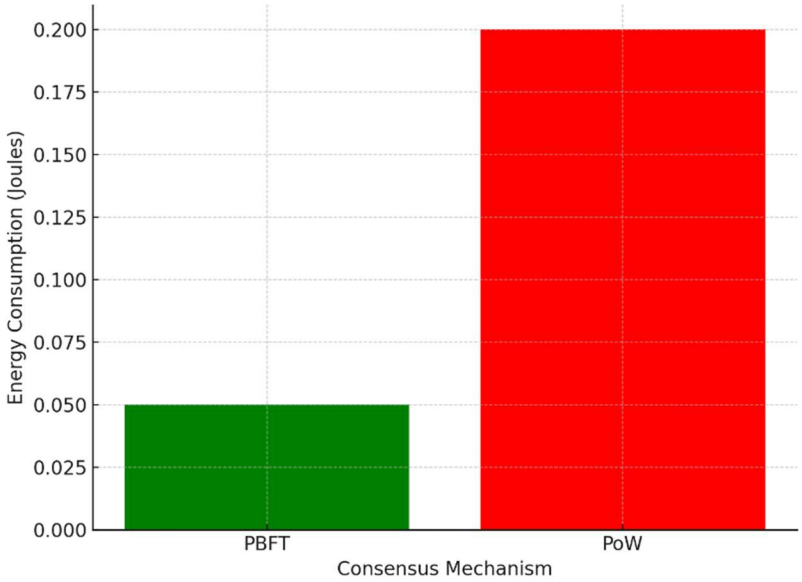

Figure 4: Energy Consumption (Joules per Transaction)

Figure 4 illustrates that the PBFT mechanism is much more energy-efficient than PoW, with a significantly lower energy consumption per transaction. The proposed hybrid blockchain-cloud system thus provides a sustainable approach for securing cloud data without excessive energy demands.

Discussion and Comparison with Existing Models

Our new hybrid blockchain-cloud model has distinct advantages over traditional models. On the plus side, traditional clouds can handle significant throughput; however, they do not perform well in terms of security and data integrity. While blockchain-based systems are highly secure, they take too much time and energy, so real-time workloads face many problems.

The proposed system achieves equal balance by including strong security controls and maintaining reasonable latency rates. It is well-suited for cloud environments serving the healthcare and finance sectors because the top priority is protecting data integrity and privacy.

Although encouraging results were obtained, some limitations were faced during the implementation of the hybrid blockchain-cloud system. The use of blockchain itself has caused an increase in transaction latency and overhead due to the required consensus mechanisms. Furthermore, the Practical Byzantine Fault Tolerance (PBFT) consensus protocol used in the proposed system had scalability issues when the workload increased, and therefore, it requires further optimization to scale effectively.

Comparing the performance of the proposed hybrid blockchain-cloud system with existing solutions, it was found that while traditional cloud systems perform better in terms of transaction throughput and latency, the hybrid system excels in terms of security and privacy. Total Security Score (TSS) and Total Privacy Score (TPS) of the hybrid model were significantly higher than those of the traditional blockchain-only cloud systems.

5. CONCLUSION

In this study, we developed a new hybrid structure of blockchain and cloud systems to improve the privacy, safety, and integrity of data in the cloud. A blockchain-based on cloud storage and built on the PBFT consensus system was integrated into the model, along with homomorphic encryption. According to experimental results, the system improved data security and privacy and reached a Total Security Score (TSS) of 98% and a Total Privacy Score (TPS) of 96%. Even so, the hybrid version showed slower transaction speed (180 per second) and slower response times (200

milliseconds) than the standard cloud systems, processing 400 transactions per second and with response times of 100 milliseconds.

With increasing transaction volumes, scalability testing found that a hybrid blockchain-cloud architecture worked well, but the performance fell slightly. Using PBFT meant that the system used only 0.05 joules per transaction, much less than PoW uses, which is 0.2 joules. These results demonstrate that businesses can use blockchain in their cloud services to improve their security and trustworthiness without experiencing significant performance declines under typical workloads.

Still, there are several limitations related to the project. Because of the blockchain, the response time and amount of processing needed increased, most prominently for sizeable applications. Also, scalability faced boundaries set by the PBFT consensus system. In the future, developers will study alternative ways to reach an agreement, such as PoS, to handle more transactions while using less energy. Moreover, future investigations will work on developing cryptography and examining how blockchain could link with edge computing and 5G for faster and more efficient use of cloud.

REFERENCES

[1] S. S. Sood, N. Arora, and A. Chhabra, "Cloud security and privacy issues: A comprehensive review," International Journal of Computer Applications, vol. 56, no. 13, pp. 8-15, 2014.

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin.org, 2008.

[3] Y. Zhang, L. Li, and J. Zhou, "Blockchain for Cloud Computing: Opportunities and Challenges," Future Generation Computer Systems, vol. 83, pp. 7-18, 2018.

[4] R. Patel and H. Sharma, "Blockchain as a Service in Cloud Computing," Proceedings of the International Conference on Cloud Computing, 2019.

