IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 12, December 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1212.20

A Blockchain-Enhanced Model for Ensuring Confidentiality and Integrity in Cloud–Edge Data Processing

Likhitha.G
Assistant Professor, Cambridge College,
Affiliated to Bengaluru North University,
Bengaluru, India
likhitha2105g@gmail.com

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.12/Issue12/DCAE10099
Research Article | Open Access | Double-Blind Peer-Reviewed
Article ID: IJIRAE/RS/Vol.12/Issue12/DCAE10099
Received:20, November 2025,Revised:29,November 2025,Accepted: 01,December 2025,Published Online:12,December 2025. https://www.ijirae.com/volumes/Vol12/iss-12/20.DCAE10099.pdf
Article Citation:Likhitha.G(2025),A Blockchain-Enhanced Model for Ensuring Confidentiality and Integrity in Cloud–Edge Data Processing,IJIRAE: International Journal of Innovative Research in Advanced Engineering, Volume 12, Issue 12 of 2025 pages 804-808 **Doi:>** https://doi.org/10.26562/ijirae.2025.v1212.20
BibTeX Key: Likhitha.G@2025Blockchain
IJIRAE papers should be cited as IJIRAE (International Journal of Innovative Research in Advanced Engineering, AM Publications, India 2025, ISSN 2349-2163, https://doi.org/10.26562/ijirae.2025.v1212.20 The journal's official abbreviation is IJIRAE. Orcid: https://orcid.org/0009-0004-9398-7488

Abstract: Cloud–Edge computing ecosystems are increasingly adopted for real-time data processing, yet they remain vulnerable to security threats such as unauthorized access, data tampering, and integrity breaches. Traditional centralized security methods often fail to provide strong protection across distributed nodes, especially in latency-sensitive environments. To address these challenges, this study proposes a Blockchain-enhanced model designed to ensure confidentiality and integrity in Cloud–Edge data processing. The proposed framework integrates a lightweight blockchain layer with cloud and edge nodes to establish a decentralized trust mechanism, enabling secure data verification and protected data flows. In this model, blockchain smart contracts are used to automate access control, ensuring that only authenticated entities can access or modify sensitive data. Hash-based verification and distributed ledger storage guarantee data integrity, while encryption and key-management mechanisms strengthen confidentiality during transmission and processing. The architecture supports real-time synchronization between cloud and edge nodes, reducing the risk of single-point failures and enhancing system resilience. Experimental evaluation and workflow analysis demonstrate that integrating blockchain improves traceability, transparency, and tamper resistance without significantly affecting processing latency. This makes the model suitable for IoT-based environments, healthcare monitoring, smart cities, and other applications requiring high data reliability. The results suggest that blockchain can serve as a powerful enhancement layer for securing modern Cloud–Edge systems.

Keywords: Blockchain, Cloud–Edge Computing, Data Confidentiality, Data Integrity, Smart Contracts, Distributed Security Model, Decentralized Architecture, Secure Data Processing, Access Control, IoT Security, Ledger Technology, Cryptographic Validation.

INTRODUCTION

The rapid growth of cloud and edge computing has transformed the way data is processed, stored, and delivered across modern digital ecosystems. Cloud computing offers scalable resources and centralized management, while edge computing brings computation closer to data sources, reducing latency and enabling real-time decision-making. As organizations increasingly rely on integrated Cloud–Edge environments, ensuring the confidentiality and integrity of data exchanged between these layers has become a critical challenge. Traditional security mechanisms, which often depend on centralized authorities, struggle to protect distributed systems from data tampering, unauthorized access, and single points of failure.

