A Comprehensive Survey of Blockchain, AI, and Deep Learning for Secure Heterogeneous ICT Networks

Dr.Asha K H[1] *, Dr. Rubini P*[2]
[1*] Lincoln University College, Petaling Jaya, Selangor Darul Ehsan-47301, Malaysia.
[2] CMR University, Bangalore, Karnataka, India
Email ID
[1*] asha.kh06@gmail.com, [2]prubini.cs@gmail.com

Abstract: The rapid convergence of Internet of Things (IoT), edge computing, cloud services, industrial control systems, mobile devices, and intelligent applications has created heterogeneous ICT environments in which security, trust, interoperability, data integrity, communication efficiency, and resource utilization are tightly coupled. Conventional centralized security and analytics architectures are increasingly challenged by distributed attack surfaces, single points of failure, privacy constraints, non-uniform device capabilities, and high communication overhead. This paper surveys blockchain, artificial intelligence (AI), deep learning (DL), federated learning (FL), edge intelligence, peer-to-peer (P2P) communication, and intelligent resource optimization for heterogeneous ICT networks. The review is organized around four core capabilities: infrastructure protection, verifiable data integrity and trust, decentralized P2P communication, and adaptive resource optimization. The analysis identifies a persistent integration gap: most existing studies address one or two capabilities, whereas comparatively few provide an end-to-end architecture that jointly coordinates all four. To address this gap, a five-layer blockchain-enabled AI/DL framework is proposed, integrating heterogeneous infrastructure, secure P2P data exchange, a blockchain trust layer, AI/DL analytics, and security-aware resource optimization. The framework is intended as a research foundation for future empirical validation in realistic edge-cloud and cyber-physical environments.

Keywords: Blockchain; Artificial Intelligence; Deep Learning; Internet of Things; Federated Learning; P2P Communication; Data Integrity; Cybersecurity; Edge Computing; Resource Optimization; Heterogeneous ICT Networks.

Introduction

Heterogeneous ICT networks combine devices and systems with different computing capabilities, communication protocols, trust assumptions, data formats, and security requirements. Examples include IoT sensors, industrial controllers, mobile devices, edge gateways, cloud platforms, smart-city infrastructure, healthcare systems, transportation networks, and energy systems. These environments continuously generate operational and security data and increasingly require low-latency decisions. At the same time, their distributed nature enlarges the attack surface and makes centralized security management difficult.

Blockchain provides decentralized trust, tamper-evident records, provenance, and programmable access control through smart contracts. AI and DL complement blockchain by learning from large-scale telemetry and detecting abnormal behavior, attacks, failures, and resource-demand patterns. Federated learning enables collaborative model training while keeping raw training data at local nodes, which is attractive for privacy-sensitive edge environments. Recent surveys report increasing research activity at the intersection of blockchain, federated learning, AI, and IoT security [1]–[7].

However, these technologies should not be treated as independent add-ons. Blockchain introduces consensus, storage, and transaction overhead; AI/DL introduces computational, privacy, and model-security requirements; P2P communication introduces routing and trust challenges; and heterogeneous resources make static allocation inefficient. A unified framework must therefore coordinate security, integrity, communication, intelligence, and resource optimization.

Related Work

A. Blockchain for IoT Security and Data Integrity

Blockchain has been widely investigated as a mechanism for trust, traceability, access control, and data integrity in IoT environments. Distributed ledgers can record hashes, access events, model-update metadata, and transactions so that subsequent unauthorized modification becomes detectable. Smart contracts can automate authentication, authorization, incentives, and policy enforcement. Nevertheless, consensus latency, ledger growth, throughput, and the limited resources of edge devices remain significant constraints [1].

B. Blockchain and Federated Learning

Blockchain-enabled federated learning combines decentralized trust with collaborative model training. BlockFL research covers personal IoT, industrial IoT, Internet of Vehicles, and Internet of Health Things, with emphasis on security, privacy, trust, efficiency, and data diversity [3]. Recent work has also combined blockchain with device-clustering FL, personalized differential privacy, and game-theoretic mechanisms to jointly address efficiency and privacy [4], [5].

C. AI/DL for Infrastructure Protection

AI and DL models, including CNNs, LSTMs, transformers, autoencoders, graph neural networks, and reinforcement learning, are increasingly used for intrusion detection, anomaly detection, malware classification, fault prediction, and cyber-physical monitoring. Blockchain–AI reviews identify anomaly detection, predictive analytics, and adaptive policy control as important opportunities [7]. However, adversarial examples, poisoned training data, model drift, explainability, and inference cost remain concerns.

D. Edge Intelligence, P2P Communication and Resource Optimization

Edge computing moves processing closer to data sources and can reduce latency. Federated and distributed learning reduce raw-data movement but introduce communication and device-heterogeneity challenges. Recent edge-IoT FL surveys emphasize joint optimization of computing, communication, privacy, and security [2]. Reinforcement learning and related adaptive methods can optimize task offloading, bandwidth, energy, routing, and service placement.

