International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/221885 Volume 10, Issue 3, May – June (2023)

RESEARCH ARTICLE

An Enhanced Authorization Protocol in Blockchain for Personal Health Information Management System

Thakur Saikumari
Department of Computer Science and Engineering, Dr. M.G.R. Educational and Research Institute, Chennai, Tamil Nadu, India.
neelima0318phd@gmail.com

G. Victo Sudha George
Department of Computer Science and Engineering, Dr. M.G.R. Educational and Research Institute, Chennai, Tamil Nadu, India.
victosudhageorge@drmgrdu.ac.in

Received: 24 March 2023 / Revised: 27 April 2023 / Accepted: 01 May 2023 / Published: 30 June 2023

Abstract – Blockchain and cloud-edge computing paradigms have gradually evolved as a profitable alternative for managing patient data in clinical Internet-of-Things (IoT) devices. Various studies are presented to secure medical records in IoT devices using blockchain schemes. Amongst, eHealthChain is developed to handle medical records obtained from clinical IoT systems. It utilizes Hyperledger Fabric as a blockchain policy to accumulate private medical records. The client's medical record is collected by utilizing the OAuth 2.0 protocol that guarantees the client's authority. Besides, a Message Queuing Telemetry Transport (MQTT) protocol is applied to communicate within an IoT platform. The reliability of the medical data is guaranteed by a consensus method called Kafka. However, the standard OAuth 2.0 protocol neglects the client security problem. Though MQTT offers many-to-many transmissions, the restricted sleep time of devices related to the fixed query waiting is ineffective for resource-constrained networks. Hence, the major contributions of this article are: (i) to develop an Enhanced OAuth (EOAuth) 2.0-based protocol which solves the client security problem and (ii) to utilize a protocol called Constrained Application Protocol (CoAP) for reliable transmission. It reduces the user verification time by obtaining more trusted clients according to their trust level. Also, a certified security service is employed to get the client's input securely and conduct the cryptographic processes. Finally, the implementation findings exhibit that the EOAuth and CoAP achieve higher efficiency than the standard protocols.

Index Terms – Blockchain, Cloud-Edge Computing, IoT Networks, eHealthChain, OAuth 2.0, MQTT, Consensus, CoAP, Kafka.

1. INTRODUCTION

With the increase in the number of IoT systems and related records, internet provider known as information traders or data exporters has emerged. Because security requirements are concealed within long agreements, users are not explicitly told about how personal information is collected, processed, and validated. To solve this issue, blockchain technology has been developed in these decades. According to the NIST, Blockchain is a dispersed digital record of cryptographically retained transactions, which are clustered into blocks [1, 2, 3].

All blocks are cryptographically connected to the preceding ones (creating tamper proof) after confirmation and experiencing a consent result. Because novel blocks are inserted, older blocks turn into highly complex to alter (producing tamper resistance). Novel blocks are simulated across duplicates of the record in the system and encounters are solved inevitably by well-known procedures. Therefore, blockchain, in other words, is a technology that offers available and certifiable information management over the decentralized system to all contributed nodes rapidly and conveniently. No particular or centralized authority is needed to authenticate the nodes. Instead, to contribute to a system, a node has to authenticate itself by resolving a Proof-Of-Work (POW), which ensures information secrecy. A node, which succeeds in the POW will adopt a block that characterizes a set of data including transactions and other related data [4]. Then, the block having the maximum compromise can be approved to be inserted into the system and other blocks are rejected later by the system.

Nowadays, Blockchain technology emerges in a wide range of real-time applications [5], including industry 5.0 [6], healthcare 5.0 [7], etc. Amongst, healthcare is one of the foremost significant applications, which impacts individual survival. Healthcare 5.0 provides several prospects for digital clinical application. Distant hospitals, telesurgeries, and distant clinical monitoring are promising healthcare 5.0. On the other hand, challenges of concealment, safety, and immutability will be solved by integrating blockchain in healthcare 5.0. The deployment chances for integrating

RESEARCH ARTICLE

blockchain with Healthcare 5.0 can overcome the challenges of concealment, safety, immutability, and transparency [8, 9, 10, 11]. Thus, a Personal Health Information Management System (PHIMS) can run on the blockchain to handle patient's records, confirm medical tests, update clinical credentials, and confidentiality to the clinical supply chain. Thus, the blockchain-enabled PHIMS avoids intermediation in the information distribution procedure, as well as, protects information when dealing with insurance claims, PHI, and other clinical records.

