Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

AI-Driven Blockchain Framework for Secure and Efficient IoT Data Analysis

Dr.V. Saidulu[1], Dr. C. Vijayalakshmi[2], Dr.A. Deepa[3], G. Rajakumar[4], Anitha Jaganathan[5]

[1]Assistant Professor, ECE Department, Mahatma Gandhi Institute of Technology, JNTUH University, Hyderabad. vsaidulu_ece@mgit.ac.in
[2]Assistant Professor (Senior Grade), Department of Computer Science and Engineering, B S Abdur Rahman Crescent Institute of Science and Technology, Chennai – 600048. vijayalakshmi@crescent.education
[3]Associate Professor, Department of Computer Science and Engineering, School of Computing, Sathyabama Institute of Science and Technology, Chennai. nraj.deepa@gmail.com
[4]Assistant Professor, Department of Computer Science and Engineering, Chennai Institute of Technology, Chennai. ka.rajakumar@gmail.com
[5]Assistant Professor, Department of Artificial Intelligence and Data Science, Panimalar Engineering College, Chennai. anitha@panimalar.ac.in

ARTICLE INFO

Received: 30 Dec 2024

Revised: 05 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

With the advent of the Internet of Things (IoT), which is used to link a vast number of intelligent and self-sufficient devices for a variety of purposes, ubiquitous computing has become a reality. Big data analytics greatly benefits from artificial intelligence, which provides precise data analysis instantly. However, there are certain problems with confidentiality, safety of training data, and centralized architecture when using artificial intelligence to build large data analyses. This article proposes a blockchain-based IoT architecture with AI, showcasing the combination of AI and blockchain for Internet of Things applications. Both qualitative and quantitative measurements are used to assess the suggested architecture's performance. In terms of qualitative evaluation, the explanation of Artificial-oriented BC as well as BC-oriented AI clarifies how blockchain technology and AI work together to address various issues. The performance of the proposed AI-BC IoT Framework structure is evaluated and compared with existing qualitative measuring techniques. According to the experimental analysis, the suggested framework outperforms the current cutting edge methods.

Keywords: Blockchain, the Internet of Things (IoT), Data analysis, Artificial intelligence (AI), Qualitative measuring techniques.

INTRODUCTION

The Internet of Things (IoT) is primarily aided by 6G, the sixth-generation wireless communication standard and technology. With the development of 6G interaction a number of novel innovations have surfaced to enhance the customer experience by providing seamless connectivity and high quality-of-service (QoS) [1]. The Internet of Everything (IoE), device-to-device (D2D) connections, and machine- to-machine, or M2M, connections are among the technologies created within the auspices of 5G networks. Unmanned aerial vehicle (UAV) access point use has recently been investigated as a potential option for delivering service on-demand for 6G networks. The traditional network architecture can be supported by the UAV base stations' ability to ad hoc connect to ground users. These issues are resolved by integrating blockchain and AI for IoT into a decentralized database framework. Additionally, techniques facilitated by artificial intelligence (AI) were additionally proposed to enhance 6G networks' quality of service (QoS) [2]. In order to do this, a lot of effort has been put into optimizing 6G-enabled wireless networks through AI; however, less focus has been placed on optimizing AI models' device-level resources, particularly for applications in UAVs. As a result, AI-driven 6G networks will take advantage of the opportunities presented by the previously described technologies to create new applications [3].

Blockchain technology offers a distributed, safe, and decentralized network. In blockchain technology, every node has connectivity in a decentralized peer-to-peer fashion, allowing transactions to be shared without external intervention and promptly recorded with timestamps. For industries including finance, security, healthcare, and agriculture, the blockchain approach offers an effective solution [4]. Cryptographic hashing is used to further bind and secure the data that is available in blocks in links with digital signs. Because each block is related to the previous block, hackers cannot introduce harmful input to the system to hijack transactions. These issues are resolved by integrating blockchain and AI for IoT into a decentralized database framework. When distributing the transaction with anyone else in a network, it must be safe, digitally signed, unchangeable, verified, and explicable [5]. Most industries, including healthcare, smart homes, agriculture, the military, industry, autonomous vehicles, and many more, may use this kind of secure transaction.

