Leveraging Blockchain and AI for Secure and Scalable Edge Computing in Iot

Dheeraj
TigerAnshu
Malhotra Nishu

Abstract:
The fast spread of the Internet of Things (IoT) presents major security, scalability, and data privacy related problems. Conventional cloud-based systems find it difficult to manage vast data flows produced by Internet of Things devices and suffer with latency. By bringing processing resources next to data sources, edge computing offers a possible substitute. Still, trust problems and security flaws continue. This work presents an integrated framework combining Blockchain with Artificial Intelligence (AI) to improve security, efficiency, and scalability in edge computing environments. Blockchain guarantees safe, tamper-proof transactions and distributed authentication; artificial intelligence-driven analytics allow real-time data processing. The paper investigates real-world applications in smart cities, healthcare, and industrial IoT, together with the system architecture and main implementation difficulties. We also stress future directions in artificial intelligence-blockchain convergence for next-generation computer architectures.

Keywords: Blockchain, Artificial Intelligence, Edge Computing, IoT Security, Smart Contracts, Decentralized Systems

1.1 Background and Motivation:

With billions of linked devices creating enormous volumes of real-time data, the Internet of Things (IoT) ecosystem has seen explosive expansion. These devices range in kind from smart home assistants and industrial sensors to autonomous cars and healthcare monitoring systems. Real-time decision-making depends on the data produced by IoT devices being timely processed. Constrained bandwidth, latency, and centralized security vulnerabilities abound in conventional cloud-centric designs. By distributing data processing and putting computation closer to end devices, edge computing reduces reliance on cloud data centers and improves responsiveness, hence addressing these concerns. Edge computing can, however, bring unique security issues like data tampering, illegal access, and vulnerability to cyberattacks.

1.2 Edge Computing's Part Played By Blockchain:

By use of a distributed trust model, blockchain technology [4] guarantees data integrity and safe transactions free from depending on a central power. It provides immutability, openness, and consensus-driven security systems that can strengthen edge computing systems against malevolent attacks. Blockchain integration into edge computing allows one to authenticate devices, safely save data, and run self-enforcing agreements via smart contracts [5].

1.3 Edge Computing: The Function of Artificial Intelligence:

Artificial intelligence (AI), meantime, is absolutely vital for improving edge environment decision-making. Automated anomaly detection, resource allocation

DOI: https://doi.org/10.5281/zenodo.15113059

optimization, and edge data analytics improvement made possible by AI-driven solutions help, By dynamically allocating bandwidth, analyzing network traffic for possible hazards, and forecasting system breakdowns before they start, artificial intelligence algorithms help IoT networks be generally more efficient and secure

1.4 Synergy For Secure Edge Computing Between Blockchain and Artificial Intelligence

Blockchain and artificial intelligence together present a hopeful way to get above the restrictions of conventional edge computing designs. Blockchain offers distributed security; artificial intelligence allows intelligent automation, hence strengthening the system's resilience and adaptation. The synergy between artificial intelligence and blockchain is investigated in this work in order to provide an intelligent, scalable, safe edge computing architecture for Internet of Things [2] uses. We address how analytics driven by artificial intelligence might improve real-time threat detection, lower transaction overhead, and optimise blockchain consensus systems.

1.5 Goals and contributions:

This analysis seeks to:

- Create a conceptual framework including blockchain and artificial intelligence into edge computing.
- Examining security issues in edge computing, provide AI-driven mitigating techniques.
- Show how blockchain improves IoT network openness and trust.
- Investigate practical uses [1] of edge computing driven by artificial intelligence-blockchains in several fields.
- The suggested method improves edge computing security, best uses resources, and promotes environmentally friendly IoT installations. By means of our work, we help to close the research gap in AI-blockchain-enabled edge computing systems and emphasize important directions for further investigations.

2. Background and Related Projects

2.1 Edge Computing: Prospects and Difficulties

Edge computing reduces latency and bandwidth use by processing data close to the source, hence extending cloud services. Important obstacles consist:

- Security Risks: Cyberattacks find systems vulnerable in dispersed edge nodes.
- Data Integrity and Trust: Verifying the genuineness of data passed between edge devices
- Managing heterogeneous devices and limited resources presents challenges [10] in scalability.
- Sensitive IoT data being handled at the edge has to be protected against illegal access.
- Edge devices sometimes have low processing capability, so they need for optimized algorithms.

