Blockchain-based e-Medical Record and Data Security Service Management based on IoMT resource

Raaid Alubady[1,*], Rawan A.shlaka[2], Hussein Alaa Diame[3], Sarah Ali Abdulkareem[4], Ragheed Hussam[5], Sahar Yassine[6], Venkatesan Rajinikanth[7]

[1]Technical Engineering College, Al-Ayen University, Thi-Qar, Iraq
[2]Department of Medical Devices Engineering Technologies, National University of Science and Technology, Dhi Qar, Nasiriyah, Iraq
[3]Technical Computer Engineering Department, Al-Kunooze University College, Basrah, Iraq
[4]Computer Technologies Engineering, Al-Turath University College, Baghdad,Iraq
[5]Medical instruments engineering techniques, Al-farahidi University, Baghdad, Iraq
[6]Department of Applied Data Science, Noroff University College, Kristiansand, Norway
[7]Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai 602105, India.

Emails: alubadyraaid@alayen.edu.iq; rawan-a.shlaka@nust.edu.iq; Hussein.Alaa@Kunoozu . Edu . Iq; sarah.ali@turath.edu.iq ; Ragheed Hussam@uoalfarahidi.edu.iq; sahar.yassine@noroff.no; v.rajinikanth@ieee.org
[*]Corresponding Author: alubadyraaid@alayen.edu.iq

Abstract

The confidentiality of electronic medical records (E-Medical records) is of the utmost importance. Consequently, healthcare companies are responsible for ensuring their patients' medical records' privacy, security, and service management. Innovative agreements will ensure patient satisfaction for management. The study's primary goals are to enhance data security service management and reduce the amount of external involvement with healthcare data. This study explores a novel approach to improve the security and confidentiality of e-medical information by examining the feasibility of utilizing the blockchain system within the context of the IoMT (Internet of Medical Things). The medical care management platform uses blockchain technology to manage e-health records effectively. This paper presents a paradigm for e-medical record services based on IoMT resources, which integrates blockchain technology with Secure Federated Learning (BT-SFL-IoMT). The data is stored on blockchain, and predictions and analyses are made using secure federated learning. Hyper ledger Analyzer is used to assess the latency and speed of blockchain transactions and capture access activity and authorization events. As verified by the results, the functionality is resistant to unauthorized retrievals and fits the needs of real-world settings while securing e-medical records. Many metrics, including testing accuracy of federated learning, Convergence speed, and Performance analysis of the proposed model, demonstrate its efficient use in secure databases.

Keywords: e-health; blockchain; Internet of Medical Things; health information management

DOI: https://doi.org/10.54216/JISIoT.080207
Received: August 21, 2022 Accepted: February 26, 2023 (corrected version: January 17, 2024)

1. Introduction

Medical information is growing as the level of digitization in healthcare organizations keeps growing. The effective integration of healthcare resources and enhancing physicians' diagnostic and therapeutic capabilities depend on the broad adoption of e-medical records [1]. Contrarily, individuals' medical records are an invaluable asset that contains a wealth of sensitive data. There is a grave danger to patients' lives and possessions in exchanging medical data due to the high probability of data breaches and misuse [2].

Informational islands are created because medical records are dispersed among different healthcare organizations, and information retention formats make it challenging to achieve data exchange [3]. It has led to the realization that there is an urgent need to solve the problems of medical security and data management to facilitate data exchange and eliminate information barriers across different medical data systems [4]. Individuals have to have faith that the entities responsible for maintaining their medical records will not misuse their information for greed or any other reason. Patients should be able to manage who can access their medical records and where and for what reasons, as they are the data owners [5]. A patient's medical records, including their diagnosis, prescriptions, surgeries, and dietary restrictions, are recorded on the blockchain. Protecting the sensitive information in electronic medical records from prying eyes is paramount [6]. In conventional data storage, unauthorized individuals or hackers can access the information in the electronic medical form. Internet of Things (IoT) devices have been in considerable demand in recent years for a variety of reasons, including the need for more efficient and speedy manufacturing processes, the need to upgrade military capabilities, and the desire to turn everyday objects into clever ones in the form of homes, factories, and cities [7]. Despite their many advantages, IoMT devices aren't without their flaws [8]. Figure 1 depicts the layers of the IoMT structure, including the device, edge computing, blockchain, and Application layers.

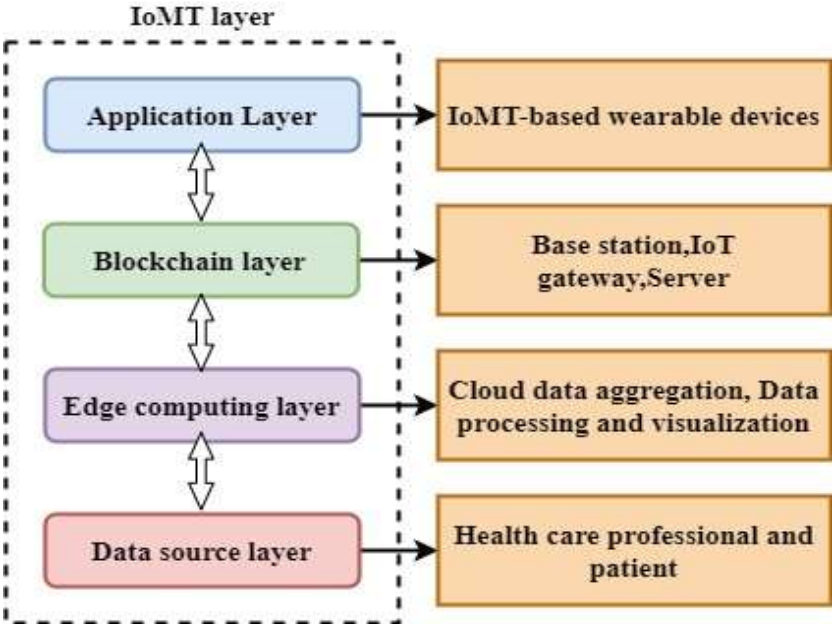

Fig1. IoMT structure

The data source layer is responsible for gathering information straight from the source and drawing meaningful conclusions from it. The data source layer is responsible for gathering information straight from the source and drawing meaningful conclusions from it. The data collection sublayer uses a variety of medical perception and communications gathering equipment to perform its primary function, which is to provide the edge computing layer with perception based on the acquired data. Graphic codes, radio frequency identification, and global positioning systems are the most frequently used methods to achieve signals [9-10]. The computing layer collects data via short-term data transfer strategies like Bluetooth connectivity, Wireless Fidelity (Wi-Fi), ZigBee, etc. It sends it to the blockchain layer, which provides services related to platforms and interfaces and offers secure data transmission methods [11]. With the data collected at the network layer, the apps at the application layer maintain the patient's