[6] Benefits arise from the combination of artificial intelligence and the Internet of Things in terms of gathering and analyzing the most data possible. With the ongoing development of intelligent and digital technologies in recent years, artificial intelligence, blockchain, and the Internet of Things have drawn interest from a wide range of researchers and emerged as the most widely used technologies, offering novel ideas for numerous research fields [7]. For Internet of Things applications, Figure 1 shows the basic convergence of blockchain technology and AI. Concerns about privacy, latency, accuracy, and centralization are among the issues that arise when blockchain and AI are combined for Internet of Things applications [8].

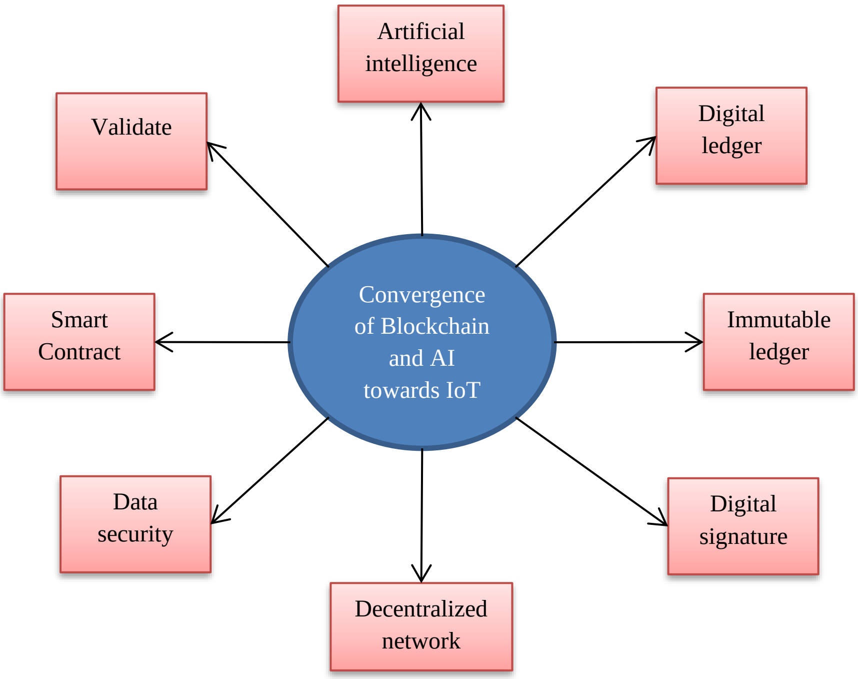

Figure 1: Blockchain and AI Integration for Internet of Things Applications

Figure 1 demonstrates the fundamentals of blockchain and AI for Internet of Things applications. This paper's primary contributions are:

- Artificial intelligence and blockchain are being researched for Internet of Things applications [9].
- A safe sophisticated blockchain architecture with four abilities is suggested in light of the benefits of combining blockchain mining and artificial intelligence. The proposed model incorporates edge, fog, cloud, and device intelligence.
- The research difficulties and their answers are summarized in this paper [10].
- The recommended method for fusing artificial intelligence and blockchain technology is provided.
- The suggested architecture is analyzed both qualitatively and quantitatively. Taking into account factors like energy usage, the delay, reliability, silence, and information security [11].

LITERATURE REVIEW

Aslam et al [12] introduced Blockchain and 6G-enabled IoT. 6G-capable A platform for fast and low-latency information gathering and processing is made possible by IoT technology. In a world with more connection, there are still problems that must be resolved, especially those related to security and privacy. Additionally, issues with device seamless integration, authentication management, the potential for a single point of failure, and significant computational expense can occasionally be ignored by the conventional centralized architecture. Strong security and privacy are required in a variety of IoT-enabled industrial applications, given the development of decentralized control systems for entry. Information sharing has altered since the advent of blockchain technology. Blockchain can remove the need for third-party authorities while establishing trust in a distributed, safe platform. For the majority of infrastructure providers, the combination of these two technologies depends on regulatory adaptation. We contend that scalability, storage of data security, as well as embedded instrument inclusion, require the study's interest and collaborative efforts to guarantee that both websites (6G-enabled IoT and blockchain) work efficiently together, even though recent research concentrates on the problems with common agreement along with mining algorithms for blockchain-enabled systems.