2.2 Blockchain for Comfortable Computing

Blockchain guarantees distributed authentication by smart contracts and tamper-proof data sharing. Important traits include:

- Data transactions entered onto a blockchain cannot be changed; they are immutable.
- Eliminating middlemen would help to build decentralized trust.
- Smart contracts are self-executing agreements improving IoT network automation.
- Proof-of- Work (PoW), Proof-of- Stake (PoS), Byzantine Fault Tolerance (BFT) safe methods all help blockchain networks to protect transactions.
- Blockchain guarantees openness in IoT data transactions by means of traceability, therefore supporting data provenance and auditing.

DOI: https://doi.org/10.5281/zenodo.15113059

2.3 AI for Maximizing Data:

AI enhances edge computing via:

- Forecasting trends and anomalies in real time, predictive analytics
- Autonomous Decision-Making: Models driven by artificial intelligence provide automated threat detection and response.
- Resource Optimization: Improving processing effectiveness and lowering computational overhead
- Distributed machine learning, under federated learning, lets edge devices cooperatively train models while maintaining data privacy.
- Cognitive edge computing is artificial intelligence improving contextual awareness and real-time data interpretation**.**

2.4 Related Studies and Holes:

Although current research focus on blockchain-based security [11] and AI-driven edge computing independently, a consistent framework combining both technologies is still much lacking.

Important knowledge gaps include:

- Lack of AI-Blockchain Synergy: Though not its combined effect, current models concentrate on either AI-driven optimization or blockchain security.
- Computational Overhead: Combining blockchain and artificial intelligence has to strike security and efficiency without overloading limited edge devices with resources.
- Scalability of Blockchain in Edge Environments: Traditional blockchain systems need optimal consensus techniques since they suffer with transaction speed and scalability in Edge environments.
- Privacy-Preserving AI Models: Edge AI calls for safe approaches to teach models without revealing private information.
- Blockchain improves trust in decentralised edge networks; nonetheless, trust models for dynamic edge environments require more improvement.

This work intends to solve these difficulties by suggesting a strong edge computing architecture supported by artificial intelligence-blockchains. We provide IoT applications a scalable, reliable edge computing solution by combining blockchain security with AI-powered optimization.

3. Proposed Framework: Integration of AI-Blockchains for Safe Edge Computing:

3.1 System Architectural Framework:

Designed to improve edge computing environments' security, efficiency, and dependability, the proposed AI-Blockchain framework. The following main elements define the architecture:

Among IoT Edge Devices are sensors, actuators, and other embedded systems creating real-time data for processing. These devices need safe procedures for processing and communication and function as the main data sources.

Combining machine learning techniques for security monitoring, anomaly detection, and predictive analytics, this AI module. It guarantees real-time edge decision-making while lowering latency and dependency on centralized cloud architecture [2].

Blockchain Layer: A distributed ledger system guaranteeing secure execution of smart contracts, data integrity, and tamper-proof transactions. It offers an honest way for edge device transaction logging.

This technique validates transactions and preserves blockchain integrity under consensus. Consensus procedures two most often used are discussed for this framework:

Proof-of- Stake (PoS) lets validators be selected depending on their stake, therefore lowering energy consumption and accelerating transaction validation.

Byzantine Fault Tolerance (BFT) guarantees consistency in a distributed network and strengthens resistance against malevolent nodes.

