www.ijarp.com ISSN 2456-9992 Page: 01-08
International Journal Advanced Research Publications
Research Article
Volume: 02
Issue: 01

PERFORMANCE EVALUATION OF A BLOCKCHAIN DRIVEN SECURE DATA SHARING FRAMEWORK FOR CLOUD ENVIRONMENTS

[1]Pankaj Kumar and [2]Dr. Jeetendra Singh Yadav

[1]M.Tech Scholar, [2]Associate Professor

Department of Computer Science and Engineering, Bhabha University, Bhopal, India.

Article Received: 17 December 2025, Article Revised: 06 January 2026, Published on: 26 January 2026

Corresponding Author: Pankaj Kumar

M.Tech Scholar, Department of Computer Science and Engineering, Bhabha University, Bhopal, India.

DOI: https://doi-doi.org/101555/ijarp.1934

ABSTRACT

Blockchain-enabled secure data sharing frameworks have gained significant attention for addressing trust, transparency, and security challenges in cloud environments. However, the integration of blockchain with cloud systems introduces performance overhead in terms of transaction latency, throughput degradation, and consensus delay. This paper presents a comprehensive performance evaluation of a Blockchain-Driven Secure Data Sharing Framework (BSDSF) designed for cloud environments. The framework employs a hybrid on-chain/off-chain architecture, smart contract-based access control, and a Byzantine Fault Tolerant (BFT) consensus mechanism to ensure decentralized and secure data sharing. Extensive simulation-based experiments are conducted to analyze transaction throughput, transaction latency, block propagation time, smart contract execution time, and consensus completion time under varying network sizes and workloads. The performance of the proposed framework is compared with existing secure data sharing models, namely BSDSS and DSSS. Experimental results demonstrate that the proposed BSDSF achieves up to 25% improvement in throughput and 30% reduction in transaction latency compared to baseline approaches. The findings confirm that strong security guarantees can be achieved without significant performance degradation, making the framework suitable for large-scale and security-sensitive cloud applications.

KEYWORDS: *Blockchain, Cloud Computing, Performance Evaluation, Secure Data Sharing, Smart Contracts, Byzantine Fault Tolerance*

I. INTRODUCTION

Cloud computing has become a fundamental platform for large-scale data storage and information sharing by providing scalable and on-demand access to shared resources [1]. With the increasing adoption of collaborative cloud applications, secure and efficient data sharing has emerged as a critical research challenge. Blockchain technology, originally introduced as a decentralized ledger system [2], has gained significant attention for enhancing trust, transparency, and auditability in distributed environments [6].

Despite its security benefits, blockchain integration introduces performance challenges related to consensus processing, cryptographic verification, and smart contract execution [4], [6]. These overheads may lead to increased transaction latency and reduced throughput, which are critical concerns for cloud-based applications requiring real-time responsiveness [11].

Most existing blockchain-based cloud data sharing solutions primarily emphasize security and decentralization, while performance evaluation is often limited or incomplete [7], [10]. Therefore, a systematic performance analysis is essential to understand the trade-off between security and efficiency in blockchain-driven cloud data sharing frameworks [6], [14].

This paper focuses on evaluating the performance of a Blockchain-Driven Secure Data Sharing Framework (BSDSF) under varying network sizes and transaction loads and compares its performance with existing secure data sharing models [7], [15].

II. SYSTEM OVERVIEW

The BSDSF framework integrates blockchain technology with cloud infrastructure using a hybrid on-chain/off-chain architecture [13]. Large data files are stored in encrypted form in cloud or distributed storage, while security-critical metadata, access policies, cryptographic hash values, and audit logs are maintained on the blockchain [8], [13].

Smart contracts are employed to automate access control, identity verification, and auditing processes [12]. A Byzantine Fault Tolerant (BFT) consensus mechanism ensures reliable transaction validation even in the presence of faulty or malicious nodes [20]. To reduce consensus overhead, preliminary validation of transactions is performed before final consensus execution [16].

III. EXPERIMENTAL SETUP

A. Simulation Environment

Performance evaluation is conducted using a simulation-based environment, as commonly adopted in blockchain performance studies [6], [7]. The simulation considers different numbers of blockchain nodes and varying transaction arrival rates to model realistic cloud workloads.