Sharma et al [13] suggested sustainable smart cities: convergence of artificial intelligence and blockchain. Big data analytics greatly benefits from artificial intelligence, which provides precise data analysis instantly. However, there are certain problems with safety, confidentiality of training data, and centralized architecture when using artificial intelligence to build large data analyses. This article proposes a blockchain-based IoT architecture with AI, showcasing the combination of AI and blockchain for Internet of Things applications. The performance of the recommended architecture is evaluated using qualitative as well as quantitative metrics. In terms of qualitative evaluation, the explanation of Intelligent-oriented BC and BC-oriented AI clarifies how blockchain technology and AI work together to address various issues. Experiments show that combining blockchain technology with artificial intelligence effectively tackles the difficulties in achieving high security and accuracy as well as low latency through decentralized networks. Accuracy, latency, and security issues are successfully resolved by combining blockchain technology with artificial intelligence; however, the suggested framework did not entirely address the processing power problem.

Li et al. [14] proposed Blockchain-based data security for artificial intelligence applications in 6G networks. Using algorithmic thinking (AI) to facilitate the rapid and intelligent development of network functions is the concept behind 6G network architecture. Large-scale data processing, including computation, analysis, and storage, is an inevitable part of intelligent services. Consequently, the information could be vulnerable to modification or contamination by unauthorized individuals. In this research, we propose a privacy protection strategy based on blockchain for AI applications in 6G networks. The 6G architecture, which stands for space-air-ground-underwater interconnected network, is specifically what we start with. In the context of 6G, we then discuss two AI-enabled applications: interior environments and driverless cars. Using a case study of an indoor navigation system, we demonstrate the effectiveness of distributed ledger technology in data security. The outcomes of the simulation demonstrate how resistant blockchain data is to manipulation. Furthermore, we have identified a number of possible lines of inquiry.

Zawish et al [15] presented on-device AI and blockchain for 6g-enabled agricultural supply chain management. 6G aims to improve the network's quality-of-service (QoS) and guarantee the best possible use of its resources with artificial intelligence (AI)-powered solutions. To ensure traceability, transparency, and the tracking of inventory and contracts, In this paper, we propose a blockchain, AI, and UAV-based farming supply chain administration architecture in combination. We provide a method to enable on-device AI by generating an outline of algorithms with various resource-accuracy trade-offs. Using photos taken by the UAV, a convolutional neural network (FCN) model is employed to estimate biomass. We encourage the use of incremental pruning to produce numerous task-specific models with varying complexities and accuracy in place of a single condensed FCN model to facilitate deployment on UAVs. A convolutional neural network (FCN) emulation is used for estimating biomass production from UAV-captured pictures. Instead of using a single compacted FCN model to make deployment on UAVs easier, we recommend using incremental pruning to generate many task-specific models with different complexities and accuracy.

Puri et al [16] introduced an artificial intelligence-powered decentralized framework for the Internet of Things in Healthcare 4.0. Transactions on Emerging Telecommunications Technologies, 35(4), e4245. Due to their improved access to affordable healthcare services, distant monitoring of patients and data administration have become increasingly popular in recent years. Numerous options for gathering patient data are available with a cloud-based healthcare system, which also gives patients and healthcare professionals well-managed reports whenever they need them. To address these issues, this paper suggests a decentralized healthcare framework powered by artificial intelligence (AI) that can access and authenticate Internet of Things (IoT) devices and foster transparency and confidence in patient healthcare records (PHR). The technique is based on AI-enabled smart contracts and a general blockchain protocol notion. The system's intriguing IoT nodes are identified by this methodology. The real-time test environment is used for the experimental investigations, and notable enhancements are recommended in terms of transaction cost, average latency, throughput, data request time, and device energy consumption. The suggested framework is tested in a real-time environment, and its performance is assessed in terms of transaction throughput, average latency, gas consumption, device energy consumption, and the amount of time needed to originate and register requests.