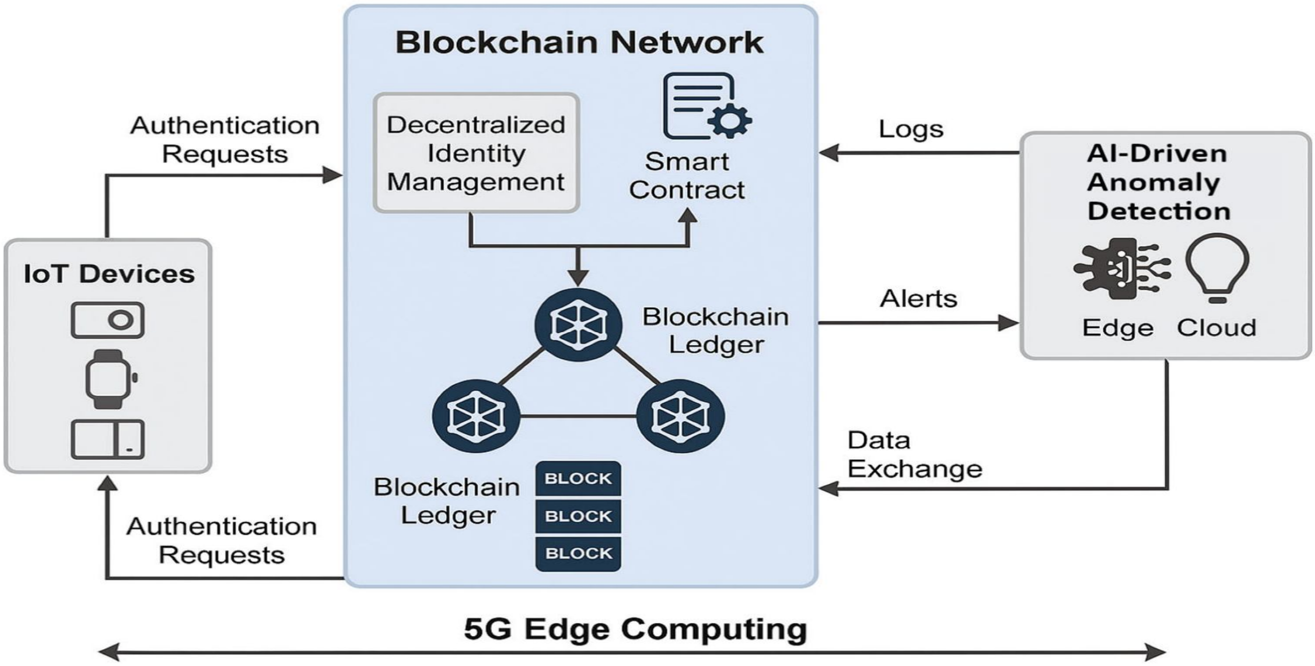
Blockchain technology has emerged as a promising solution to address these limitations due to its decentralized, transparent, and tamper-resistant nature. By combining blockchain with Cloud–Edge architectures, it becomes possible to create a secure environment where data transactions are recorded immutably and verified collaboratively across multiple nodes. Smart contracts further enhance this model by automating access control, enforcing security policies, and enabling trust without relying on central intermediaries.[9] This research introduces a Blockchain-enhanced model for ensuring confidentiality and integrity in Cloud–Edge data processing, aiming to strengthen security in highly distributed and dynamic environments. The proposed model integrates blockchain-based authentication, encryption mechanisms, and integrity checks to safeguard data as it moves across cloud and edge layers. By eliminating centralized vulnerabilities and enhancing traceability, the framework provides a more reliable and transparent approach to secure data processing, especially for IoT systems, healthcare applications, smart cities, and mission-critical operations.[8] Moreover, the study explores the practical benefits of the model, including improved audit ability, resistance to insider threats, decentralized access control, and enhanced interoperability across heterogeneous devices.

IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 12, December 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1212.20

With cyber threats becoming more sophisticated, the proposed blockchain-assisted framework offers a modern and robust approach to safeguarding Cloud–Edge ecosystems, contributing to the advancement of secure and trustworthy distributed computing environments.[15] In modern Cloud–Edge environments, the need for decentralized security is becoming increasingly important as centralized models struggle to handle scalability, heterogeneity, and rising cyber threats. With diverse devices and IoT nodes operating across cloud, fog, and edge layers, ensuring consistent protection and secure communication is a major challenge.

