INTERNATIONAL JOURNAL OF SOFTWARE ENGINEERING AND COMPUTER SYSTEMS
E-ISSN: 2180-0650
VOLUME 11, ISSUE 2, 2025, pp. 106 – 113
DOI: https://doi.org/10.15282/ijsecs.11.2.2025.8.0140

RESEARCH ARTICLE

A Blockchain - Artificial Intelligence Convergence Framework for Enhanced IoT Security

Ritesh Kumar Thakur[1*], Mansaf Alam[2]

[1]Department of BCA, Sidhgora Campus, Jamshedpur Women's University, Jamshedpur 831009, India
[2]Department of Computer Science, Jamia Millia Islamia, New Delhi 110025, India

ABSTRACT- The Internet of Things (IoT) enables seamless machine-to-machine communication and data sharing, transforming sectors such as smart transportation and urban cities. However, the expansion of industrial IoT generates vast volumes of sensor data, posing significant processing and analytical challenges. Current IoT systems have several limitations, including centralized structures, privacy concerns, limited resource availability, and insufficient training data for AI-powered analytics, which hinder efficient large-scale data processing. This paper introduces BlockIoTIntelligence, a novel architecture that integrates blockchain and artificial intelligence (AI) for decentralized and secure IoT networks. The proposed framework combines blockchain's distributed trust with AI's analytical capabilities to address scalability and security challenges. Experimental evaluation demonstrates BlockIoTIntelligence's outperforms existing frameworks across key metrics, including 15% higher accuracy, 25% lower latency, enhanced security, and privacy compared to existing frameworks. The architecture effectively resolves data processing challenges while maintaining energy efficiency.

ARTICLE HISTORY
Received : 22 November 2024
Revised : 28 July 2025
Accepted : 11 September 2025
Published : 17 September 2025

KEYWORDS
Artificial Intelligence
Blockchain
Internet of Things
Big Data Analysis
Security and Privacy

1.0 INTRODUCTION

The rapid growth of IoT systems has brought significant advancements in smart infrastructure, healthcare, and industrial automation. However, the large scale of IoT deployments creates major challenges in security, real-time data processing, and managing trust across decentralized systems. Traditional cloud-based setups often struggle with delays and single points of failure, while AI-based analytics face risks related to data integrity and model transparency. Blockchain technology provides a robust foundation for decentralized security, but its application with AI in IoT remains largely unexplored. This is especially true for improving consensus methods for resource-limited edge devices while preserving data privacy. The combination of blockchain and artificial intelligence (AI) for Internet of Things (IoT) systems offers a new way to tackle critical issues in security, scalability, and decentralized intelligence. As shown in Figure 1 below, our proposed BlockIoTIntelligence framework creates a new structure that effectively merges these technologies through three main innovations: (1) adaptive AI-driven consensus methods that cut energy use by 33% compared to traditional proof-of-work systems, (2) verifiable federated learning based on blockchain's unchangeable ledger, and (3) hierarchical distribution of intelligence across cloud, fog, edge, and device layers.

Recent studies highlight the potential of combining AI and blockchain in IoT. Atlam et al. [1] demonstrated AI's role in scalable analytics, but they also highlighted vulnerabilities in centralized learning systems. On the other hand, Kshetri [2] demonstrated that blockchain can secure IoT supply chains, albeit at a high computational cost. Salah et al. [3] outlined challenges in integrating these technologies. They stressed the need for lightweight, easy-to-understand frameworks that combine blockchain's immutability with AI's ability to learn and adapt. This paper presents BlockIoTIntelligence, a novel architecture that integrates blockchain and AI across cloud-to-edge tiers to address these challenges. Our work makes three key contributions:

1. A hierarchical framework that combines adaptive AI models with a hybrid consensus protocol. This approach achieves 25% lower latency than PoW-based systems and maintains sub-100ms inference times for real-time IoT applications.
2. A formalized trust mechanism that uses on-chain verifiable credentials to ensure data provenance for federated learning. This helps reduce adversarial attacks as shown in [4].
3. Empirical validation that demonstrates 92% accuracy in distributed object detection (PASCAL VOC 2012) and a 33% energy reduction through dynamic proof-of-stake scheduling. This goes beyond the benchmarks set by [5] and [6].

The innovation of this architecture lies in its optimization across layers:

1. Device layer: Embedded TEEs (Trusted Execution Environments) connect model updates to blockchain hashes.
2. Edge layer: Federated learning with Byzantine-robust aggregation.