PROPOSED METHODOLOGY

Images taken by UAVs are utilized to estimate biomass using a network of convolutional neural networks (FCN) models. Instead of using a single condensed FCN simulation to make deployment on UAVs easier, we recommend using incremental pruning to generate many task-specific models with different complexities and accuracy. A suggested design illustrates how the integration of BC and AI addresses massive data analysis, centralization concerns, and security difficulties. A massive quantity of data is produced by several diverse smart gadgets and devices. However, the network contributors are unaware of how the data they contribute to the internet service provider is being used. Furthermore, large amounts of network bandwidth are needed for centralized data storage. Furthermore, it is quite difficult to provide data openness using a centralized design. In the centralized system mode, the central point of failure functions as a mystery. Another issue with centralized IoT security and performance is coordination with exterior computing facilities. Since 6G-based IoT networks are often dispersed and therefore more vulnerable to threats and attacks, establishing a high degree of safety and confidentiality in these networks is a realistic problem. It's also critical to meet the need for data privacy in free exchange systems in multi-layer 6G networks (such as data sharing amongst driverless cars).

Blockchain is a cutting-edge disruptive technology that can offer creative answers to privacy and security issues in 6G-IoT networks. The blockchain is a decentralized, transparent, and immutable database that can be handled without the need for a central authority. A peer-to-peer network architecture that grants any entity (such as Internet of Things device) equal authority to manage and approve the data stored in the blockchain makes this feasible. By combining blockchain technology with IoT, the data-sharing framework will be developed through transparency, audibility, and trustability.

Since 6G-based IoT networks are often dispersed and therefore more vulnerable to threats and attacks, establishing a high degree of privacy and safety in these networks is a realistic problem. It's also critical to meet the need for data privacy in open-sharing systems in multi-layer 6G networks (such as data sharing amongst driverless cars). Blockchain is a cutting-edge disruptive technology that can offer creative answers to privacy and security issues in 6G-IoT networks. This is made possible by a distributed network architecture that gives every entity (such a Web of Things item) the same ability to oversee and authorize the data kept in the blockchain. By combining blockchain technology with IoT, the data-sharing framework will be developed through transparency, audibility, and trustability. In such an improved architecture, information is shared on a trustworthy and traceable platform. The blockchain is a decentralized, transparent, and immutable database that can be handled without the need for a central authority. The multilayered structure of the suggested AI-BC integrated blockchain design for Internet of Things applications is shown in Figure 3. The four operational platforms that make up the suggested model are fog, cloud, edge, and intelligence at the device platform for intelligence. Several smart devices combining AI and BC implementation make up the initial platform and device deployment. Massive volumes of data are produced by this platform and sent to an external intelligence platform. The subsequent platform, called periphery intelligence, consists of a base station with an AI focus at the network's edge linked to the blockchain. Each blockchain-enabled fog node in the fog platform is made up of a base station with artificial intelligence.