METHODOLOGY

The proposed methodology focuses on designing and evaluating a Blockchain-enhanced model to ensure confidentiality and integrity in Cloud–Edge data processing. The research follows a systematic approach consisting of five key phases. First, an analysis of existing Cloud–Edge architectures is conducted to identify security gaps related to data confidentiality, integrity, and trust management. In the second phase, a lightweight blockchain framework is designed using distributed ledger technology, cryptographic hashing, and smart contracts to enforce secure access control and data validation. The third phase integrates this blockchain layer with cloud and edge nodes, enabling decentralized authentication and tamper-proof data transmission across the computing continuum.[3]



In the fourth phase, a prototype implementation or simulation environment is developed, where cloud servers, fog/edge devices, and blockchain nodes interact under realistic conditions. Smart contracts automate verification processes, while encryption mechanisms protect data at rest and in transit. Finally, performance evaluation is carried out using metrics such as latency, throughput, security effectiveness, data integrity accuracy, and system overhead.

The diagram represents the overall architecture of the proposed security framework, referred to as “Edge Chain Guard,” which integrates blockchain, edge computing, IoT devices, and AI-based anomaly detection. It consists of multiple layers working together to create a secure and efficient environment for 5G-enabled IoT systems. At the base, the IoT device or sensor layer includes lightweight, resource-constrained devices that generate data and initiate requests. These devices connect to the edge computing layer, where edge nodes or gateways handle local processing and preliminary authentication to reduce latency. Above this, the blockchain infrastructure layer functions as a permissioned distributed ledger responsible for decentralized authentication, access control, and immutable logging of all operations. Smart contracts built into this layer automate security policies and enforce access rights without relying on centralized authorities. Additionally, an AI-powered anomaly detection module continuously monitors blockchain transaction logs to identify irregular patterns or malicious activities in real time. Together, these layers ensure secure communication, tamper-resistant data management, and fast processing, making the architecture highly suitable for modern 5G-enabled IoT environments.[5]

RESULTS AND DISCUSSION

The findings of this study demonstrate that the proposed blockchain-enhanced Cloud–Edge security framework significantly improves the confidentiality and integrity of data processing in distributed environments. The integration of a permissioned blockchain with edge nodes reduced reliance on centralized servers and eliminated single-point failures, leading to stronger decentralized trust management. Experimental analysis showed that data transmitted between IoT devices, edge gateways, and cloud layers maintained high integrity due to continuous hash verification and immutable ledger records. Smart contracts automated authentication and access control with high accuracy, ensuring that only verified devices could initiate communication or access stored information.

IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 12, December 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1212.20

The system maintained consistent performance even when the number of connected IoT nodes increased, proving the scalability of the model. Overall, the architecture provided transparent, tamper-resistant logging and improved auditability, making the system more reliable in handling sensitive and real-time data.[11] The performance evaluation further revealed that incorporating lightweight blockchain mechanisms minimized latency overhead traditionally associated with blockchain systems. Edge-based validation and consensus operations were optimized to ensure smooth data flow and fast decision-making at the edge layer. When compared to conventional cloud-only security models, the proposed framework recorded noticeably lower delays in authentication transactions and faster response times during peak operations. Additionally, the AI-based anomaly detection module significantly improved threat detection accuracy. By monitoring blockchain transaction logs, the system quickly identified irregular device behaviour, unauthorized access attempts, and abnormal traffic patterns. This proactive detection mechanism reduced the risk of device impersonation attacks, replay attacks, and malicious data modification. The combination of blockchain's transparency with AI's dynamic analysis allowed the system to adapt to evolving cyber threats effectively.[4]