From this perspective, clinical IoT industrialists might combine blockchain in their PHIMS applications as a discriminating feature or illustrate their prominence towards concealment [12]. But, blockchain-based PHIMS increases the total product costs and decreases the possibilities for monetization of patient data. Because of the quantity of information raises in the PHIMS, there would be also an essential growth in consideration of the processing of information from various participants. Authorized and moral problems might occur relating to proprietorship and access to the information among many participants including the users like the secluded blockchain provider, PHIMS designer, insurance, and open/secret medical providers. To combat this issue, the eHealthChain system was developed by Pawar et al. [13] to handle medical records obtained from clinical IoT systems and connected applications.

An application use-case of the eHealthChain arrangement utilizes Hyperledger Fabric [14, 15] as a blockchain policy to store private medical records obtained from the different IoT systems. The eHealthChain arrangement interacts with clinical IoT systems and blockchain storage utilizing a modified connector module, which gathers information from IoT systems and stores it in the blockchain. The connector module retrieves information from blockchain storage and transmits it to the system, which offers an intelligible opinion of accumulated information. The design of eHealthChain comprises different layers and they are (i) a blockchain layer to host a blockchain record; (ii) an IoT system layer to get private medical information; (iii) An application layer to enable medical information distribution and (iv) An connector layer that interacts the blockchain and application layers. The patient's medical information is collected by the OAuth 2.0 protocol that guarantees the patient's authority. OAuth 2.0 is an authorizing program [16] that allows third-party apps to get restricted access to sensitive data depending on client agreement. Besides, eHealthChain uses an MQTT protocol to transfer within an IoT platform. The MQTT is a communication protocol [17] that employs the publish-subscribe service model, in which the users (patients or physicians) do not demand upgrades, leading to a reduction in required resources, making this model ideal for usage in a low-bandwidth scenario. Moreover, in eHealthChain, all users have their duplicate of the record that is simulated with other users and the reliability of this data is guaranteed by the consensus method called Kafka [18]. Conversely, the eHealthChain has a few major limitations: (i) the standard OAuth 2.0 protocol does not consider the client's security problem and has many susceptibilities that can jeopardize the client's security privileges; and (ii) Though the usage of the MQTT protocol in IoT systems achieves many-to-many transmission and a less overhead; the idle time of systems was limited because of fixed delay for request in resource-constrained systems.

Therefore in this manuscript, EOAuth 2.0 with CoAP-based protocol is proposed to enhance the security of healthcare systems. The EOAuth 2.0 protocol resolves the client security problem by incorporating a pseudonym-based signature policy and a signature delegation policy into the OAuth 2.0 protocol. It enables clients to self-create client-specific and app-specific pseudonyms on-demand and confirms security-improved client verification at the service provider end. Also, a certified security service is employed to acquire the client's input securely and perform the cryptographic functionalities needed for the EOAuth 2.0 protocol. Besides, the trust score of each client is determined to discover highly trusted clients and reduce the authentication period. Moreover, the CoAP is applied to achieve a reliable transmission between the client and server based on the Retransmission Timeout (RTO). Thus, the user authentication and data transmission protocols are enhanced in the eHealthChain-based clinical networks.

The rest of the paper is arranged as follows: Section 2 reviews the different recent blockchain models in the healthcare domain. Section 3 explains the EOAuth 2.0 and CoAP protocols in the eHealthChain network. Section 4 illustrates its performance. Section 5 summarizes the entire work and gives future directions.

2. LITERATURE SURVEY

Ichikawa et al. [19] developed a Tamper-Resistant (TR) mHealth model using a blockchain scheme that facilitates trusted and auditable computing by a decentralized network. This model was designed for the cognitive-behavioral treatment of insomnia with the help of a smartphone app. First, the participant details were gathered and accumulated in JavaScript entity representation form and transmitted to the blockchain system. Then, the tamper resistance of the information was analyzed against the inconsistencies caused by artificial failures. But, there was susceptibility around both the blockchain and consensus schemes.

