Journal of Network and Computer Applications 233 (2025) 104037

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Research paper

Leveraging blockchain and federated learning in Edge-Fog-Cloud computing environments for intelligent decision-making with ECG data in IoT

Shinu M. Rajagopal [a,*], Supriya M. [a], Rajkumar Buyya [b]

[a] Department of Computer Science and Engineering, Amrita School of Computing, Bengaluru, Amrita Vishwa Vidyapeetham, India
[b] Cloud Computing and Distributed Systems (CLOUDS) Lab, School of Computing and Information Systems, The University of Melbourne, Australia

ARTICLE INFO

Keywords:
Blockchain
Edge computing
Federated learning
Fog computing
Internet of Things

ABSTRACT

Blockchain technology combined with Federated Learning (FL) offers a promising solution for enhancing privacy, security, and efficiency in medical IoT applications across edge, fog, and cloud computing environments. This approach enables multiple medical IoT devices at the network edge to collaboratively train a global machine learning model without sharing raw data, addressing privacy concerns associated with centralized data storage. This paper presents a blockchain and FL-based Smart Decision Making framework for ECG data in microservice-based IoT medical applications. Leveraging edge/fog computing for real-time critical applications, the framework implements a FL model across edge, fog, and cloud layers. Evaluation criteria including energy consumption, latency, execution time, cost, and network usage show that edge-based deployment outperforms fog and cloud, with significant advantages in energy consumption (0.1% vs. Fog, 0.9% vs. Cloud), network usage (1.1% vs. Fog, 31% vs. Cloud), cost (3% vs. Fog, 20% vs. Cloud), execution time (16% vs. Fog, 28% vs. Cloud), and latency (1% vs. Fog, 79% vs. Cloud).

1. Introduction

The integration of the Internet of Things (IoT) with medical applications has brought about a significant transformation in healthcare, particularly in real-time patient monitoring facilitated by connected medical devices. Among these advancements, Electrocardiogram (ECG) anomaly detection stands out as a critical tool in identifying cardiovascular irregularities, potentially preventing life-threatening conditions. However, the effectiveness of ECG anomaly detection heavily relies on processing extensive and sensitive medical data generated by distributed IoT devices (Moghadas et al., 2020). Traditionally, such data processing has been centralized in the cloud. However, transitioning to edge and fog computing is now imperative for real-time analysis at the network's edge, ensuring minimal latency in identifying cardiac abnormalities. Edge/fog computing allows for the timely detection of potentially life-threatening ECG signal abnormalities, thus significantly enhancing patient care (Prakash et al., 2017).

Nevertheless, this shift towards edge/fog computing also raises concerns, particularly regarding data privacy, security, and latency, especially in time-critical medical applications. Addressing these challenges, FL has emerged as a promising solution. Federated Learning (FL) facilitates collaborative training of a global machine-learning model among multiple IoT devices while preserving data decentralization and security. It offers enhanced privacy and security by avoiding the need to share sensitive data with a central server, making it particularly well-suited for medical IoT applications. Despite these advantages, FL still faces limitations such as communication overhead and vulnerability to Byzantine attacks (Lakhan et al., 2022).

In response to these challenges, blockchain technology has garnered increasing attention. By combining blockchain's decentralized and tamper-proof ledger with FL, a distributed and trustless environment is created for training machine learning models (Mohanta et al., 2019). Blockchain ensures data integrity and eliminates the dependence on a single entity for data aggregation and model updates, thereby further enhancing decision-making processes within the healthcare domain (Ratta et al., 2021). This paper's research contributions are outlined below:

- Design of an early warning system to detect anomalies in ECG readings.
- Integration of Blockchain-based Federated Learning, a privacy-preserving method, into critical healthcare applications to protect end-user data.
- Identification of the most suitable placement policy for deploying the Blockchain-based Federated Learning module within the architecture's Edge, Fog, and Cloud layers.

* Corresponding author.
E-mail addresses: mr_shinu@blr.amrita.edu (S.M. Rajagopal), m_supriya@blr.amrita.edu (S. M.), rbuyya@unimelb.edu.au (R. Buyya).

https://doi.org/10.1016/j.jnca.2024.104037
Received 8 March 2024; Received in revised form 29 June 2024; Accepted 25 September 2024
Available online 19 October 2024

The rest of this paper is organized as follows. Section 2 and Section 3 discuss the background and related work. Section 4 presents the proposed method followed by the experimental setup in Section 5. Section 6 summarizes the results, and Section 7 concludes the paper.

2. Background and motivation

The integration of IoT with healthcare, commonly referred to as medical IoT, has undergone significant growth, offering opportunities for real-time patient monitoring and personalized healthcare. ECG anomaly detection stands out among the various medical IoT applications for its crucial role in identifying potential cardiovascular irregularities and aiding in timely diagnosis and treatment. Accurate ECG anomaly detection is paramount for preventing life-threatening conditions and improving patient outcomes (Prabhu and Hanumanthaiah, 2022). However, traditional centralized approaches to ECG anomaly detection, which involve storing medical data in cloud-based infrastructures for model training, raise concerns regarding data privacy, security, and latency. Medical data, being highly sensitive and regulated, requires stringent protection to comply with data privacy laws and maintain patient trust. Moreover, reliance on centralized servers introduces vulnerabilities, making the system susceptible to cyber-attacks and data breaches (Bharathi et al., 2022).

To address these challenges, FL offers a promising solution by decentralizing data processing and keeping data locally processed on user devices. This decentralized approach minimizes the risk of data breaches and facilitates compliance with data protection regulations, ensuring that sensitive medical information remains with the users who generate it (Jin and Dong, 2018). However, FL still faces limitations in resource-constrained IoT environments, including communication overhead, limited computational capabilities of edge devices, and the potential for Byzantine attacks (Zhang et al., 2020a).

Wearable devices and IoT technologies continuously generate vast amount of data, posing significant security challenges. Particularly in the realm of medical data, a thorough investigation has revealed numerous issues related to the security and privacy of healthcare information. Globally, medical data breaches threaten patient confidentiality, exposing sensitive health information to unauthorized access. These breaches not only raise individual privacy concerns but also risk the integrity of healthcare systems and undermine trust in the protection of critical medical data worldwide. In this context, blockchain technology emerges as a complementary solution to enhance the security, transparency, and efficiency of FL in medical IoT environments. By providing a tamper-proof and decentralized ledger, blockchain ensures the integrity and transparency of data and model updates. When combined with FL, blockchain creates a distributed and trustless environment for collaborative training (Cheikhrouhou et al., 2021).

This research aims to leverage blockchain-based Federated Learning for ECG anomaly detection in Edge-Fog-Cloud computing environments. By harnessing blockchain's immutability and decentralization, we seek to address the privacy and security concerns of medical data while enabling efficient and accurate ECG anomaly detection. Our implementation will empower medical IoT devices, edge, and fog nodes to collaboratively participate in the training process, thereby improving model accuracy and robustness. This research endeavor aims to contribute to the advancement of healthcare services by presenting a cutting-edge solution that guarantees data privacy, security, and efficient model training. Integrating blockchain and FL in medical IoT applications has the potential to revolutionize patient care, enabling more personalized and timely medical interventions while upholding the highest standards of data protection and confidentiality. The motivation for this study stems from the inadequacy of existing research on edge/fog/cloud-based FL methods in addressing healthcare concerns related to the detection of ECG anomalies within microservice-oriented IoT healthcare applications.

3. Related work

The previous section highlights the importance of using blockchain-based FL in edge/fog/cloud computing applications. The following paragraphs delve into the current advancements in the utilization of blockchain technology for FL within the context of IoT applications spanning edge, fog, and cloud computing

Cherukuri et al. and Awan et al. both propose blockchain-based solutions to address the challenges of federated learning, such as the single point of failure and data leakage (Cherukuri et al., 2024; Awan et al., 2019). Cherukuri et al. (2024) uses blockchain as a model aggregator and incorporates a privacy-preserving technique, while the proposed framework in Awan et al. (2019) leverages blockchain's immutability and decentralized trust for secure aggregation of local model updates. Dias et al. introduces BlockLearning, a modular framework that supports vertical federated learning and various blockchain algorithms (Dias and Meratnia, 2022). Zhang et al. presents a blockchain-based protocol for federated learning, emphasizing secure communication in physically distributed datasets (Zhang et al., 2020b). These studies collectively highlight the potential of blockchain in enhancing the security, privacy, and reliability of federated learning.

Ali et al. emphasizes the importance of addressing privacy concerns in IoT systems leveraging blockchain and FL technologies. It highlights the need for research on privacy preservation techniques in blockchain-enabled IoT and the potential of FL in decentralized learning (Ali et al., 2021). Fan et al. proposes a hybrid blockchain-based resource trading system to incentivize heterogeneous edge node participation, addressing the need for fair market establishment among distinct edge companies (Fan et al., 2020). Qu et al. suggests the growing importance of addressing privacy and efficiency concerns in fog computing through innovative approaches like blockchain-enabled Federated Learning (FL-Block). It highlights FL-Block's capability to facilitate autonomous machine learning without central authority, mitigating privacy risks while enhancing efficiency and resilience against poisoning attacks (Qu et al., 2020a). Wan et al. highlights the growing importance of addressing privacy concerns in edge computing, especially with the advent of 5G and beyond 5G networks. It emphasizes the utilization of FL to preserve privacy, while acknowledging existing challenges such as centralized processing costs and data falsification issues (Wan et al., 2022).

Lu et al. present a secure data-sharing architecture using blockchain technology, integrating privacy-preserving FL into the consensus mechanism of a permissioned blockchain, thus utilizing computational efforts for both consensus and federated training (Lu et al., 2020a). Pokhrel et al. implement FL in vehicular communication networks autonomously, utilizing blockchain technology to ensure privacy and efficiency by decentralizing the exchange and validation of local machine-learning model updates on vehicles (Pokhrel and Choi, 2020).

Aich et al. propose a two-stage workflow: customers train an initial model using smartphones and the mobile edge computing (MEC) server, sending signed models to the blockchain for protection against malicious activities. In the second stage, manufacturers select customers as miners to compute the averaged model, utilizing differential privacy and a novel normalization technique to safeguard customer privacy and enhance test accuracy (Aich et al., 2021). Lu et al. introduce an asynchronous FL approach for training models with edge data, emphasizing efficiency by selectively involving nodes to minimize costs. Additionally, they enhance model reliability by integrating learned parameters into a blockchain and ensuring their integrity via a two-stage verification procedure (Lu et al., 2020b). Lu et al. propose a novel blockchain-driven FL model that replaces the central authority with a custom-designed blockchain, integrating decentralized privacy protocols. This enables local updates from end devices to be transmitted to servers inside fog devices for generating and storing global updates. Notably, the blockchain manages only the pointer to global updates, while data is securely stored using a distributed hash table (DHT), ensuring resilience, privacy, and protection against potential poisoning attacks on fog servers (Qu et al., 2020b).