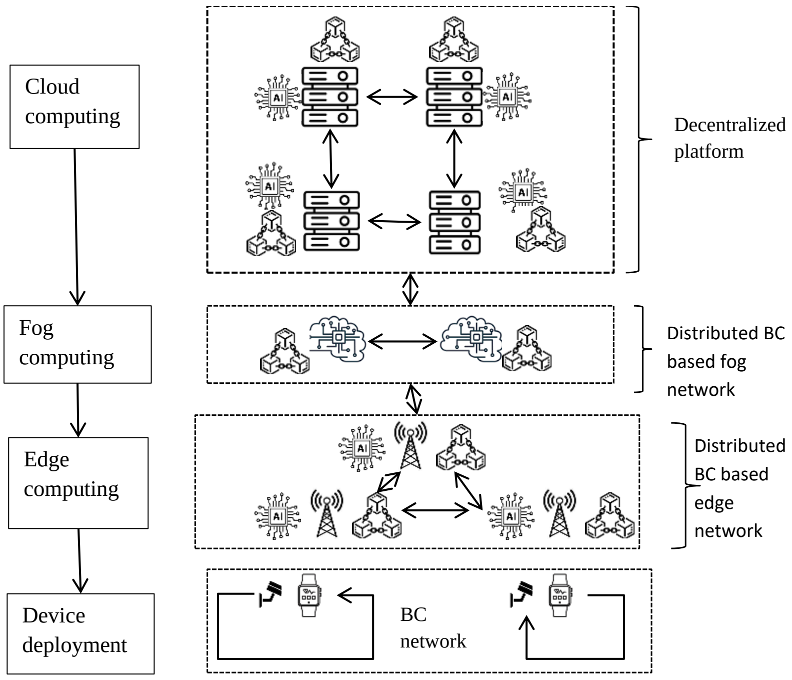

Figure 2: Architecture of Proposed System

The data flow of the proposed AI-BC architecture is depicted in Figure 2. The information flow has six operational layers. The first layer consists of a physical layer associated with the device installation stage for real-time data collection. The communication and administrative layer is responsible for edge computing. Fog computing is represented by the service and managing layer, whereas cloud computing is represented by the application layer. The physical layer of cloud computing determines variables like location, weather, brightness of light (lux), temperatures (C), and dampness (%). Numerous issues and data privacy hazards occur at the physical layer when information is transferred between specific nodes. Blockchain technology, which uses Bitcoin and Ethereum to facilitate transactions between nodes, is used in artificial intelligence to address these problems.

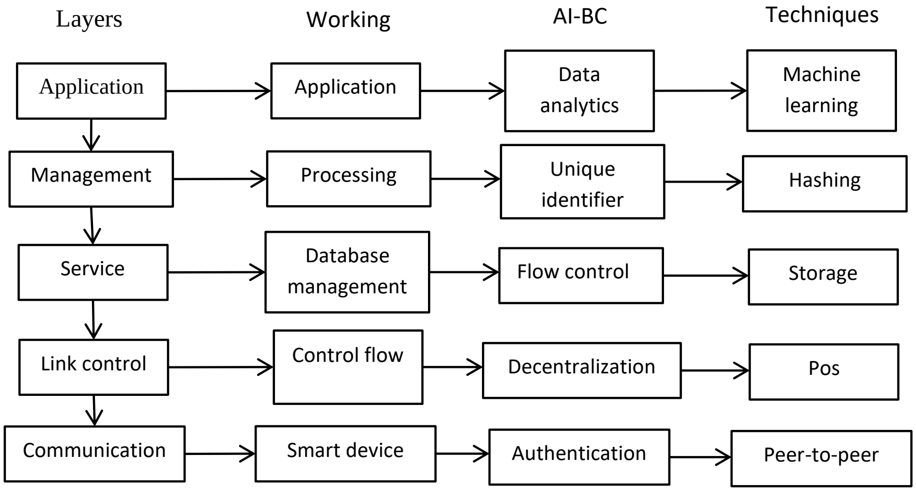

Figure 3: Flow of Proposed AI-BC architecture

This method ranks each convolutional layer's filters according to a certain scoring function, such as the l1-norm or average percentage of zeros. Usually the top-m-scored filters are retained for fine-tuning after similar scoring processes have been employed to evaluate the significance of screens for task reliability. The model is refined and pruned using this one-stage pruning method, which reduces the computational complexity for end-device deployment.

A distributed infrastructure of cloud, cognitive storage, and smart contracts is used in the blockchain integration of AI to provide secure validation at this layer. The data flow to the management layer handles data management and setting network connectivity standards for the software layer. Cryptography hashing, digital identification, and encryption codes are produced through the combination of blockchain technology and artificial intelligence. Broadcast and multicast technologies can be used to increase network capacity and greatly reduce traffic load in a multi-layered satellite communication system. Furthermore, a wide range of services are offered based on the satellite networks worldwide coverage, such as rescue efforts, mapping and transportation, and so forth. Numerous mobile aircraft types, including UAVs, drones, balloons, airplanes, and more, are part of the air network. These transportable aircraft units, which operate at various altitudes, are flying BSs. It will be necessary to strengthen the reliability of the system's physical layers in order to provide a higher level of protection than that provided by encryption technology. This should apply to a large number of devices and PCs. A sophisticated data analytics solution that guarantees privacy and security of data in the network is created by combining blockchain technology with artificial intelligence.

