IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cloud-Edge-Terminal Collaborated AIoT Framework Design: A Short Survey

Pavan Ashok Shanbhag[1], Preetam Divakar[2], Rohan Raju Navalyal[3], Sathvik K[4], SaiChirag B[5], and Shobha T[6]

[1,2,3,4,5,6]Department of Information Science and Engineering, BMS College of Engineering, Bangalore, India

Abstract

To overcome the demerits of Cloud Computing as well as Edge Computing, the amalgamation of both the Cloud and Edge computing methodologies are consid- ered. The ongoing trend of collaboration of AI with IoT, called Artificial Intelligence of Things, comes into the picture as it helps to resolve delays in data processing, privacy, and security issues. Studies have provided various concerns that arise when the Cloud-Edge Terminal Collaboration with AIoT possesses some already discussed issues individually. This paper helps understand the issues in detail and helps to devise a plan to design framework architecture that surpasses the flaws or drawbacks of the existing model and also discusses two important ideas to con- template the feasible design. The first idea is Asynchronous Federated Learning with Quantization for Cloud-Edge-based computing. The second idea states us- ing Mobile Edge Computing with Blockchain that is built on a Block Coordinate Descent algorithm which focuses on solving Joint Mixed-Integer and non-convex task offloading schedules, radio spectrum resource allocation as well as computing resources allocation that minimizes the energy consumption and reduces the delay in the processing of data. Several other ideas exist to solve the ongoing problems by introducing AIoT in Cloud-Edge Computing which advises the use of Blockchain technologies to increase the security and privacy of data by authenticating Terminal devices and Differential Privacy concept in a parallel way to promote the sharing of only data features rather than the actual raw data.

Keywords: AIoT, Blockchain, Cloud-Edge Computing, Differential Privacy, Blockchain, Joint Mixed Integer Schedule.

1 Introduction

Cloud communication is widespread in many applications in today’s world. The need for fast communication in a short time or less should be taken into consideration because all useful products have many disadvantages. Cloud computing is such a situation that encounters coordination problems in many connections, causing service delays and other problems. Another important issue that arises is data privacy and resource management. For this reason, the concept of edge computing has emerged with the cloud, which focuses on local data instead of global data, where limited resources are used to solve some of the problems encountered. Edge computing uses the concept of priority demand, which determines the media stream that will access the connection instead of passing the connection and causing delay. It also works on application-based communication strategies to reduce latency and increase reliability, thus reducing power consumption in end devices [1]. The next challenge we face is fast data processing and fast learning to smooth the data processing experience, which gives rise to the idea of working with the concept of AIoT, which is an important concept in the field of creating an advanced ecosystem that enables intelligence decision making. In addition, concepts such as edge offloading, asynchronous federated learning [2], mobile edge computing [3], distributed ledger [4], blockchain, and quantum blockchain [5], which can work fast and secure. An environment that overcomes all the current problems, protects data, and manages resources very effectively. This article covers most of the simple concepts used one by one, lists the main problems in design implementations, and encourages other industries related to the field. This is to recognize the framework in which all their work is built on real-world ideas. We discuss the research literature and provide details on the existing strategies used in various areas of enabling AIoT through cloud computing [6]. The main objective of this article is to explain how to measure flexibility and complexity while preserving privacy and security, keeping in mind the key concepts of the IoT era.

2 Background and Literature Overview

2.1 Cloud Computing: An Introduction

Cloud computing gives computing assets such as information capacity and preparing control to administrations without the require for client administration. Whereas the number of exchanges is diminished by utilizing a cash dissemination and installment show, cheese is too a delicious treat. There are three sorts of clamor: open commotion, private commotion, and blended commotion. Third-party benefit suppliers ordinarily advance the most proficient and compelling strategies. Private cloud computing is committed to a particular organization and gives way better security, adaptability, and control [7]. Cross breed cloud combines open and private framework to progress execution by utilizing the open cloud for transmission capacity or voice and the clamor and noise-free environment for voice. The benefits of cloud computing incorporate back for inaccessible working, more noteworthy adaptability, made strides execution and proficiency, and bolster for innovations such as counterfeit insights and quantum computing. This makes it a effective commerce instrument that gives a way for adaptability, proficiency, and advancement.