The following paragraphs present the current state of the art in blockchain-based FL methods used in medical applications. In real-world scenarios, hospitals and relevant institutions often exhibit reluctance when it comes to sharing patient data, primarily to protect patient privacy. This reluctance poses a significant challenge in obtaining essential information for the detection of cognitive diseases. However, the emergence of wearable devices and advancements in computing technology has facilitated the gathering of valuable health data. Smart healthcare solutions leverage machine learning models trained on ample user data while ensuring privacy preservation by the incorporation of blockchain technology (Myrzashova et al., 2023). FedHealth employs FL and homomorphic encryption to aggregate data from multiple organizations, creating personalized models through transfer learning while strictly preserving user privacy without any data leakage during the parameter sharing process (Chen et al., 2020). A novel secure aggregation protocol is proposed by Passerat et al., combining hardware components and an encryption toolkit native to Ethereum that ensures security (Passerat-Palmbach et al., 2019). Kumar et al. present a framework that consolidates a limited volume of data originating from various origins, including diverse hospitals and global deep learning model training via blockchain-based FL (Kumar et al., 2021).

Passerat et al. introduce the aggregation actor, a trusted third-party or a central entity with secure hardware like Intel SGX, centralizing the collection of updates from participants to create new model versions. However, this centralization entails risks, such as training interruptions if the server fails or potential malicious actions affecting the training process. To mitigate these concerns, they employ blockchain as a decentralized alternative to coordinate the process (Passerat-Palmbach et al., 2020). The presence of incorrect masked gradients and unmasked shares uploaded by dishonest local trainers to the parameter server, undermines the integrity of FL and hinders its ability to attract sufficient distributed training data and computation power. To address this, Bao et al. proposes FLChain, a decentralized, public auditable, and incentivized FL ecosystem that ensures trust and incentive where FLChain nodes collect and combine locally documented gradients, and later submit the aggregated results back to FLChain (Bao et al., 2019). A summary of the related work can be seen in Table 1.

Various methods exist for determining the participants of the mining process, type of data being updated on the blockchain, and the location where the aggregation of models occur. These methods depend on the architecture and design of the blockchain and FL based IoT application. The selection of devices participating in the mining process can be based on factors such as computational power, network connectivity, or pre-defined roles. The data being updated on the blockchain include local model updates, training progress, and consensus-related information (Wang et al., 2019). The decision on what data to store on the blockchain is influenced by the specific use case and the desired level of transparency and security. Regarding the aggregation of local models, it can happen either at a central server or through a distributed consensus algorithm. In the central server approach, all participating devices send their local model updates to a centralized entity responsible for aggregating the models into a global model. On the other hand, in a distributed consensus algorithm, devices collaborate directly with each other to collectively update the global model. The choice between these methods depend on factors like the scale of the IoT network, communication latency, privacy requirements, and the desired level of decentralization. Each approach has its benefits and trade-offs, and the final design should align with the specific needs and goals of the blockchain and FL based IoT application (Zhang et al., 2021).

In the literature, several methods have been proposed for developing a global model in a blockchain and FL based IoT application using fog/edge devices. One of the proposals involves fog/edge devices actively participating in the mining process and collaboratively developing the global model with the assistance of consensus algorithms (Kim et al., 2019). The updated global model is then broadcast to end devices, ensuring that all participants have the latest version (Zhao et al., 2020). In another method, fog/edge devices also participate in the mining process, but instead of directly developing the global model, they send their local model updates to the network. End devices receive these updates and collectively generate the global model through aggregation (Drungilas et al., 2021). A combination of fog/edge devices and end nodes collaboratively participate in the mining process to develop the global model collectively (Rahman et al., 2020). Each method offers unique advantages and challenges, and the choice depends on factors like network scale, privacy concerns, and the desired level of decentralization (Ejaz et al., 2021). In the present state of the field, there is a noticeable research gap surrounding the collaborative involvement of fog/edge devices and end nodes in the mining process, working together to develop a global model collectively. This innovative approach diverges from the traditional method of constructing the global model directly. Instead, these entities choose to distribute their local model updates with the network, with the global model generation taking place at the end device. This unique paradigm which is proposed here has significant advantages such as complete decentralization and improved quality global model generation. A summary of the proposed approach and comparison with existing work can be seen in Table 2.

4. Proposed method

4.1. Key elements from prior base application - FedSDM

We will briefly outline the base project in the following paragraph to provide an overview of our proposed method. It is important to note that comprehensive details about the base approach can be found in our previous paper (Rajagopal et al., 2023). This summary aims to serve as a concise introduction to the core concepts and foundations upon which our current research builds. The summary will encompass key aspects of the base project, including its architecture, mobility concepts, microservice principles, and evaluation metrics, which have been detailed in our previous work.

Federated Learning-based Smart Decision Making (FedSDM) is a decision-making module designed for ECG data management within the IoT Edge-Fog-Cloud computing environment. Leveraging FL, it offers intelligent decision-making capabilities. This module operates at the intersection of healthcare and advanced computing, demonstrating its capacity to harness ECG data efficiently while considering factors such as mobility, latency, and resource allocation. The edge and fog computing integration, optimizes real-time processing, enabling timely and critical health assessments. This architecture leverages edge/fog computing to address latency and bandwidth challenges in healthcare applications, emphasizing efficient utilization of intermediate edge/fog devices. It incorporates virtual machine partitioning on edge/fog nodes to manage data processing and adopts a modular microservice approach to support real-time medical applications.

The integrated edge/fog healthcare application follows a multi-tier placement with IoT devices in tier 0, edge/fog nodes in tiers 1 and 2, and the cloud in tier 3, utilizing fog as an intermediary for real-time healthcare data processing which is depicted in Fig. 1. Edge/fog nodes are equipped with virtualized resources, and requests are processed locally if resource requirements are met; otherwise, they are forwarded to neighboring devices with adequate resources. The mobility of edge/fog nodes and IoT devices poses a challenge for resource proximity in fog computing. iFogSim2 addresses this by incorporating a mobility component, enabling distributed node movements and customization of device mobility, thereby enhancing the realism and accuracy of system simulations. Resource augmentation is vital for resource-limited fog environments, and iFogSim2's clustering technique fosters dynamic coordination among multiple nodes, improving resource utilization efficiency in fog computing. This approach enables

Table 1
Summary of related works.

Paper	Area	Technology	Advantages	Drawbacks
Lu et al. (2020a)	Industrial IoT	FL with secure data-sharing architecture	Distributed	Consensus
Pokhrel and Choi (2020)	Vehicular Communication Networking	Distributed model updates	Autonomous	Update complexities
Aich et al. (2021)	MEC	Differential privacy	Two-stage	Blockchain overhead
Lu et al. (2020b)	Edge Data Processing	Asynchronous FL	Efficient	Integration complexity
Qu et al. (2020b)	Decentralized Privacy	Robustness	Decentralizing	Protocol challenges
Chen et al. (2020)	Medical Applications	Homomorphic encryption	Preserving privacy	Implementation complexity
Passerat-Palmbach et al. (2019)	General Blockchain	Secure aggregation protocol	Enhanced security	Reliance on Ethereum
Kumar et al. (2021)	Medical Applications	Blockchain-based FL	Global training	Cooperation requirement
Passerat-Palmbach et al. (2020)	Various Applications	Decentralization	Risk-mitigating	Trust reliance
Bao et al. (2019)	Various Applications	Incentivized participation	Decentralized	Implementation complexity
Proposed	**Edge-Fog-Cloud Computing**	**Blockchain and Federated Learning**	**Intelligent Decision-Making**	**Data scalability**

Table 2
Proposed approach comparison with existing works.

Paper	Area	Mining	Global model update	Enhanced security	Complete decentralization
Passerat-Palmbach et al. (2020)	Blockchain and FL based IoT	Fog/edge devices	Yes	No (Limited node participation)	No (Limited decentralization since only edge and fog nodes participation)
Bao et al. (2019)	Blockchain and FL based IoT	Fog/edge devices	Yes	No (Limited node participation)	No (Limited decentralization since only edge and fog nodes participation)
Wang et al. (2019)	Blockchain and FL based IoT	Fog/edge devices and end nodes	Yes	No (Limited node participation)	Yes (Greater decentralization since edge, fog, and end nodes participation)
Zhang et al. (2021)	Blockchain and FL based IoT	Fog/edge devices and end nodes	Yes	No (Centralized global model update)	No (Centralized control)
Kim et al. (2019)	Blockchain and FL based IoT	Fog/edge devices and end nodes	Yes	Yes (Broader node participation)	No (Centralized control)
Proposed	**Blockchain and FL based IoT**	**Fog/edge devices and end nodes**	**Yes**	**Yes (Broader node participation)**	**Yes (Greater decentralization since edge, fog, and end nodes participation)**

nodes to query and register cluster members based on specific policies, enhancing overall effectiveness. The proposed system adopts edge/fog computing and microservice architecture featuring small, independent microservices that communicate efficiently through lightweight protocols. These microservices offer numerous benefits, including scalability, resilience, and ease of deployment, making them ideal for large-scale IoT applications. The system's application model comprises three core microservices: the client, residing on users' smartphones to receive ECG data; the preprocessing service, responsible for data validation and cleaning; and the decision-making service, which analyzes ECG data in real-time and sends health alerts. These microservices can be deployed on edge or fog nodes based on placement policies, and a fog architecture that incorporates multiple hierarchical levels. This optimizes resource provisioning and enhances system performance by distributing containerized microservices effectively within the edge/fog environment, which is presented in Fig. 2.

In the proposed system, edge/fog devices leverage the FedAvg methodology for the FL module, which efficiently reduces communication costs between servers and clients by employing multiple local SGD updates and a single aggregation step in each communication cycle. This decentralized approach enhances the efficiency and effectiveness of FL, eliminating the need for substantial storage and computing capacity typically associated with traditional cloud deployments as depicted in Fig. 3.

The proposed architecture employs an autoencoder implemented with Artificial Neural Networks (ANN) to classify ECG data as normal or anomalous based on the reconstruction error. It utilizes a self-supervised learning approach by training the model on standard ECG

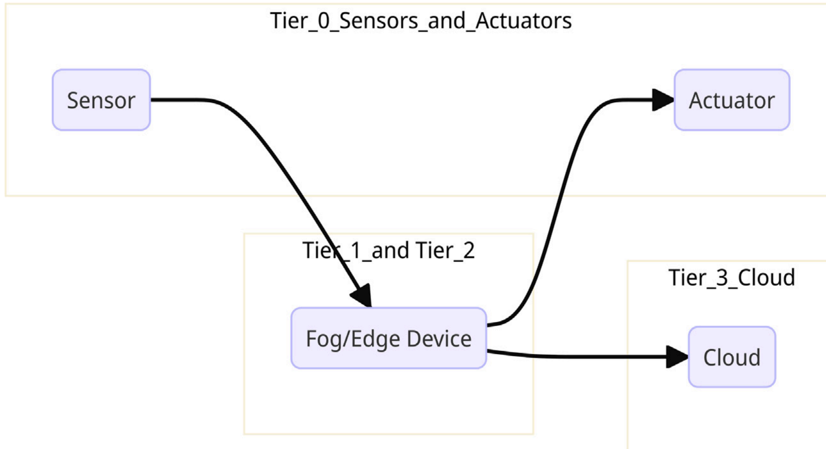


Fig. 1. Multitier placement of devices.