RESULT AND DISCUSSIONS

This section discusses the performance evaluation of the suggested system design. An independently developed Ethereum blockchain system is investigated throughout the program. Comparing the suggested framework to other current methods reveals significant differences in its basic workings. The proposed AI-BC structure in Raspberry Pi is evaluated experimentally using four metrics: accuracy, delays, and security/privacy analysis. The assessment of reliability for the object identification application is computed using 5345 instances for deep learning operations. It is discovered that as a number of border nodes increases, so does the accuracy percentage. The training sample and object detection accuracy both rise with the number of nodes contributing. To give more information about the latency improvement, the improvement in object recognition time is assessed for the entire number of edge nodes. To calculate the level of protection and privacy analysis in an IoT connected community network, the similarity index and an object's Euclidian distance are evaluated. The proportionality index value falls as the Euclidian distance increases. Consequently, the security and the decrease in the similarity index value increase privacy in IoT items.

Quantitative as well as qualitative data are used to assess the performance of the proposed architecture. To determine the benefits of integrating blockchain (BC) with machine learning for the internet of Things applications, two examples are analyzed qualitatively. The first example shows a blockchain-based artificial intelligence system for Internet of Things applications, while the second example shows a blockchain-based artificial intelligence system for IoT frameworks. Blockchain-oriented AI and blockchain-oriented AI for Network of Things applications are two examples provided in measurement metrics. Conversely, artificial intelligence (AI) improves blockchain technology by providing accurate prediction and efficient decisions for Network of Things applications. Thus, the way AI handles blockchain problems is known as the artificial intelligence-oriented blockchain, or case 1, while the way BC handles AI problems is known as BC-oriented AI, or case 2. The performance of the suggested AI-BC architecture is assessed and contrasted with the most cutting-edge methods already in use, taking into consideration a variety of parameters such as efficiency, latency, data security and secrecy, energy consumption, and computer complexity. Table 1 shows the proposed AI-Blockchain IoT system outperforming existing methods in speed, security, and efficiency.

Table 1: Analysis of the suggested system numerically

Category	**Performance indices**					
	Accuracy	**Latency (ms)**		**Energy consumption**	**Computational complexity**	
		Low	**High**		**CPU usage**	**Memory usage**
Edge computing	79	47.0	51.7	-	37.2	26
Fog Computing	70	49.5	52.8	-	77	87
Cloud	87	-	-	55	-	-

computing						
Device deployment	82	64.7	77.4	-	34.7	26

The lowest and maximum latency values are expressed in milliseconds. The reported lower and higher latency values at device deployment, and intelligence, are 34.7ms and 87ms, respectively. The measured lowest and highest latency values for edge computing are 47.0ms and 77.4ms, respectively. The measured lower and higher latency values at fog computing are 0.0ms and 12ms, respectively. To gauge security and privacy, a parallel index with the highest and lowest values is calculated. The range of 1.2 to 0.02 is where the device deployment intelligence similarity index has its highest and lowest levels. The range of the similarity index's highest and lowest values is 0.59 to 0.3 for edge computing and 0.8 to 0.1 for fog computing. CPU and memory usage are used to quantify computational complexity. The observed CPU use at unit installation intelligence ranges from 4.4% to 3.9% for IoT devices and from 29.8% for edge devices. IoT device platforms have memory usage ranging from 15.3% to 12.8%, whereas edge devices have memory usage of 35%. The observed CPU utilization at edge computing ranges from 4.7% to 5.3% for IoT devices and 26% for edge devices.

Figure 4 shows a comparison between the suggested AI-BC architecture and the most advanced methods now available for cloud computing, edge computing, fog computing, and intelligent device deployment.