Table 1. Summary of Landscape Based on the Four Core Capabilities of the Proposed Framework: Identifying the Integration Gap

Representative Work	Infrastructure Protection	Data Integrity & Trust	P2P Communication	Resource Optimization	Integration Observation
IoT blockchain survey [1]	Partial	Strong	Yes	Limited	Strong trust/integrity focus; limited end-to-end intelligence and optimization.

Edge-IoT FL survey [2]	Yes	Partial	Partial	Yes	Secure distributed learning and edge efficiency; trust is not fully integrated.
BlockFL survey [3]	Partial	Strong	Yes	Yes	Strong blockchain-FL integration; broader infrastructure protection remains fragmented.
IoT data sharing [4]	Partial	Strong	Yes	Partial	Secure sharing and clustered FL; limited holistic resource/security coordination.
Decentralized BCFL [5]	Partial	Strong	Yes	Strong	Joint privacy-efficiency optimization, but not a complete four-capability architecture.
Blockchain–AI review [7]	Strong	Strong	Yes	Partial	Strong security intelligence; adaptive resource management is less central.
Blockchain + FL aggregation survey [8]	Partial	Strong	Yes	Strong	Industrial-IoT-focused blockchain-FL aggregation; resource efficiency is considered, but comprehensive infrastructure protection and AI-driven intelligence remain limited.
Blockchain-enabled Federated Reinforcement Learning (B-FRL) [9]	Strong	Strong	Yes	Strong	Combines blockchain, federated reinforcement learning, privacy preservation, and adaptive decision-making; however, a complete heterogeneous ICT infrastructure architecture is not addressed.
Blockchain Integrated FL in Edge-Fog-Cloud IoT Healthcare [10]	Strong	Strong	Yes	Strong	Integrates blockchain-FL across edge-fog-cloud environments with emphasis on security and resource efficiency; application is healthcare-specific rather than a generalized heterogeneous ICT framework.
Proposed framework	Strong	Strong	Strong	Strong	Unified end-to-end architecture connecting all four capabilities.

Table 1 shows that the literature contains substantial progress in each individual capability and in selected pairs of capabilities. The integration gap is therefore architectural rather than technological: infrastructure protection, verifiable integrity and trust, decentralized communication, and adaptive resource optimization are rarely designed as one coupled system. This gap motivates the proposed framework.

Proposed Framework (Design)

The proposed architecture is organized into five coordinated layers. The design separates physical/data inputs, secure integration and trust, intelligent analytics, optimization, and application/decision services.

Layer 1: Heterogeneous Infrastructure/Data Layer

IoT sensors, industrial devices, mobile nodes, edge servers, gateways, cloud services, and application systems generate network, operational, environmental, and security telemetry. Local preprocessing reduces unnecessary transmission and supports latency-sensitive processing.

Layer 2: Secure Data and P2P Communication Layer

Authenticated P2P channels, identity management, encryption, access control, secure routing, and policy enforcement protect data exchange. Trust scores can help identify and isolate unreliable nodes.

Layer 3: Blockchain Trust and Integrity Layer

A permissioned blockchain is suitable for many infrastructure settings. The ledger stores hashes, access events, model-update metadata, security alerts, and resource-allocation decisions rather than large raw datasets. Smart contracts automate verification and policy enforcement.

Layer 4: AI and Deep Learning Intelligence Layer

CNNs, autoencoders, LSTM/Transformer models, graph models, and federated learning analyze network flows, device behavior, logs, sensor streams, and blockchain events. Robust aggregation and privacy mechanisms reduce malicious-update risks.

Layer 5: Intelligent Resource Optimization and Decision Layer

Reinforcement learning, multi-agent learning, or mathematical optimization allocates bandwidth, computation, energy, storage, routing, and edge/cloud placement while considering security risk, trust, latency, and service requirements.

Objectives

1. Design a unified blockchain-enabled AI/DL architecture for secure heterogeneous ICT infrastructures.
2. Provide tamper-evident data provenance, decentralized trust, access control, and secure P2P communication.
3. Integrate AI/DL and federated learning for real-time anomaly, intrusion, and infrastructure-threat detection.
4. Develop intelligent resource-optimization mechanisms for bandwidth, computation, energy, routing, and service placement.
5. Define an evaluation strategy covering security, integrity, latency, communication cost, model accuracy, scalability, energy consumption, and resource utilization.

Scope

The framework targets heterogeneous IoT, industrial IoT, smart-city, healthcare, transportation, energy, and other cyber-physical ICT environments. It focuses on infrastructure protection, trusted data exchange, P2P coordination, intelligent detection, and resource optimization, with emphasis on edge–cloud environments and permissioned blockchain deployments. Large raw datasets are not intended to be stored directly on-chain;

instead, hashes, metadata, proofs, and relevant events are recorded while data remain at authorized sources or storage.