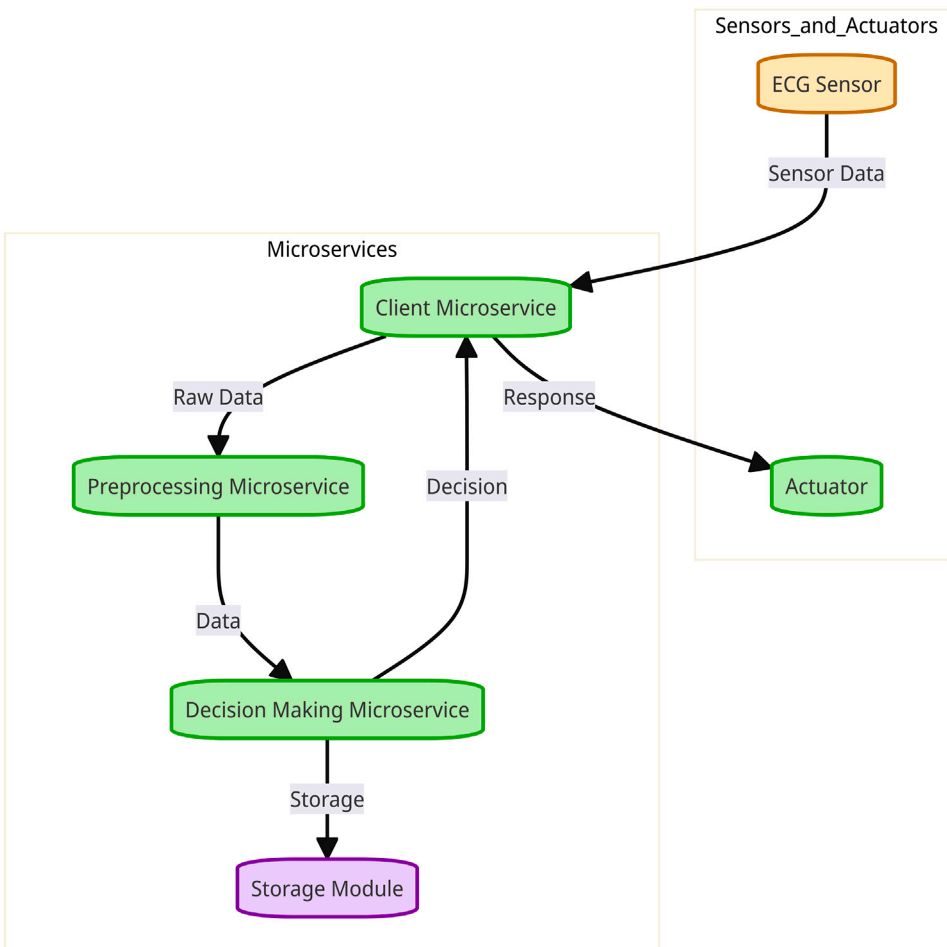


Fig. 2. Data Flow Diagram for the proposed approach.

data and identifying anomalies when the reconstruction error exceeds a predefined threshold, improving healthcare monitoring accuracy. The proposed system leverages the Flower framework for large-scale FL experiments, offering advanced tools for heterogeneous device environments, even accommodating up to 15 million clients with just a pair of high-end GPUs. Within this framework, the integration of the autoencoder enhances FL's capabilities, enabling the effective detection of anomalies in ECG data during the FL process and enhancing healthcare monitoring which is presented as sequence diagram in Fig. 4.

In evaluating the FedSDM system, we utilized key performance indicators (KPIs) such as latency, network use, cost, execution time, and energy consumption to assess the suitability of edge/fog/cloud computing in various use case scenarios. We present the formulas for parameter evaluations concisely in Table 3, with a detailed description of these formulas provided in our previous work (Rajagopal et al., 2023) and notations used in measurements of evaluation metrics equations in Table 4.

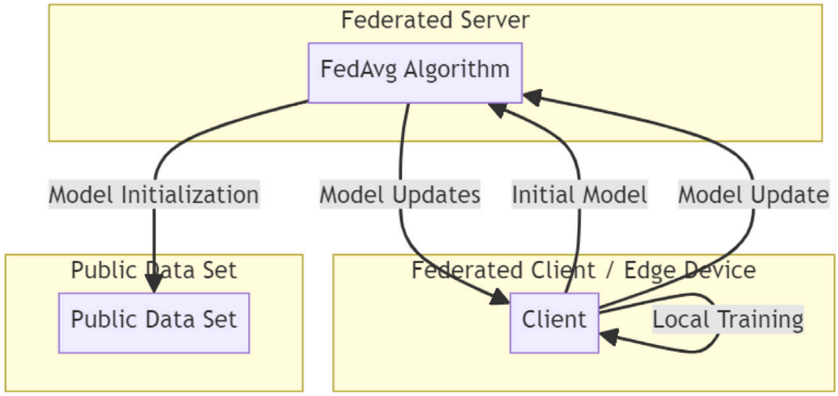


Fig. 3. Operational Concept of Federated Learning.

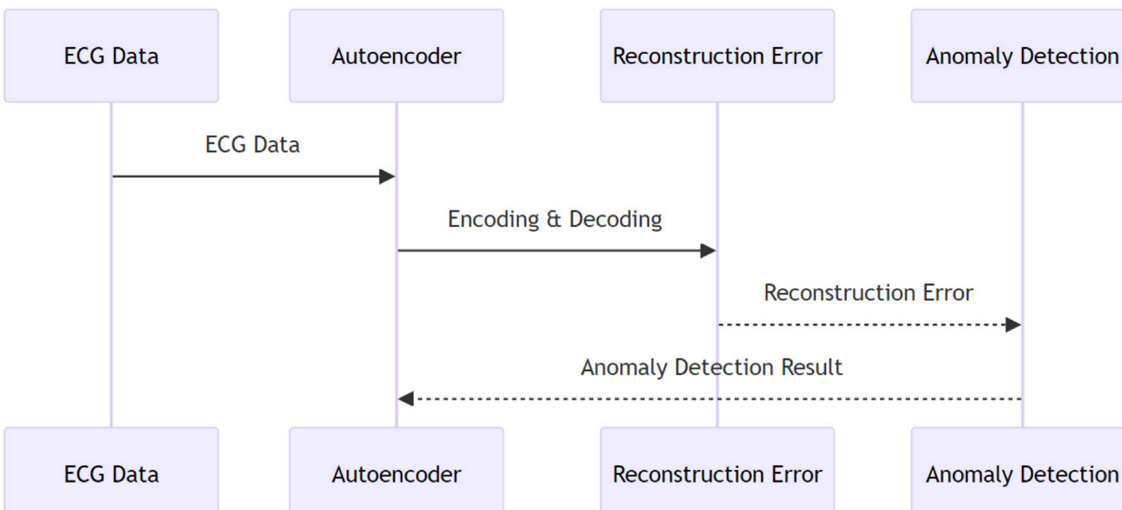


Fig. 4. Autoencoder working sequence diagram.

Table 3
Evaluation of parameters.

Parameter	Formula
Execution Time (TXT)	$\sum_m [EXT(N_i)]$
Latency (TL)	$\sum_m CAL$
Energy Consumption	$\sum_{i=0}^m (\sum_{k=1}^n EN_{i_k} + E_0)$
Network Usage (NU)	$\sum_n (l * TNS)$
Total Cost	$\sum_{T_k^i \in N_i \text{ Tasks}} \text{cost}(T_k^i)$

4.2. Proposed advanced application model: Blockchain-based federated learning integration

Blockchain technology plays a crucial role in enhancing the trustworthiness of the FL process by creating a decentralized and tamper-proof ledger. Unlike traditional FL systems, which often rely on a central authority and are vulnerable to single points of failure and centralization, blockchain distributes trust across all participants. This decentralized trust mechanism ensures that no single entity has control over the system, thereby reducing the risk of centralization-related vulnerabilities and ensuring that all participants have equal confidence in the integrity of the system.

The utilization of blockchain-based FL in the edge/fog/cloud layer for ECG anomaly detection holds great promise for developing precise and effective anomaly detection models while ensuring the security and privacy of sensitive medical data. However, numerous research gaps remain that require attention to fully harness the potential of blockchain and FL in this field. In the current literature, there is a lack of existing research on actively involving both participating edge/fog devices and end devices in the mining process to collectively enhance the quality of the global model in blockchain and FL based IoT applications. Our proposed work aims to develop a blockchain-based FL model for ECG monitoring, which on successful implementation, could offer improved data privacy, increased data diversity, efficient resource utilization, and real-time updates by enabling active participation from both edge/fog devices and end devices in the mining process to improve the global model's quality collaboratively. The proposed Blockchain-based FedSDM model predicts ECG anomalies by implementing FL in edge, fog, and cloud layers while also providing appropriate usage guidelines.

The proposed approach adopts a strategy centered around federated clients. Within this framework, every client is furnished with a pre-existing model from the federated server. This model is curated using a public data set, which serves as a foundational resource for initializing the training procedures of individual clients. By leveraging the knowledge encapsulated within this initial model, federated clients can then embark on personalized training based on their local data, ultimately contributing to the collective learning process in a distributed and privacy-preserving manner. This distributed architecture enables clients to harness the power of collective data while maintaining data privacy on their local devices. Leveraging this access, each federated client autonomously undertakes model training using its own local data, tailoring the model to its unique circumstances and requirements.

Table 4
Notations used in evaluation metrics equations.

Symbol	Meaning	Symbol	Meaning
T	Tasks	E_0	Power required for the server in an idle state
N	Nodes	NU	Network use
m	The Number of servers	l	Latency experienced by the network
n	Number of VMs inside the host	TNS	Tuple network size
$EXT(N_i)$	The execution time required by node N_i	$cost(T_k^i)$	Cost for processing task T_k^i
TXT	Total execution time	$M(T_k^i)$	Memory needed by task T_k^i
TL	Total latency	$Bw(T_k^i)$	Bandwidth needed by task T_k^i
CAL	Current average latency	NU	Network use
CC	Simulator clock		
ET	Execution time of the tuple		
E	Total energy consumption		
EN_{ik}	Energy consumption by the task T_k		

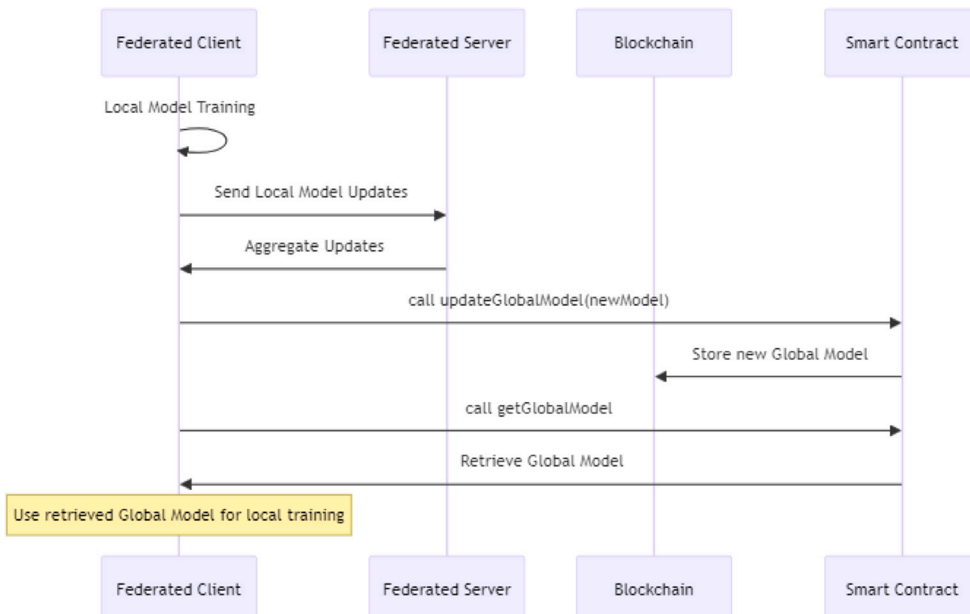


Fig. 5. Sequence diagram of the Proposed BCFL architecture for a single federated client.