Zhang et al. [20] investigated the demands of blockchain techniques for medical file transfer. Then, a blockchain-based structure called FHIRChain was developed by encapsulating HL7's Fast Healthcare Interoperability Resources (FHIR) for distributed medical files. Also, an FHIRChain-based decentralized app was established by the digital medical

RESEARCH ARTICLE

characteristics to verify contributors in cooperative decision-making. But, it does not analyze the clinical interoperability challenges.

Huang et al. [21] developed a confidential decentralized information-sharing scheme depending on the BC to accomplish privacy-preserving when multiple users interact via the smart systems. In this scheme, proxy encryption was applied for ensuring that the organizations may decipher the shared transitional ciphertext enciphered through the semi-honest proxy cloud server. But, it was not appropriate to generate 0-data evidence, and the verification key size was high.

Benil & Jasper [22] designed an Elliptical curve Certificateless Aggregate Cryptography Signature (EC-ACS) based on a blockchain scheme to authenticate the clinical data owner and secure the eHealth data. First, a modified Elliptic Curve Cryptography (ECC) was applied to encipher the eHealth records and the Certificateless Aggregate Signature (CAS) was applied to produce the unique identifier for exchanging and accumulating data in the server memory. Then, bilinear ECC was used to create the session codes among the cloud provider, client, and clinical cloud server for securely disseminated data. But, the authentication time was high.

Chelladurai & Pandian [23] developed blockchain smart contracts to distribute medical data on a blockchain model for creating a smart healthcare system. In this model, an absolute patient log generation with an altered Merkle tree data structure was introduced for protected storage and quick access to medicinal files, modifying and distributing them among various traders and viewership agreements on the peer-to-peer blockchain system. But, it needs to guarantee content reliability.

Nguyen et al. [24] designed a novel decentralized medical system called BEdgeHealth that combines mobile edge computing and blockchain for data offloading and distribution in shared clinical systems. Initially, a data offloading method was developed where mobile nodes can offload medical information to the adjacent mobile edge server. Also, a data distribution method was employed which facilitates data exchanges among medical clients by leveraging blockchain and interplanetary record systems. Moreover, a smart contract-based verification method was used to execute decentralized client access authentication at the system edge without a centralized authority. But, the authentication time was high.

Ejaz et al. [25] developed a model to integrate the abilities of edge computing and blockchain techniques. In this model, data privacy protection was enhanced by constraining the propagation of private information at the local and edge networks rather than transmitting each data to the cloud. But, it needs to highly use the attributes of the blockchain in fetching confidence between various stakeholders of multifaceted medical transmission and storage systems.

3. PROPOSED METHODOLOGY

In this section, the blockchain-based healthcare system and 3-tier edge-IoT system models are initially outlined. The structure of the proposed eHealthChain system and its components are presented. Moreover, the proposed EOAuth 2.0-based protocol and CoAP procedures are explained briefly.

3.1. Blockchain-Based Healthcare System Model

An extensive scenario of blockchain technique for clinical data handling system [13] is shown in Figure 1, where several data files like portable medical services, health insurance data, family medical data, physician's prescription, etc., are accumulated in the blockchain server on cloud and are retrieved from the certified physicians/patients/scientists depending on the patient permission.

3.2. Blockchain-Based 3-Tier Edge-IoT System Model

Combining blockchain and edge computing allows many chances for Healthcare 4.0 applications and improve the Quality-of-Service (QoS), Quality-of-Experience (QoE), distributed trust, confidentiality, and resource utilization. There are 3 kinds of IoT structure models accessible such as classical cloud-IoT, edge-IoT, and 3-tier edge-IoT [26]. In this study, the concept of the 3-tier edge-IoT paradigm is considered as presented in Figure 2(a), which deploys the local IoT edge and makes a decision at the local networks. This is critical in many IoT systems to handle possible network issues and limit the dissemination of extremely confidential information outside of that specific network. For example, Figure 2(b) shows the healthcare applications using the blockchain-based 3-tier edge-IoT model.

Figure 3 emphasizes the blockchain-edge model for healthcare IoT applications, which has multiple IoT groups, and all of them are linked to the corresponding edge nodes. IoT groups are resource-constrained; so such IoT groups are merged with respective edge nodes through a gateway. As a result, it enables performing a few data pre-processing (cleaning), storage, and transmission in the vicinity and satisfies the minimum delay demands for local latency-critical stages.