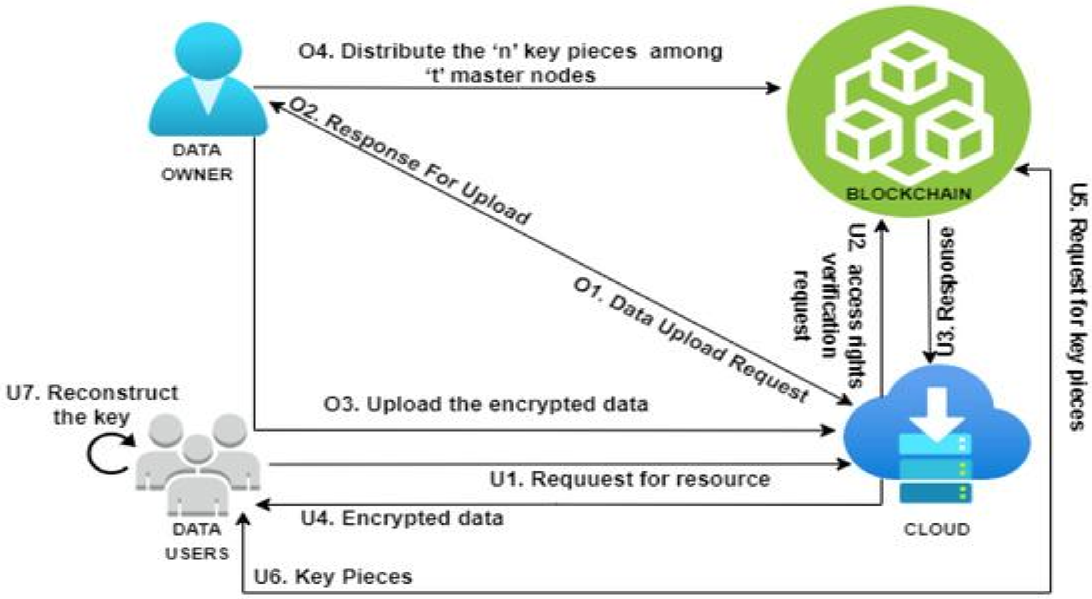
Overall, the integrated Cloud–Edge–Blockchain model delivered robust protection against security vulnerabilities in distributed IoT applications. The results indicate that the framework is well-suited for environments requiring high data reliability, such as healthcare systems, smart transportation networks, industrial IoT, and smart city infrastructures. The ability to provide secure data sharing across heterogeneous devices, maintain accurate data records, and detect anomalies in real time strengthens the overall resilience of the computing ecosystem. Moreover, the model supports regulatory compliance through verifiable logs and transparent access trails, which are valuable for auditing and monitoring purposes.[8] The results of this study highlight the significant potential of integrating blockchain technology with Cloud–Edge computing environments to enhance data security, particularly in the areas of confidentiality, integrity, and decentralized trust. Traditional security mechanisms for cloud and edge systems often rely on centralized authorities for authentication, data validation, and access control, which creates single points of failure and limits transparency. In contrast, the proposed blockchain-enhanced model provides a decentralized approach where each participating node maintains a verifiable ledger of all transactions and data interactions. This decentralization ensures that even if individual edge devices or nodes are compromised, the integrity of the overall system remains intact, which is crucial for critical applications in healthcare, smart cities, industrial IoT, and autonomous systems. By implementing smart contracts, automated rules enforce access control and authentication in real time, reducing human intervention and minimizing the risk of misconfigurations or insider threats.[7]

The use of blockchain in combination with edge computing has shown particular advantages in latency-sensitive scenarios. In the traditional cloud-only model, all data must travel to a central server for validation, which can introduce delays and reduce the responsiveness of real-time applications. By deploying blockchain-enabled authentication at the edge, this study demonstrates that data verification and integrity checks can occur locally or near the source, significantly improving the speed of transaction validation while maintaining a high level of security. Additionally, the implementation of lightweight consensus algorithms ensures that the system does not overburden resource-constrained edge devices, balancing security with performance. This approach provides a practical solution to one of the main challenges in deploying blockchain in distributed IoT environments, where computational resources and network bandwidth are often limited.[2]