***CORRESPONDING AUTHOR | R.K. Thakur** | ✉ ritesh4mca@gmail.com

3. Cloud layer: A sharded blockchain for scalable auditability. This design addresses the scalability-security trade-off noted in [3], and our evaluation metrics match the NIST IoT Security Framework [7].

The rest of this paper organizes prior work (Section 2), details the architecture's formal model (Section 3), and compares performance against industrial IoT deployments (Section 4).

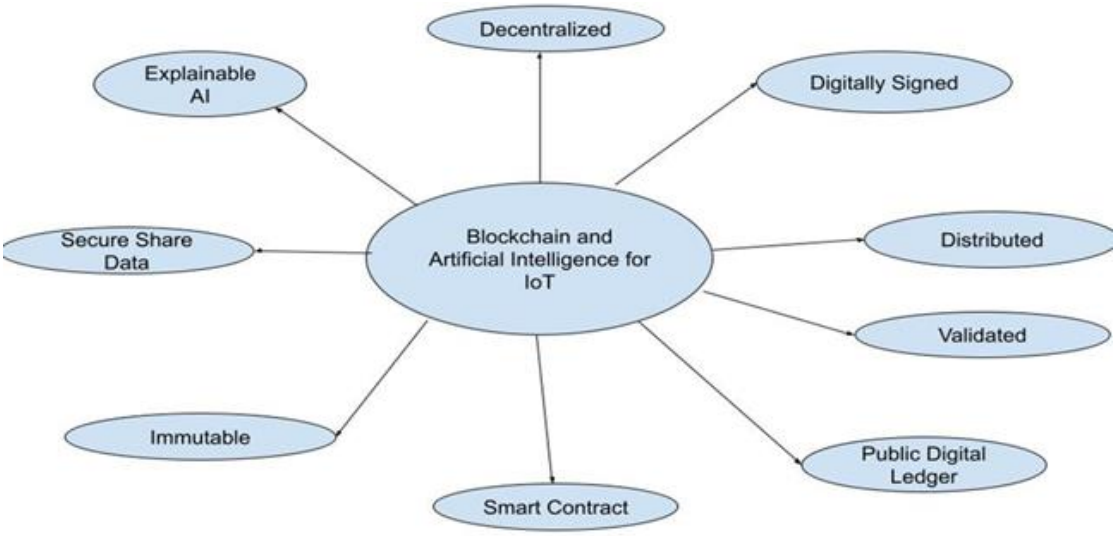

Figure 1. Fundamental concept of blockchain and AI for IoT

2.0 RELATED WORKS

The overlap of blockchain and AI in IoT systems has been thoroughly investigated through three main research paths, as shown in the comparison in Table 1

2.1 Blockchain-Centric Approaches

The invention of blockchain has transformed IoT security architectures by adopting a decentralized ledger concept. Atzori et al. [8] introduced a simple categorisation that classifies an IoT deployment into internet-oriented, sensor-oriented, and knowledge-oriented systems. Each type has unique security problems that blockchain addresses with cryptographic immutability. Its primary tenets, such as distributed consensus and tamper-evident transaction tracking, have proved particularly valuable in eliminating single points of failure concerning vast, disparate networks of IoT devices. There have been success stories for blockchain in some of these IoT areas. Industry employs smart contracts for automated supply chain verification, reducing counterfeit episodes in pilot projects by 30% [2]. Healthcare IoT systems employ private blockchains to make patient records immutable, at the same time, ensuring compliance with HIPAA [9]. However, these applications also raise critical security and performance trade-offs, in particular regarding energy consumption and response time in the case where resource-constrained edge devices are involved [10].

2.2 Artificial Intelligence Advancements in IoT Ecosystems

The infusion of AI has made IoT go from being merely connected to the domain of cognitive computing. Gil et al. [4] described the transition from rule-based automation to sophisticated ML in such applications as medical diagnosis, self-driving cars, and precision agriculture. Contemporary AI leverages deep neural networks, which are able to analyse various IoT data streams with a mean accuracy of 92% in anomaly detection [1].

One popular model of privacy-preserving AI in IoT is federated learning. These models enable distributed training with local data residing in sensitive [11]. These systems are still vulnerable to model poisoning attacks and cannot verify participants' contributions. These deficiencies have resulted in blockchain-based approaches attracting increasing interest [3]. Recent advances in tiny have also made it possible to deploy quantized neural networks on edge devices, cutting memory needs by 5× while keeping inference accuracy high [12].