DOI: https://doi.org/10.5281/zenodo.15113059

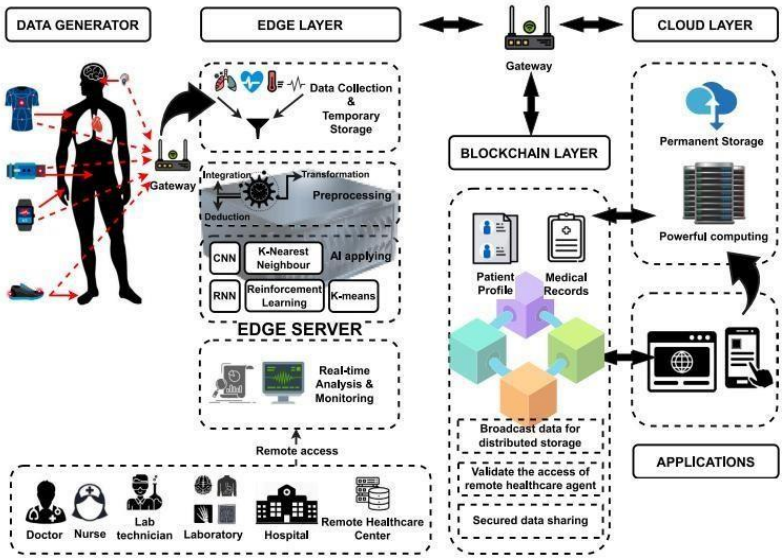


Figure 1: Blockchain Integrated Edge Computing Architecture in AI[9]

Figure 1 shows a picture of IoT edge devices, artificial intelligence module, blockchain layer, and consensus mechanism illustrating architectural design

3.2 Security Devices:

The proposed framework combines sophisticated security techniques to guarantee a strong and safe edge computing environment:

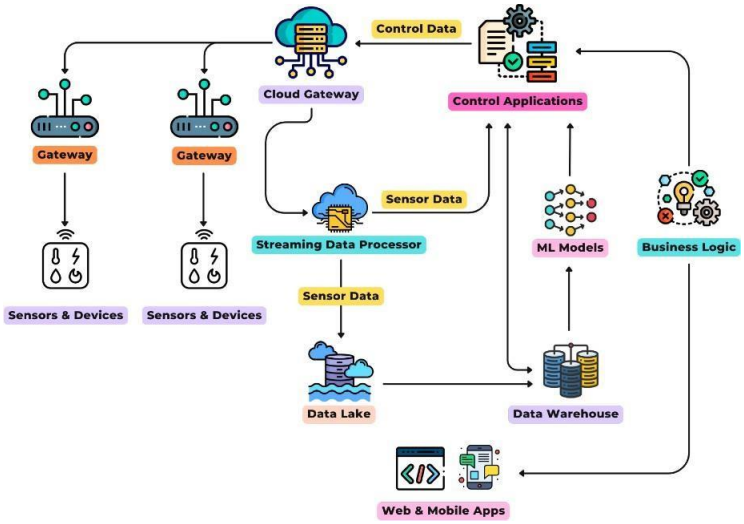
• AI-Powered Intrusion Detection: In real-time, analyzes network traffic using machine learning models to identify possible cyberthreats including malware, illegal access, and aberrant behavior.

• Blockchain-Based Authentication: Uses blockchain to implement cryptographic authentication systems thereby facilitating safe access control. Leveraged are public key infrastructure (PKI) and distributed identity management to stop identity spoofing and illegal access.

• Privacy-preserving data processing guarantees safe management via:

o Homomorphic Encryption: Guarantures privacy during processing by letting computations on encrypted data without decryption.

Zero-Knowledge Proofs (ZKP) let data verification take place without disclosing underlying private information.



DOI: https://doi.org/10.5281/zenodo.15113059

Figure 2: AI-Blockchain Edge Computing Security Mechanisms [7]

Figure 2 depicts an illustration highlighting privacy-preserving strategies, authentication, and intrusion detection.

3.3 Techniques for Performance Optimization:

Following optimization techniques helps to improve the scalability and efficiency of AI-Blockchain integrated edge computing: Federated learning permits distributed artificial intelligence model training among several edge devices without sending raw data to a central server. This method lowers bandwidth use and improves data privacy.

By spreading blockchain storage into smaller, more controllable shards, blockchain sharding improves transaction speed and scalability. Every shard individually handles transactions, therefore lowering computational overhead.

AI-Driven Network Optimization: To raise general system efficiency, dynamically allocate resources using AI algorithms, so optimizing bandwidth utilization, computing power, and network latency.

These techniques improve security, privacy, and performance in edge computing together, so AI-Blockchain integration[3]is a feasible solution for distributed, next-generation safe systems.

4. Use Cases and Applications:

4.1 Intelligent Hospitality:

Using machine learning algorithms, artificial intelligence-powered diagnostics help to identify diseases and create tailored treatment regimens. Blockchain-based electronic health records (EHRs) guarantee patient data integrity, therefore allowing safe and open access among approved medical professionals. This integration increases interoperability, lowers medical mistakes, and guards private patient data from illegal access.