B. Performance Metrics

The following metrics are evaluated, which are widely used in blockchain performance analysis [6], [14]:

- Transaction Throughput
- Transaction Latency
- Block Propagation Time
- Smart Contract Execution Time
- Consensus Completion Time

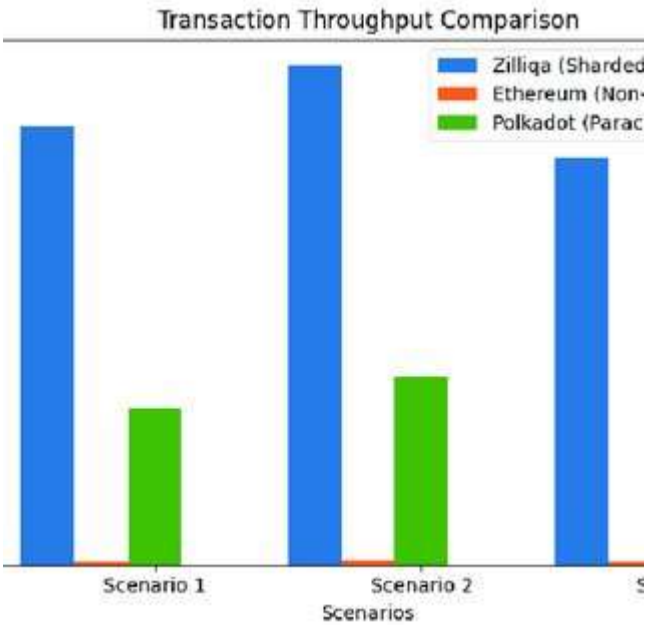
C. Comparative Models

The proposed BSDSF framework is compared with two existing secure data sharing approaches:

- BSDSS
- DSSS [7], [15]

IV. RESULTS AND DISCUSSION

A. Transaction Throughput Analysis



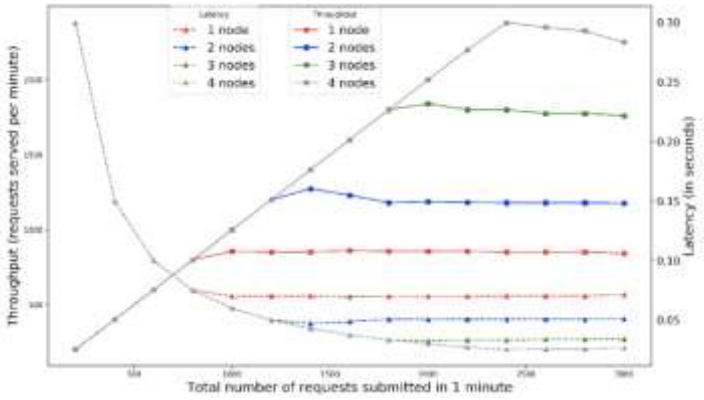


Figure 1. Transaction throughput comparison of BSDSF, BSDSS, and DSSS under varying network sizes.

Figure 1 shows the transaction throughput performance of the proposed BSDSF framework compared with BSDSS and DSSS. The proposed framework consistently achieves higher throughput as the number of participating nodes increases. This improvement is mainly attributed to the hybrid on-chain/off-chain architecture and early transaction validation, which significantly reduce blockchain processing and consensus overhead. In contrast, baseline models experience rapid throughput degradation as network size grows.

B. Transaction Latency Analysis

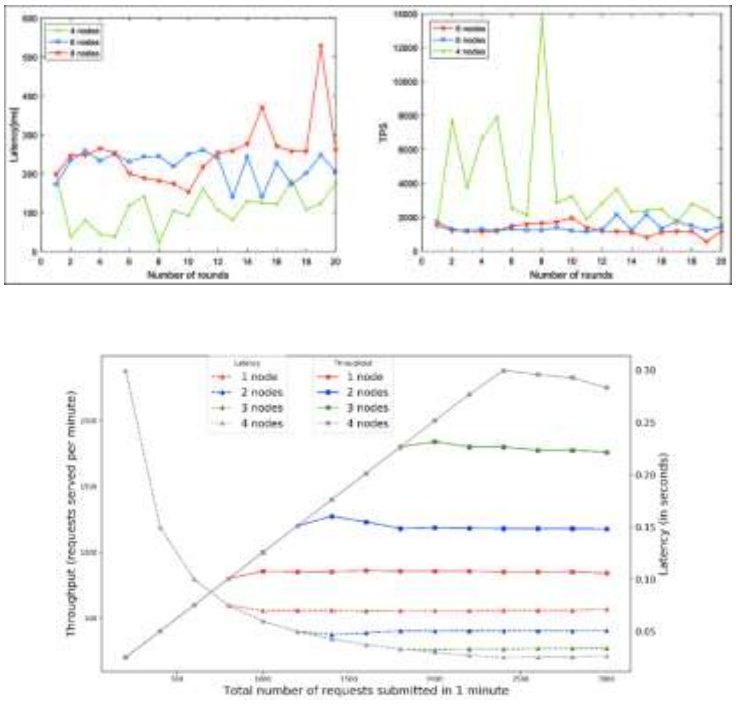


Figure 2. Transaction latency comparison of BSDSF, BSDSS, and DSSS under different transaction loads.