DOI: https://doi.org/10.54216/JISIoT.080207
Received: August 21, 2022 Accepted: February 26, 2023 (corrected version: January 17, 2024)

medical record [12]. While the medical data decision-making application layer handles the analysis of various pieces of information, the medical information application layer stores various healthcare equipment and other information-related materials for keeping patient records [13]. For example, they produce massive amounts of data, use a lot of energy when operating, and raise concerns about trust due to their centralization and the fact that an administrator can alter the system's core components or disable them altogether. Devices connected to the IoMT can gather data from their immediate environment, share it, and send it to an administrative server [14]. Data collected by IoMT devices can be safely and consistently shared between them or uploaded to an edge server using blockchain technology.

Combined learning on top of blockchain technology was used to mitigate these risks and weaknesses. A revolutionary approach to deep knowledge, Secure Federated Learning renders it possible to acquire information in decentralized settings [15]. This research suggests a resolution to prevent this problem by implementing automated preservation of e-medical records on a blockchain. This tool also makes it easier to analyze the patient's EMR and other historical data to build a recommendation system for personalized treatment.

The main contribution of the paper include

1. The BT-SFL-IoMT paradigm for e-medical record services uses blockchain technology and Heterogeneous Federated Learning.

2. Hybrid federated learning predicts and analyzes blockchain data. Hyper ledger analyzer measures blockchain transaction latency, speed, access activity, and authorization events.

3. The results show that the functionality secures e-medical records and meets real-world needs. Recall, accuracy, and F1 scores show its efficiency in cloud-safe databases.

The paper is structured in the following manner: Section 2 provides an overview of the current body of research on the subject. Section 3 proposes novel methods for the BT-HFL-IoMT paradigm in electronic medical records. Section 4 gives the experiment's findings—and finally, Section 5 offers concluding remarks.

2. Related Works

2.1. Integrated EMR Management

[16] proposed a safe data-sharing architecture for dispersed multiple parties empowered by blockchain technology. Privacy-preserving federated learning converts the issue of sharing data into a problem related to machine learning. Data privacy is efficiently maintained by revealing the data model instead of the actual data. Integrating federated learning with permissioned blockchain consensus enables the reutilization of computational resources for federated training. The suggested data-sharing strategy gets excellent efficiency, higher safety, and outstanding accuracy, according to statistical results obtained from datasets from the real world.

[17] present an efficient framework for intelligent healthcare that uses blockchain technology and federated learning to protect patient privacy when using Internet of Things (IoT) cloud services. Healthcare and other scalability machine learning applications often use Federated Learning technology. On top of that, consumers don't need to upload sensitive data to the cloud to get a well-trained ML model. In addition, the article covered the uses of federated learning in a technologically advanced city's decentralized, secure infrastructure.

[18] proposed a blockchain-based federated Learning framework with Committee consensus (BFLC), a distributed blockchain-based solution to overcome safety concerns in federated learning. The framework employs blockchain technology for global and local model storage and version exchange, eliminating the need for a centralized server. The novel panel agreement system enables the suggested BFLC and successfully decreases the processing power required for consensus and the frequency of malicious attacks. Finally, experiments were performed on many frameworks using the actual data set FEMNIST and the

DOI: https://doi.org/10.54216/JISIoT.080207
Received: August 21, 2022 Accepted: February 26, 2023 (corrected version: January 17, 2024)

AlexNet model, all inside the context of a FISCO blockchain technology network. The experimental results prove the BFLC framework to be effective and secure.

[19] suggested a two-stage federated learning method based on blockchain technology (2-stage FL-BT). Without transmitting information to a central database, IoMT devices can collaborate in training a global model. Specifically, it has created a blockchain-based data-sharing system that could fix the problem of lousy training results on non-independent, equally distributed data by drastically improving the model's accuracy without compromising user privacy—the method in simulated environments using three well-known datasets: MFNIST, Fashion at MNIST, and CIFAR-10.

[20] proposed an Edge-Enabled Blockchain Federated Learning system (EE-BFL) to manage resources in the IoMT, which will help with the security challenges. The federated learning system offers a linear regression model as an improved global learning strategy. The enhanced security features of blockchain also benefit edge computing and the IoMT. In addition, for tracking and preservation, the distributed ledger securely stores all transactions that include IoMT and peripheral devices. The outcomes demonstrate that the suggested approach decreases computing expenses while accomplishing privacy and security goals. Research into the recommended system also turned up no security holes.

[21] offer a BGFL, which stands for blockchain-enabled gossip federated learning, to address issues with security and performance. Instead of using a central server, BGFL now uses a blockchain-enabled system to store and exchange models worldwide. In addition, clients communicate through gossip training to speed up the training convergence. The next step is to evaluate the capabilities using the MNIST and CIFAR datasets in trials that do not involve IID scenarios. The experimental findings of the BGFL framework demonstrate practicality and good performance.

[22] provide a FedDual, a method for large-scale decentralized FL networks that is sequential and centralized, with three distinct safety issues for local gradient aggregation and global model updates. FedDual surpasses gossip-based decentralized FL methods in communication efficacy and confidentiality and blockchain-assisted distributed FL methods in computing efficiency. FedDual's local differential privacy (LDP) implementation aggregates local gradients individually via a pair-wise gossip approach. First and most importantly, the noise reduction method allows FedDual to create global models with better predictors and faster convergence than LDP-based FL methods.

[23] present an analytics framework that works with the edge and uses Federated Learning to retrain local machine learning models with user data. This architecture can potentially employ pre-trained models to derive user-specific insights while protecting the privacy of users and Cloud resources. There is also a discussion of many potential use cases and issues with the proposed framework for further study.