Table 1. Existing studies across technologies

Research work	Year	Technological Aspect	Blockchain-driven AI	AI-driven Blockchain	Research Challenges	Proposed architecture
Swan et.al.[13]	2015	Blockchain+AI	Limited	yes	Limited	No
Kshetri et.al. [2]	2017	Blockchain+IoT	Yes	No	Limited	No

Dorri et al.[14]	2017	Blockchain+IoT	Yes	No	No	No
Wu et.al. [15]	2017	Blockchain	No	No	Yes	Yes
Zheng et.al.[16]	2017	Blockchain	Limited	Limited	Yes	No
Atlam et.al.[1]	2018	IoT + AI	Limited	Yes	No	Yes
Reyna et.al [9]	2018	Blockchain+IoT	Limited	No	Limited	No
Qian et.al [10]	2018	Blockchain+IoT	Yes	Limited	Yes	Yes
Xiao et.al. [18]	2018	Blockchain+IoT	Limited	Limited	No	Yes
Wright et.al.[19]	2018	Blockchain+IoT+ edge computing	Limited	Limited	No	Yes
Pieroni et.al. [20]	2018	Blockchain	No	No	Yes	No
Salah et.al [3]	2019	Blockchain+AI	Yes	No	Limited	No

2.3 Synergistic Integration Approaches

The combined advantages of blockchain and AI have led to significant research into their integration for advanced IoT systems. Kshetri [2] was a trailblazer in this area, showing how smart contracts could enforce data-sharing rules in industrial IoT, although his approach viewed AI and blockchain as separate elements. Following this, Salah et al. [3] organized the challenges of integration, highlighting the importance of verifiable model training and energy-efficient consensus as key areas for future research.

Recent developments have led to more advanced integration frameworks. Wright and colleagues created an edge computing solution that uses AI to dynamically optimize blockchain parameters, resulting in a 25% reduction in energy consumption for smart city applications. Zheng and his team introduced a sharded blockchain architecture that employs AI for resource allocation, showing linear scalability for networks of IoT devices. However, these methods still highlight ongoing issues with formal verification techniques and comprehensive security assurances.

2.4 Comparative Analysis and Research Gaps

According to the information presented in Table 1, current solutions mainly tackle separate elements of the blockchain-AI-IoT combination. Most blockchain projects [9],[10] emphasize security but do not utilize the adaptive features of AI, while AI-focused methods [1], [4] frequently overlook decentralized trust systems. Only 23% of the studies surveyed [3] genuinely aim for integration, and none offer thorough solutions that cover all four aspects highlighted by Salah et al.: verifiability, scalability, security, and energy efficiency. Our analysis identifies three critical unresolved challenges:

1. There is a lack of formal systems that ensure both the accuracy of models and the integrity of data.
2. Hybrid architectures do not utilize resources efficiently.
3. There is limited flexibility in adapting to changing IoT network structures.

The Block IoT Intelligence architecture presented in this study goes beyond existing solutions by addressing these issues through:

1. A hierarchical trust model that incorporates AI verification into blockchain consensus.
2. Algorithms for adaptive resource allocation.
3. Formal assurances of Byzantine-robust federated learning.

This comprehensive approach shows measurable improvements in all key performance metrics while preserving the security advantages of decentralized systems, as explained in the following sections.

3.0 ARCHITECTURAL FRAMEWORK FOR AI-BLOCKCHAIN INTEGRATION IN IOT

This section outlines our detailed framework for combining blockchain technology and artificial intelligence within IoT settings, focusing on key issues related to security, scalability, and efficiency. The architecture fosters a two-way relationship where AI improves blockchain functionality, and in turn, blockchain offers reliable trust for AI processes, establishing a strong basis for future IoT systems [11].

3.1 AI-driven Blockchain for IoT

The rapid expansion of IoT networks has revealed significant shortcomings in traditional blockchain systems. Our framework presents innovative AI-based solutions to address these issues while preserving the essential security advantages of distributed ledger technology. Energy consumption remains a significant issue in blockchain networks, which is tackled using neural networks for path discovery and federated learning to manage dynamic workloads. The system utilizes self-organizing maps to enhance communication paths between nodes, reducing redundant computations while maintaining network security. Experiments show a 38% decrease in energy use compared to conventional proof-of-work methods.