Upon the local training phase's completion, the federated clients transmit their model updates back to the federated server. This communication process facilitates information exchange, allowing the federated server to consolidate the various local models into a unified and robust global model. The aggregation of insights from diverse data sources enhances the overall model's accuracy and adaptability. Notably, the federated server employs a mining process that involves the active participation of all federated clients and edge devices. Smart contracts play a crucial role in this stage, ensuring the mining process's transparency, security, and fairness. This collaborative mining process is vital for producing a reliable and trustworthy global model that caters to the collective needs of the federated ecosystem. To ensure tamper-proof storage and easy accessibility, the resulting global model is securely stored inside a blockchain. The immutable nature of blockchain technology ensures the integrity of the model and enables efficient retrieval whenever needed. This integration of FL with blockchain offers a cutting-edge solution that combines privacy, decentralization, and reliability, fostering a new paradigm for collaborative and secure machine learning in diverse applications. The sequence diagram corresponding to the previously described explanation with one federated client can be found in Fig. 5. The described approach functions in the following manner: Patient-generated ECG sensor data is stored on the edge device, for instance, a mobile phone. Computation tasks are managed by the client and data preprocessing microservices, respectively, both located at the edge. Subsequently, the preprocessed ECG data is transferred to the Smart Decision Making module for anomaly analysis. In the event of anomaly detection, a notification is sent to the end device to inform the user of potential health concerns.

The presented architecture assesses and contrasts the effectiveness of various placement strategies for the decision-making module built on FL, as outlined in the preceding section. In every placement circumstance, be it at the Edge, Fog, or Cloud, the individual updates from the associated devices or nodes are consolidated within their respective tiers. Following each round of FL, the clients and edge devices collaborate in the data extraction process and engage in the execution of smart contracts.

The key functions of smart contract are “updateGlobalModel” and “getGlobalModel”. The former allows for updating the global model with a new model represented as an array, ensuring that the new model's length matches the existing global model's length to prevent invalid updates. The latter function enables clients to retrieve the latest version of the global model. This smart contract is intended to be used in conjunction with the FL system, where a federated server generates a new global model after each round of training, and clients interact with the smart contract using web3.js to obtain the global model for their local training, enabling collaborative machine learning while preserving data privacy on the blockchain. Consequently, the globally generated model is securely stored on the Ganache blockchain and is treated as a transaction. The integration of blockchain technology enhances the system's resilience, facilitating smooth cooperation among participants while safeguarding data privacy and preventing any unauthorized alterations to the global model. Smart contract algorithm proposed in this work is presented in Algorithm 1.

The proposed method explores three different deployment scenarios for FedAvg in various layers: edge, fog, and cloud. In the edge scenario, the computation and model training takes place on the edge devices closer to the end users. In the fog scenario, the computation occurs on intermediate fog nodes, while in the cloud scenario, the central server handles the computation and aggregation of the global model. Each scenario offers unique advantages and trade-offs in terms of communication efficiency, latency, and resource utilization, allowing the system to adapt and optimize according to the application's specific requirements. Following every round of FL, the clients and edge devices actively engage in the mining process and execute smart contracts. As a result, the collectively generated global model is securely stored within the Ganache blockchain, where it is treated as a transaction. This decentralized and immutable ledger ensures the integrity and transparency of the model updates, enhancing the overall security and trustworthiness of the FL system. By leveraging blockchain technology, the process becomes more robust, enabling seamless collaboration among the participants while preserving data privacy and preventing unauthorized modifications to the global model.

Each deployment policy is assessed for its learning efficiency and Quality of Service (QoS) parameters, which are detailed in the subsequent section of the study. By comparing the results from various deployment options, the proposed method aims to determine the most effective and efficient approach for integrating FL in the healthcare system for ECG anomaly detection in real time.

The suggested approach includes applying blockchain-based FedSDM in the edge, fog, and cloud layers to assess effectiveness and cost-efficiency. The equations and strategy analyze resource usage and expenses, providing valuable insights for deploying blockchain-based FedSDM across diverse layers in the distributed computing environment. While the blockchain does not store sensitive medical data directly, it plays a vital role in securely logging global model updates. Each validated update to the global model is recorded immutably on the blockchain, creating a permanent and verifiable history of all changes. This approach ensures that the global model's integrity is preserved, as any attempt to tamper with the updates would be immediately detectable. The immutable nature of the blockchain ledger thus provides a robust security mechanism, preventing unauthorized alterations and ensuring that the FL process remains transparent and trustworthy. The integration of blockchain into the FL system significantly enhances the security of the global model. By safeguarding the model against potential malicious actors, blockchain ensures that all updates are recorded transparently and immutably, preventing any manipulation of the model. This is particularly important in environments where the integrity and security of data are paramount, such as in medical applications. The combination of decentralized trust and immutable recording provided by blockchain technology reinforces the reliability of the FL process, making it a more secure and trustworthy solution for critical applications.

Algorithm 1 Smart Contract for Global Model

Initialize the global model in the smart contract with zeros in the constructor.

Function `updateGlobalModel(`*newModel: array*`)`:
    if *newModel.length == globalModel.length* **then**
        require newModel.length == globalModel.length, "Invalid model size"
        globalModel = newModel
    end
Function `getGlobalModel()`:
    return globalModel
call UPDATEGLOBALMODEL(newModel) ▷ Passing the new model parameters as an array
call GETGLOBALMODEL ▷ To retrieve the latest version of the global model
    ▷ Clients use the retrieved global model for local training ▷ and updates in subsequent rounds of Federated Learning

5. Experimental setup

5.1. IFogSim2

In our study, we have carefully considered various simulators available for modeling and simulating cloud, fog, and edge computing infrastructures and services. Among the available options such as FogNetSim+, Yet Another Fog Simulator (YAFS), Edge-Fog, PureEdgeSim, and EdgeNetworkCloudSim, we have chosen iFogSim2 as our simulator of choice. iFogSim2 is an extension of Cloudsim, a widely-used simulation framework that offers several advantages for our experiments (Mahmud et al., 2022).

iFogSim2 allows us to create and execute experiments for edge, fog and cloud devices, considering factors like I/O, compute, VM allocation, memory, and VM power models. It provides a comprehensive environment for simulating the behavior of fog computing scenarios, including properties such as service migration, microservice orchestration, and distributed cluster building across fog nodes. The simulator's components, such as mobility microservices and clustering, are loosely coupled, making it highly flexible and suitable for simulation in various scenarios.

An important benefit of iFogSim2 is its integration of actual datasets to assess the effectiveness of various service management strategies in fog computing settings. This feature sets it apart from most existing solutions and allows us to conduct realistic and accurate simulations.

By leveraging iFogSim2's capabilities, we can validate the performance of our proposed approach in the fog computing environment, using real-world datasets and benchmarking against various service management strategies, including mobility management, microservice orchestration, and node clustering. This simulation framework enables us to make informed decisions about the efficiency and effectiveness of our approach, ensuring that it can meet the challenges and requirements of real-world healthcare applications.

In the iFogSim2 simulation framework, the core classes, namely AppModule, FogDevice, Sensor, and Actuator, are interconnected through object references within the Controller class. This interconnection enables seamless communication and coordination between different components of the simulation.

The FogDevice class represents the fog computing nodes in the simulation, and it encapsulates the properties and functionalities of these devices. The AppModule class represents the applications running on the fog devices and defines the modules that process the data. The Sensor class simulates the sensors attached to the devices and is responsible for generating data from the devices. The Actuator class represents the actuators connected to the fog devices, which perform actions based on the outcomes of the applications.

The Tuple class is accessed through an Application object, which represents the data structure used to transmit information between nodes in the fog computing environment. It allows data to be exchanged and processed between different components of the simulation.

To incorporate the mobility component into the iFogSim2 simulation, the framework comprises classes such as DataParser and MobilityController. The DataParser class is responsible for parsing and processing the mobility-related data, enabling dynamic mobility patterns for fog devices or users, and is pivotal in managing location data from various IoT end devices by segregating and assimilating the data to enable application services tailored to their distinct mobility patterns. The MobilityController class manages and controls the movement of devices or users in the simulation, facilitating realistic and dynamic scenarios for evaluating the performance of the fog computing environment with mobile elements. This manages dynamic adjustments by triggering consecutive and concurrent actions on distinct FogDevice

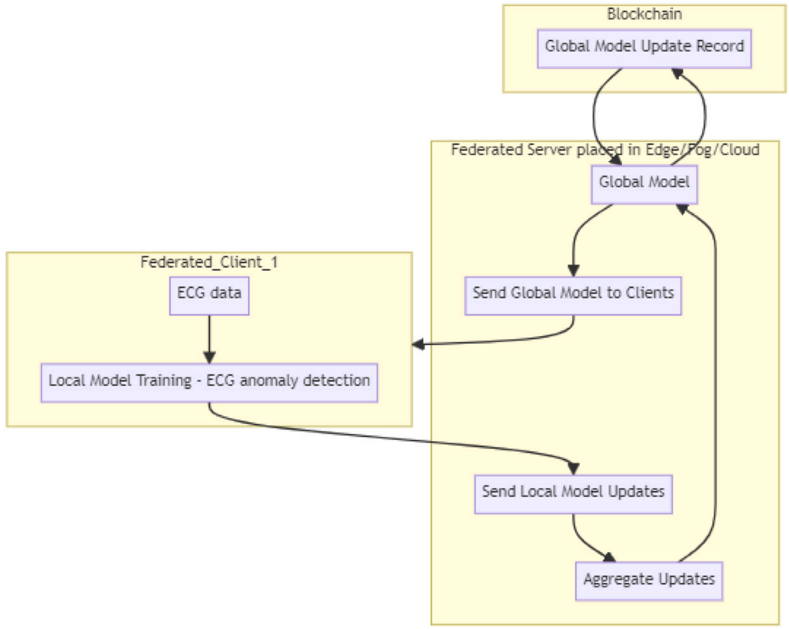


Fig. 6. Data flow process - BCFL.

and AppModule referenced objects, ensuring seamless handling of mobility events, like devices relocating or connecting to new fog nodes, through change detection and responsive actions.

By incorporating these functionalities and classes, iFogSim2 provides a comprehensive simulation environment for modeling and evaluating distributed fog computing scenarios, including dynamic collaboration and coordination among multiple fog devices and the mobility of devices or users. This allows for more realistic and accurate simulations of fog computing systems, considering various real-world scenarios and challenges.

During the simulation process, our proposed model considers two types of mobility patterns: 'RANDOM MOBILITY' and 'DIRECTIONAL MOBILITY'. In the 'DIRECTIONAL MOBILITY' model, the user or IoT device maintains a constant speed by having equal time intervals between consecutive motions. This pattern involves multiple consecutive coordinates placed at specific distances across the Melbourne Central Business District, representing the movement of the associated end IoT device. These coordinates serve as events to simulate the continuous movement of the IoT device in a consistent direction.