[24] developed an FL-BETS (Federated Learning-Based Blockchain-Enabled Task Scheduling) framework for blockchain-enabled task scheduling using several dynamic heuristics. The study examines distributed fog and cloud node-based healthcare applications with hard and soft restrictions. FL-BETS reduces energy consumption and delays while fulfilling healthcare workload deadlines by identifying and protecting data privacy and fraud at various layers, including local fog nodes and remote clouds. FL-BETS beat all machine learning and blockchain methods in healthcare applications with energy, time, information validation, and fraud investigation constraints.

3. System Methodology

3.1 Overview of BT-SFL-IoMT

The standard methods of storing electronic medical records must be safeguarded against online assaults and independent verification due to the sensitive nature of their information. Figure 2 offered the structure of the BT-SFL-IoMT approach as a solution to this problem. E-medical records have recently replaced paper ones in several institutions. An IoMT clever healthcare network consists of several interconnected intelligent medical equipment. The IoMT paradigm is the building block of innovative healthcare. Initially, a patient's vital signs will be recorded utilizing a Wireless Sensor Network (WSN), which consists of sophisticated sensors embedded in wearable devices. This e-medical record will make the patient's diagnosis, treatment, and other relevant forms available anytime. E-medical documents that rely on IoMT must prioritize providing necessary security

DOI: https://doi.org/10.54216/JISIoT.080207
Received: August 21, 2022 Accepted: February 26, 2023 (corrected version: January 17, 2024)

measures. AI can also enhance IoMT security by identifying intrusions into networks and subsequent security attacks within IoMT systems.

Medical servers that use electronic health records, such as MedRec, can benefit from blockchain technology in the IoMT by enhancing the security of their data management, access control, and permission processes. Because it includes personal information about the patient, e-medical records must be encrypted. In the proposed technology, an e-medical record system is secured based on the gossip digital ledger that has been unveiled. Hyperledger Fabric is used for data storage to monitor when a record is modified. Secure Federated learning-based data management suggestion is another primary focus of the effort. Safe federated learning has become more common in these settings, and distributed optimization, large-scale machine learning, and privacy must progress for federated learning to materialize. A potential approach for developing cost-effective, innovative healthcare applications that enhance data management and privacy protection is secure in federated learning. Theoretically, safe training is a decentralized AI approach that aggregates and averages local updates from different health data clients, like IoMT devices, to enable the development of great AI models. It conceals user choices and data, lowering the risk of privacy leaks.

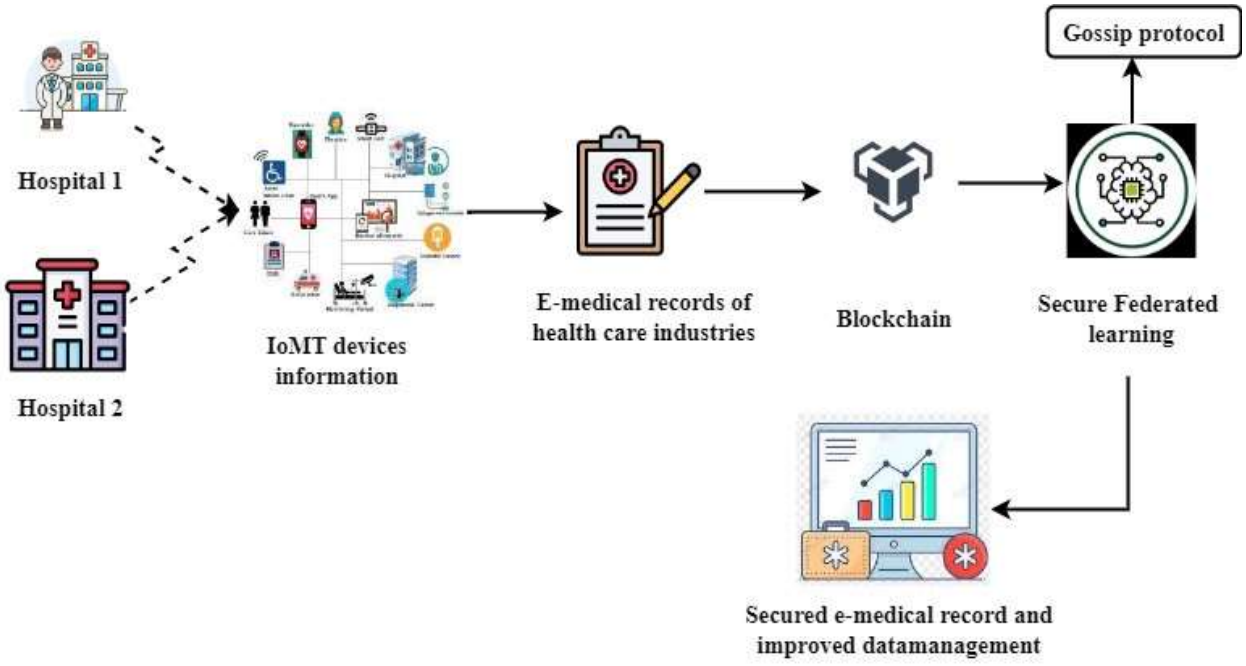

Fig.2 Structure of BT-SFL-IoMT

Another use case for blockchain technology is enhancing the safety of e-medical records in the IoMT network. The blockchain has a complete patient medical history record, including diagnosis, medications, surgeries, and dietary restrictions. Stringent security measures must be in place to protect the susceptible information contained in e-medical records from prying eyes. E-medical documents stored in the conventional are vulnerable to data retrieval by unauthorized individuals or intruders. Appropriate data processing and comprehension techniques based on AI can be used for analysis after receiving medical data. The suggested model for the IoMT network involves integrating secure federated learning with blockchain technology, which allows for the recording and tracking electronic medical records up to an expiration period. Data management, which is the process of gathering, storing, and using data safely, efficiently, and cost-effectively, is the proposed activity's primary objective.