Consider lightweight secret/consented blockchain at the IoT-edge systems that can enable protected and confidential distribution of the desired data among various IoT-edge groups. At the local systems, a blockchain is an advantageous mechanism for data analysis and transmission. With smart contracts (stakeholders related to healthcare), a sub-contractor (various healthcare organizations) can validate the data

RESEARCH ARTICLE

sources and other participants in the chain. The local blockchain certifies the verification and access control methods in the local system. If the needed service/resource is inaccessible to the local systems, the request is sent to the fog systems. Fog networks run with no link to the public system or the neighboring access system base station. Edge nodes send requests to fog systems to process data and execute high-resource demanding tasks. The fog system is obligatory in offering variable resources and services with low-latency access for intelligent healthcare scenarios.

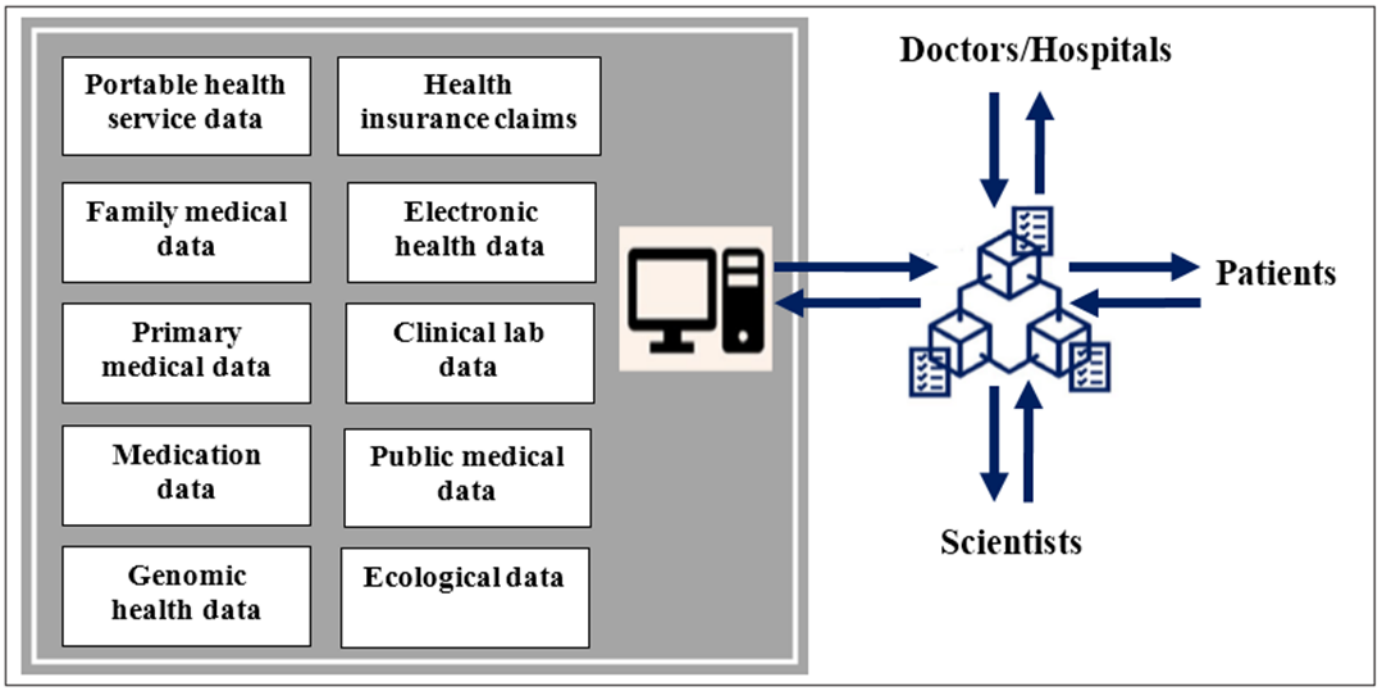

Figure 1 Blockchain-Enabled Medical Data Handling System

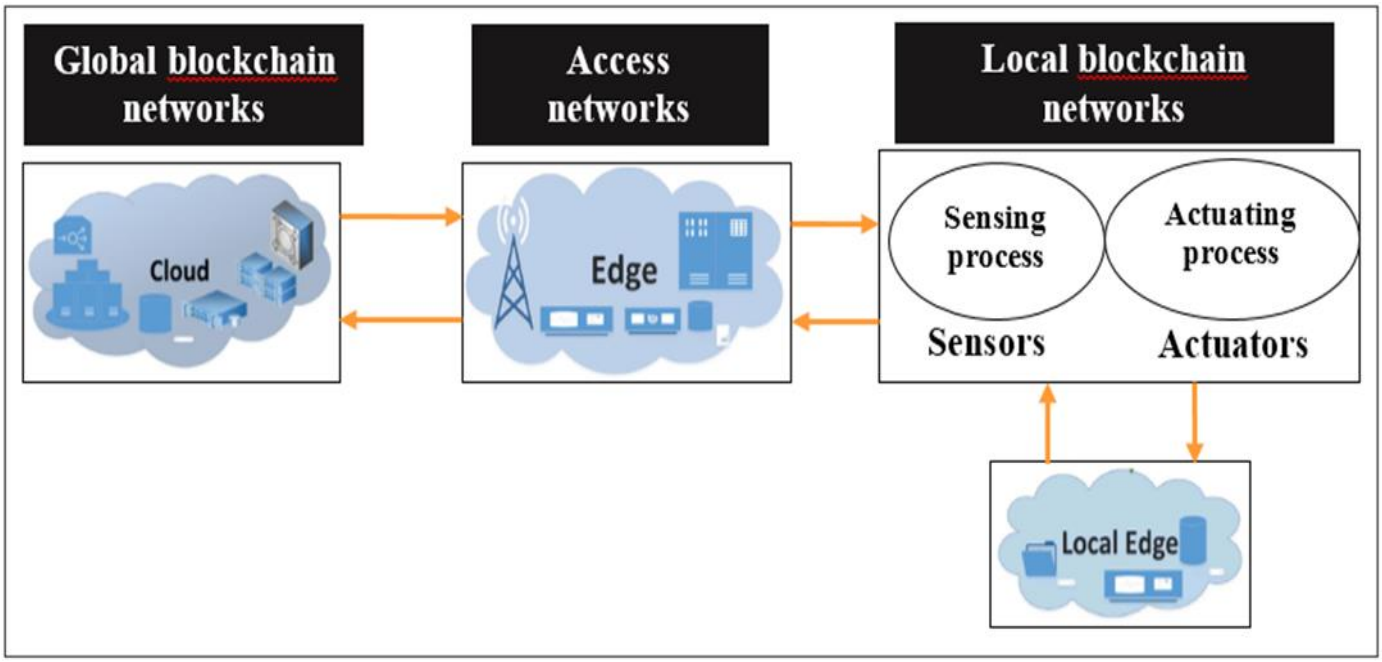

Figure 2(a) Structure of Blockchain-Based 3-Tier Edge-IoT Network

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/221885 Volume 10, Issue 3, May – June (2023)