2.2 Edge Computing's Role in AIoT

Cloud computing plays a key part in the Web of Things (AIoT) by empowering proficient, centralized information handling, progressed information processing, and AI models. It organizes a part of data produced by the Web of Things and powerfully designates as- sets agreeing to necessities. Centralized cloud capacity bolsters real-time choice mak- ing by putting away and overseeing IoT information. In expansion, cloud capacity and large-scale operation makes a difference degree IoT information utilizing state-of-the-art strategies and machine learning models to make trade value [8]. It moreover makes AI models more brilliant by part the code and diminishing the improvement time of com- plex frameworks. Additionally, the coordinates cloud-edge system in AIoT moves forward information administration, asset allotment, and work conveyance, making it proficient and compelling by fathoming issues such as inactivity, electrical vitality utilization, and private information [8].

3 Collaborative Mechanism

3.1 Data Processing and Management

In cloud-edge architecture, data collection, processing, and transmission are managed across layers. End devices such as sensors and actuators collect raw data and perform initial filtering and preprocessing to reduce noise and ensure that only relevant data is passed to the next layer. The edge layer is closer to the edge device and performs more complex tasks, enabling local decision making for time-consuming applications such as detecting signs of poor health in smart pain relief. The edge layer reduces dependency on the cloud by implementing real-time analytics, thereby reducing latency and bandwidth usage. The cloud performs comprehensive analysis, long-term storage, and recognition of perfect patterns. This layer increases responsiveness, optimizes bandwidth, and im- proves latency-sensitive Internet of Things (IoT) applications. Research shows that edge computing can reduce data transfer by up to 80%, improving operational efficiency [7].

3.2 Training and Implementing the Model

Cloud-edge collaboration makes strides AI demonstrate preparing and arrangement. The cloud makes a difference share the computing control of huge datasets, counting the con- trol to construct complex models like profound neural systems. This demonstrate is at that point sent to the edge for neighborhood reflection, decreased inactivity, expanded strength, and decreased arrange reliance. Innovations like state learning have made a difference gadgets collaborate to share worldwide measures without sharing crude infor- mation, tackling security and transfer speed issues [9]. This approach empowers adjust- ment to changes in the environment, such as vehicle upkeep and work robotization, by supporting modern models. The system equalizations execution, inactivity, and opera- tional effectiveness by preparing information at the edge for moment bits of knowledge and utilizing cloud assets for optimization.

3.3 Offloading Tasks and Allocating Resources

Effective allocation and outsourcing of resources in the cloud optimizes computing perfor- mance and minimizes energy consumption by spanning tasks according to device capac- ity, network bandwidth, and latency conditions. The edge layer handles latency-sensitive tasks to ensure immediate response, while the cloud manages intensive services such as deep analytics and AI model training. Adaptive resource management dynamically adjusts processing placement to prioritize edge computing to maintain consistent per- formance during network changes. Energy-saving techniques can extend the lifetime of devices, especially batteries in IoT systems. This process reduces latency, optimizes bandwidth, improves data privacy, and increases performance, supporting applications such as healthcare, smart grids, and agriculture, while laying a solid foundation for the advancement of AIoT technology [10].

4 Significant Strategies in Existing Research for Cloud- Edge Terminal Collaboration with AIoT

4.1 Overview of the Cloud-Edge-Terminal Architecture

The cloud, edge, and edge devices form a distributed computing architecture where each layer works specifically to improve data processing, latency, and scalability. Terminals such as sensors collect data and send only the essential information to the edge or cloud for further processing. Edge devices close to the data source handle tasks such as prepro- cessing and filtering to achieve faster local responses, while the cloud handles complex tasks that require the use of global data. This collaboration increases productivity and enables efficient use of resources in the system [2].

4.2 Asynchronous Federated Learning with Quantization

Asynchronous Federated Learning (AFL) tackles the heterogeneity of edge nodes while en- suring data privacy and participant security. Various privacy techniques such as Laplace and Gaussian methods improve data security by obfuscating individual details. Fixed- point quantization reduces storage requirements and enhances neural network training efficiency by suppressing noise [11]. Aggregation modeling preserves privacy by sharing non-raw information through combining participants' parameters or outputs into global models. While centralized FL relies on servers for aggregation, decentralized FL uses peer-to-peer aggregation, thus improving scalability and efficiency. This process supports learning by optimizing the model, reducing communication overhead, and improving se- curity [12].