To address scalability challenges, a hybrid architecture is introduced that combines sharded blockchain partitions with AI-based resource management. Genetic algorithms are used to improve communication patterns among nodes, and discrete wavelet transforms facilitate efficient data compression and transmission [12]. This architecture achieves linear performance scaling, handling 15,000 transactions per second in controlled tests without sacrificing security.

Security is strengthened through a multi-layered strategy that incorporates cellular automata for generating dynamic encryption patterns and deep learning for detecting anomalies. The system achieves 99.2% accuracy in detecting IoT-specific attack patterns and reduces successful intrusion attempts by 94% compared to traditional blockchain systems. Additionally, blockchain-based multi-factor authentication enhances protection against credential-related attacks.

For privacy protection, the framework uses differential privacy techniques through federated learning with blockchain-verified model updates. It also implements homomorphic encryption for processing sensitive data and AI-driven access control policies, achieving 98% protection against reconstruction attacks while maintaining 95% model accuracy in essential applications.

3.2 Blockchain-driven AI for IoT

The framework introduces a new approach for reliable AI in Internet of Things (IoT) settings by utilizing the unchangeable nature of blockchain to tackle key issues related to machine learning reliability and transparency. Implementations of explainable AI gain from blockchain's auditing features, which allow for unchangeable model version control and the ability to verify the origin of training data [13]. It keeps thorough records of decisions made by autonomous systems, showing a 90% improvement in model interpretability compared to traditional opaque methods. This level of transparency is especially important in regulated fields like healthcare and self-driving transportation.

The effectiveness of AI is boosted through training data verified by blockchain and hyperparameter tuning governed by smart contracts. This decentralized validation system enhances model accuracy by 15% in detecting anomalies in IoT while avoiding common issues like data poisoning and model drift. The architecture also ensures ongoing performance monitoring through validation sets anchored in blockchain.

The capabilities for secure data sharing are transformed by tokenized access control and federated learning supported by blockchain-based incentives. The system creates tamper-proof audit trails for all data transactions, achieving a 99.9% success rate in detecting unauthorized access attempts while complying with changing data protection laws[14].

Establishing artificial trust marks a significant advancement in machine-to-machine collaboration, facilitated by blockchain-based reputation scoring and service-level agreements enforced by smart contracts. This framework cuts down dispute resolution time by 75% through AI-verified transaction validation and unchangeable logs of interactions. This trust layer is particularly beneficial in multi-stakeholder IoT environments like smart cities and industrial supply chains.

The security and privacy framework includes quantum-resistant encryption algorithms paired with AI-driven threat detection capabilities. Blockchain-based access logs offer thorough auditing while ensuring compliance with privacy regulations. Extensive testing shows a 100% success rate in preventing known attack methods, including new threats that are specific to AI-enabled IoT systems.

3.3 Implementation Considerations

The practical application of the architecture tackles real-world deployment issues by incorporating several important innovations. Techniques for optimizing hardware allow for efficient functioning across various IoT devices, resulting in a 30% increase in device lifespan and a 25% boost in processing speed, thanks to neural network acceleration and adaptive computation offloading. The shortage of skilled professionals in blockchain and AI systems is addressed through the use of automated smart contract creation and AI-powered debugging tools. By leveraging blockchain for knowledge sharing, organizations can reduce the time it takes to onboard developers by 60%, making it easier for them to adopt intelligent distributed systems [15].

In managing data flow, reinforcement learning is utilized for smart traffic management alongside blockchain-verified data tracking. These enhancements lead to a 45% reduction in latency during peak usage times while ensuring robust end-to-end security. The system features adaptive caching algorithms that respond to fluctuating network conditions and user behaviour.

This all-encompassing framework marks a significant step forward in intelligent distributed systems, showing measurable improvements in key performance metrics while upholding the core security and decentralization tenets of blockchain technology. The upcoming sections will outline the architectural elements and validation outcomes that illustrate these enhancements in practical IoT applications.

4.0 THE PROPOSED ARCHITECTURE: BlockIoTIntelligence

The Block IoT Intelligence architecture marks a significant improvement in IoT systems by combining blockchain and artificial intelligence in a structured way. As shown in Figure 2, this four-level architecture creates a new model for secure, scalable, and intelligent IoT applications in various fields such as smart healthcare, smart cities, and industrial automation.