RESEARCH ARTICLE

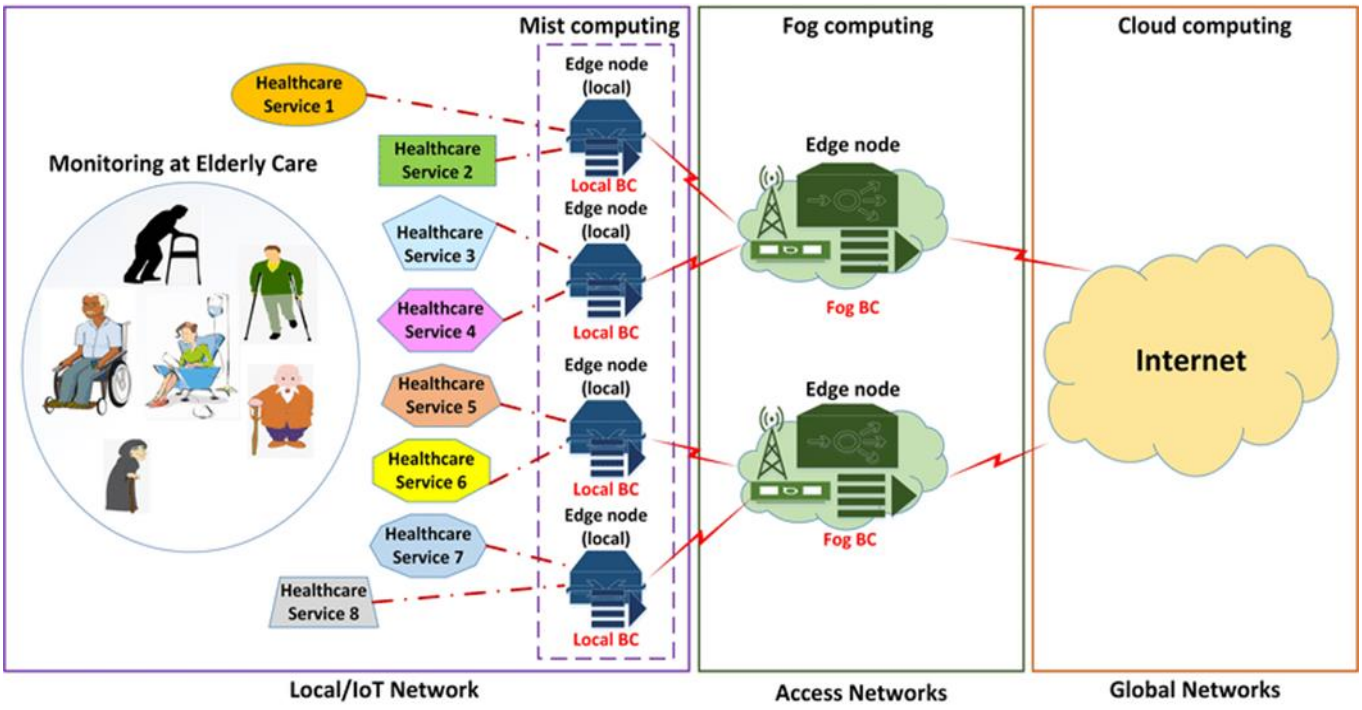

Figure 2(b) Example of Blockchain-Based 3-Tier Edge-IoT Network Model in Healthcare Applications (Source: [20])

