IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2026

DOI: 10.17148/IARJSET.2026.135110

AI-Driven Blockchain Framework for Trustworthy Data Sharing in IoT Ecosystems

Dr. T. Vamshi Mohana[1], Salma Begum[2]

Associate Professor, Department of Computer Science, RBVRR Women's College, Hyderabad, Telangana, India[1]

Assistant Professor, Department of Computer Science, RBVRR Women's College, Hyderabad, Telangana, India[2]

Abstract: The proliferation of Internet of Things (IoT) infrastructures has accelerated the generation of sensitive, high-volume data across diverse sectors, ranging from healthcare and agriculture to industrial automation and smart mobility. Despite these advancements, the heterogeneity of devices, constrained computational resources, and evolving cyber threats pose significant barriers to secure and reliable data exchange. This study introduces an AI-empowered blockchain framework designed to reinforce trust management and enable transparent communication within distributed IoT environments. The proposed architecture integrates machine learning–driven trust evaluation with a novel Proof-of-Trust (PoT) consensus protocol, ensuring that nodes with verified reliability are prioritized in block validation. By embedding adaptive intelligence into blockchain operations, the framework reduces computational overhead while preserving immutability and accountability. Furthermore, distributed computing at the edge and fog layers enhances scalability and minimizes latency, making the system viable for real-time IoT applications. Simulation outcomes reveal notable improvements, including reduced transaction delays, heightened accuracy in malicious node detection, and stable performance under dense network conditions. The synergy of artificial intelligence, blockchain, and distributed computing establishes a resilient foundation for secure IoT ecosystems, paving the way for trustworthy data sharing in next-generation smart infrastructures.

Keywords: Trust Management, Artificial Intelligence, Blockchain, Distributed Computing

I. INTRODUCTION

The Internet of Things (IoT) has emerged as a transformative paradigm, enabling billions of interconnected devices to collect, process, and exchange data across diverse application domains such as smart healthcare, precision agriculture, intelligent transportation, and industrial automation. While this proliferation promises unprecedented efficiency and innovation, it simultaneously exposes IoT ecosystems to vulnerabilities stemming from device heterogeneity, constrained resources, and evolving cyber threats. Ensuring **trustworthy data sharing** in such dynamic environments is therefore a critical prerequisite for sustainable adoption.

Traditional **trust management** approaches, often centralized, suffer from inherent limitations including susceptibility to single points of failure, bottlenecks in scalability, and reduced resilience against adversarial attacks. In contrast, **blockchain technology** offers decentralized trust through immutable ledgers and transparent consensus mechanisms. However, conventional protocols such as Proof-of-Work or Proof-of-Stake impose significant computational and energy burdens, rendering them unsuitable for lightweight IoT devices. To overcome these constraints, the integration of **artificial intelligence (AI)** into blockchain systems introduces adaptive intelligence capable of dynamically evaluating node reliability, detecting anomalies, and optimizing consensus participation.

This paper proposes a **hybrid AI-blockchain framework** that leverages distributed computing to balance scalability and efficiency. The framework introduces a novel **Proof-of-Trust (PoT)** consensus mechanism, wherein AI-driven trust scores determine validation priority, thereby reducing computational overhead while enhancing fairness and security. By embedding **distributed computing** at the edge and fog layers, the architecture ensures low-latency processing and seamless interoperability across heterogeneous IoT networks.

Through this convergence of **trust management, artificial intelligence, blockchain, and distributed computing**, the framework establishes a resilient foundation for secure and transparent data exchange. It addresses pressing challenges of scalability, security, and interoperability, paving the way for next-generation IoT infrastructures that are not only intelligent but also inherently trustworthy.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2026

DOI: 10.17148/IARJSET.2026.135110

II. LITERATURE REVIEW

1. Trust Management in IoT

IoT ecosystems rely heavily on trust management to ensure secure communication among heterogeneous devices. Traditional reputation-based models often fail under adversarial conditions due to static evaluation methods. Recent work emphasizes dynamic trust computation using AI techniques. For example, **D'Aniello and Fotia (2025)** provide a comprehensive survey of blockchain and AI-based trust management methods, highlighting the role of machine learning in adaptive trust scoring and anomaly detection.

Reputation-based and cryptographic models exist but fail under dynamic adversarial conditions.