4.3 Mobile Edge Computing with Blockchain

Mobile Edge Computing (MEC) helps solve the aforementioned issues by offloading computing tasks to edge servers. By offloading workloads from clients to servers, ser- vice quality is improved, such as reducing energy consumption and increasing efficiency. Blockchain technology is seen as the ultimate solution to trust issues. Unlike digital business models that rely on national trust companies, blockchain uses community-based proof-of-concept to synchronize and distribute data streams across multiple nodes [13].

5 Addressing Key Issues in AIoT Frameworks

5.1 Delays in Data Processing

For IoT applications that need to make decisions quickly, real-time processing is cru- cial because relying only on cloud analysis may result in latency issues. By permitting localized data processing, Asynchronous Federated Learning (AFL) and Mobile Edge Computing (MEC) reduce latency. IoT devices can train models locally and update them asynchronously thanks to AFL, which also improves scalability, lowers latency, and enhances data security by storing sensitive data on devices. MEC further reduces reliance on the cloud by processing data at the edge, reducing network congestion, and facilitat- ing real-time responses for critical applications such as automation and healthcare. In dynamic and resource-constrained environments, both technologies improve efficiency, privacy, and reliability [14].

5.2 Security and Privacy Concerns

Blockchain technology and differential privacy are used to improve security in AIoT sys- tems by mitigating the risks of unauthorized access and data breaches during data trans- mission. Blockchain provides enhanced authorization, decentralized, tamper-resistant storage, and protection against data breaches by reducing single points of failure, all of which contribute to safe data transfer. By introducing statistical noise, differential pri- vacy ensures anonymity while maintaining data utility, protecting sensitive data. This method safeguards machine learning models by preventing adversaries from obtaining personal data, and it complies with privacy laws such as GDPR. When combined, these actions provide a strong foundation for private and secure data processing in multi-layered AIoT environments [15].

5.3 Energy Efficiency

AIoT device energy consumption must be efficiently managed, especially in remote or energy-constrained environments. By processing and sending only the most impor- tant data, minimizing pointless transfers, and extending device lifetimes through dy- namic power adjustments, energy-aware task scheduling increases efficiency [16]. Energy- efficient AI models, microcontrollers, and sensors are examples of low-power hardware that reduce computational load and extend operation time.

Table Title: Comparison of Techniques in Cloud-Edge-Terminal Collaboration for AIoT Systems

The table illustrates a comparison among three pivotal methods utilized in Cloud- Edge-Terminal collaboration for the Artificial Intelligence of Things (AIoT). Each method demonstrates unique advancements and limitations. For example, the Asynchronous Fed- erated Learning with Quantization (AFL) method manages edge variability and ensures data privacy through differential privacy techniques, while also reducing storage needs. However, it faces challenges such as communication costs and quantization effects. Mobile Edge Computing with Blockchain (MEC) focuses on reducing energy usage by processing data at the edge and enhancing security through blockchain. On the other hand, the general Cloud-Edge-Terminal collaboration method presents an adaptable solution for dynamic systems but faces scaling and communication issues in extensive networks.

Criteria	**Asynchronous Federated Learning with Quantization (AFL)**	**Mobile Edge Computing with Blockchain (MEC)**	**General Cloud-Edge-Terminal Collaboration**
Advancements	• Handles edge node hetero- geneity. • Ensures data privacy using differential pri- vacy techniques. • Reduces storage requirements with fixed-point quantization. • Decentralized federated learn- ing improves scalability.	• Reduces latency and energy consumption by processing data at edge servers. • Enhances trust with blockchain through decen- tralized verifica- tion. • Improves task processing qual- ity. • Distributed computing opti- mizes resource utilization. • Localized edge processing mini- mizes delays. • Cloud han- dles complex operations for scalability and performance.	• Generalized re- source manage- ment. • Optimized task offloading strategies. • Cloud for scal- ability, edge for local processing.
Criteria	**Asynchronous Federated Learning with Quantization (AFL)**	**Mobile Edge Computing with Blockchain (MEC)**	**General Cloud-Edge-Terminal Collaboration**

