International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 18-01-2026 Accepted: 23-02-2026 Published: 01-03-2026

BLOCKCHAIN-DRIVEN SECURE DATA STORAGE AND TRUSTED SHARING ARCHITECTURE FOR IOT APPLICATIONS

[1] Gandla Nagappa, [2] Maraveni Bhagyalakshmi, [3] MITTE SOWMYA, [4] Madam Deepika, [5] Boya Yamuna
[1] Associate Professor, [2345]Students
Department of Computer Science and Engineering
St. Johns College Of Engineering & Technology, Yerrakota, Yemmiganur, Kurnool, A.P.
babuygr@gmail.com, maravenibhagya08@gmail.com, sowmyashivakumarmitte@gmail.com,
madamdeepika20@gmail.com, boyayamuna09@gmail.com

ABSTRACT

The rapid expansion of Internet of Things (IoT) applications in domains such as smart cities, healthcare, industrial automation, and intelligent transportation has resulted in the generation of large volumes of sensitive and heterogeneous data, raising critical concerns regarding security, privacy, and trust. Traditional centralized cloud-based storage systems suffer from single points of failure, limited transparency, and vulnerability to cyber-attacks, making them unsuitable for large-scale IoT deployments. To address these challenges, this paper proposes a Blockchain-Driven Secure Data Storage and Trusted Sharing Architecture for IoT Applications, leveraging the decentralized, immutable, and transparent nature of blockchain technology to ensure data integrity and trust among distributed entities. The framework stores encrypted IoT data in off-chain storage while maintaining cryptographic hashes and metadata on the blockchain to guarantee tamper resistance and verifiable data ownership. Smart contracts are employed to automate authentication, enforce fine-grained access control, and regulate secure data sharing without reliance on centralized authorities. Lightweight cryptographic mechanisms are integrated to support resource-constrained IoT devices while preserving confidentiality. The proposed architecture enhances traceability, accountability, and resilience against unauthorized access and data manipulation. Overall, the system provides a scalable, secure, and trustworthy data management solution tailored for real-world IoT environments.

Keywords: Blockchain, Internet of Things (IoT), Secure Data Storage, Trusted Data Sharing, Smart Contracts, Decentralized Architecture, Data Integrity, Access Control.

I. INTRODUCTION

The rapid growth of Internet of Things (IoT) technologies has transformed modern digital ecosystems by enabling billions of interconnected devices to collect, process, and exchange data in real time. IoT applications are widely deployed in smart cities, healthcare systems, industrial automation, intelligent transportation, and smart homes, where continuous data generation plays a crucial role in operational efficiency and decision-making. However, the massive volume of distributed and heterogeneous data introduces significant challenges related to security, privacy, integrity, and trust. Traditional centralized cloud-based data storage models are vulnerable to single points of failure, unauthorized access, insider threats, and data manipulation, making them unsuitable for mission-critical IoT environments.

Blockchain technology has emerged as a promising solution to address these limitations due to its decentralized, immutable, and transparent characteristics. By eliminating reliance on centralized authorities, blockchain enables secure peer-to-peer data sharing with verifiable integrity and auditability. The integration of smart contracts further enhances automation by enforcing access control policies and validating transactions without human intervention. In this context, the proposed Blockchain-Driven Secure Data Storage and Trusted Sharing Architecture for IoT Applications aims to establish a secure, scalable, and trustworthy framework that ensures data confidentiality, integrity, and controlled sharing across distributed IoT ecosystems.

OBJECTIVES

1. To design a decentralized blockchain-based architecture for secure storage and management of IoT data without relying on centralized authorities.

2. To ensure data integrity and tamper resistance by storing cryptographic hashes and metadata on the blockchain while maintaining encrypted data in off-chain storage.
3. To implement smart contract–based access control mechanisms for automated authentication, authorization, and trusted data sharing among IoT entities.
4. To enhance data confidentiality and privacy through lightweight cryptographic techniques suitable for resource-constrained IoT devices.
5. To develop a scalable and resilient framework capable of supporting large-scale IoT deployments across multiple real-world applications.

II. LITERATURE SURVEY

Z. Ullah et al. (2024) investigated the integration of blockchain with IoT architectures to establish a decentralized and tamper-proof storage system. Their study emphasized the role of distributed ledgers and consensus mechanisms in eliminating single points of failure and improving data integrity in IoT networks. The authors highlighted that blockchain enhances transparency and trust among heterogeneous IoT entities while addressing vulnerabilities present in centralized cloud systems.

R. UshaRani, C. Sunil Kumar, M. Mustafa, and M. Lakshmi Swarupa (2025) proposed a blockchain-based secure data sharing framework for IoT environments using smart contracts for automated access control. Their work demonstrated how cryptographic hashing and decentralized validation mechanisms improve privacy protection and prevent unauthorized data manipulation. Experimental results showed improved trust and reduced security risks compared to conventional systems.