Conversely, the 'RANDOM MOBILITY' model integrates a range of random mobility patterns accessible within the simulator. These patterns denotes diverse user behaviors regarding direction, stopping time, velocity, location, and duration within the communication coverage of each edge/fog node. This simulation accurately emulates real-time user and IoT device behavior, enhancing the precision of the evaluation of our proposed system's performance.

By considering both 'RANDOM MOBILITY' and 'DIRECTIONAL MOBILITY' patterns during simulation, we can create dynamic scenarios that closely resemble real-world user movements and interactions with the edge/fog nodes. This comprehensive approach helps us assess the effectiveness and efficiency of our proposed system under various mobility conditions and ensures a more reliable evaluation of its performance in practical scenarios. Fig. 6 is a schematic representation of the entire data flow process, beginning with the acquisition of ECG data from medical IoT devices and culminating in the global update within the blockchain.

5.2. Ganache

Ganache is a popular personal blockchain designed specifically for Ethereum development and testing purposes. It serves as a local and private Ethereum network, enabling developers to deploy, interact, and debug their smart contracts without the need for real transactions on the main Ethereum network. One of its essential functionalities is providing a local blockchain environment, which significantly speeds up development and testing cycles. Ganache comes with predefined accounts containing test Ether, facilitating the testing of various scenarios and functionalities in smart contracts. Interaction with the local blockchain through the RPC interface using JSON-RPC or web3.js, making it easy to integrate with smart contract development tools and libraries. Although Ganache is a local network, it simulates gas prices and limits, giving developers insights into how their smart contracts would perform on the main Ethereum network. Another crucial feature is the ability to take snapshots of the blockchain state and later reset it, allowing for easy testing and debugging with different initial states. Ganache also offers transaction tracing and logs, enabling detailed analysis and debugging of smart contract executions. Integrated seamlessly with the Truffle development framework, Ganache provides Ethereum developers with a convenient and efficient environment for local testing, making smart contract development a smoother and more enjoyable experience (Lee and Lee, 2019)

In our proposed approach, Ganache is set up with port 7545 selected for accessibility through 'localhost' or '127.0.0.1'. A smart contract was then created using Truffle, a widely used development framework that streamlines the building and deployment of smart contracts. The contract was meticulously compiled to ensure its precision and efficiency. The smart contract was successfully deployed to the Ganache blockchain, leveraging Truffle's migration scripts, making it readily available and operational on the network. The web3.js library, a powerful JavaScript framework, was utilized to facilitate interaction with the deployed smart contract. This integration with web3.js enabled seamless communication with the smart contract, empowering the applications to invoke its functions and execute transactions with ease.

5.3. Simulation environment

This section presents the simulation environment utilized to assess the proposed approach. The sensors are responsible for detecting the patient's ECG data, which is then regularly transmitted to the fog nodes. On the fog nodes, the data undergoes processing and analysis to determine the patient's health condition, whether it is normal or

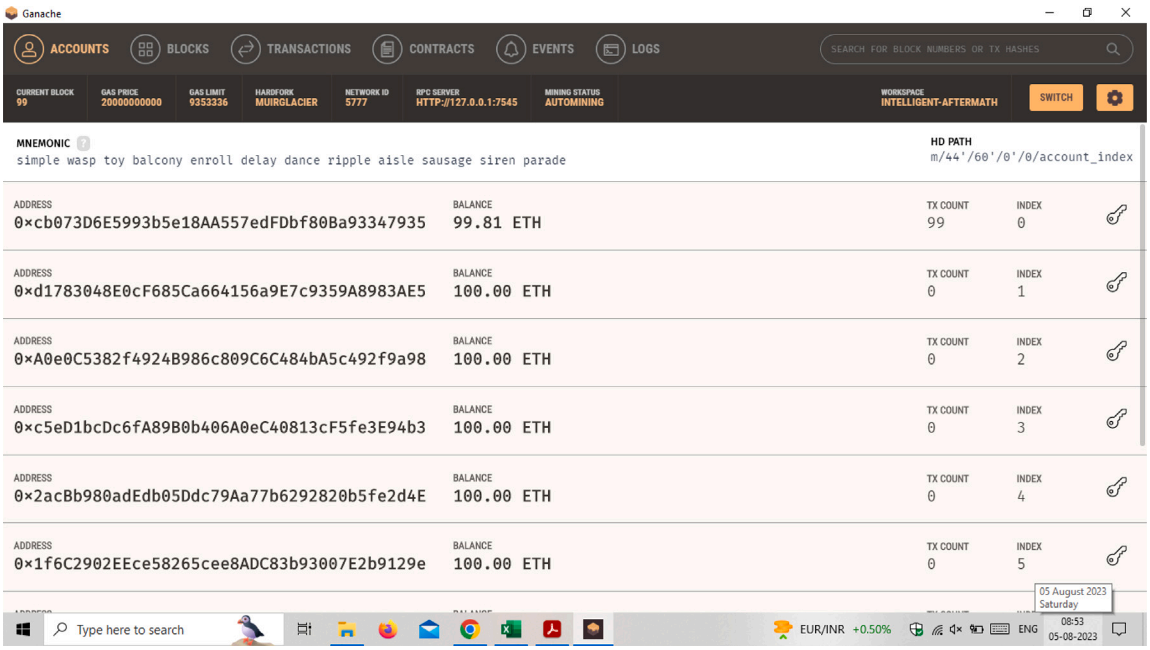


Fig. 7. Ganache interface.

Table 5
Configuration parameters (Mahmud et al., 2022).

Parameter	Cloud	Fog	Smartphone
CPU length (MIPS)	44 800	2800	2800
RAM (MB)	40 000	4000	4000
Uplink BW (MB)	100	10 000	10 000
Downlink BW (MB)	10 000	10 000	10 000
Busy power (J)	16*103	107.339	87.53
Idle power (J)	16*83.25	83.433	82.44

critical. The outcomes are subsequently transmitted to the patient's smartphone and cloud for storage. To establish the connection between the fog nodes and the cloud server, a proxy server is employed.

To collect sensor data, the client module is seamlessly incorporated into IoT devices. In contrast, the processing module is embedded within the edge/fog nodes, enabling them to handle the incoming data and conduct a thorough evaluation of the patient's health condition. After the analysis is finished, the edge/fog node forwards the findings to the connected IoT device, which then presents the information to the user.

Various parameters need to be defined during the generation of fog devices in iFogSim2, such as CPU length, Bandwidth, RAM, and more. The settings employed for device configuration in iFogSim2 (Mahmud et al., 2022) are listed in Table 5.

In summary, this simulation environment facilitates the evaluation of the proposed approach's performance by simulating the flow of ECG data from sensors to fog nodes, cloud storage, and end-user devices. It allows for the examination of various system configurations and parameter values to assess the efficiency and effectiveness of the proposed system in processing and analyzing real-time critical healthcare data.

In the iFogSim2 simulation, computational devices are categorized into fog devices, and they are available at various levels. The highest level, Level 3, represents the parent node, which functions as the cloud server. At Level 2, the fog nodes are connected to the cloud server through a proxy server. These fog nodes, situated at Level 1, are closer to the end-users and are considered edge devices. They offer more frequent computational and storage capabilities. At the lowest level, Level 0, IoT devices are equipped with sensors and actuators.

In iFogSim2, the physical topology is simulated using the MicroserviceFogDevice, Sensor, and Actuator classes. The scenarios are conducted on a computer system with an Intel Core i7 CPU running at 1.80 GHz and 4 GB of RAM. The input–output relationship's fractional selectivity within a module is configured to a value of 1.0.

This configuration enables the simulation of the proposed system's behavior across different levels of computational devices, from edge to fog and cloud servers, with realistic processing capabilities and communication links. The simulation is conducted on a standard computer setup, allowing for comprehensive evaluations of performance and efficiency under various scenarios.

6. Results and discussion

6.1. Dataset

6.1.1. Dataset for federated learning

The dataset utilized in this study, sourced from Kaggle (Lee and Lee, 2019), comprises 5000 ECG readings, each with 140 data points. The dataset also includes a label encoded as 0 or 1, indicating whether the corresponding ECG is considered abnormal or normal. The data points in columns 0–139 are represented as floating-point numbers, capturing the ECG readings for each patient. It is pertinent to mention that the dataset is not preprocessed, as the preprocessing of ECG values had already been conducted by the source of the dataset.

In terms of class distribution, the dataset contains approximately 58% of the tuples belonging to the normal class and the remaining 42% belonging to the abnormal class which helps in developing and evaluating the proposed approach efficiently.

6.1.2. Dataset for mobility

The EUA dataset (Lai et al., 2018) comprises geographical location details for numerous fog nodes situated within the Central Business District regions of major Australian cities, specifically Melbourne and Sydney. This dataset is structured into various regions, which are further subdivided into multiple blocks. In each block, one node is randomly assigned as the proxy server, ensuring a fine level of detail within the dataset. Within a given block, all nodes, with the exception of the proxy server, operate as gateways for IoT devices.

This repository contains a collection of EUA datasets sourced from real-world data. The datasets are openly accessible to the public and serve as valuable resources for supporting research in the domain of edge computing. The data provided in these datasets pertain to

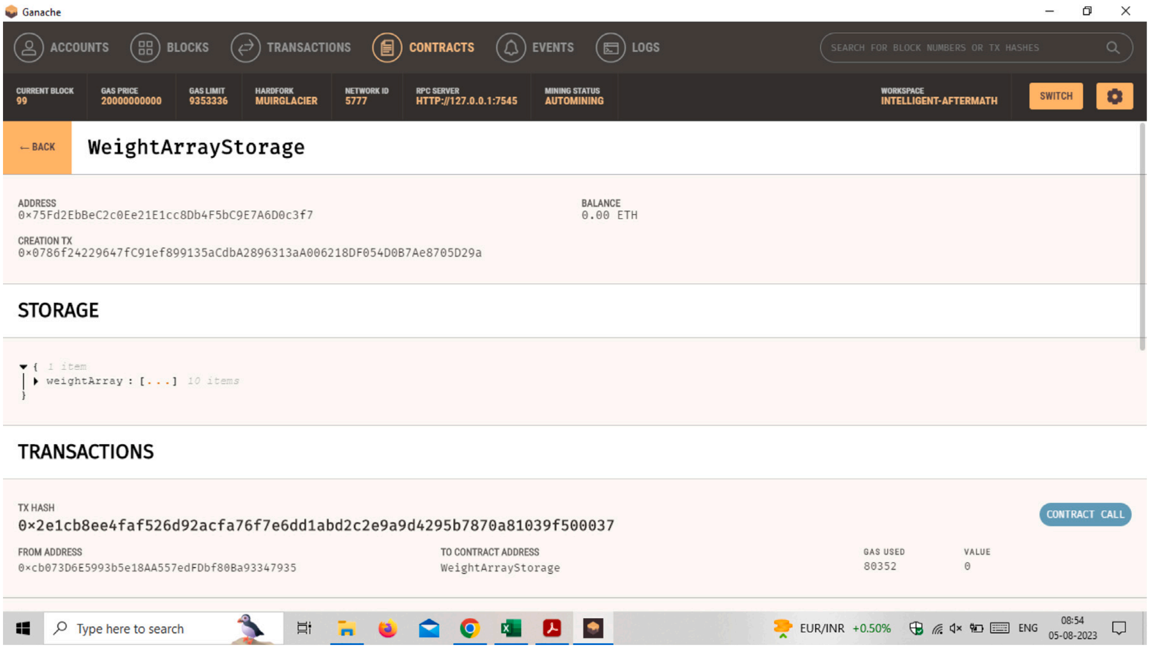


Fig. 8. Smart contract deployment.