Key Contribution

- A unified survey perspective connecting blockchain trust, AI/DL security, P2P communication, federated learning, and intelligent resource optimization.
- A five-layer reference architecture for heterogeneous ICT networks.
- A comparative landscape organized around four core capabilities and used to identify the integration gap.
- A security-aware optimization view in which resource allocation considers risk, trust, latency, and energy together.
- A research agenda covering adversarial AI, poisoning resistance, blockchain scalability, interoperability, explainability, privacy, and real-world validation.

Discussions

The reviewed literature supports complementary roles for blockchain and AI. Blockchain is well suited to trust, provenance, auditability, and decentralized policy enforcement, whereas AI/DL is suited to extracting patterns from high-volume and heterogeneous data. Federated learning adds collaborative training without centralizing raw data, but it does not by itself guarantee trustworthiness because model updates can be manipulated. Blockchain can record provenance and validation metadata, but it cannot guarantee that a data item was correct before it was written to the ledger.

Scalability is a major concern. Storing every IoT event on-chain is impractical in high-throughput environments. The proposed design therefore separates large data from blockchain metadata and recommends off-chain storage with on-chain hashes or proofs. Consensus should be selected according to latency, trust, and energy requirements.

AI security is another major issue. Attackers may manipulate input streams, poison federated updates, evade detection models, or exploit explanations. Model validation, robust aggregation, adversarial testing, drift monitoring, and explainability should therefore be included. Resource optimization must also be security-aware: a policy that minimizes latency but assigns sensitive tasks to low-trust nodes may improve performance while weakening security. Trust and risk should therefore be optimized jointly with latency, energy, bandwidth, and computation.

Conclusions

1.Problem Addressed/Motivation: The existing literature demonstrates significant progress in blockchain, AI/DL, federated learning, P2P communication, and intelligent resource optimization. However, these capabilities are generally investigated independently or in partial combinations. In particular, the simultaneous integration of infrastructure protection, verifiable data integrity and trust, decentralized communication, and adaptive resource management remains limited, creating an important integration gap in heterogeneous ICT networks.

2.Proposed Method: A five-layer blockchain-enabled AI/DL framework is proposed to address this gap by synchronizing heterogeneous infrastructure, secure P2P communication, blockchain-based trust and data

provenance, AI/DL-driven intelligent analytics, and security-aware resource optimization within a unified architecture.

3.Key Research Gap and Motivation: The comparative literature analysis indicates that no reviewed approach comprehensively unifies all four core capabilities within a single end-to-end architecture. Existing studies typically focus on blockchain-based security and integrity, AI/DL-based threat detection, federated learning, P2P

trust, or resource optimization individually or in selected combinations. This identified integration gap provides the primary motivation for the proposed framework.

4.Limitations and Future Work: The present study is limited to survey-based analysis, comparative literature positioning, and framework design and does not claim empirical performance for the complete architecture. The immediate next step is to develop and validate a prototype using a realistic heterogeneous ICT/edge-cloud testbed and standardized evaluation metrics. Future validation should specifically examine blockchain scalability, AI adversarial robustness, federated-learning privacy leakage, interoperability, explainable AI, communication overhead, and security-aware adaptive resource optimization.

References

[1] "Blockchain Applications for Internet of Things — A Survey," Internet of Things, vol. 27, 101254, 2024.

[2] H. Li, L. Ge, and L. Tian, "Survey: federated learning data security and privacy-preserving in edge-Internet of Things," Artificial Intelligence Review, vol. 57, art. 130, 2024.

[3] W. Ni and R. P. Liu, "Blockchained Federated Learning for Internet of Things: A Comprehensive Survey," ACM Computing Surveys, vol. 56, no. 10, 2024.

[4] "IoT data sharing technology based on blockchain and federated learning algorithms," Intelligent Systems with Applications, vol. 22, 200359, 2024.

[5] Z. Cheng et al., "Decentralized IoT data sharing: A blockchain-based federated learning approach with joint optimizations for efficiency and privacy," Future Generation Computer Systems, vol. 160, pp. 547–563, 2024.

[6] J. Wang and J. Li, "Blockchain and Access Control Encryption-Empowered IoT Knowledge Sharing for Cloud-Edge Orchestrated Personalized Privacy-Preserving Federated Learning," Applied Sciences, vol. 14, no. 5, 1743, 2024.

[7] "Synergizing blockchain and AI to fortify IoT security: a comprehensive review," Artificial Intelligence Review, 2025.

[8] M. Shawkat et al., "Blockchain and federated learning based on aggregation techniques for industrial IoT: A contemporary survey," Peer-to-Peer Networking and Applications, vol. 18, art. 192, 2025.

[9] T. Alam et al., "Blockchain-Enabled Federated Reinforcement Learning (B-FRL) Model for Privacy Preservation Service in IoT Systems," Wireless Personal Communications, vol. 136, pp. 2545–2571, 2024.

[10] S. M. Rajagopal, Supriya M., and R. Buyya, "Blockchain Integrated Federated Learning in Edge-Fog-Cloud Systems for IoT based Healthcare Applications: A Survey," arXiv:2406.05517, 2024.