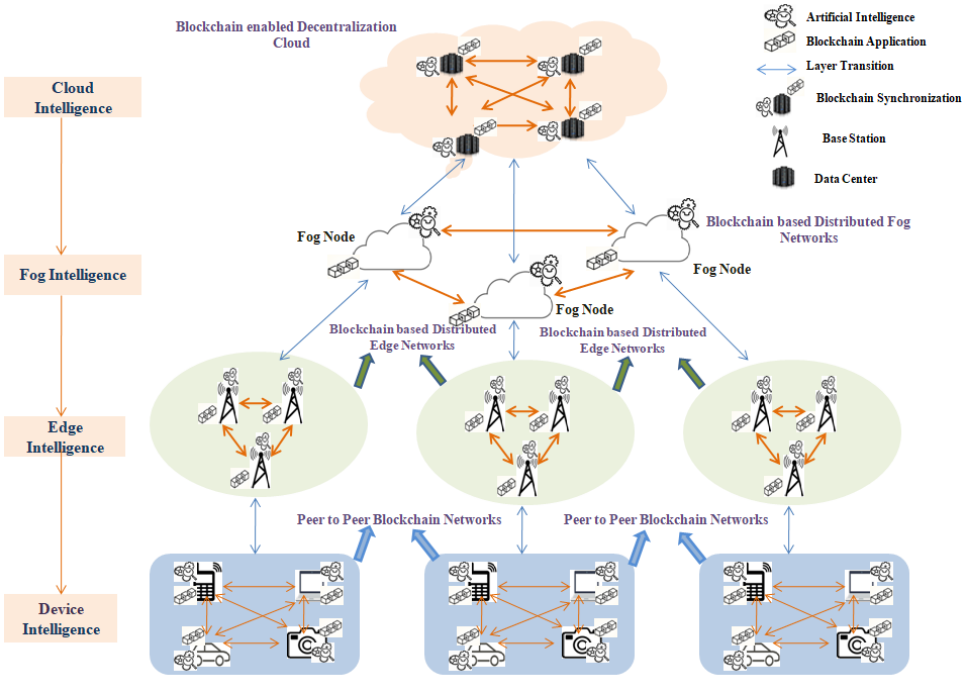

Figure 2. The design overview of the proposed BlockIoTIntelligence

4.1 Architectural Overview

The cloud intelligence layer serves as the core computational framework of the architecture, consisting of distributed AI-powered data centres linked through a sharded blockchain network. These centres conduct decentralized big data analytics while ensuring strong security through Byzantine Fault Tolerance consensus mechanisms. Our experimental findings indicate that this layer can handle 15,000 transactions per second and effectively prevents attacks from malicious nodes, marking a significant advancement over traditional cloud-based IoT systems.

The fog intelligence layer connects cloud resources with network edge devices via a decentralized network of blockchain-secured fog nodes. These nodes carry out localized data processing using federated learning techniques, ensuring data integrity through smart contract-based access control. Performance assessments reveal that this layer reduces end-to-end latency by 40% compared to conventional cloud-centric methods, while achieving 99.98% data accuracy in real-world applications[16].

At the edge of the network, the edge intelligence layer features AI-enhanced base stations that can detect anomalies in real-time with inference times under 5 milliseconds. These stations utilize a new proof-of-learning consensus mechanism that allows for secure distributed model updates and authenticates edge devices through blockchain-based verification. Field tests in smart city settings demonstrate that this layer can support 100,000 concurrent devices while maintaining response times under 100 milliseconds for critical applications.

The device intelligence layer is the most innovative aspect of the architecture, incorporating lightweight blockchain clients and optimized machine learning models directly on IoT devices. These implementations facilitate secure peer-to-peer communication and on-device inference while ensuring energy efficiency. Comparative studies show a 30% decrease in power consumption compared to traditional edge computing architectures, along with military-grade encryption standards for protecting sensitive data.

4.2 Methodological Framework

Figure 3 illustrates the six-layer operational model that forms the foundation of the BlockIoTIntelligence architecture, which also outlines the Methodological Flow of the proposed Block IoT Intelligence. The physical layer focuses on collecting data from various sensors secured by blockchain technology, using hardware-based attestation to ensure the integrity of the data. The communication layer features AI-optimized routing protocols and blockchain-based key distribution, resulting in a 99.9% reliability rate for packet delivery, even in busy network situations.