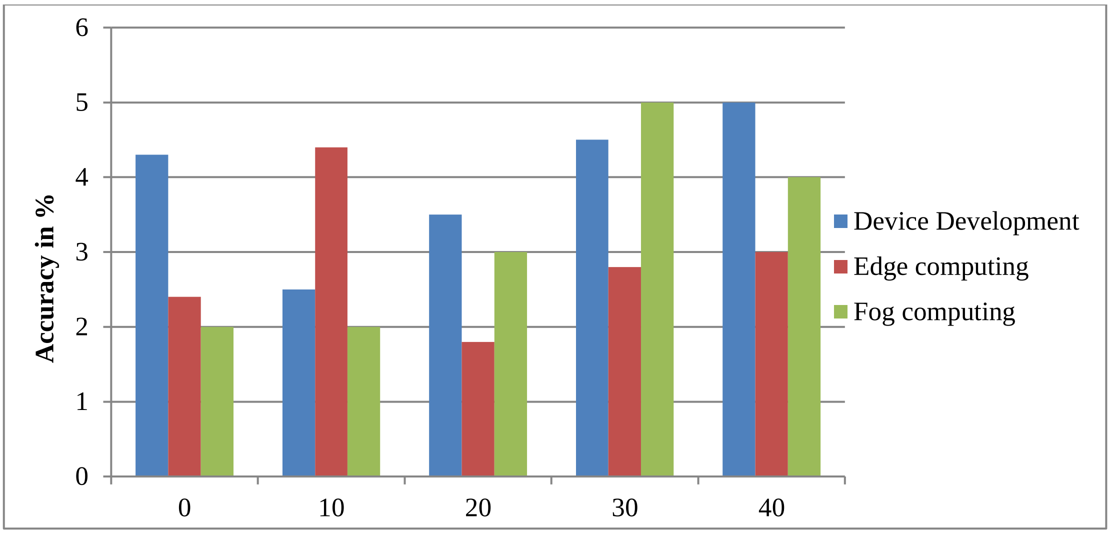

Figure 4: Accuracy comparison of the suggested integrated AI-BC

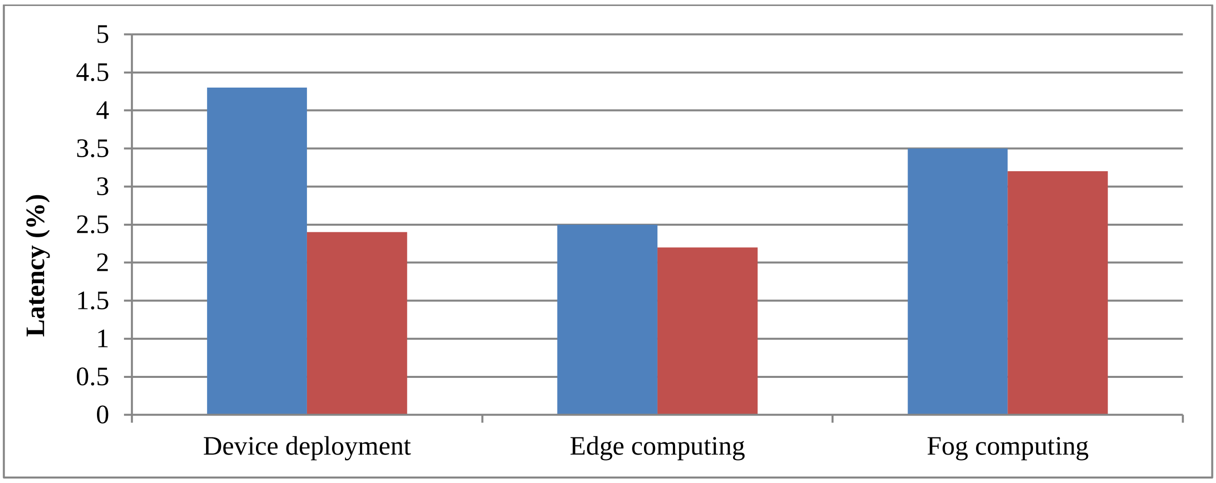

Figure 5: AI-BC's relative latency

Figure 5 displays a comparison accuracy study of the proposed combined AI-BC architecture. When using blockchain technology to deploy intelligent devices, the highest percentage accuracy is 75%. The precision, latency, and security issues are successfully resolved by the suggested approach, a safe intelligent blockchain architecture.

Secure transactions and real-time energy consumption monitoring are the main advantages of the suggested strategy. Given the vast number of connected equipment in smart city settings, the suggested system may offer complete, hence limited, and maximum access to the data contained in a single database without posing security or privacy issues. The suggested plan serves as an incentive tool that may be used to encourage people to embrace different smart city applications.

CONCLUSION

The use of blockchain technology and artificial intelligence in 6G wireless networks has been examined in this article. The architecture of 6G, a four-tier network that integrates space, air, ground, and underwater, was first shown. Achieving scalable and secure transactions in the Internet of Things at the device, cloud, fog, and edge intelligence levels was the aim of this study. Both qualitative and quantitative metrics were taken into consideration when analyzing the suggested architecture's performance. Both AI-oriented BC and BC-oriented AI were given standard taxonomy in qualitative measurement. The performance of the suggested framework with centralized and encrypted big data analytics for 6G-enabled Internet of Things apps was assessed through experimental research. The precision, latency, and security issues are successfully resolved by combining blockchain technology with artificial intelligence.