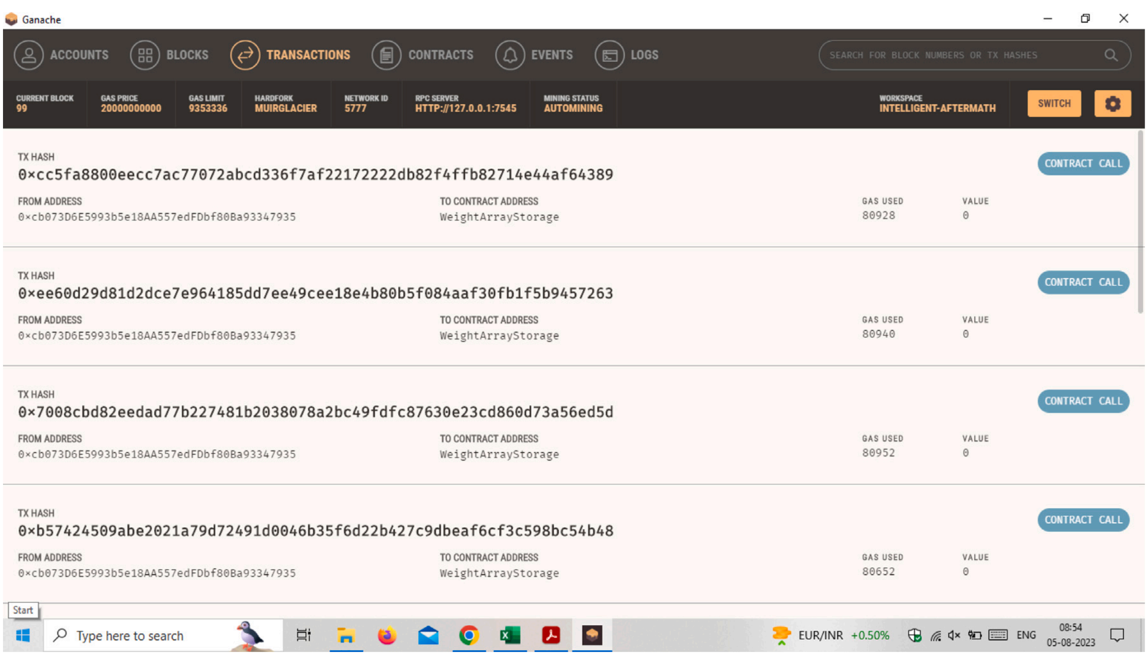


Fig. 9. Transactions.

the Australian region and are instrumental in creating more realistic simulations of natural time environments.

6.2. Analysis and observations

6.2.1. Blockchain-based federated learning (BCFL) deployment results in Ganche interface

The Ganache Interface encompasses functionalities for account management, network configuration, blockchain data, logs, and events. It enables users to create, import, and fund Ethereum accounts, configure network settings, and access vital blockchain information. Fig. 7 provides the snapshot of Ganache Interface of the proposed approach. The Smart Contract Deployment Interface within Ganache facilitates compiling and deploying Solidity contracts to the local or test Ethereum network. It includes a transaction history recording deployment details like transaction IDs and statuses, along with interaction capabilities for deployed contracts. Fig. 8 provides the snapshot of smart contract deployment interface component of the proposed approach. The Transactions page presents a comprehensive transaction history, displaying sender and receiver information, gas costs, timestamps, and transaction hashes. It aids in tracking transaction flow and associated data. Fig. 9 provides the snapshot of transactions of the proposed approach. The Created Blocks page serves as a block explorer, offering insights into each added block's details such as block numbers, timestamps, gas usage, and included transactions. It also provides information on the mining process and helps developers monitor blockchain structure and

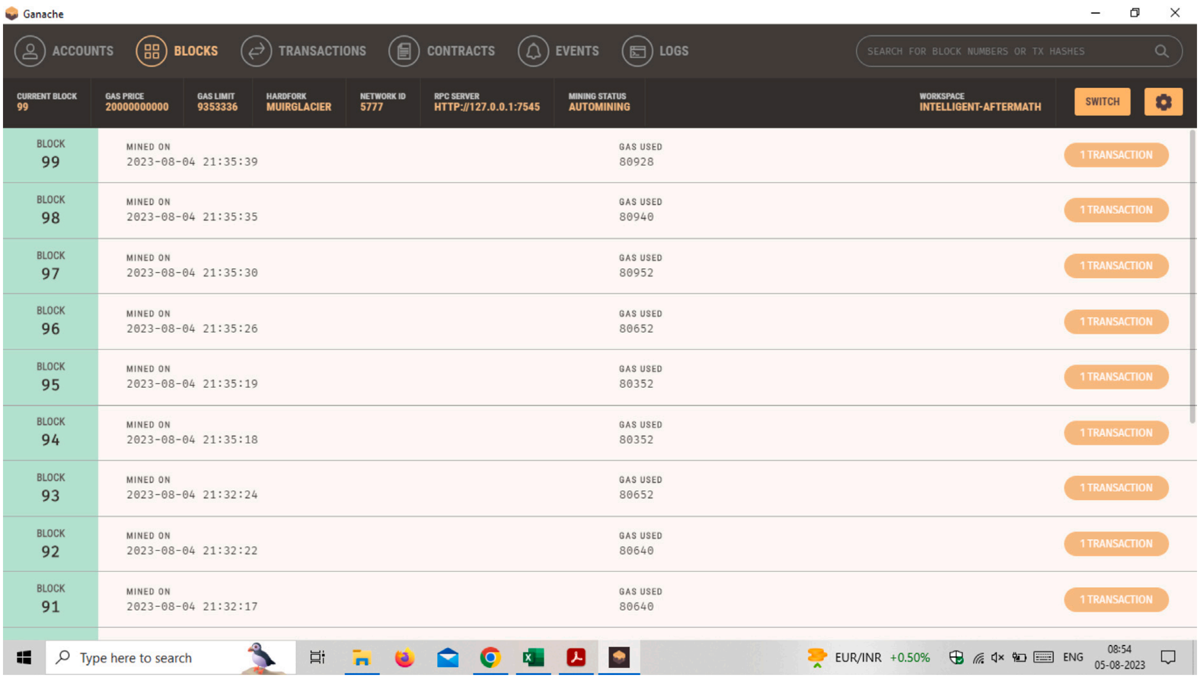


Fig. 10. Created blocks.

relationships between blocks and transactions. Fig. 10 provides the snapshot of details of the created blocks in the proposed approach.

After compiling the smart contract to generate bytecode, a process facilitated by Ganache's smart contract deployment interface, the interface provides tools to compile the Solidity contracts into bytecode and subsequently deploy them onto the local or test Ethereum network. Following successful deployment, interactions with the deployed smart contract are conducted through the Ganache interface. Specifically, calls to the functions defined within the smart contract which is described in 1, such as updateGlobalModel and getGlobalModel, are made to update and retrieve the latest version of the global model, respectively. During the evaluation process of the BCFL model, these interactions with the deployed smart contract play a crucial role. Clients participating in the FL process utilize the retrieved global model for local training and subsequently update it in the following rounds of federated learning. This iterative process allows for the seamless integration of the blockchain technology facilitated by Ganache into the BCFL model evaluation, ensuring transparency and integrity in the training process.

6.2.2. BCFL results for different layers placement of decision-making module

In this section, we present the results and observations of the proposed model, which were evaluated using different placement policies, as explained in the preceding sections. These reconstructed ECGs play a crucial role in predicting whether the ECG readings are anomalous. An ECG is considered anomalous if its reconstruction error surpasses a predefined threshold. The error values calculated from these figures facilitate the classification of ECG readings.

Fig. 11 also provides a comprehensive comparison of the performance parameters for various placement policies examined within this research. When the FL module is deployed in the edge layer, significant improvements are observed compared to placing it in the cloud layer. Specifically, deploying FL in the edge layer reduces cloud energy consumption by 1%, decreases network usage by 32%, cuts down costs by 23%, reduces execution time by 40%, and decreases latency by 80%.

Similarly, when comparing the FL module placement in the fog layer against the cloud layer, significant improvements are also observed. Deploying FL in the fog layer reduces cloud energy consumption by

Table 6
Comparison of Edge and Fog FL placement against Cloud.

Metric	Edge FL placement	Fog FL placement
Energy Consumption (J)	1.07%	.95%
Network Use (KB)	32%	31%
Cost ($)	23%	20%
Latency (ms)	80%	79%
Execution Time (ms)	40%	28%

Table 7
Comparison of Edge FL placement against Fog.

Metric	Edge FL placement
Energy Consumption (J)	0.1%
Network Use (KB)	1.1%
Cost ($)	3%
Latency (ms)	1%
Execution Time (ms)	16%

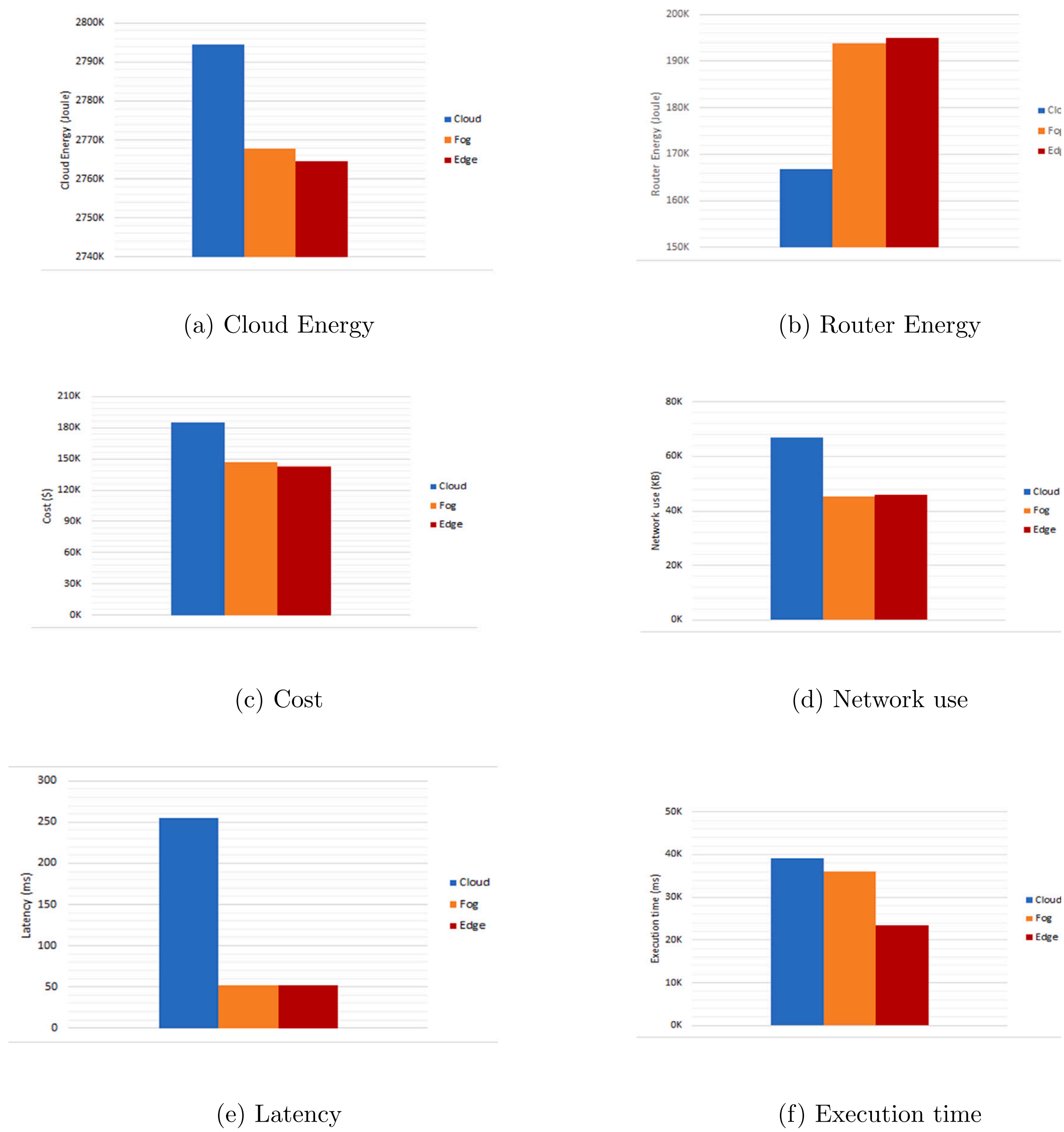
0,9%, decreases network usage by 31%, lowers costs by 20%, reduces execution time by 28%, and decreases latency by 79%.