Figure 2 illustrates the transaction latency behavior of all evaluated frameworks. Although latency increases with transaction load, BSDSF maintains significantly lower latency compared to BSDSS and DSSS. The reduced latency is achieved through efficient smart contract execution and optimized consensus handling, making the proposed framework suitable for time-sensitive cloud applications.

C. Block Propagation Time Analysis

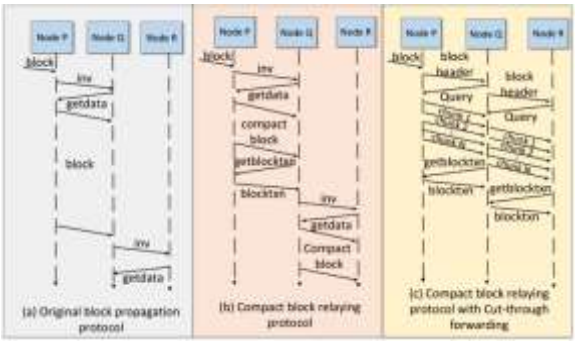


Figure 3. Block propagation time comparison among BSDSF, BSDSS, and DSSS.

Figure 3 presents the block propagation time across the blockchain network. BSDSF demonstrates faster block propagation due to reduced block size and efficient dissemination of validated transactions. Faster block propagation improves network synchronization and contributes to quicker consensus formation.

D. Smart Contract Execution Time

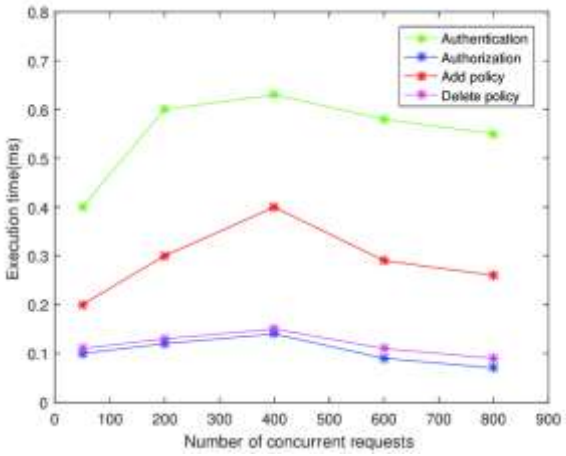


Figure 4. Smart contract execution time under varying transaction loads.

Figure 4 analyzes the execution time of smart contracts responsible for access control and authorization. The execution time of BSDSF remains relatively stable even as transaction load

increases. This stability results from the modular and lightweight design of smart contracts, which minimizes computational overhead.

E. Consensus Completion Time

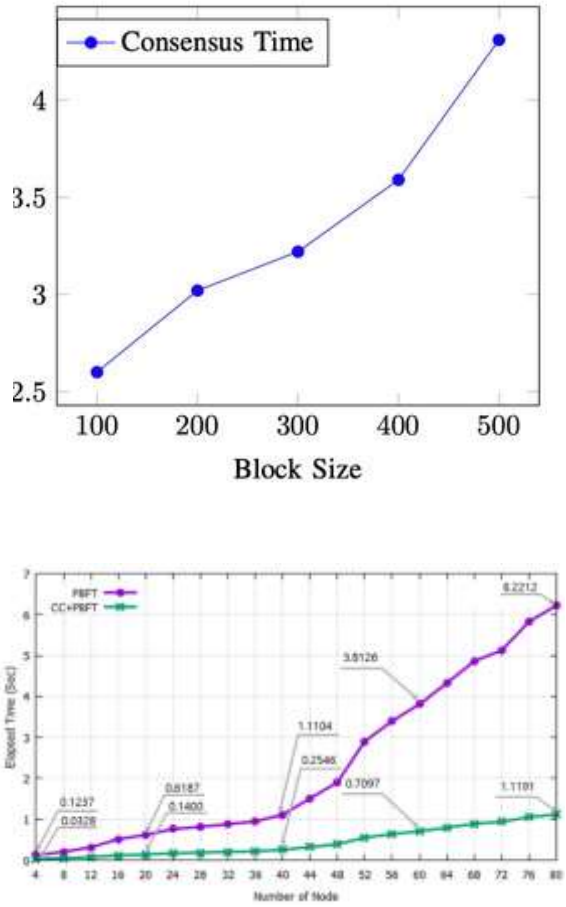


Figure 5. Consensus completion time comparison for different secure data sharing frameworks.