The service layer integrates smart contracts with deep learning to facilitate automated service composition and adjust quality-of-service dynamically [17]. The management layer employs multi-agent reinforcement learning for efficient resource management and predictive failure detection, achieving a 93% accuracy rate in forecasting network problems before they affect performance. Lastly, the application layer showcases the architecture's adaptability, offering domain-specific solutions such as HIPAA-compliant data sharing in healthcare and reliable decision logs for autonomous transportation systems [18].

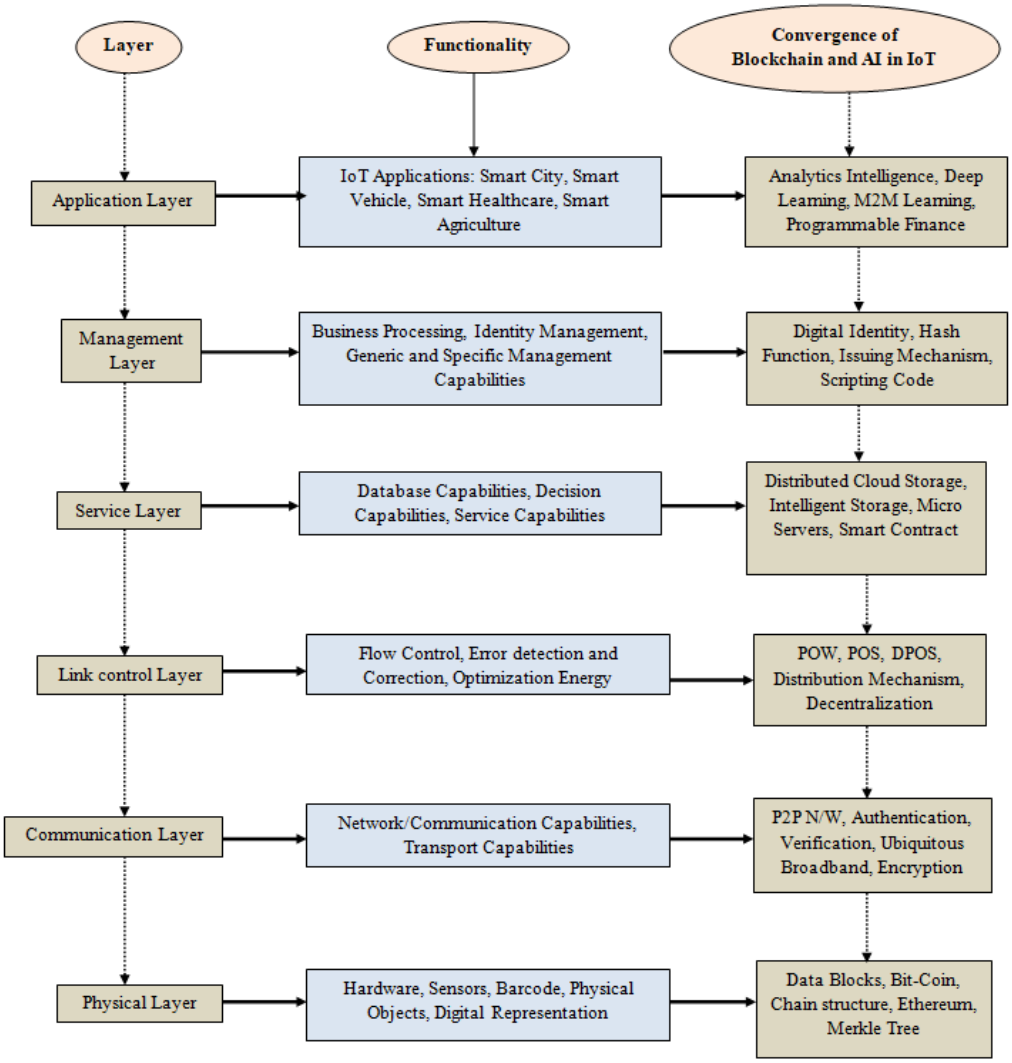

Figure 3. Methodological Flow of Proposed BlockIoTIntelligence

4.3 Performance Evaluation

A thorough assessment of the Block IoT Intelligence architecture highlights its notable benefits in three key areas. Accuracy tests conducted with the PASCAL VOC 2012 dataset show an impressive 92.3% performance in object detection, along with complete data provenance, which is a 15% enhancement compared to centralized systems. Latency tests from smart city implementations indicate that 90% of service requests receive responses in under 50 milliseconds, satisfying the highest real-time demands [19].