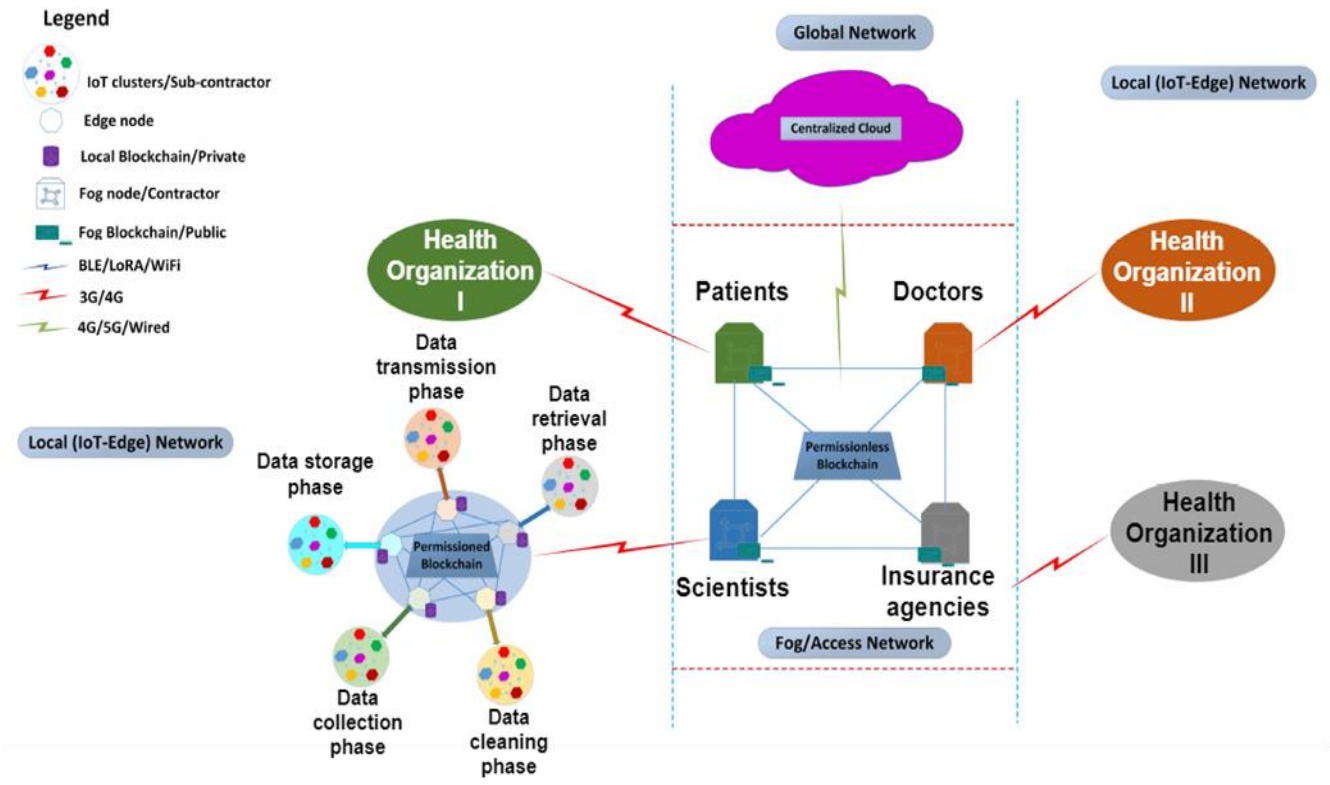

Figure 3 Blockchain-Edge Model for Healthcare IoT Systems

RESEARCH ARTICLE

Fog nodes deliver innovative and more sophisticated processes like artificial intelligence-based information processing and decision-making. The other major operation in fog systems is the orchestration/adaptive distribution of several resources. Fog systems will deliver a healthcare paradigm wherein the provider will generate the data sources and give authority to the user. Several fog nodes can necessitate distributing essential data of ongoing procedures. They take consentless or public blockchains and distribute the partial data in the system. The global system will deliver the maximum resource competencies than the local systems. It pursues the customary integrated cloud computing methods, which deliver an accessible service policy for systems necessitating great memory and computational ability. Transactions happening between several systems and administrations are kept on the blockchain as eternal archives. To effectively implement the different stages, each of the networks must operate collaboratively at all stages.

3.3. Proposed eHealthChain Model

The eHealthChain model is a blockchain technique-based PHIMS proposal for the collection, handling, and distribution of individual medical data acquired from clinical IoT systems. It interfaces clinical IoT systems and blockchain storage using a unique interface unit. This interface unit is used to gather information from IoT systems and accumulate them in the blockchain. Also, it retrieves information from the blockchain and transmits it to the app, which gives a client-friendly stance of accumulated information. Figure 4 illustrates the structure of eHealthChain, which involves 4 major layers: blockchain, interface, application, and system layer.

- Blockchain layer: Blockchain is a distributed Hyperledger Fabric that preserves each transaction data. The clinical data captured by the healthcare IoT systems is accumulated in a blockchain record. Admittance to this record is given merely to the approved individuals depending on the permission of the owner. Consensus is the task of granting and synchronizing ledger files across the network. In a blockchain network, all clients have separate duplication of the record that is simulated with other clients, and the data reliability is certified by the Kafka-based consensus method. It shares the ledger data and practices to revise the ledger using the CoAP.
- Interface layer: It has the task of interaction between the application and the blockchain layers. It receives the client's medical information using the EOAuth 2.0 protocol that ensures the client's authority. It also utilizes REST APIs given by the blockchain to write medical information to the blockchain.
- Application layer: It encompasses mobile apps that gather information from client medical gadgets. Generally, such apps facilitate information distribution to outside individuals by the EOAuth 2.0 protocol. EOAuth is a consensus scheme, which permits third-party apps to get restricted admission to client profiles.
- System layer: It comprises clinical IoT gadgets which are connected to portable cellphones by short-range wireless techniques like Bluetooth. In the eHealthChain model, a patient is directed to revise particular medical data. The patient can validate other stakeholders who have access to their information.

3.4. Enhanced OAuth 2.0-Based Protocol for Client Authentication

3.4.1. System Configuration

System configuration needs clients and Consent Servers (CSs) to complete a registration in the eHealthChain Security Server (SS) as portrayed in Figure 5. Clients have to give their actual identities and choose a username and secret code (name,src), which can be utilized to recognize the client by the SS during the EOAuth 2.0-based client verification and to access their private profiles in the SS. In such profiles, the client places confidential data, e.g., the client's original identity that is ready to distribute with another CS. The SS will reveal this data to a CS when the CS is approved for consent by the client.