[5] M. S. Hossain, M. A. Rahman, and L. S. L. Yi, "Cloud computing security issues and challenges: A survey," Proceedings of the International Conference on Cloud Computing and Big Data, 2019.

[6] M. Castro, D. Schenato, and R. Silva, "Blockchain and Cloud Computing Integration: A Survey," Journal of Cloud Computing: Advances, Systems and Applications, vol. 8, no. 1, pp. 1-21, 2020.

[7] P. Chen, H. Wang, and J. Liu, "Scalable Blockchain Technology for Cloud Storage Security," Cloud Computing and Security, vol. 6, no. 2, pp. 66-78, 2018.

[8] H. J. Chang and D. H. Kim, "Blockchain scalability: Challenges and solutions," International Journal of Blockchain Technology and Applications, vol. 2, no. 4, pp. 311-324, 2019.

[9] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. L. Llorente, "A break in the clouds: Towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, 2009.

[10] K. H. Kim and Y. C. Lee, "Privacy protection in cloud computing," Cloud Computing: Principles and Paradigms, Wiley, 2011.

[11] Z. Zhao, G. Zhong, and F. Liu, "A survey of cloud computing security issues and solutions," International Journal of Computer Science and Network Security, vol. 12, no. 5, pp. 29-37, 2012.

[12] C. P. Wei and W. K. Lee, "Cloud computing security and privacy issues," International Journal of Computer Science and Information Security, vol. 7, no. 4, pp. 263-267, 2010.

[13] M. R. L. Sanchez, J. Alcaraz, and J. Lopez, "Blockchain and cloud computing: A security perspective," International Journal of Computer Applications, vol. 180, no. 12, pp. 10-17, 2019.

[14] Y. Lee, "Blockchain technology in cloud computing: Review and future prospects," IEEE Access, vol. 7, pp. 123-134, 2019.

[15] R. Gaurav and A. Agarwal, "Blockchain and cloud for secure healthcare management system," Journal of Cloud Computing, vol. 9, no. 1, pp. 1-12, 2020.

[16] S. Gupta and K. Soni, "Challenges in blockchain integration with cloud computing," International Journal of Computer Science, vol. 10, no. 5, pp. 432-439, 2021.

[17] D. Gupta and V. Kumar, "Blockchain based secure data storage for cloud systems," Journal of Cloud Computing: Advances, Systems and Applications, vol. 9, no. 3, pp. 55-63, 2020.

[18] T. Zhang and L. Wang, "Leveraging blockchain for securing cloud data storage and access," International Journal of Cloud Computing and Services Science, vol. 8, no. 4, pp. 78-86, 2019.

[19] A. Rao, A. Jadhav, and P. Sharma, "Privacy-preserving cloud computing with blockchain and homomorphic encryption," IEEE Transactions on Cloud Computing, vol. 11, no. 5, pp. 1472-1481, 2020.

[20] K. Y. Zhi, "Smart contract-based privacy protection in cloud systems," Cloud Computing and Security, vol. 12, pp. 115-125, 2019.
[21] M. Patel, S. Garg, and P. Chauhan, "Hybrid blockchain-cloud architecture for enhanced data security," International Journal of Cloud Computing and Technology, vol. 7, no. 2, pp. 33-43, 2021.
[22] M. S. Ahmed, A. Nasir, and K. U. Rehman, "Decentralized cloud storage with blockchain integration," Journal of Blockchain Technology and Applications, vol. 5, no. 6, pp. 125-136, 2020.
[23] R. Banerjee, "Smart contract-based cloud resource management," Cloud Computing and Blockchain Journal, vol. 3, pp. 87-99, 2021.
[24] S. Agarwal and D. Verma, "Decentralized cloud storage using smart contracts," IEEE Access, vol. 8, pp. 35021-35034, 2020.
[25] S. Lee, "Blockchain consensus mechanisms: Impacts on cloud computing performance," Proceedings of the International Conference on Cloud Computing, 2019.
[26] M. T. Fisher and Y. Liu, "Blockchain with Proof of Stake for scalable cloud applications," Journal of Cloud Computing Technology, vol. 4, pp. 34-46, 2020.
[27] S. Al-Bassam and A. M. Al-Mohannadi, "Practical Byzantine fault tolerance for cloud networks," IEEE Transactions on Cloud Computing, vol. 6, no. 3, pp. 214-223, 2021.
[28] P. Chen, Z. Zhang, and C. Liu, "Hybrid Proof of Stake and cloud computing model," Cloud Computing and Data Science Review, vol. 5, no. 1, pp. 105-116, 2021.
[29] H. J. Lee and M. L. Park, "Blockchain-based decentralized cloud management," International Journal of Blockchain Computing, vol. 7, pp. 99-112, 2020.
[30] A. Roy, M. S. Kumar, and R. Gupta, "Decentralized cloud federation using blockchain," Cloud Computing Innovations Journal, vol. 10, pp. 201-214, 2021.