3.2 Blockchain technology

Blockchain technology can record and keep data and transactions because of its organized block structure. But, the blockchain functions as a trustworthy decentralized database. Information on the time, date, price, and parties involved in a transaction is contained in a data block. Almost a single node in the distributed ledger technology known as blockchain checks the legitimacy of transactions without ever meeting each other. Every block in the network has two hash codes: one from before and one from now. For data privacy and security on the blockchain to be maintained, any changes made to one block must be reflected in all other blocks that contain that change within a reasonable amount of time. All blocks in the network are securely connected and

DOI: https://doi.org/10.54216/JISIoT.080207
Received: August 21, 2022 Accepted: February 26, 2023 (corrected version: January 17, 2024)

safeguarded by crypto and transaction codes. Miner nodes can validate these blocks using robust mathematical techniques; the blocks are put into the blockchain. Blockchain technology guarantees both security and openness. A system that saves information in a series of blocks following predetermined rules is known as blockchain technology. Every node in the network operates independently but is subject to the same protocol, which allows them to form transactions by adding blocks to the chain. There is a record of every transaction that has ever taken place on the Blockchain network, which includes details about all participants and the transactions themselves. Public and private information coexist on these networks. They lack complete decentralization. One such platform is Hyperledger Fabric. The private blockchain network ensures the utmost secrecy of all data and transactions. This information is only visible to authorized users of the network. Like in a consortium network, the admin node is the only one to add nodes. For instance, many blockchain systems, Hyperledger, etc. When protecting sensitive medical information, blockchain is the way to go. This paper focuses on Secure patient medical data, which employs blockchain technology and the Hyperledger fabric. In addition to securing the data, the proposed effort aims to lay the groundwork for a recommendation system. Finally, after reviewing the patient's medical record, it presents the suggestion module to provide an individualized treatment plan. The dataset is also used to train machine learning models to advise patients on the most appropriate tailored treatment.

3.3 Secure federated learning with blockchain

Secure federated learning is based on the idea of learning from devices nearby. Communication with additional locations or central servers is unnecessary for data generated by end users or any equipment installed in hospitals or homes. Privacy of data is protected. Each IoMT may build its model using locally collected data using the suggested method; there's no need for connectivity with the central server in the cloud. Next, every IoMT sends its primarily trained local model to the prominent edge server. The benefit of federated learning leads to its adoption in numerous other fields, including healthcare, business, internet safety, etc. Using the Internet of Medical Things (IoMT) devices, Fig. 3 shows how secure joint learning occurs. Its primary goal is to use blockchain technology to record financial transactions securely and secretly. Every single block has several transactions in it. In exchange for their work, mining workers obtain rewards for validating all those operations.

There are two sections to the proposed work:

1. E-health records stored in several blockchains by various healthcare services.

2. It uses federated learning and the gossip protocol to apply data from many sources.

Many healthcare facilities store patient information on blockchains, including hospitals, clinics, and diagnostics groups. This data is gathered from many blockchain types. Each blockchain protocol has its own unique set of features and capabilities. Several operations are recorded in each block, and miners are incentivized to verify and store this data in the blocks. Medical information acquired via a federated server is then processed using the blockchain, which keeps the data in the blockchain using Hyper ledger fabric and IPFS. Since federated learning (FL) systems are vulnerable to security threats, including ingestion, speculation, and backdoors, it is crucial to investigate safe solutions for FL-enabled medical applications to avoid unreliable updates—a novel idea, reputation, within the framework of FL-enabled healthcare systems. An essential part of preventing various security breaches is using trustworthy device choices. When learning local training models with low-quality and noiseless data, it is crucial to choose devices reliably.

Algorithm 1 of federated learning

1. Input (x,a)
2. Wait for del_g
3. Loop
4. For every node, N in parallel, do
5. send (x,a) N
6. receive (x_r, a_r) from d
7. end
8. x $\frac{1}{|k|\sum y_N}$ N belongs to k

DOI: https://doi.org/10.54216/JISIoT.080207
Received: August 21, 2022 Accepted: February 26, 2023 (corrected version: January 17, 2024)

9. x⟵x+K
10. a_r⟵aggregate(a_r, x)
11. a⟵a+ a_r
12. end loop
13. Procedure on receive model (x,a)
14. x, a⟵ update(x_k, a_k)(d_k)
15. Send(x_k, compress (a_k))⟵N
16. end

The federated learning algorithms reveal that the administrator updates all workers with the current model x and gathers their responses. And ignore any responses from employees whose arrival delays are more than del_g. The master will aggregate the received gradients and refresh the model when the g time units have passed. Similarly, send and keep the model's age k depending on the average trained example count, allowing for variable learning rates in local learning. While these algorithms are incredibly general, federated learning is defined by the specifics of its updating process and compression technique. By default, the received model x is the starting point for a mini gradient decomposition process that updates the local data.

When securing intelligent healthcare, decentralized, federated learning offers hope for overcoming the untrustworthy variable servers that plague centralized learning systems. Decentralized federated learning solutions commonly rely on consensus, discussion, and gossip protocol. Proposing a decentralized, federated learning system that employs a segmental gossip aggregation technique is one approach to secure federated data training efficiency. Every data client can act like a worker and choose a few nearby workers to transmit the model segment to in each training iteration, maximizing the efficiency of data management and communication resources for all clients.

Assuming worker i has completed the segment, retrieves and constructs r mixed models, denoted as x0, x1, x2,..., xr. Then, aggregate a single local model L and r hybrid models for each segment i. To aggregate segment i, the following equation 1: Ni = set of workers that contribute component i, and |dj | = dataset size of worker j.

$$x(L) = \frac{\sum_{j \in N_i} |d_j| x_r(L)}{\sum_{j \in N_i} |d_j|} \quad (1)$$

Recreate the final aggregation result by combining all the aggregated segments. Simplifying the form of an authentic risk minimization issue, the federated learning problem is identified using equation 2, where a loss function that depends on an array of input-output data pairs specifies its parameter f_i.

$$(x) = \sum_{k=1}^{K} \frac{n_k}{n} \frac{1}{|k| f_i} \quad (2)$$

Unreliable participating clients require further privacy safeguards. Ensuring equal reliability among all clients is an unattainable goal.