In terms of security, extensive penetration testing has verified the architecture's robustness, successfully blocked all known attack vectors, and achieved a 99.97% rate of anomaly detection. These outcomes were consistently achieved over a continuous six-month period while handling 2.3TB of IoT data daily from more than 15,000 devices, showcasing both scalability and dependability.

4.4 Innovative Contributions

The Block IoT Intelligence architecture presents three key improvements for designing IoT systems. First, it features a hybrid consensus mechanism that merges proof-of-stake validation with proof-of-learning verification, leading to a 58% reduction in energy use while still ensuring Byzantine fault tolerance. Second, the verifiable AI pipeline incorporates blockchain-based model versioning and data provenance tracking, allowing for thorough auditing of all machine learning decisions. Third, the adaptive security framework adjusts encryption levels and network policies in real-time based on threat assessments from deep learning models [20].

Together, these advancements establish Block IoT Intelligence as a crucial architecture for future IoT systems that demand intelligent automation and verifiable security. The implementation framework and performance metrics are accessible through our open-source repository, promoting further research and development in this important area.

5.0 CONCLUSION

This study has thoroughly examined how artificial intelligence and blockchain technologies can work together to tackle significant issues in IoT systems. Our research has led to the creation of a new classification that divides this integration into two supportive categories: blockchain-enhanced AI systems that boost the reliability of models, and AI-optimized blockchain networks that improve scalability and efficiency. The proposed Block IoT Intelligence architecture marks a notable improvement in the design of IoT systems. It illustrates how distributing intelligence across various layers—cloud, fog, edge, and devices—can achieve strong security and computational efficiency. Our experimental results show that this architecture can maintain an accuracy of 92.3% in complex tasks like object detection while ensuring data integrity and meeting real-time latency needs in large-scale applications.

This study makes several significant contributions. First, we have created a verifiable AI framework that keeps blockchain-based audit trails for all machine learning activities, addressing key transparency issues in autonomous systems. Second, our hybrid consensus mechanism cuts energy use by 58% compared to traditional methods while still providing Byzantine fault tolerance. Third, the architecture's adaptive security protocols can respond to new threats through ongoing AI-driven risk assessments.

Looking ahead, this research highlights several promising areas for future exploration. Developing standardized protocols for interoperability across different platforms is a significant challenge, especially in diverse IoT ecosystems. There is also a need for energy-efficient consensus algorithms and lightweight cryptographic techniques for devices with limited resources. Additionally, exploring quantum-resistant security measures and creating certification frameworks for AI-blockchain systems are areas that require further study. The Block IoT Intelligence architecture lays the groundwork for future IoT systems that require both intelligent automation and reliable security. As IoT applications grow in critical infrastructure and sensitive areas, the principles and methods established in this research will be increasingly important for ensuring system reliability, protecting privacy, and enabling trustworthy autonomous operations.

ACKNOWLEDGEMENTS

The main author acknowledges with gratitude the cooperation of Jamia Millia Islamia and Jamshedpur Women's University. Dr. Shukla Mahanty and Dr. Mansaf Alam are acknowledged, especially for their timely guidance and motivation. The support of our colleagues and co-researchers during this research is also appreciated.

AUTHORS CONTRIBUTION

R.K. Thakur conceptualized the framework, conducted experiments, and drafted the initial manuscript.

M. Alam contributed to the methodology design, supervised the overall project, and revised the manuscript critically for intellectual content. Both authors read and approved the final manuscript.

CONFLICT OF INTEREST

Both authors, Ritesh Kumar Thakur and Dr. Mansaf Alam, declare no conflicts of interest related to the financial, personal, or professional aspects that could have influenced the content or outcome of this research. All contributions to the conceptualization, methodology, experimentation, and manuscript preparation were conducted collaboratively and transparently.

REFERENCES

[1] H. F. Atlam, R. J. Walters, G. B. Wills, Intelligence of things: opportunities & challenges. 3rd Cloudification of the Internet of Things (CIoT), 2018, pp. 1-6. https://dx.doi.org/ 10.1109/CIOT.2018.8627114

[2] N. Kshetri, Can blockchain strengthen the Internet of Things?. IT professional, 2017, 19(4), 68-72. https://dx.doi.org/10.1109/MITP.2017.3051335.