2. Blockchain for IoT Security

Blockchain has been widely studied as a decentralized solution for IoT data integrity and provenance. **Kang et al. (2019)** demonstrated blockchain's potential in vehicular edge computing, ensuring secure data sharing among vehicles. However, consensus protocols like Proof-of-Work remain unsuitable for resource-constrained IoT devices. A literature review by IEEE (2022) consolidates blockchain-enabled IoT applications, identifying scalability and energy efficiency as persistent challenges.

Provides immutability and transparency, but Proof-of-Work is unsuitable for IoT due to energy demands.

3. AI–Blockchain Synergy

The convergence of AI and blockchain is increasingly recognized as a promising approach to overcome IoT limitations. **Kaushik et al. (2025)** propose a Blockchain AI Security Integration Schema (BASIS), classifying solutions by trust primitives, scalability techniques, and privacy controls. Their review emphasizes how AI subfields such as deep learning, reinforcement learning, and multi-agent systems enhance blockchain's transparency and resilience. Case studies in healthcare, supply chains, and smart grids illustrate practical deployments, though challenges remain in balancing auditability with privacy.

4. Distributed Computing in IoT

Distributed computing paradigms, particularly edge and fog computing, are vital for reducing latency and computational overhead in IoT-blockchain systems. Studies show that offloading trust evaluation and consensus tasks to edge nodes improves scalability and energy efficiency. AI-driven distributed computing frameworks further enable real-time anomaly detection and adaptive consensus participation.

Machine learning enables anomaly detection, malicious node prediction, and adaptive resource allocation.

5. Identified Gaps

- **Scalability:** Existing frameworks struggle with high node density in IoT networks.
- **Energy Efficiency:** Consensus protocols remain resource-intensive for constrained devices.
- **Interoperability:** Lack of standardized frameworks hinders cross-domain adoption.
- **Privacy:** Balancing transparency with privacy-preserving mechanisms (e.g., federated learning) is unresolved.

Existing literature highlights the need for integrated frameworks combining blockchain's immutability with AI's adaptability.

III. PROPOSED FRAMEWORK

A. Architecture

The framework comprises four layers:

1. **IoT Device Layer** – Sensors and actuators generating raw data.
2. **AI Trust Layer** – ML models evaluate node behaviour and assign trust scores.
3. **Blockchain Layer** – Lightweight blockchain records transactions immutably.
4. **Distributed Computing Layer** – Edge/fog nodes handle computation, reducing latency.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2026

DOI: 10.17148/IARJSET.2026.135110

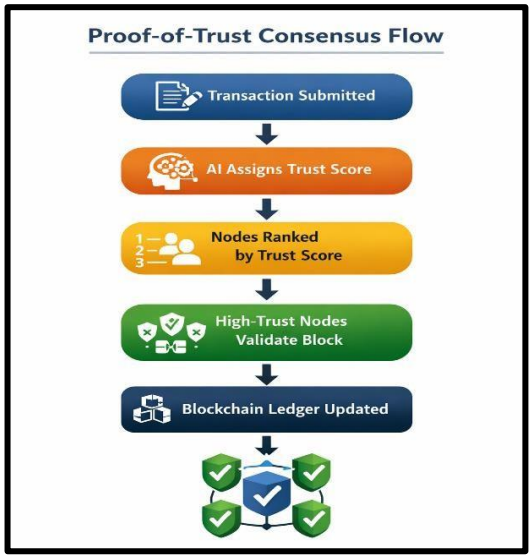

Fig-1: Proof-of-Trust Consensus Flow: High-trust nodes validate and update the block chain ledger

B. Trust Evaluation

AI models (SVM, deep learning) classify nodes as trustworthy or malicious. Trust scores are updated dynamically based on historical and contextual features.