Furthermore, a comparison between FL module placement in the edge and fog layers reveals that edge deployment outperforms fog deployment. Specifically, edge deployment shows improvements of 0.1%, 1.1%, 3%, 16%, and 1% in terms of energy consumption, network usage, costs, execution time, and latency, respectively.

Tables 6 and 7 compile the findings, facilitating a more comprehensive comprehension of the conducted comparisons. To summarize, the deployment of the FL module in the edge layer outperforms both fog and cloud layer deployments, supporting the incorporation of AI at the edge for efficient and intelligent healthcare systems. This configuration allows for immediate processing of clinical tests, enabling real-time or advanced remote patient monitoring.

6.2.3. BCFL results comparison with FL

In the upcoming paragraph, the results of the BCFL model are compared with those of the FL model without Blockchain, as depicted in Fig. 12. This comparative analysis aims to provide insights into the performance, efficiency, and effectiveness of the BCFL model in the

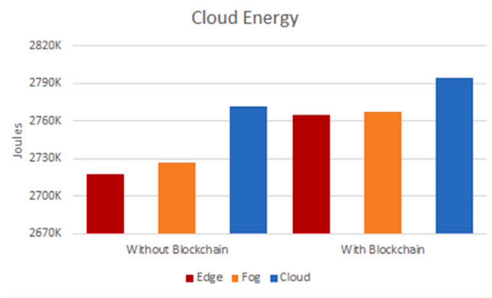


(a) Cloud Energy
(b) Router Energy
(c) Cost
(d) Network use
(e) Latency
(f) Execution time

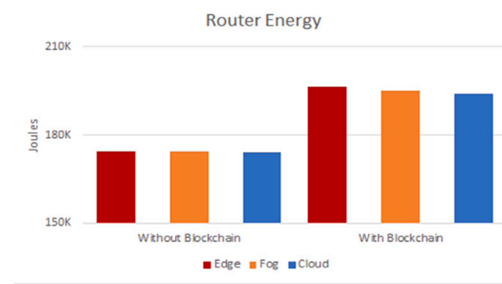
Fig. 11. Result of BCFL deployment in Edge/Fog/Cloud layers.

context of the specific application or scenario under investigation. The following description presents the findings from the comparison.

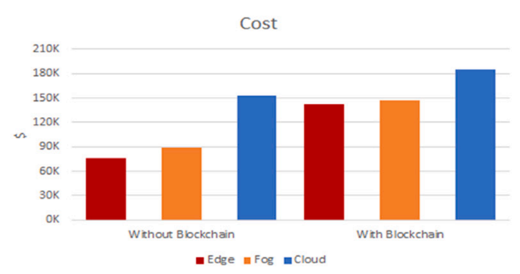
- The utilization of blockchain technology leads to a marginal increase in cloud energy consumption in comparison to scenarios where blockchain is not integrated. This elevated energy consumption can be attributed to the additional computational requirements associated with maintaining the blockchain network and validating transactions, ultimately impacting the overall energy expenditure in cloud environments.
- The incorporation of blockchain technology increases router energy consumption across edge, fog, and cloud layers when contrasted with setups without blockchain. This increase in energy usage can be attributed to the added computational demands imposed by blockchain-related processes, such as consensus mechanisms and cryptographic operations, impacting energy consumption in all layers of the network infrastructure.
- The cost associated with implementing blockchain deployments is greater when compared to setups that do not incorporate blockchain across edge, fog, and cloud layers. This increased cost can be attributed to several factors, including the complexity of blockchain infrastructure and the additional operational overhead required for maintaining blockchain networks, all of which collectively contribute to the higher overall costs in these multi-layer implementations.
- The utilization of network resources experiences a slight upsurge when blockchain technology is integrated, as opposed to scenarios where blockchain is not employed in the implementation across edge, fog, and cloud layers. This increment in network use can be due to the increased data transmission requirements associated with blockchain transactions and the propagation of blocks among nodes, which collectively contribute to the increased network usage observed in these multi-layer implementations.
- In the context of edge, fog, and cloud layer implementations, there is a slight increase in latency when blockchain technology is integrated, in contrast to setups where blockchain is not utilized. This heightened latency can be attributed to the additional computational processes and consensus mechanisms inherent to the



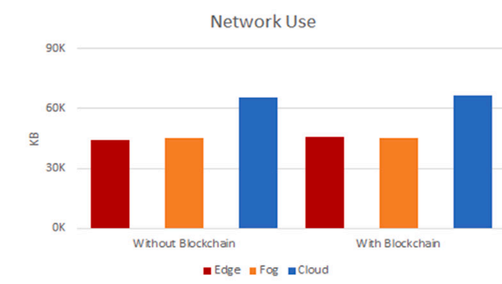
(a) Cloud Energy



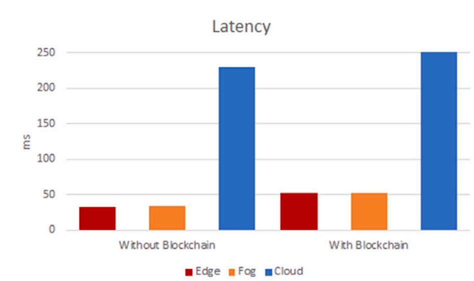
(b) Router Energy



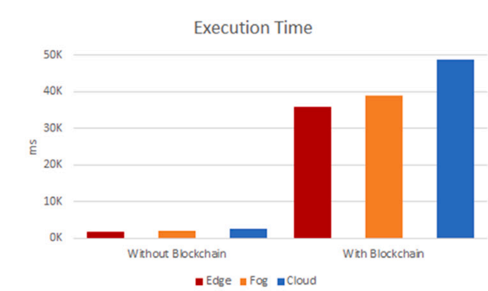
(c) Cost



(d) Network use



(e) Latency



(f) Execution time

Fig. 12. Result of FL deployment in Edge/Fog/Cloud layers with and without Blockchain integration.

blockchain, resulting in a delay in data processing and transmission, which ultimately leads to the observed increase in latency across these layers.

- Across the edge, fog, and cloud layer implementations, the execution time experiences an increase when blockchain technology is integrated, as opposed to scenarios where blockchain is omitted. This increase can be attributed to the additional computational processes and cryptographic operations that blockchain entails, leading to a delay in overall task completion and causing the observed increase in execution time across these layers.

In conclusion, the deployment of Blockchain-based Federated Learning (BCFL) in the Ganache interface brings significant advantages to the field of decentralized healthcare systems. Ganache's versatile interface streamlines account management, network configuration, and access to crucial blockchain data, while also facilitating logs and events tracking. Additionally, the results and observations obtained from the deployment of BCFL with different layers of decision-making modules showcase the effectiveness of this approach in optimizing healthcare systems. When BCFL is deployed in the edge layer, it leads to significant improvements, reducing cloud energy consumption, network usage, costs, execution time, and latency. Similar enhancements are observed when comparing BCFL deployment in the fog layer against the cloud layer. This data emphasizes the value of edge computing in healthcare, enabling real-time and advanced remote patient monitoring through the immediate processing of clinical tests. Furthermore, a comparison between BCFL and traditional FL models without blockchain integration reveals that BCFL introduces marginal increase in cloud energy and router energy consumption due to the added computations associated with blockchain maintenance and validation. The cost of implementing blockchain deployments and network resource utilization are higher, mainly due to the complexity of blockchain infrastructure and operational overhead. In addition, there is a minor increase in latency and execution time. Despite these trade-offs, BCFL presents promising opportunities for secure and efficient healthcare systems, particularly when deployed in edge computing environments. One notable limitation of the proposed approach lies in its partial consideration of energy consumption calculation aspects, neglecting comprehensive coverage. While it is true that blockchain introduces additional computational and network overheads, its usefulness in our approach is multifaceted and addresses several critical issues inherent in federated learning. The primary purpose of introducing blockchain is to tackle the security challenges associated with medical data and ensure privacy. Furthermore, the omission of thorough examination regarding real-time deployment issues further underscores a gap in the approach's scope.

7. Conclusions and future directions

In edge/fog environments, safeguarding patient privacy is pivotal due to the dynamic demands of critical medical IoT applications. This study investigates a blockchain-driven Federated Learning module tailored for ECG data in microservice-based IoT medical systems. We evaluate its efficacy across three deployment strategies—edge, fog, and cloud layers. Deploying Blockchain-based FL in Ganache streamlines healthcare solutions, with notable performance enhancements observed in edge deployment. However, integrating blockchain entails trade-offs in energy usage and expenses. Emphasizing privacy and security, Blockchain-driven Federated Learning emerges as essential for upholding the integrity of medical IoT applications and ensuring patient confidentiality. Even with improved Key Performance Indicators, safeguarding data privacy remains paramount. Likewise, FL deployments are significant for optimizing KPIs, provided there is a readiness to compromise on data privacy and security.

Future research will address the limitations of this work and focus on experimenting with the model's energy usage. The proposed method will be implemented, and additional aggregation techniques will be explored and deployed to enhance prediction models. Moreover, blockchain techniques will be leveraged to enhance system security in real-time edge/fog/cloud enviornments.

CRediT authorship contribution statement

Shinu M. Rajagopal: Conceptualization, Visualization, Writing – original draft, Validation, Methodology, Investigation, Formal analysis, Data curation, . **Supriya M.:** Writing – review & editing, Visualization, Validation, Supervision, Project administration, Methodology, Investigation, Formal analysis, Conceptualization, . **Rajkumar Buyya:** Writing – review & editing, Visualization, Validation, Supervision, Software, Resources, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

Aich, S., Sinai, N.K., Kumar, S., Ali, M., Choi, Y.R., Joo, M.-I., Kim, H.-C., 2021. Protecting personal healthcare record using blockchain federated learning technologies. In: 2021 23rd International Conference on Advanced Communication Technology. ICACT, pp. 109–112. http://dx.doi.org/10.23919/ICACT51234.2021.9370566.