DOI: https://doi.org/10.54216/JISIoT.080207
Received: August 21, 2022 Accepted: February 26, 2023 (corrected version: January 17, 2024)

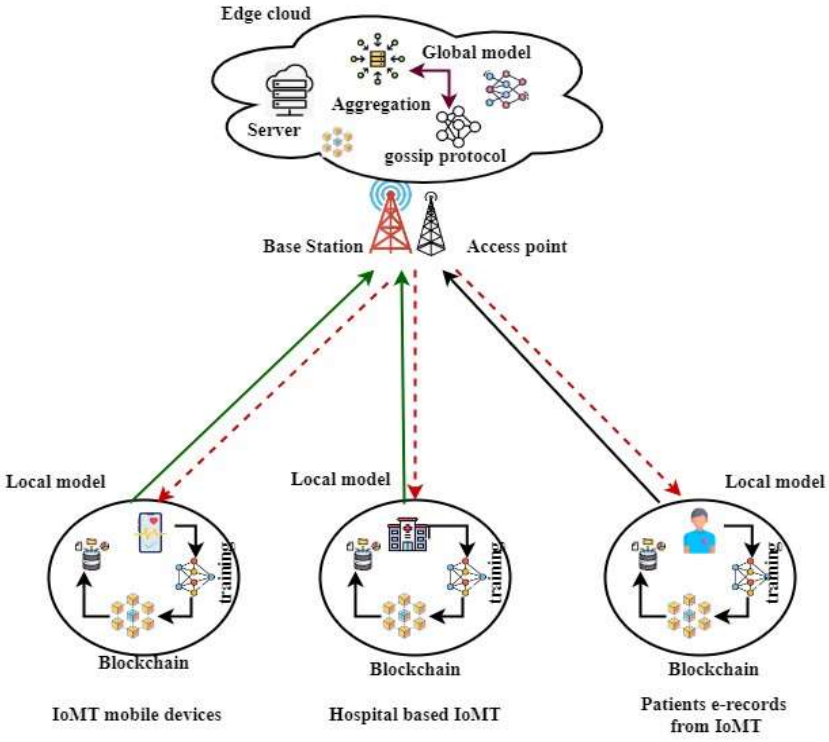

Fig.3 Design of Secure federated learning with blockchain

The model aggregation step is halted until all the drawing demands are fulfilled. Subsequently, the worker combines the third-party model sections with the local model and consolidates the segments to reconstruct the model. Upon receiving the gossip protocol result, the worker completes the initial step and commences the subsequent training iteration. Compared to centralized federated learning, the simulation findings demonstrate that it outperforms the latter regarding training time reduction in realistic network architecture and bandwidth conditions with minimal degradation of accuracy. Secure federated learning is illustrated in Figure 4 as part of a gossip protocol architecture for protecting healthcare data. One distributed method for training models using dispersed data sets is Gossip Learning. Typical applications for the gossip protocol in distributed systems include consensus, error detection, and keeping track of which nodes are system members. The federated learning algorithm allows IoMT devices connected to the hospitals and other health clients to communicate via peer-to-peer networks after allowing local clients to execute local updates for multiple iterations. This method streamlines client-to-client communication and parameter sharing by doing away with the requirement to upload models to a remote central server.

DOI: https://doi.org/10.54216/JISIoT.080207
Received: August 21, 2022 Accepted: February 26, 2023 (corrected version: January 17, 2024)

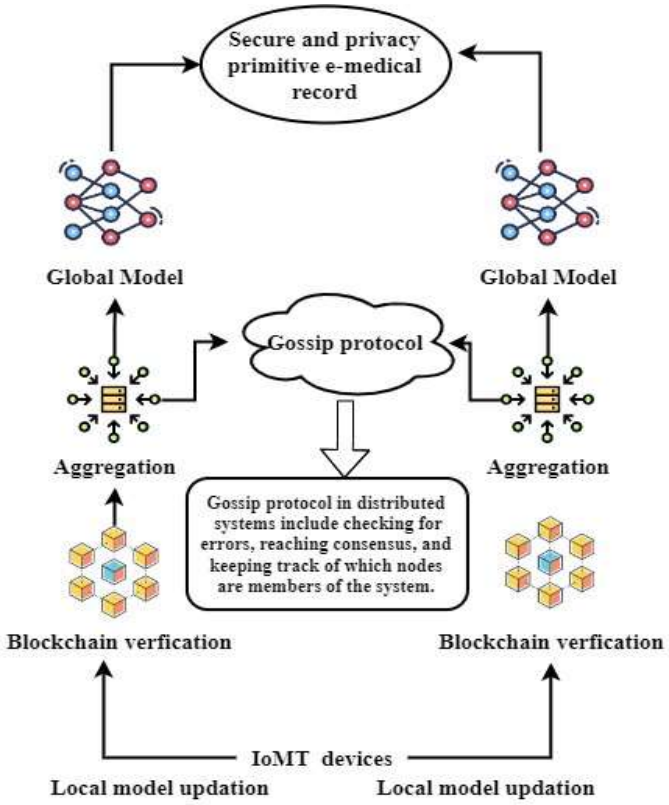

Fig.4 Secure blockchain communication with federated learning in e-medical care

A possible approach to these issues is the implementation of federated learning using blockchain technology to verify the legitimacy of IoMT users. Specifically, incorporating blockchain technology into federated settings allows for decentralized learning, eliminating the need for a centralized server for aggregating models. The blockchain can potentially synchronize the computation of local and global models through peer-to-peer block consensus. Another area of research in decentralized, federated learning-enabled healthcare systems is using blockchain technology to safeguard against unreliable servers and outside threats. The blockchain technology in the server can eliminate the need for a central server; consider how IoMT devices compete in each round of global communication to add a new block to their local ledgers by hashing it.

Fig. 4 shows a single interaction round in an e-medical care system federated learning and connected to the blockchain. The following are the primary phases of a worldwide competition of this kind of blockchain federated learning software.

- Training at the local level: With the data stored locally, each IoMT device trains its blockchain with a federated learning model.
- Model distributing and confirmation: The process involves each device adding its electronic signature to a model and then disseminating it to the other devices in the IoMT network over gossip protocols. All other IoMT devices in the network subsequently confirm the device's transaction.
- Without a centralized authority, Gossip Learning can learn models from distributed data. Every node, k starts by setting the parameters of a local model, x_k, and its age, a_k. Repeatedly, another node in the network receives this. An intermediary, the so-called sample service, helps with the initial node selection. When a node receives a model n_r, it updates its local model by merging it with the locally stored data set d_k.