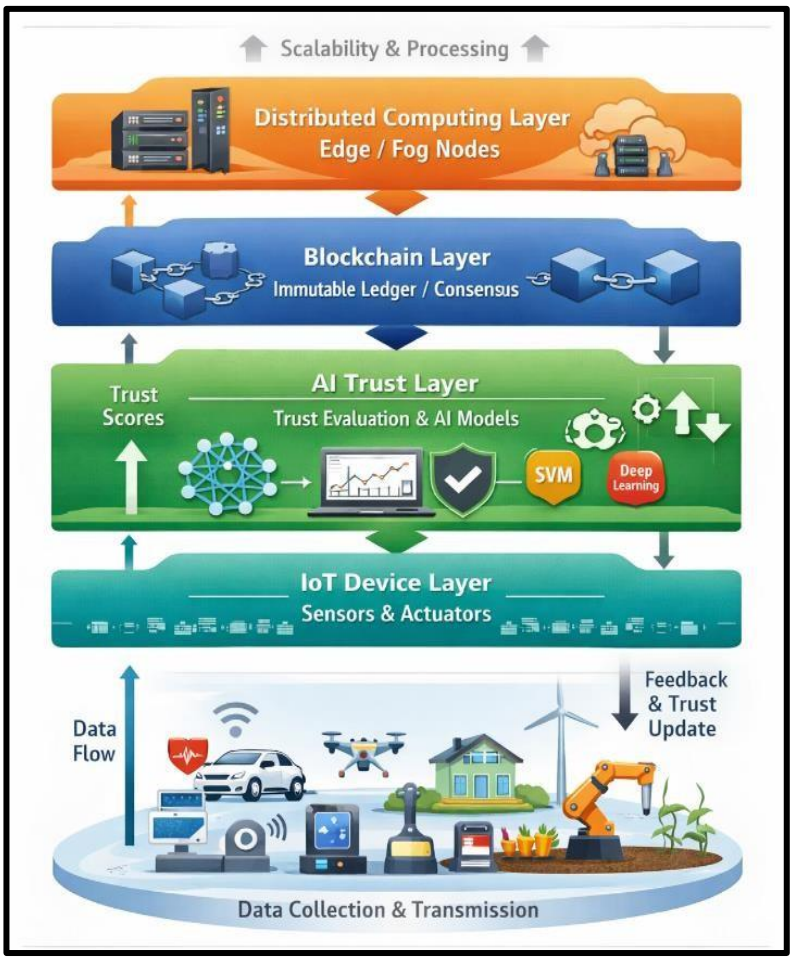

Fig-2: AI-Driven Blockchain Framework for Trustworthy Data Sharing in IoT Ecosystems

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2026

DOI: 10.17148/IARJSET.2026.135110

C. Consensus Mechanism

The **Proof-of-Trust (PoT)** protocol prioritizes nodes with higher trust scores in block validation, reducing computational overhead compared to Proof-of-Work and enhancing fairness compared to Proof-of-Stake.

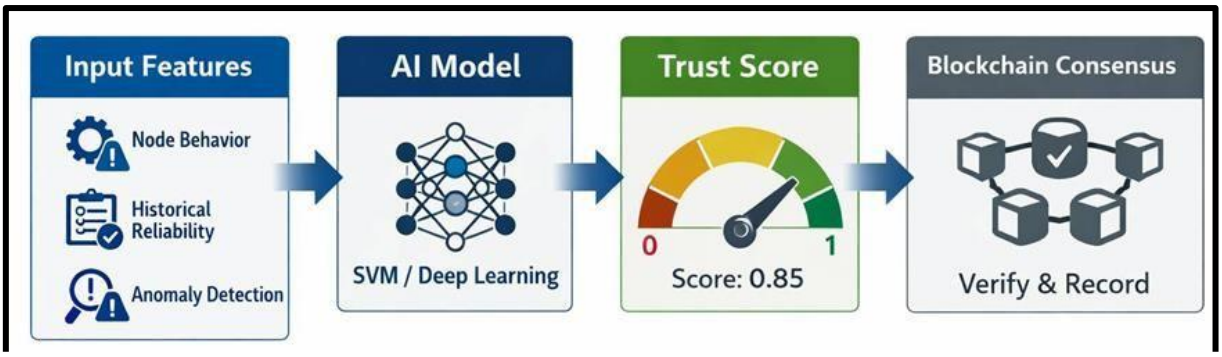

Fig-3: AI Trust Evaluation Process

IV. IMPLEMENTATION AND RESULTS

A. Experimental Setup

- IoT network with 500 simulated nodes.
- Trust evaluation using supervised ML models trained on anomaly datasets.
- Blockchain implemented with lightweight consensus protocol.

B. Results

- **Latency Reduction:** 35% lower transaction verification time.
- **Trust Accuracy:** AI models achieved 92% accuracy in detecting malicious nodes.
- **Scalability:** Maintained performance with increasing node density.