REFERENCES

[1] Singh, S. K., Rathore, S., & Park, J. H. (2020). Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. Future Generation Computer Systems, 110, 721-743.

[2] Latif, S. A., Wen, F. B. X., Iwendi, C., Li-Li, F. W., Mohsin, S. M., Han, Z., & Band, S. S. (2022). AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. Computer Communications, 181, 274-283.

[3] Mitra, A., Bera, B., Das, A. K., Jamal, S. S., & You, I. (2023). Impact on blockchain-based AI/ML-enabled big data analytics for Cognitive Internet of Things environment. Computer Communications, 197, 173-185.

[4] AlGhamdi, R., Alassafi, M. O., Alshdadi, A. A., Dessouky, M. M., Ramdan, R. A., & Aboshosha, B. W. (2022). Developing trusted IoT healthcare information-based AI and blockchain. Processes, 11(1), 34.

[5] Girija, D. K., Rashmi, M., William, P., & Yogeesh, N. (2023, May). Framework for integrating the synergies of blockchain with AI and IoT for secure distributed systems. In International Conference on Data Analytics and Insights (pp. 257-267). Singapore: Springer Nature Singapore.

[6] Kapadiya, K., Patel, U., Gupta, R., Alshehri, M. D., Tanwar, S., Sharma, G., & Bokoro, P. N. (2022). Blockchain and AI-empowered healthcare insurance fraud detection: an analysis, architecture, and future prospects. IEEE Access, 10, 79606-79627.

[7] Ahmed, A., Abdullah, S., Bukhsh, M., Ahmad, I., & Mushtaq, Z. (2022). An energy-efficient data aggregation mechanism for IoT secured by blockchain. IEEE Access, 10, 11404-11419.

[8] Rane, N., Choudhary, S., & Rane, J. (2023). Artificial Intelligence (AI) and Internet of Things (IoT)-based sensors for monitoring and controlling in architecture, engineering, and construction: applications, challenges, and opportunities. Available at SSRN 4642197.

[9] Dhar Dwivedi, A., Singh, R., Kaushik, K., Rao Mukkamala, R., & Alnumay, W. S. (2024). Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions. Transactions on Emerging Telecommunications Technologies, 35(4), e4329.

[10] Kuznetsov, O., Sernani, P., Romeo, L., Frontoni, E., & Mancini, A. (2024). On the integration of artificial intelligence and blockchain technology: a perspective about security. IEEE Access, 12, 3881-3897.

[11] Hannah, S., Deepa, A. J., Chooralil, V. S., BrillySangeetha, S., Yuvaraj, N., Arshath Raja, R., ... & Alene, A. (2022). [Retracted] Blockchain-Based Deep Learning to Process IoT Data Acquisition in Cognitive Data. BioMed Research International, 2022(1), 5038851.

[12] Pajooh, H. H., Demidenko, S., Aslam, S., & Harris, M. (2022). Blockchain and 6G-enabled IoT. Inventions, 7(4), 109.

[13] Sharma, A., Podoplelova, E., Shapovalov, G., Tselykh, A., & Tselykh, A. (2021). Sustainable smart cities: convergence of artificial intelligence and blockchain. Sustainability, 13(23), 13076.

[14] Li, W., Su, Z., Li, R., Zhang, K., & Wang, Y. (2020). Blockchain-based data security for artificial intelligence applications in 6G networks. IEEE Network, 34(6), 31-37.

[15] Zawish, M., Ashraf, N., Ansari, R. I., Davy, S., Qureshi, H. K., Aslam, N., & Hassan, S. A. (2022). Toward on-device ai and blockchain for 6g-enabled agricultural supply chain management. IEEE Internet of Things Magazine, 5(2), 160-166.

[16] Puri, V., Kataria, A., & Sharma, V. (2024). Artificial intelligence-powered decentralized framework for Internet of Things in Healthcare 4.0. Transactions on Emerging Telecommunications Technologies, 35(4), e4245.