Drawbacks	• Quantization may degrade model accuracy. • High communication costs in large-scale sys- tems. • Asynchronous updates may cause slower global model convergence.	• Blockchain adds computational overhead and in- creases latency for verification. • Requires substantial initial deployment cost and technical expertise. • Heavy reliance on robust connectivity be- tween terminals, edge, and cloud. • Security and privacy chal- lenges during data transmis- sion.	• Latency in large-scale cloud-Edge net- works. • Communication overhead for real-time pro- cessing.
Privacy and Security	• Utilizes differen- tial privacy and model aggrega- tion to enhance data security.	• Blockchain ensures tamper-resistant, de- centralized data storage and secure data transmission.	• Privacy depends on system-level encryption; terminal-level vulnerabilities may remain.
Energy Efficiency	• Quantization reduces compu- tation overhead and power con- sumption on edge devices.	• Reduces en- ergy by shifting workloads to edge servers and optimizing task processing.	• Energy-aware task scheduling optimizes device operations and resource alloca- tion.

Criteria	Asynchronous Federated Learning with Quantization (AFL)	Mobile Edge Computing with Blockchain (MEC)	General Cloud-Edge-Terminal Collaboration
Scalability	• Decentralized FL architecture promotes better scalability for large AioT net- works.	• Blockchain scal- ability depends on consensus mechanisms and node capacity.	• Scalability de- pends on cloud infrastructure and efficient edge- terminal integration.
Key Application Areas	• Privacy- sensitive IoT applications such as health- care, finance, and smart cities.	• Secure, real- time applica- tions like smart grids, supply chains, and critical infras- tructure.	• General-purpose AioT sys- tems requiring dynamic pro- cessing and scalability.

Table 1: Comparison of Techniques in Cloud-Edge-Terminal Collaboration for AIoT Systems

6 Case Studies on Leading Applications of Cloud- Edge-Terminal AIoT Collaboration

6.1 Smart Healthcare

The Internet of Medical Things (IoMT) combined with cloud-based AI roles plays a significant role in instantaneous data processing and analysis of healthcare devices. These systems can monitor health and improve disease prevention using advanced chips in medical IoT devices. Cloud computing improves data management, reduces latency, and solves network coordination issues while also incorporating edge learning capabilities and data privacy for AI applications. Future advancements, including the integration of blockchain, machine learning, and 6G networks, are expected to improve personalized healthcare[17].

6.2 Edge2Analysis: A Novel AIoT Stage for Atrial Fibrillation Acknowledgement and Discovery

Edge2Analysis is a professional AIoT platform designed to detect atrial fibrillation (AF) using edge technology, providing no latency, low power consumption, and enhanced pri- vacy. The system achieves classification accuracy of up to 90% while minimizing resource consumption and privacy risks by processing ECG signals locally. It makes personal- ized predictions based on patient-specific information, making it suitable for emergency applications, but requires further validation in resource-limited settings[18].

6.3 6G Cognitive Data Hypothesis: A Post Box Viewpoint

This paper introduces the “6G mailbox theory”, which optimizes data transmission, re- duces redundancy, and improves performance by collecting and identifying information as value. It considers the integration of edge networks, artificial intelligence algorithms, and computational intelligence to achieve real-time intelligence and service delivery. Signifi- cant advances such as blockchain, infographics, and deep learning have improved decision making and data recognition, while data fusion technology has improved the accuracy and reliability of 6G chip applications and solved the problems of security, privacy, and rich data[19].

7 Conclusion

The concept of cloud-edge integration is much better than cloud or edge devices in terms of the combination of intelligence and IoT to make a good decision. Now there is a need to create a framework that adapts to suitable projects such as asynchronous federated learning[2], mobile edge technology[3], differential privacy[4], and blockchain[5]. This ar- ticle focuses on understanding them in detail and examining the designs currently used as advanced techniques to support the growth of needs and requirements. In addition to the immediate implementation of decisions, the strategy also needs to create strong solutions that have become the need of the day to create a better tomorrow. We also need to work hard to overcome the problems arising from this and ensure unity. The goal of integrating these hot solutions is endless. They are also more secure, have greater capacity, and use less energy than other methods, allowing for better resource management[1]. Although it is still difficult to know for sure, it is necessary to try to think about the possibility of changing the fate of the website with the help of these ideas.