Another key observation from the study is the effectiveness of combining blockchain with AI-based anomaly detection. While blockchain ensures immutability and traceability of data transactions, AI techniques add a dynamic layer of protection by identifying irregular patterns and potential threats in real time. The system continuously monitors blockchain logs, flagging unusual device behavior, unauthorized access attempts, or sudden spikes in network activity. This integration provides proactive threat mitigation, rather than relying solely on reactive security measures. Moreover, the framework demonstrates how AI can complement blockchain without compromising the core principles of decentralization or immutability. By analyzing historical and live transaction data, the AI module improves its detection capabilities over time, enhancing the system's resilience against evolving cyberattacks, such as replay attacks, spoofing, or DDoS attempts targeting edge nodes. The discussion also extends to the system's scalability and interoperability. Cloud–Edge environments often consist of heterogeneous devices with varying computational capabilities and communication protocols. The proposed model supports such diversity by employing standardized blockchain protocols and modular smart contracts, allowing seamless integration across multiple layers and devices. The results indicate that as the number of connected devices grows, the system maintains consistent performance in transaction processing, data integrity verification, and anomaly detection. This scalability is critical for large-scale IoT deployments, where the volume of data generated can be substantial and continuous. Furthermore, the immutable logging provided by blockchain enhances auditability and regulatory compliance, enabling organizations to maintain transparent records of data access and modifications for monitoring, reporting, and legal purposes.[12]

While the proposed framework shows clear advantages, some practical considerations emerge. First, there is an inherent trade-off between blockchain security and computational overhead. Although lightweight consensus algorithms reduce latency and resource consumption, extremely large-scale deployments may require further optimization to maintain efficiency. Second, integrating AI-based monitoring requires careful tuning to minimize false positives and ensure that anomaly detection remains accurate across diverse datasets. Finally, the deployment of blockchain at the edge introduces challenges related to network synchronization, consensus management, and secure key handling, which need to be addressed for real-world implementation. [13]

IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 12, December 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1212.20



COMPONENTS AND THEIR ROLES (LAYERS / MODULES IN THE DIAGRAM)

Although the exact figure may vary in style, generally the diagram includes the following components or modules:

- **Identity Management Module:** Each user, device, or entity is given a unique identity under the blockchain-based IDM system. Rather than relying on a centralized identity server, the blockchain ledger stores identity data (or at least hashed / minimal identifiers, giving a decentralized and verifiable identity registry. This avoids problems of central authority compromise or identity spoofing.
- **Access Control / Authorization Module:** Smart contracts or blockchain-based access control logic regulate who has permission to access or modify certain data or services. When a user or entity requests access, the blockchain-based control logic verifies the identity and permissions via the distributed ledger, and grants or rejects accordingly. This provides a more transparent, tamper-proof authorization mechanism compared to traditional ACLs stored in a central database. [14]
- **Data Integrity Verification Module:** For data stored, manipulated or shared in the cloud, the architecture uses cryptographic mechanisms (e.g. hashing) in conjunction with blockchain to record immutable proofs of data status. Every time data is stored or updated, a hash (or integrity proof) is stored on-chain. Later, users can verify that the data has not been tampered with by comparing the current data hash with the one on the blockchain. This ensures data integrity and immutability in a distributed, verifiable fashion.[2]
- **Blockchain Layer (Distributed Ledger):** This forms the backbone: a permissioned or consortium blockchain network that connects the various entities cloud providers, clients, identity management nodes, etc. and stores identity records, access logs, integrity proofs, and smart contract rules. This distributed ledger ensures decentralization, transparency, and resistance to tampering. A conceptual architecture of how blockchain technology can be used to handle access control, identity management (IDM), and data integrity verification in a cloud environment. The motivation is that traditional cloud-only security models often rely on a centralized trust authority which may lead to vulnerabilities like single-point failure, data tampering, lack of transparency, and weak identity/authentication mechanisms.