4.2 IIoT, or industrial IoT:

Blockchain improves security in industrial environments by means of a tamper-proof ledger documenting supply chain activities. Using sensor data and machine learning models, artificial intelligence-powered predictive maintenance seeks possible breakdowns before they start, therefore lowering operational costs and downtime. Blockchain and artificial intelligence together guarantees dependable, automated, safe industrial processes.:

4.3 Contemporary Cities:

Blockchain-based smart contracts help smart cities by allowing open and safe transactions in energy networks, hence supporting distributed energy trade. Real-time traffic data analysis by AI-driven traffic management systems helps to maximize signal timing, ease congestion, and improve public transportation effectiveness. These technologies advance citizen services and help to create sustainable cities.

DOI: https://doi.org/10.5281/zenodo.15113059

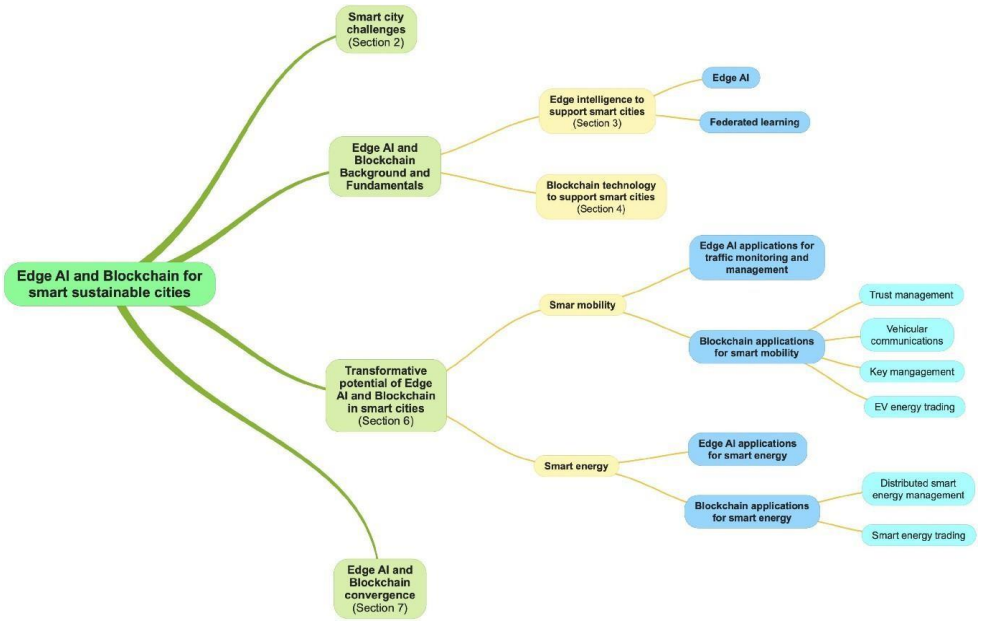


Figure 3: Artificial Intelligence-Blockchain Uses in Urban Areas[8]

Figure 3 illustrates the blockchain and artificial intelligence uses in smart city infrastructure.

4.4 Independent Cars

Blockchain plus artificial intelligence improves autonomous cars' efficiency and safety. Blockchain guarantees safe vehicle-to----vehicle (V2V) communication, therefore stopping cyber-attacks on car systems. Real-time sensor data processing by AI-driven collision avoidance systems generates split-second judgments meant to stop collisions. These developments open the path for dependable and safer autonomous driving .

4.5 DeFi's Financial Services:

Blockchain transforms financial services by means of distributed finance (DeFi) systems, therefore guaranteeing open, safe, tamper-proof transactions. By means of pattern recognition, AI improves fraud detection by spotting irregularities in financial transactions therefore reducing risks. AI-powered risk assessment models enhance credit scoring, investment strategies, and automated trading, so strengthening financial ecosystems by means of more safe and effective solutions.

5. Difficulties and Future Investigative Approaches

Even with the benefits, including blockchain and artificial intelligence in edge computing provide some difficulties:

Computational Overhead: AI and blockchain processes [6] demand large processing capability, which could be a restriction in edge contexts with limited resources.