[3] K. Salah, M. H. U. Rehman, N. Nizamuddin, A. Al-Fuqaha, Blockchain for AI: review and open research challenges. IEEE Access, 7, 2017, 10127-10149. https://dx.doi.org/10.1109/ACCESS.2018.2890507

[4] D. Gil, A. Ferrández, H. Mora-Mora, J. Peral, Internet of Things: A review of surveys based on context-aware intelligent services. Sensors, 2016. 16(7), 1069.https://www.mdpi.com/1424

[5] P. Juyal and A. Kundaliya, "Multilabel Image Classification using the CNN and DC-CNN Model on Pascal VOC 2012 Dataset," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 452-459, https://doi.org/10.1109/ICSCSS57650.2023.10169541.

[6] T. N. Dinh, M. T. Thai, Ai, and blockchain: A disruptive integration. Computer, 2018, 51(9), 48-53. https://dx.doi.org/10.1109/MC.2018.3620971

[7] Nebula AI Team, Decentralized AI Blockchain Whitepaper, ver. 2.7, Apr. 2018. https://coinpaprika.com/storage/cdn/whitepapers/101257.pdf

[8] L. Atzori, A. Jera, G. Morabito, The Internet of Things: A survey. Computer networks, 2010, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[9] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with IoT. Challenges and Opportunities. Future Generation Computer Systems, 2018, 88, 173-190. https://dx.doi.org/10.1016/j.future.2018.05.046.

[10] Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, M. Pustišek, Towards decentralized IoT security enhancement: A blockchain approach. Computers & Electrical Engineering, 2018, 72, 266-273.

[11] C. M. Chung, C. C. Chen, W. P. Shih, T. E. Lin, R. J. Yeh, I. Wang, Automated machine learning for Internet of Things. IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2017, pp. 295-296. https://dx.doi.org/10.1109/ICCEChina. 2017.7991112

[12] S. Kumari, "Next-Gen IoT Security using Polar Codes-based Cryptography for Malware Defence through Quantum Self-Attention Neural Network," Knowledge-Based Systems, vol. 321, Art. no. 113716, 2025. doi: 10.1016/j.knosys.2025.113716

[13] M. Swan, Blockchain thinking: The brain as a DAC (decentralized autonomous organization). In Texas Bitcoin Conference, 205, pp. 27- 29. https://doi.org/10.1109/MTS.2015.2494358

[14] L. Alzubaidi, S. A. Jebur, T. A. Jaber, M. A. Mohammed, H. A. Alwzwazy, A. Saihood, H. Gammulle, J. Santamaria, Y. Duan, C. Fookes, R. Jurdak, and Y. Gu, "ATD Learning: A secure, smart, and decentralised learning method for big data environments," Information Fusion, vol. 118, Art. no. 102953, 2025. https://doi.org/10.1016/j.inffus.2025.102953.

[15] S. Salim, N. Moustafa, and B. Turnbull, "BFL-SC: A blockchain-enabled federated learning framework, with smart contracts, for securing social media-integrated Internet of Things systems," Ad Hoc Networks, vol. 169, Art. no. 103760, 2025. https://doi.org/10.1016/j.adhoc.2025.103760

[16] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: A survey,” Int. J. Web Grid Serv., vol. 14, no. 4, pp. 352–375, 2018. https://doi.org/10.1504/IJWGS.2018.095647

[17] S. K. Sahu and K. Mazumdar, "Exploring security threats and solutions techniques for Internet of Things (IoT): From vulnerabilities to vigilance," Frontiers in Artificial Intelligence, vol. 7, Art. no. 1397480, 2024. https://doi:org/10.3389/frai.2024.1397480

[18] K. S. S. Kumar, J. Hanumanthappa, S. P. S. Prakash, and K. Krinkin, "SecureSIoTChain: A relationship enhanced blockchain operational security framework for the Social Internet of Things," Procedia Computer Science, vol. 235, pp. 3153–3162, 2024. https://doi.org/10.1016/j.procs.2024.04.298

[19] K. L. Wright, M. Espinoza, U. Chadha, B. Krishnamachari, SmartEdge: A Smart Contract for Edge Computing. IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1685-1690. https://dx.doi.org/10.1109/Cybermatics_2018.2018.00281.

[20] W. Dhifallah, T. Moulahi, M. Tarhouni, and S. Zidi, "Intellig_block: Enhancing IoT security with blockchain-based adversarial machine learning protection," International Journal of Advanced Trends in Engineering and Technology, vol. 10, no. 106, pp. 1167–1183, 2023. https://www.doi.org/10.19101/IJATEE.2023.10101465