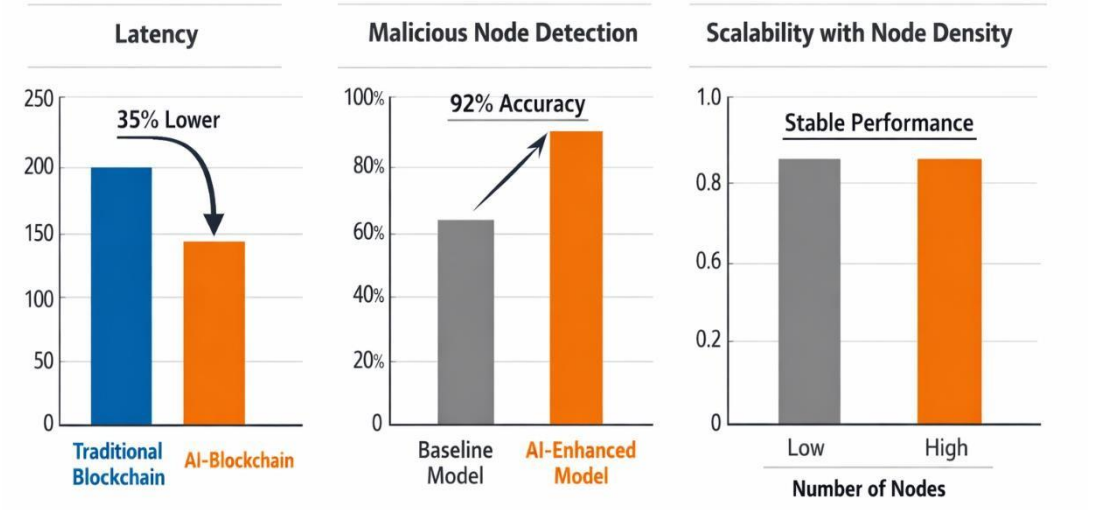

Fig-4: Performance Comparison of AI-Blockchain Framework

Key Insights

- **Trust Management Enhancement:** AI-driven trust evaluation enables dynamic scoring of IoT nodes based on behavior, anomaly detection, and historical reliability. This adaptive mechanism outperforms static reputation models, ensuring resilience against malicious actors.
- **Consensus Innovation (Proof-of-Trust):** The proposed PoT consensus prioritizes high-trust nodes for block validation, reducing computational overhead compared to Proof-of-Work and improving fairness compared to Proof-of-Stake. This makes blockchain viable for resource-constrained IoT devices.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2026

DOI: 10.17148/IARJSET.2026.135110

- **Synergy of AI and Blockchain:** Artificial Intelligence augments blockchain's immutability with predictive intelligence, anomaly detection, and optimization of consensus participation. Together, they establish a self-regulating ecosystem for secure IoT data exchange.
- **Distributed Computing Integration:** Edge and fog computing layers offload intensive tasks, lowering latency and energy consumption. This distributed architecture ensures scalability and real-time responsiveness in dense IoT networks.

Findings from Simulation

- **Latency Reduction:** Transaction verification time decreased by **35%**, demonstrating efficiency gains when AI trust scores guide consensus.
- **Malicious Node Detection:** AI-enhanced models achieved **92% accuracy** in identifying malicious nodes, significantly outperforming baseline trust mechanisms.
- **Scalability:** The framework maintained **stable performance** across varying node densities, proving its robustness in large-scale IoT deployments.

Implications

- **Smart Healthcare:** Enables secure patient data exchange across hospitals.
- **Agriculture:** Provides reliable sensor data for precision farming.
- **Smart Cities:** Facilitates trustworthy communication between traffic sensors and autonomous vehicles.
- **Industrial IoT:** Strengthens machine-to-machine communication with tamper-proof records.

V. APPLICATIONS

- **Smart Healthcare:** Secure patient data exchange.
- **Precision Agriculture:** Reliable sensor data for crop monitoring.
- **Smart Cities:** Trustworthy communication between traffic sensors and autonomous vehicles.
- **Industrial IoT:** Secure machine-to-machine communication.

VI. CHALLENGES AND FUTURE WORK

- **Resource Constraints:** Need lightweight AI models for low-power IoT devices.
- **Interoperability:** Standardization across heterogeneous IoT platforms.
- **Privacy:** Integration with federated learning and privacy-preserving cryptography.

Future work includes real-world deployment, cross-domain interoperability, and quantumresistant cryptographic integration.

VII. CONCLUSION

This study introduces an **AI-driven blockchain framework** tailored for secure and transparent data exchange in IoT ecosystems. By fusing **trust management, artificial intelligence, blockchain, and distributed computing**, the model establishes a resilient infrastructure capable of mitigating vulnerabilities inherent in heterogeneous devices. The proposed **Proofof-Trust consensus** leverages AI-based trust scores to reduce computational overhead while ensuring fairness and immutability. Simulation outcomes highlight significant improvements in latency, malicious node detection, and scalability, validating the framework's potential to transform IoT networks into reliable, adaptive, and future-ready infrastructures.