Algorithm of gossip learning

1. Initialize (x_k, a_k)
2. loop
3. Wait for Del_g
4. N select
5. Send(x_k, compress (a_k))N

DOI: https://doi.org/10.54216/JISIoT.080207
Received: August 21, 2022 Accepted: February 26, 2023 (corrected version: January 17, 2024)

6. End loop
7. Procedure on receive model(x_r, a_r)
8. x_k, a_k merge(x_k, a_k)(x_r, a_r)
9. x_k, a_k update(x_k, a_k)(d_k)
10. end procedure

- Averaging the model parameters is a common way to accomplish merging; all it takes is to replace the local model.
- Verification of blocks: IoMT devices add the current block to their local ledgers if it is verified. After confirmation, a new communication round begins, and each device updates its local model. In addition, the analysis of the maximum value of the function's loss.

It is demonstrated that this bound depends on the communication rounds and other aspects, including the time it takes to train each local competition, the aggregation time, the learning rate, the data distribution, and the computing time. The main points of this work are the use of contract theory to entice reputable IoMT devices and a public blockchain technique to handle FL device reputation updates securely. The fact that external attackers cannot learn about the multiparty aggregation at the central server is a significant concern when protecting FL. A secure aggregation method should also provide the following requirements: It can handle high-dimensional user updates, efficient communication even with large user bases, and resistant to user participation and unavailability. It can ensure security even in unfavourable conditions, like transmission channels without authentication and edge nodes with limited resources.

4. Software analysis and performance evaluation

The proposed model utilizes the Medical record dataset. https://www.kaggle.com/datasets/cankatsrc/medical-records-dataset [25]. This dataset includes what appear to be medical records for an imaginary patient population. To build this dataset, we used the Python Faker package to make data that seemed authentic but was phoney. Each patient's record in the dataset has the following information: An integer that uniquely identifies each patient, known as a patient ID. Full name: An entirely created string. Birthdate: A randomly generated birthdate ranging from one hundred years old (date). A line representing a randomly chosen gender, either male or female. Medications: a row of three distinct words for medical conditions. Medications: a string consisting of three separate terms that stand for drugs. Allergies: a series of three words that stand in for allergies. The last appointment date: a randomly selected day between 2018 and 2019. The suggested model's performance metrics encompass its efficiency in testing, its speed of convergence, its analysis of running time, and overall performance. Traditional models like BFLC, 2-stage FL-BT, and EE-BFL are contrasted with the suggested approach.

Testing the accuracy of federated learning

As seen in Figure 5, the data affects the model's accuracy. On the other hand, the difference is too small to render the training results useless. For each total client count, it was essential to average their results to represent the blockchain in the local models correctly. The accuracy of the global model was compared to the mean precision of the local models using the gossip protocol. Then, a comparison was used to assess the new secure federated learning system and create the global model for all N customers first. They examined the confusion matrix the global model performed after adding together the weights of different clients' local models.

DOI: https://doi.org/10.54216/JISIoT.080207
Received: August 21, 2022 Accepted: February 26, 2023 (corrected version: January 17, 2024)

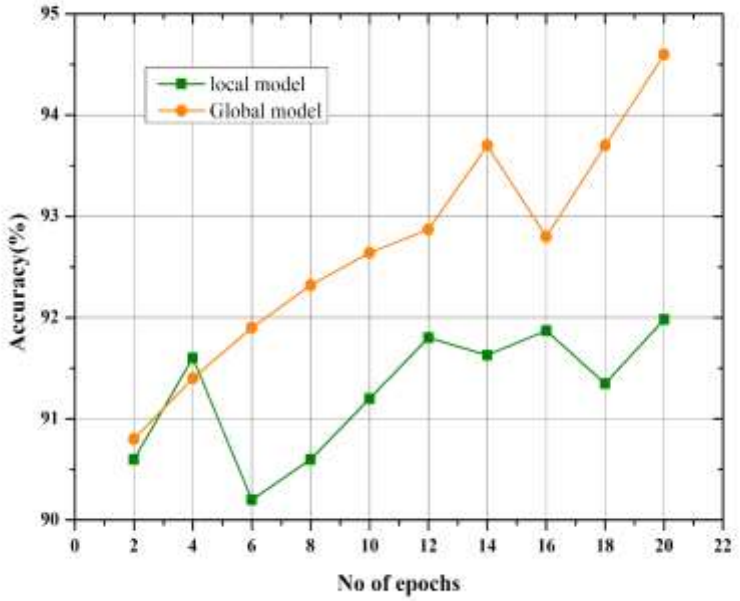

Fig.5 Testing accuracy of federated learning

Next, comparing the global models' accuracy with that of the N local ones, based on testing, it was observed that the model performs relative to a set of locally trained models that average out. Lastly, compared the global model's accuracy to the average local model and displayed the results in Figure 6. The findings show that the global model maintains or even improves upon its average local model accuracy with an increase in the number of clients. This finding demonstrates that the federated learning system can reduce the impact of weight aggregation. The improvement method, which gives the top-performing local model a more extensive scaling factor, is responsible for this boost in accuracy. Additionally, it's observed that the global model reaches its maximum accuracy of 94.75 per cent.

Convergence speed

The speed at which a convergent process approaches its limit is called the rate of convergence. The interval of convergence is determined by the set of x values for which the sequence converges. Integrating blockchain and federated learning demonstrates a noticeable acceleration while maintaining the final validation accuracy. Assess the scalability of these proposed techniques by comparing the training time required to achieve a predetermined accuracy threshold with different numbers of medical records. Based on Figure 6, the model achieves convergence at approximately 88% validation accuracy. Given that the objective is not to achieve the highest level of accuracy and from a practical standpoint, it is not worthwhile to invest a significant amount of time for a mere 2% or 3% improvement in accuracy. The observation suggests that implementing secure federated learning with blockchain technology is more scalable than the centralized approach in an IoMT network.