References

[1] Chiara Caiazzab, Silvia Giordanoc, Valerio Luconid, and Alessio Vecchioa. Edge computing vs centralized cloud: Impact of communication latency on the energy consumption of lte terminal nodes. 2023.

[2] Cheng Chi, Zihang Yin, Yang Liu, and Senchun Chai. A trusted cloud–edge decision architecture based on blockchain and mlp for aiot. 2024.

[3] Zufan Zhang, Kewen Zeng, and Yinxue Yi. Blockchain-empowered secure aerial edge computing for aiot devices. 2024.

[4] Zecan Yang, Botao Xiong, Kai Chen, Laurence T. Yang, Xianjun Deng, and Chenlu Zhu. Differentially private federated tensor completion for cloud–edge collaborative aiot data prediction. *Journal of AIoT Systems*, 11(1), 2024.

[5] Ye Liu, Peishan Huang, Fan Yang, Kai Huang, and Lei Shu. Quasyncfl: Asyn- chronous federated learning with quantization for cloud–edge–terminal collaboration enabled aiot. *AIoT Advances*, 11(1), 2024.

[6] Junlong Zhou, Kun Cao, Jin Sun, and Keqin Li. Fusion and integration of clouds, edges, and devices. 2025.

[7] Y. Zhang et al. Decentralized blockchain-based data verification in iot networks. *Journal of Network and Computer Applications*, 2019.

[8] Cao J. Zhang Q. Li Y. Shi, W. and L Xu. Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 2016.

[9] C. Zhang and Y. Zheng. Cloud computing and big data analysis for intelligent iot applications. 2019.

[10] Saad Aljubayrin, Ghadah Aldehim, Nuha Alruwais, Khalid Mahmood, Mesfer Al- Duhayyim, Hong Min, Lewis Nkenyereye, and Wali Ullah Khan. Dynamic offloading strategy for computational energy efficiency of wireless power transfer-based mec networks in industry 5.0. 2023.

[11] Chenhao Xu, Youyang Qu, Yong Xiang, and Longxiang Gao. Asynchronous feder- ated learning on heterogeneous devices: A survey. 2023.

[12] Juncheng Jia, Ji Liu, Chendi Zhou, Hao Tian, Mianxiong Dong, and Dejing Dou. Efficient

asynchronous federated learning with sparsification and quantization. 2024.

[13] K. Li and H. Li. Blockchain-based mobile edge computing for iot security and privacy. *Future Generation Computer Systems*, 113:1–12, 2020.

[14] Y. Zhang and K. Li. Edge computing and federated learning for iot: Challenges and solutions. *IEEE Internet of Things Journal*, 2021.

[15] Resource Allocation Strategies for Edge-Cloud Collaborative Computing. *ScienceDi- rect*, 2020.

[16] L. Wang and Z. Li. Aiot: Combining ai and iot for smarter systems. *International Journal of Computer Science and Information Security*, 16(9):1–8, 2018.

[17] Karisma Trinanda Putra Nur Hayati, Ahmad Zaki Arrayyan, Firdaus, Cahya Damar- jati, Abu Bakar, and Hsing-Chung Chen. A review on the application of internet of medical things in wearable personal health monitoring: A cloud-edge artificial intelligence approach. 2023.

[18] Jiarong Chen, Yingfang Zheng, Yingshan Liang, Zehui Zhan, Mingzhe Jiang, Xian- bin Zhang, Daniel S. da Silva, Wanqing Wu, and Victor Hugo C. de Albuquerque. Edge2analysis: A novel aiot platform for atrial fibrillation recognition and detection. 2023.

[19] Yixue Hao, Yiming Miao, Min Chen, Hamid Gharavi, and Victor C. M. Leung. 6g cognitive information theory: A mailbox perspective. 2021.

[20] L. Zhang and Y. Liang. Edge ai and iot: Intelligent data processing and decision- making. *IEEE Access*, 7:162984–162992, 2019.