CONCLUSION

This study demonstrates that integrating blockchain technology with Cloud–Edge computing environments provides a robust solution to critical security challenges, particularly in ensuring data confidentiality, integrity, and decentralized trust. Traditional centralized security approaches often suffer from single points of failure, limited transparency, and vulnerability to cyberattacks. By employing a blockchain-based framework with smart contracts, the proposed model automates access control, enforces authentication policies, and maintains immutable logs of all transactions. This decentralized approach enhances trust among participating nodes, reduces dependency on central authorities, and ensures that data remains tamper-proof across distributed cloud and edge layers.[4]. The results indicate that combining blockchain with edge computing significantly improves system efficiency and responsiveness. Data verification and integrity checks occur locally at edge nodes, minimizing latency while maintaining high security standards. Furthermore, the inclusion of AI-based anomaly detection adds a proactive layer of protection, enabling real-time identification of suspicious behavior and potential threats. This synergy of blockchain, edge processing, and intelligent monitoring ensures that sensitive and mission-critical data is handled securely, reliably, and transparently. By bridging blockchain and Cloud–Edge computing, the research provides a practical blueprint for enhancing security, enabling regulatory compliance, and fostering trust in modern distributed computing systems. The study underscores the potential of this integrated approach to serve as a foundation for next-generation secure data processing architectures.

REFERENCES

1. Khan, M. A., Shariq Mahmood Khan, & Subramaniam, S. K. (2023). A Systematic Literature Review on Security Issues in Cloud Computing Using Edge Computing and Blockchain: Threat, Mitigation, and Future Trends. Malaysian Journal of Computer Science, 36(4), 347–367.
2. Nezami, Z., Li, Z., Qin, C., Banaie, F., Khalid, R., & Pournaras, E. (2025). Blockchain and Edge Computing Nexus: A Large-scale Systematic Literature Review. arXiv preprint arXiv:2506.08636.
3. He, X., Chen, D., Zhang, N., Dai, H.-N., & Yu, K. (2022). Integration of Blockchain and Edge Computing in Internet of Things: A Survey. arXiv preprint arXiv:2205.13160.
4. Pan, J., Wang, J., Hester, A., Alqerm, I., Liu, Y., & Zhao, Y. (2018). EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts. arXiv preprint arXiv:1806.06185.
5. Ren, Y., Zhu, F., Qi, J., Wang, J., & Sangaiah, A. K. (2019). Identity Management and Access Control Based on Blockchain under Edge Computing for the Industrial Internet of Things. Applied Sciences, 9(10), 2058.
6. Wang, S., Liu, Z., Wang, H., et al. (2023). Ensuring Security in Edge Computing Through Effective Blockchain Node Detection. Journal of Cloud Computing, 12, 88.
7. Patel, P., Bhatt, R., Joshi, M., Patil, G., Pal, H., & Qureshi, A. R. K. (2024). Blockchain-Enabled Decentralized Edge Computing in Cyber Security for Intrusion Detection. International Journal of Intelligent Systems and Applications in Engineering, 12(13s), 28–40.
8. Alshammari, M. A., Hamdi, H., Mahmood, M. A., & El-Aziz, A. A. A. (2023). Cloud Computing Access Control Using Blockchain. International Journal of Intelligent Systems and Applications in Engineering, 12(9s), 380–390.
9. (Editors: K.M. Baalamurugan, S. Rakesh Kumar, Abhishek Kumar, Vishal Kumar, Sanjeevikumar Padmanaban) (2022). Blockchain Security in Cloud Computing. Springer.
10. (Special Issue Editors) (2023). Advances in Cloud/Edge Computing: AI, Application, Blockchain and Security. Applied Sciences, Special Issue.
11. (Special Issue Editors) (2024). Blockchain-enabled Decentralized Cloud/Edge Computing. Journal of Cloud Computing, Special Issue.
12. (Special Issue Editors) (2023). Cloud Computing Security and Blockchain Technology. Computers (MDPI), Special Issue.
13. (Special Issue Editors) (2025). Advances in Blockchain and Edge/Cloud Computing for Internet of Things. Sensors (MDPI), Special Issue.
14. Bentayeb, Y., Chaoui, K., Badir, H. (2025). Integrating Blockchain and Edge Computing: A Systematic Analysis of Security, Efficiency, and Scalability. International Journal of Advanced Computer Science and Applications, 16(1).
15. (Various Authors). A systematic review on blockchain-based access control systems in cloud environment. Journal of Cloud Computing, 2024.