DOI: https://doi.org/10.54216/JISIoT.080207
Received: August 21, 2022 Accepted: February 26, 2023 (corrected version: January 17, 2024)

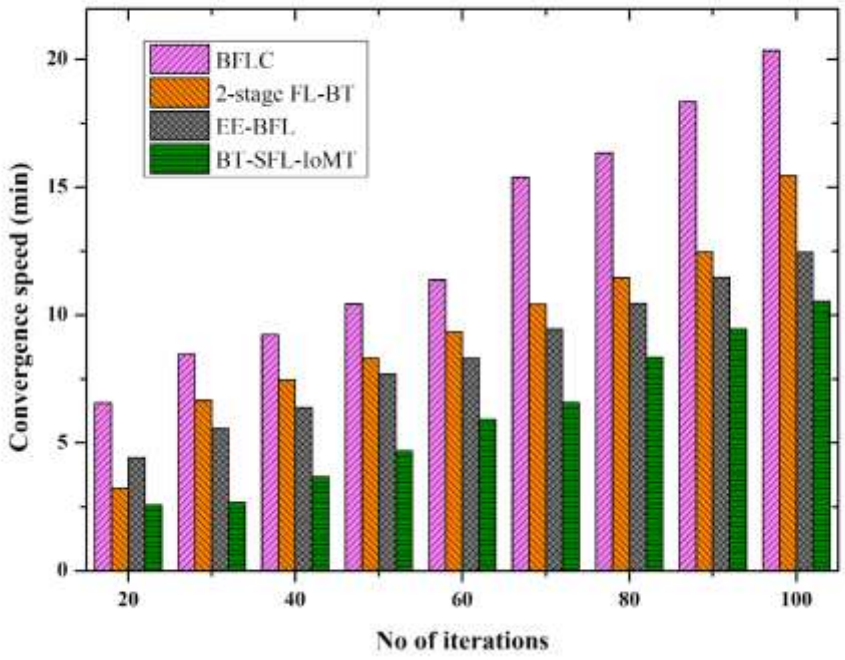

Fig.6 Convergence speed

Running time analysis

Figure 6 shows that when comparing the three methods—BFLC, 2 stage FL-BT, and EE-BFL— BFLC and EE-BFL methods have a longer running time than secure Federated Learning. It enables us to assess how blockchain affects the efficacy of federated learning training. Blockchain collaboration methodology requires time-consuming and labour-intensive processes, such as block generation, which is why this is the case. By measuring the volume of data transmitted from institutions to patients and that data's processing and transmission times, this simulation study compares the existing BFLC to the proposed BT-SFL-IoMT. Thus, medical sectors requiring a high level of security, like healthcare, are better suited to blockchain-federated learning methods, which, in exchange for some computational overhead, accomplish several security attributes like authenticity, accuracy, and resistance to attacks. The figures up top are analyses and plots of the results. The results show that the suggested system works far better than the current BFLC system.

DOI: https://doi.org/10.54216/JISIoT.080207
Received: August 21, 2022 Accepted: February 26, 2023 (corrected version: January 17, 2024)

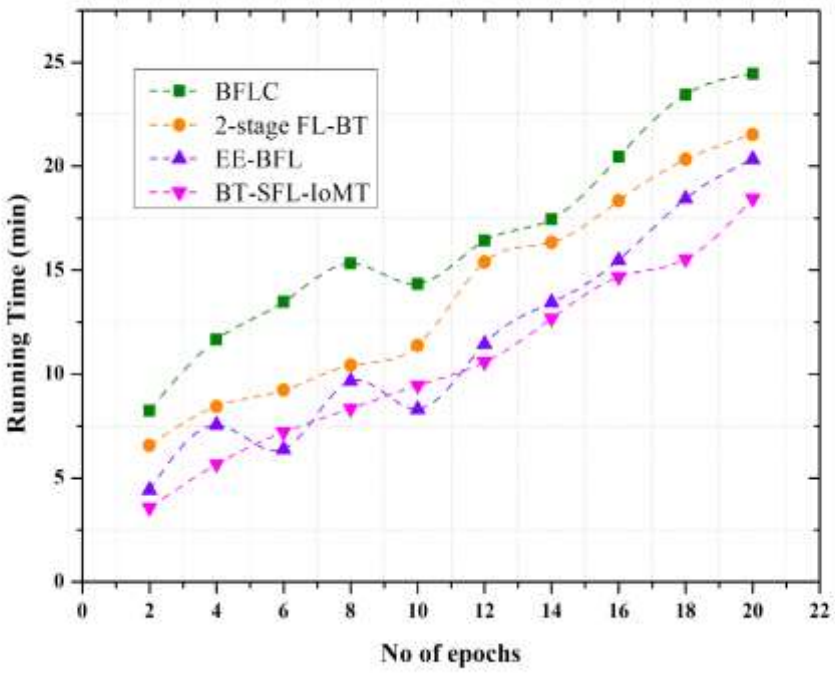

Fig.7 Running Time of the proposed model

Performance efficiency of the proposed model

Figure 8 depicts the results of the efficiency analysis of the suggested model. The planned research outlines a plan for patients to use IoMT technologies to keep their medical records safe. Initial blockchain storage for medical records and hospital data uses Hyperledger Fabric's Interplanetary File System (IPFS) protocol. The federated server obtains the data to process it further. The decentralized server uses the gossip protocol to review the data received from the federated server. The suggestion module gets this information and uses it to recommend enhancements to data management and security. The suggested model is being evaluated compared to more conventional models, such as BFLC, 2-stage FL-BT, and EE-BFL. Based on the results shown in the graph, the EE-BFL is the superior choice over the BFLC and the 2-stage FL-BT. With its use of both local and global model training methods and its increased convergence speed, the BT-SFL-IoMT model achieves better results in data security and management.

5. Conclusion and findings

This paper introduces a paradigm that addresses the challenges of flexible network components, data security, and application integrity in predictive healthcare using wearable IoMT devices. The study utilizes Hyperledger Fabric, a solution that enables the effortless tracking of e-medical records stored in the cloud. The paper's main objectives are to enhance data security services' management and decrease reliance on external entities for handling healthcare data. The study examines the IoMT architecture as a novel approach to improve the confidentiality and reliability of e-medical records by integrating blockchain and federated learning. The article presents BT-SFL-IoMT, incorporating secure Federated Learning with blockchain technology to build e-medical record systems. Specific federated learning is used to conduct predictions and analyses, with the data securely maintained on a blockchain. The results indicate that the feature effectively safeguards electronic medical records in real-world scenarios, as it is impervious to unauthorized access. Several signs point to the use of secure databases; these include the correctness of federated learning tests, the rate of convergence, and the results of the performed model. Researchers can evaluate the framework's performance by using the dataset in future studies and improving it as needed.