Ali, M., Karimipour, H., Tariq, M., 2021. Integration of blockchain and federated learning for internet of things: Recent advances and future challenges. Comput. Secur. 108, 102355.

Awan, S.M., Li, F., Luo, B., Liu, M., 2019. Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. URL https://api.semanticscholar.org/CorpusID:203645025.

Bao, X., Su, C., Xiong, Y., Huang, W., Hu, Y., 2019. Flchain: A blockchain for auditable federated learning with trust and incentive. In: 2019 5th International Conference on Big Data Computing and Communications. BIGCOM, IEEE, pp. 151–159.

Bharathi, P.D., Narayanan, V.A., Sivakumar, P.B., 2022. Fog computing enabled air quality monitoring and prediction leveraging deep learning in IoT. J. Intell. Fuzzy Systems 43 (5), 5621–5642.

Cheikhrouhou, O., Mahmud, R., Zouari, R., Ibrahim, M., Zaguia, A., Gia, T.N., 2021. One-dimensional CNN approach for ECG arrhythmia analysis in fog-cloud environments. IEEE Access 9, 103513–103523.

Chen, Y., Qin, X., Wang, J., Yu, C., Gao, W., 2020. FedHealth: A federated transfer learning framework for wearable healthcare. IEEE Intell. Syst. 35 (4), 83–93. http://dx.doi.org/10.1109/MIS.2020.2988604.

Cherukuri, R.V., Devi, G.L., Ramesh, N., 2024. Federated learning with blockchain-based model aggregation and incentives. Int. J. Comput. Appl. URL https://api.semanticscholar.org/CorpusID:268557243.

Dias, H., Meratnia, N., 2022. BlockLearning: A modular framework for blockchain-based vertical federated learning. In: International Conference on Ubiquitous Security. URL https://api.semanticscholar.org/CorpusID:256903037.

Drungilas, V., Vaičiukynas, E., Jurgelaitis, M., Butkienė, R., Čeponienė, L., 2021. Towards blockchain-based federated machine learning: Smart contract for model inference. Appl. Sci. 11 (3), 1010.

Ejaz, M., Kumar, T., Kovacevic, I., Ylianttila, M., Harjula, E., 2021. Health-blockedge: Blockchain-edge framework for reliable low-latency digital healthcare applications. Sensors 21 (7), 2502.

Fan, S., Zhang, H., Zeng, Y., Cai, W., 2020. Hybrid blockchain-based resource trading system for federated learning in edge computing. IEEE Internet Things J. 8 (4), 2252–2264.

Jin, L.-p., Dong, J., 2018. Intelligent health vessel ABC-DE: an electrocardiogram cloud computing service. IEEE Trans. Cloud Comput. 8 (3), 861–874.

Kim, H., Park, J., Bennis, M., Kim, S.-L., 2019. Blockchained on-device federated learning. IEEE Commun. Lett. 24 (6), 1279–1283.

Kumar, R., Khan, A.A., Kumar, J., Zakria, A., Golilarz, N.A., Zhang, S., Ting, Y., Zheng, C., Wang, W., 2021. Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging. IEEE Sens. J. 1. http://dx.doi.org/10.1109/JSEN.2021.3076767.

Lai, P., He, Q., Abdelrazek, M., Chen, F., Hosking, J., Grundy, J., Yang, Y., 2018. Optimal edge user allocation in edge computing with variable sized vector bin packing. In: International Conference on Service-Oriented Computing. Springer, pp. 230–245.

Lakhan, A., Mohammed, M.A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., Alkhayyat, A., Wang, W., 2022. Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. IEEE J. Biomed. Health Informat. 27 (2), 664–672.

Lee, W.-M., Lee, W.-M., 2019. Testing smart contracts using ganache. Begin. Ethereum Smart Contracts Program. With Examples Python, Solidity, JavaScript 147–167.

Lu, Y., Huang, X., Dai, Y., Maharjan, S., Zhang, Y., 2020a. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Trans. Ind. Inform. 16 (6), 4177–4186. http://dx.doi.org/10.1109/TII.2019.2942190.

Lu, Y., Huang, X., Zhang, K., Maharjan, S., Zhang, Y., 2020b. Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Trans. Veh. Technol. 69 (4), 4298–4311. http://dx.doi.org/10.1109/TVT.2020.2973651.

Mahmud, R., Pallewatta, S., Goudarzi, M., Buyya, R., 2022. IFogSim2: An extended iFogSim simulator for mobility, clustering, and microservice management in edge and fog computing environments. J. Syst. Softw. (JSS).

Moghadas, E., Rezazadeh, J., Farahbakhsh, R., 2020. An IoT patient monitoring based on fog computing and data mining: Cardiac arrhythmia usecase. Internet Things 11, 100251.

Mohanta, B.K., Jena, D., Panda, S.S., Sobhanayak, S., 2019. Blockchain technology: A survey on applications and security privacy challenges. Internet Things 8, 100107.

Myrzashova, R., Alsamhi, S.H., Shvetsov, A.V., Hawbani, A., Wei, X., 2023. Blockchain meets federated learning in healthcare: A systematic review with challenges and opportunities. IEEE Internet Things J. 1. http://dx.doi.org/10.1109/JIOT.2023.3263598.

Passerat-Palmbach, J., Farnan, T., McCoy, M., Harris, J.D., Manion, S.T., Flannery, H.L., Gleim, B., 2020. Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data. In: 2020 IEEE International Conference on Blockchain (Blockchain). pp. 550–555. http://dx.doi.org/10.1109/Blockchain50366.2020.00080.

Passerat-Palmbach, J., Farnan, T., Miller, R., Gross, M.S., Flannery, H.L., Gleim, B., 2019. A blockchain-orchestrated federated learning architecture for healthcare consortia. arXiv preprint arXiv:1910.12603.

Pokhrel, S.R., Choi, J., 2020. Federated learning with blockchain for autonomous vehicles: Analysis and design challenges. IEEE Trans. Commun. 68 (8), 4734–4746. http://dx.doi.org/10.1109/TCOMM.2020.2990686.

Prabhu, M., Hanumanthaiah, A., 2022. Edge computing-enabled healthcare framework to provide telehealth services. In: 2022 International Conference on Wireless Communications Signal Processing and Networking. WiSPNET, IEEE, pp. 349–353.

Prakash, P., Darshaun, K., Yaazhlene, P., Ganesh, M.V., Vasudha, B., 2017. Fog computing: issues, challenges and future directions. Int. J. Electr. Comput. Eng. 7 (6), 3669.

Qu, Y., Gao, L., Luan, T.H., Xiang, Y., Yu, S., Li, B., Zheng, G., 2020a. Decentralized privacy using blockchain-enabled federated learning in fog computing. IEEE Internet Things J. 7 (6), 5171–5183.

Qu, Y., Gao, L., Luan, T.H., Xiang, Y., Yu, S., Li, B., Zheng, G., 2020b. Decentralized privacy using blockchain-enabled federated learning in fog computing. IEEE Internet Things J. 7 (6), 5171–5183. http://dx.doi.org/10.1109/JIOT.2020.2977383.

Rahman, M.A., Hossain, M.S., Islam, M.S., Alrajeh, N.A., Muhammad, G., 2020. Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. Ieee Access 8, 205071–205087.

Rajagopal, S.M., Supriya, M., Buyya, R., 2023. Fedsdm: Federated learning based smart decision making module for ecg data in IoT integrated edge-fog-cloud computing environments. Internet Things 100784.

Ratta, P., Kaur, A., Sharma, S., Shabaz, M., Dhiman, G., 2021. Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. J. Food Quality 2021, 1–20.

Wan, Y., Qu, Y., Gao, L., Xiang, Y., 2022. Privacy-preserving blockchain-enabled federated learning for B5G-driven edge computing. Comput. Netw. 204, 108671.

Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., Kim, D.I., 2019. A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access 7, 22328–22370. http://dx.doi.org/10.1109/ACCESS.2019.2896108.

Zhang, W.-Z., Elgendy, I.A., Hammad, M., Iliyasu, A.M., Du, X., Guizani, M., Abd El-Latif, A.A., 2020a. Secure and optimized load balancing for multitier IoT and edge-cloud computing systems. IEEE Internet Things J. 8 (10), 8119–8132.

Zhang, Q., Palacharla, P., Sekiya, M., Suga, J., Katagiri, T., 2020b. Demo: A blockchain based protocol for federated learning. In: 2020 IEEE 28th International Conference on Network Protocols. ICNP, pp. 1–2, URL https://api.semanticscholar.org/CorpusID:227123071.

Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., Gao, Y., 2021. A survey on federated learning. Knowl.-Based Syst. 216, 106775. http://dx.doi.org/10.1016/j.knosys.2021.106775, URL https://www.sciencedirect.com/science/article/pii/S0950705121000381.

Zhao, Y., Zhao, J., Jiang, L., Tan, R., Niyato, D., Li, Z., Lyu, L., Liu, Y., 2020. Privacy-preserving blockchain-based federated learning for IoT devices. IEEE Internet Things J. 8 (3), 1817–1829.

Shinu M. Rajagopal received her B.Tech degree in Electronics and Communications from Calicut University, India, and an M.E. degree in Computer Science and Engineering from Anna University, India, in 2008. She received her Ph.D. in CSE from Amrita Vishwa Vidyapeetham, Bengaluru. She has over 12 years of teaching experience. Her research interests include Distributed Computing, Cloud Computing, Fog Computing, and Edge Computing.

Dr. Supriya M. is an Associate Professor in the Department of Computer Science & Engineering at the Amrita School of Computing, Amrita Vishwa Vidyapeetham, Bengaluru, India. She holds a Ph.D. in Computer Science and Engineering from Amrita Vishwa Vidyapeetham, India.With over 24 years of teaching experience, including 14 years in research, she has published more than 70 Scopus-indexed papers in prestigious journals and conferences. Her research spans Parallel and Distributed Computing, Cloud Computing, Edge, and Fog Computing, with a special focus on the integration of these technologies to enhance IoT systems. Additionally, she is exploring scalable computing architectures and leveraging AI for resource management within Cloud, Fog, and Edge environments, focusing on their applications in developing next-generation smart infrastructures. Dr. Supriya is an active member of the ACM Professional Chapter.

Dr. Rajkumar Buyya (Fellow, IEEE) is a Redmond Barry Distinguished Professor and Director of the Cloud Computing and Distributed Systems (CLOUDS) Laboratory at The University of Melbourne, Australia. He is also the Founder and CEO of Manjrasoft, a spin-off company commercializing cloud computing technologies. He has served as an Honorary/Visiting Professor at several elite universities, including Imperial College London, U.K., and the University of Birmingham, U.K. Dr. Buyya has written over 850 publications, including seven textbooks. He has been recognized as a Web of Science Highly Cited Researcher for five consecutive years since 2016. He was named Scopus Researcher of the Year 2017 and received the Excellence in Innovative Research Award from Elsevier and the "Best of the World" in Computing Systems by The Australian 2019 Research Review. He has authored over 850 publications and seven textbooks. He is one of the highly cited authors in computer science and software engineering worldwide (h-index 169 with 153,285+ citations). He is among the world's top 2 most influential scientists in distributed computing in terms of both single year impact and career-long impact based on a composite indicator of Scopus citation database.