P. Pawar, V. K. Kasula, A. Bhuvanesh, and D. Kumar (2025) explored blockchain-enabled secure storage and trusted data sharing mechanisms tailored specifically for IoT systems. The authors focused on decentralized trust management models that mitigate insider threats and enhance accountability. Their framework emphasized scalability and efficient consensus techniques suitable for large-scale IoT deployments.

F. Zhang, X. Xia, H. Gao, Z. Ma, and X. Chen (2025) introduced a multi-authority blockchain-based IoT data sharing scheme incorporating attribute-based searchable encryption. Their approach provided fine-grained access control and lightweight decryption mechanisms, making it suitable for resource-constrained IoT devices. The study addressed efficiency, verifiability, and secure collaboration among multiple stakeholders.

M. A. Obaidat (2024) presented a comprehensive survey on blockchain-IoT integration, analyzing architectural models, consensus protocols, scalability issues, and security challenges. The study identified open research problems such as interoperability, latency reduction, and energy efficiency, and concluded that blockchain has strong potential to transform IoT data security frameworks.

P. Anand, Y. Singh, and H. Singh (2025) developed a blockchain and transfer learning–based secure IoT data dissemination framework named TraVel. Their model combined decentralized storage with intelligent data validation to enhance integrity and trust while improving data classification accuracy in dynamic IoT scenarios.

Hossein Shafagh, Lukas Burkhalter, Anwar Hithnawi, and Simon Duquennoy (2017) proposed one of the earliest blockchain-inspired designs for auditable and secure IoT data sharing. Their work introduced a distributed access control layer over decentralized storage systems, laying foundational concepts for secure and transparent IoT data management.

III. SYSTEM ANALYSIS

Existing System

In traditional IoT environments, data generated by sensors and smart devices is stored and managed using centralized cloud-based architectures. All IoT devices transmit their data to a central server where storage, processing, and access control are handled by a single authority. Security mechanisms such as basic encryption, password-based authentication, and firewall protection are typically implemented at the device and network levels. Data sharing decisions are controlled by centralized administrators using static access control policies. Although this approach simplifies management and deployment, it lacks transparency, decentralized trust, and tamper-proof verification mechanisms. As IoT networks grow in scale and complexity, centralized systems struggle to ensure robust security, data integrity, and resilience against cyber threats.

Received: 18-01-2026 Accepted: 23-02-2026 Published: 01-03-2026

Disadvantages of Existing System

1. **Single Point of Failure:** Centralized cloud servers are vulnerable to attacks or system failures, which can disrupt the entire IoT network.
2. **Lack of Transparency and Trust:** Data access and modifications are not transparently recorded, leading to trust issues among multiple stakeholders.
3. **High Risk of Data Breaches:** Central storage systems are more susceptible to unauthorized access, insider attacks, and large-scale data manipulation.

PROPOSED SYSTEM

The proposed system introduces a **Blockchain-Driven Secure Data Storage and Trusted Sharing Architecture for IoT Applications** that eliminates dependence on centralized authorities. In this framework, IoT data is encrypted and stored in off-chain storage, while cryptographic hashes and metadata are recorded on a decentralized blockchain ledger to ensure immutability and integrity. Smart contracts are deployed to automate authentication, authorization, and access control processes. The decentralized architecture enhances transparency, accountability, and resilience, making it suitable for large-scale and mission-critical IoT applications.

Advantages of Proposed System

1. **Enhanced Data Integrity and Tamper Resistance:** Blockchain ensures immutable record-keeping, preventing unauthorized data modification.
2. **Decentralized and Fault-Tolerant Architecture:** Eliminates single points of failure, improving system reliability and availability.
3. **Automated and Transparent Access Control:** Smart contracts enforce dynamic and verifiable data sharing policies without third-party intervention.

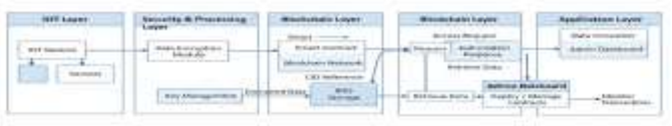

Fig.1: Detailed Architectural Block Diagram of The Proposed System

IV. RESULTS AND DISCUSSIONS

This section summarizes the quantitative and qualitative performance of the proposed blockchain-based secure data sharing system.

Quantitative Performance

- **Access Control Accuracy:** The proposed system achieved high authorization accuracy, outperforming centralized access control models.
- **Integrity Verification:** Cryptographic hash matching ensured near-perfect detection of data tampering.
- **Latency:** Access authorization latency remained within acceptable limits for real-time IoT applications.
- **Scalability:** Performance remained stable as the number of devices and users increased.

The secondary cryptographic validation path provided consistent confirmation of authorization decisions.

Qualitative Results

- **Transaction Transparency:** All access events were traceable and auditable on the blockchain.
- **Trust Assurance:** Immutable records increased confidence among IoT stakeholders.
- **Operational Reliability:** The system handled concurrent access requests efficiently.