DOI: https://doi.org/10.54216/JISIoT.080207
Received: August 21, 2022 Accepted: February 26, 2023 (corrected version: January 17, 2024)

References

[1] Nair, A. K., Sahoo, J., & Raj, E. D. (2023). Privacy preserving Federated Learning framework for IoMT based big data analysis using edge computing. *Computer Standards & Interfaces*, *86*, 103720.

[2] Kumar, Y., & Singla, R. (2021). Federated learning systems for healthcare: perspective and recent progress. *Federated Learning Systems: Towards Next-Generation AI*, 141-156.

[3] Sun, L., & Wu, J. (2022). A scalable and transferable federated learning system for classifying healthcare sensor data. *IEEE Journal of Biomedical and Health Informatics*, *27*(2), 866-877.

[4] Srivastava, G., K, D. R., Yenduri, G., Hegde, P., Gadekallu, T. R., Maddikunta, P. K. R., & Bhattacharya, S. (2023). Federated Learning Enabled Edge Computing Security for Internet of Medical Things: Concepts, Challenges and Open Issues. In *Security and Risk Analysis for Intelligent Edge Computing* (pp. 67-89). Cham: Springer International Publishing.

[5] Wang, W., Li, X., Qiu, X., Zhang, X., Brusic, V., & Zhao, J. (2023). A privacy preserving framework for federated learning in smart healthcare systems. *Information Processing & Management*, *60*(1), 103167.

[6] Akter, M., Moustafa, N., Lynar, T., & Razzak, I. (2022). Edge intelligence: Federated learning-based privacy protection framework for smart healthcare systems. *IEEE Journal of Biomedical and Health Informatics*, *26*(12), 5805-5816.

[7] Zhu, C., Zhu, X., Ren, J., & Qin, T. (2022). Blockchain-enabled federated learning for UAV edge computing network: Issues and solutions. *Ieee Access*, *10*, 56591-56610.

[8] 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 of Things Journal*.

[9] Gadekallu, T. R., Alazab, M., Hemanth, J., & Wang, W. (2023). Guest editorial federated learning for privacy preservation of healthcare data in internet of medical things and patient monitoring. *IEEE Journal of Biomedical and Health Informatics*, *27*(2), 648-651.

[10] Wadhwa, S., Saluja, K., Gupta, S., & Gupta, D. (2022). Blockchain based Federated Learning approach for Detection of COVID-19 using Io MT. *Available at SSRN 4159195*.

[11] Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2022). A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems*, *129*, 380-388.

[12] Abou El Houda, Z., Hafid, A. S., Khoukhi, L., & Brik, B. (2022). When collaborative federated learning meets blockchain to preserve privacy in healthcare. *IEEE Transactions on Network Science and Engineering*.

[13] Baucas, M. J., Spachos, P., & Plataniotis, K. N. (2023). Federated learning and blockchain-enabled fog-IoT platform for wearables in predictive healthcare. *IEEE Transactions on Computational Social Systems*.

[14] Aich, S., Sinai, N. K., Kumar, S., Ali, M., Choi, Y. R., Joo, M. I., & Kim, H. C. (2022, February). Protecting personal healthcare record using blockchain & federated learning technologies. In *2022 24th International Conference on Advanced Communication Technology (ICACT)* (pp. 109-112). IEEE.

[15] Stephanie, V., Khalil, I., Atiquzzaman, M., & Yi, X. (2022). Trustworthy privacy-preserving hierarchical ensemble and federated learning in healthcare 4.0 with blockchain. *IEEE Transactions on Industrial Informatics*.

[16] Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2019). Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Transactions on Industrial Informatics*, *16*(6), 4177-4186.

DOI: https://doi.org/10.54216/JISIoT.080207
Received: August 21, 2022 Accepted: February 26, 2023 (corrected version: January 17, 2024)

[17] Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2022). A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems*, *129*, 380-388.

[18] Li, Y., Chen, C., Liu, N., Huang, H., Zheng, Z., & Yan, Q. (2020). A blockchain-based decentralized federated learning framework with committee consensus. *IEEE Network*, *35*(1), 234-241.

[19] 19. Lian, Z., Zeng, Q., Wang, W., Gadekallu, T. R., & Su, C. (2022). Blockchain-based two-stage federated learning with non-IID data in IoMT system. *IEEE Transactions on Computational Social Systems*.

[20] Muazu, T., Yingchi, M., Muhammad, A. U., Ibrahim, M., Samuel, O., & Tiwari, P. (2023). IoMT: A Medical Resource Management System Using Edge Empowered Blockchain Federated Learning. *IEEE Transactions on Network and Service Management*.

[21] Janjua, A., Dhalla, S., Gupta, S., & Singh, S. (2023, April). A Blockchain-Enabled Decentralized Gossip Federated Learning Framework. In *2023 International Conference on Networking and Communications (ICNWC)* (pp. 1-7). IEEE.

[22] Chen, Q., Wang, Z., Wang, H., & Lin, X. (2022). FedDual: Pair-Wise Gossip Helps Federated Learning in Large Decentralized Networks. *IEEE Transactions on Information Forensics and Security*, *18*, 335-350.

[23] Hakak, S., Ray, S., Khan, W. Z., & Scheme, E. (2020, December). A framework for edge-assisted healthcare data analytics using federated learning. In *2020 IEEE International Conference on Big Data (Big Data)* (pp. 3423-3427). IEEE.

[24] Lakhan, A., Mohammed, M. A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., & Wang, W. (2022). Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. *IEEE journal of biomedical and health informatics*, *27*(2), 664-672.

[25] https://www.kaggle.com/datasets/cankatsrc/medical-records-dataset

DOI: https://doi.org/10.54216/JISIoT.080207
Received: August 21, 2022 Accepted: February 26, 2023 (corrected version: January 17, 2024)