Maintaining sustainability depends on careful energy consumption, particularly for Internet of Things devices running on batteries.

Lack of defined protocols makes seamless cross-platform communication between edge devices, blockchain networks, and artificial intelligence models difficult.

Compliance with data privacy rules (such as GDPR) and ethical AI deployment remain vital issues in real-world deployments from ethical and legal standpoint.

6. Future directions of research:

Future studies aiming at overcoming these obstacles should concentrate on:

Developing low-latency and energy-efficient consensus algorithms would help blockchain processing speed to be improved without compromising security.

By means of effective resource allocation, variable block sizes, and transaction

DOI: https://doi.org/10.5281/zenodo.15113059

prioritizing, AI-driven blockchain scalability solutions seek to improve blockchain scalability. Using privacy-preserving federated learning models inside blockchain networks will help to provide distributed and safe AI training across edge devices. Designing customized hardware accelerators for AI and blockchain workloads helps to improve processing performance at the edge by edge-AI hardware optimization. Encabling flawless interaction between several blockchain networks and artificial intelligence systems will help to build a more cohesive and scalable ecosystem. By addressing these issues and research approaches, AI-Blockchain integration in edge computing will be advanced and distributed intelligent systems will be fostered by means of security, efficiency, and decentralization.

7. Conclusion:

This work presents a fresh AI-Blockchain integrated edge computing platform addressing IoT network scalability, efficiency, and security issues. Using blockchain for distributed trust and artificial intelligence for smart decision-making guarantees strong data integrity, best use of resources, and edge computing environment resilience.

From smart healthcare to industrial IoT to smart cities to autonomous cars to financial services, the combination of artificial intelligence with blockchain presents major breakthroughs in many different fields. The suggested design supports intelligent, distributed, safe computing systems that would enable real-time analytics, fraud detection, and more automation by means of better automation tools.

Real-world implementations, performance assessments across several IoT applications, and enhancing AI-Blockchain frameworks for energy efficiency and interoperability will be the main topics of further study. By tackling these domains, AI-Blockchain integration will keep developing and open the path for a more scalable, safe, and efficient edge computing paradigm.

References

[1] Ali, M.S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., Rehmani, M.H.: Applications of blockchains in the internet of things: A comprehensive survey.IEEE Communications Surveys & Tutorials 21(2), 1676–1717 (2018)

[2] Ashton, K. (2009). That 'internet of things' thing. *RFID journal*, *22*(7), 97-114.

[3] Aruna, S., Priya, S.M., Reshmeetha, K., Sudhayini, E.S., Narayanan, A.A.: Blockchain integration with artificial intelligence and internet of things technologies. In: 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS). pp. 688–694. IEEE (2023).

[4] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, *17*(4), 2347-2376.

[5] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, pp. 2292-2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[6] Greenspan, G. (2015). Avoiding the pointless blockchain project. *Online at https://www. multichain. com/blog/2015/11/avoiding-pointless-blockchain-project*.

[7] Rupanetti, D.; Kaabouch, N. Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities. Appl. Sci. 2024, 14, 7104. https://doi.org/10.3390/app14167104.

[8]Badidi, E. Edge AI and Blockchain for Smart Sustainable Cities: Promise and Potential. *Sustainability* **2022**, *14*, 7609. https://doi.org/10.3390/su14137609.

[9] Tri Nguyen, Huong Nguyen, Tuan Nguyen Gia,Exploring the integration of

DOI: https://doi.org/10.5281/zenodo.15113059

edge computing and blockchain IoT: Principles, architectures, security, and applications, Journal of Network and Computer Applications, Volume 226,2024,103884,ISSN 1084-8045,https://doi.org/10.1016/j.jnca.2024.103884.
[10] Khan, M.A., Salah, K.: Iot security: Review, blockchain solutions, and open challenges. Future generation computer systems 82, 395–411 (2018).
[11] . Zhang, F., Wang, H., Zhou, L., Xu, D., Liu, L.: A blockchain-based security and trust mechanism for ai-enabled iiot systems. Future Generation Computer Systems 146, 78–85 (2023).

DOI: https://doi.org/10.5281/zenodo.15113059