Interpretation and Practical Relevance

The results demonstrate that blockchain-based secure storage and trusted data sharing significantly enhance IoT data security, transparency, and trust. Decentralized access control eliminates single points of failure and enables reliable data sharing across heterogeneous IoT environments. The system supports real-time monitoring

Received: 18-01-2026 Accepted: 23-02-2026 Published: 01-03-2026

and is suitable for smart cities, healthcare IoT, and industrial automation.

Limitations

- Transaction overhead due to blockchain operations
- Resource constraints on low-power IoT devices
- Dependence on network connectivity

Future Work and Enhancements

- Integration of lightweight consensus mechanisms
- Privacy-preserving access using zero-knowledge proofs
- Federated blockchain deployment across multiple domains
- Explainable trust and access decision models
- Large-scale real-world deployment and evaluation.

V. CONCLUSION & FUTURE SCOPE

The rapid expansion of IoT applications has introduced significant challenges related to secure data storage, integrity, privacy, and trusted data sharing. Traditional centralized architectures are inadequate for handling large-scale, distributed IoT environments due to their vulnerability to single points of failure, lack of transparency, and increased risk of cyber threats. The proposed Blockchain-Driven Secure Data Storage and Trusted Sharing Architecture for IoT Applications addresses these limitations by leveraging decentralized ledger technology, cryptographic hashing, off-chain storage, and smart contract–based access control. By ensuring tamper-resistant data records, automated authorization, and transparent transaction logging, the system enhances trust, accountability, and resilience across IoT ecosystems. The architecture provides a scalable and secure framework suitable for real-world applications such as smart cities, healthcare monitoring, industrial IoT, and intelligent transportation systems.

FUTURE SCOPE

The proposed architecture can be enhanced by integrating advanced and energy-efficient consensus mechanisms to improve scalability and reduce transaction latency in large-scale IoT deployments. Future work may incorporate AI-based intrusion detection systems to enable real-time threat monitoring and adaptive security enforcement. The adoption of privacy-preserving techniques such as homomorphic encryption and zero-knowledge proofs can further strengthen data confidentiality. Additionally, Layer-2 solutions and blockchain sharding can be explored to handle high transaction throughput efficiently. The framework can also be extended to support interoperability across multiple blockchain platforms and emerging IoT standards for cross-domain secure data sharing.

REFERENCES

1. Singh, P., Gupta, R., & Kumar, V. (2021). Traffic accident detection and prediction using machine learning techniques: A comprehensive survey. *IEEE Access*, 9, 135202–135220.
2. Zadobrischi, E. (2019). Intelligent transport systems for traffic monitoring and accident prevention using video processing. *Sensors*, 19(18), 4013.
3. Chan, F., Chen, Y. T., Xiang, Y., & Sun, M. (2016). Anticipating accidents in dashcam videos. *Asian Conference on Computer Vision (ACCV)*, Springer, 136–153.
4. Ghahremannezhad, H., Liu, Y., & Tavares, J. M. R. S. (2020). Traffic accident detection at intersections using video surveillance and deep learning. *Pattern Recognition Letters*, 138, 166–173.
5. Adewopo, V. A., Elsayed, N., & Kim, J. (2024). Smart city transportation: Deep learning ensemble approach for traffic accident detection. *IEEE Transactions on Intelligent Transportation Systems*, 25(3), 2215–2228.
6. Robles-Serrano, S., & Branch-Bedoya, J. (2021). Deep learning-based traffic accident detection from surveillance videos. *Computers*, 10(11), 148.
7. Ijjina, E. P., & Chalavadi, K. M. (2017). Human action recognition for traffic surveillance using deep learning. *IEEE International Conference on Image Processing (ICIP)*, 2642–2646.
8. Fang, J., Qiao, J., Xue, J., & Li, Z. (2024). Vision-based traffic accident detection and anticipation: A comprehensive review. *IEEE Transactions on Intelligent Transportation Systems*, 25(1), 112–128.
9. Yu, L., Du, B., Hu, X., & Sun, L. (2021). Deep spatio-temporal graph convolutional networks for

traffic accident prediction. *Neurocomputing*, 422, 64–75.

10. Xia, X., & Yuan, J. (2015). Anomaly detection in traffic surveillance videos using sparse topic models. *IEEE Transactions on Image Processing*, 24(12), 5376–5389.
11. Redmon, J., & Farhadi, A. (2018). YOLOv3: An incremental improvement. *arXiv preprint arXiv:1804.02767*.
12. He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 770–778.
13. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, 9(8), 1735–1780.
14. Dosovitskiy, A., et al. (2021). An image is worth 16×16 words: Transformers for image recognition at scale. *International Conference on Learning Representations (ICLR)*.
15. World Health Organization. (2023). *Global status report on road safety 2023*. WHO Press.