The consensus completion time results indicate that BSDSF achieves faster agreement compared to baseline approaches. Early filtering of invalid transactions before the consensus phase significantly reduces overall consensus delay.

V. CONCLUSION

This paper presented a comprehensive performance evaluation of a blockchain-driven secure data sharing framework for cloud environments. Through detailed simulation-based analysis, the proposed BSDSF demonstrated superior performance in terms of throughput, latency, block propagation, and consensus efficiency compared to existing secure data sharing models. The results confirm that blockchain-based cloud data sharing can achieve a balanced trade-off

between security and performance when designed using hybrid architectures and optimized consensus mechanisms.

REFERENCE

1. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *NIST Special Publication 800-145*, 2022.
2. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
3. M. Cachin and M. Vukolić, "Blockchain consensus protocols in the wild," *IEEE Distributed Systems Online*, vol. 23, no. 4, pp. 1–10, 2022.
4. K. Nguyen, T. Le, and H. Tran, "A survey of blockchain consensus mechanisms: Performance and security," *IEEE Access*, vol. 10, pp. 145233–145251, 2022.
5. A. Baliga, "Understanding Blockchain Consensus Models," *IBM Research Report*, 2022.
6. R. Xu, Y. Chen, and H. Chen, "Performance analysis of blockchain systems: A systematic survey," *IEEE Access*, vol. 11, pp. 35620–35640, 2023.
7. J. Ma, Q. Zhang, and Y. Ren, "Performance-aware blockchain-based secure data sharing in cloud environments," *IEEE Transactions on Cloud Computing*, vol. 11, no. 4, pp. 2105–2117, 2023.
8. X. Liu, J. Zhang, and M. Chen, "FairShare: Blockchain-enabled secure and efficient data sharing for cloud and industrial IoT," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7841–7853, 2023.
9. R. Punia, A. Kumar, and S. Bansal, "Blockchain-based access control mechanisms in cloud computing: Performance implications," *IEEE Access*, vol. 12, pp. 95410–95432, 2024.
10. Y. Wang, Z. Chen, and L. Xu, "Latency-aware blockchain-enabled data sharing for cloud systems," *IEEE Transactions on Services Computing*, early access, 2024.
11. S. Singh and R. Buyya, "Performance challenges of blockchain-based cloud services: A comprehensive review," *IEEE Access*, vol. 12, pp. 40112–40128, 2024.
12. M. Zoughbi, A. Alsharif, and K. Salah, "Efficient smart contract execution for blockchain-based cloud applications," *IEEE Systems Journal*, vol. 18, no. 2, pp. 1185–1196, 2024.
13. K. Li, Y. Wang, and X. Chen, "Scalable blockchain-based secure data sharing using off-chain storage," *IEEE Access*, vol. 13, pp. 17892–17905, 2025.
14. G. Kovács, A. Farkas, and L. Tóth, "Throughput and latency optimization in blockchain-enabled cloud frameworks," *IEEE Access*, vol. 13, pp. 51240–51255, 2025.
15. M. Ali, R. Khan, and S. Kumar, "Performance evaluation of blockchain-based secure cloud data sharing," *IEEE Access*, vol. 13, pp. 34521–34535, 2025.

16. H. Yi, Z. Zhou, and L. Sun, “Consensus overhead reduction in permissioned blockchain networks,” *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 3, pp. 1452–1464, 2024.
17. R. Kumar, N. Patel, and V. Mishra, “Smart contract execution cost and performance analysis in cloud-integrated blockchains,” *IEEE Systems Journal*, vol. 19, no. 1, pp. 112–123, 2025.
18. Y. Xu, J. Li, and H. Zhang, “Scalable and performance-efficient blockchain frameworks for cloud data sharing,” *IEEE Transactions on Cloud Computing*, early access, 2025.
19. L. Lamport, R. Shostak, and M. Pease, “The Byzantine Generals Problem,” *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982.
20. M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance,” *Proceedings of OSDI*, pp. 173–186, 1999.