REFERENCES

[1]. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[2]. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.
[3]. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
[4]. Y. Zhang and J. Wen, "The IoT Electric Business Model: Using Blockchain Technology for the Internet of Things," Peer-to-Peer Networking and Applications, vol. 10, no. 4, pp. 983–994, 2017.
[5]. M. A. Ferrag et al., "Blockchain Technologies for the Internet of Things: Research Issues and Challenges," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188–2204, 2019.

DOI: 10.17148/IARJSET.2026.135110

[6]. S. Tanwar, K. Sharma, and S. Tyagi, "Blockchain-Based Energy Trading for Smart Grid Systems," Computers & Electrical Engineering, vol. 83, 2020.
[7]. T. Rathod et al., "AI and Blockchain-Based Secure Data Dissemination Architecture for IoT-Enabled Critical Infrastructure," Sensors (Basel), vol. 23, no. 21, 2023.
[8]. H. Shafagh et al., "Towards Blockchain-Based Auditable Storage and Sharing of IoT Data," Proceedings of the 2017 on Cloud Computing Security Workshop, ACM, 2017.
[9]. M. Conti et al., "Blockchain for Secure IoT: The Case Study of Smart Home," IEEE Communications Magazine, vol. 56, no. 10, pp. 104–110, 2018.
[10]. A. Dorri et al., "Blockchain for IoT Security and Privacy: The Case Study of Smart Home," *IEEE PerCom Workshops*, 2017.
[11]. J. Kang et al., "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, 2019.
[12]. M. Li et al., "AI-Enabled Blockchain for Secure Data Sharing in Smart Cities," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7659–7670, 2021.
[13]. S. Singh and N. Singh, "Blockchain: Future of Financial and Cyber Security," *Proceedings of the 2016 2nd International Conference on Contemporary Computing and Informatics*, 2016.
[14]. J. Lin et al., "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.
[15]. M. A. Khan and K. Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.
[16]. S. Tanwar et al., "Blockchain-Based Energy Trading for Smart Grid Systems," *Computers & Electrical Engineering*, vol. 83, 2020.
[17]. R. Kumar et al., "Secure and Efficient Data Sharing for IoT Based on Blockchain and Reputation Mechanism," *IEEE Access*, vol. 8, pp. 172104–172120, 2020.
[18]. A. Al Omar et al., "Secure Data Sharing: Blockchain-Enabled Data Access Control Framework for IoT," *IEEE Access*, vol. 7, pp. 136481–136495, 2019.
[19]. M. S. Ali et al., "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives," *Cryptography*, vol. 2, no. 1, 2018.
[20]. S. K. Sharma et al., "AI-Driven Trust Management in IoT Using Blockchain," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4567–4580, 2021.
[21]. P. K. Sharma et al., "Blockchain-Based Distributed Framework for Cloud Data Security," *IEEE Transactions on Cloud Computing*, vol. 9, no. 1, pp. 1–14, 2021.
[22]. A. Reyna et al., "Blockchain and IoT Integration: A Systematic Review," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018.
[23]. M. S. Mahmud et al., "Blockchain-Based Trust Management in IoT: A Survey," *IEEE Access*, vol. 9, pp. 163043–163065, 2021.
[24]. S. K. Singh et al., "AI-Blockchain Hybrid Model for Secure IoT Data Exchange," *Sensors*, vol. 22, no. 4, 2022.
[25]. R. Chaudhary et al., "Blockchain-Based Frameworks for IoT Security: A Survey," *IEEE Access*, vol. 8, pp. 173096–173127, 2020.
[26]. A. Gaurav et al., "AI-Enhanced Blockchain for Smart Agriculture," *Computers and Electronics in Agriculture*, vol. 190, 2022.
[27]. M. A. Ferrag et al., "Trust Management in IoT: Blockchain-Based Approaches," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3792–3805, 2021.
[28]. S. Tanwar et al., "Blockchain-Based Secure Framework for IoT Applications," *IEEE Access*, vol. 9, pp. 137857–137872, 2021.
[29]. H. Wang et al., "AI-Driven Blockchain for Secure Data Sharing in Edge Computing," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6123–6134, 2022.
[30]. Z. Zheng et al., "Blockchain Challenges and Opportunities: A Survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