Similarly, the CSs have to register in the SS and offer a list of clients with private profiles in such CS, i.e. the list of data owners that are verified via that CS to access one or many resource servers. The SS maps the registered clients in the SS to the list of clients obtained by the CSs. As well, the CS will give a list of mobile apps that clients can utilize to access such CS. During registration, the trust is measured between the data owner and the client. Also, the CS ensures trusted clients via data owner identities. This EOAuth 2.0 enables data owners to give access rights to client apps by ensuring client trust. It controls and monitors what clients can perform with access grants achieved by this trust measure, i.e. highly trusted clients avoid the authentication process using EOAuth 2.0 protocol and obtain access rights. While granting consent, the CS has the opportunity to get consent from the end client. The end client will decrease access levels or entirely avoid consent during this phase. Therefore, the authentication time is decreased in this EOAuth 2.0 protocol because of trust measures.

Clients and CSs get the public values created by the SS after registering with the SS. Clients and CSs both get their unique values, i.e. clients get their static pseudonym ($psdm$) and CSs get their public $psdm$ and matching identity. Based on the creation of identity and static$psdm$, SS, every CS registered to the SS and the clients registered to the SS get the private and public values. On the client end, the values acquired from the SS are accumulated in the Sec-App which are utilized to

RESEARCH ARTICLE

complete the cryptographic processes during the EOAuth 2.0-based protocol. The Sec-App accumulates the SS public parameters, the CSs public $psdm$ and the client's static $psdm$ as a private value.

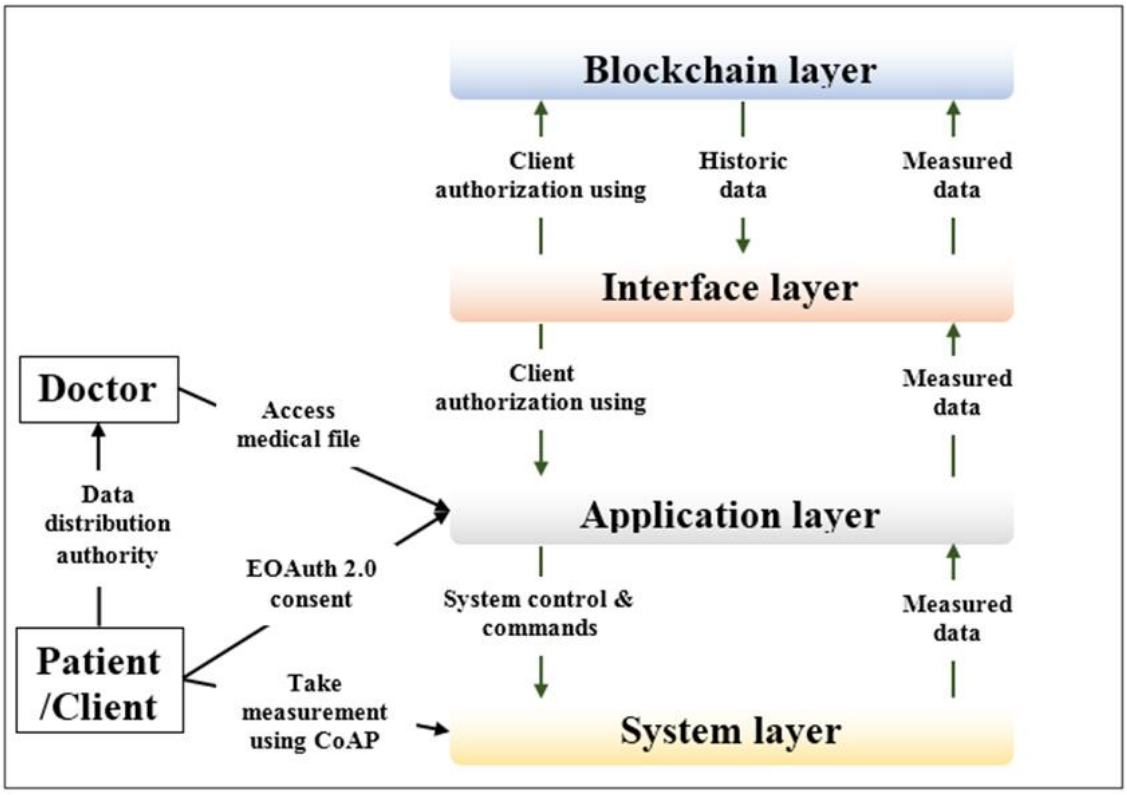

Figure 4 Structure of eHealthChain System

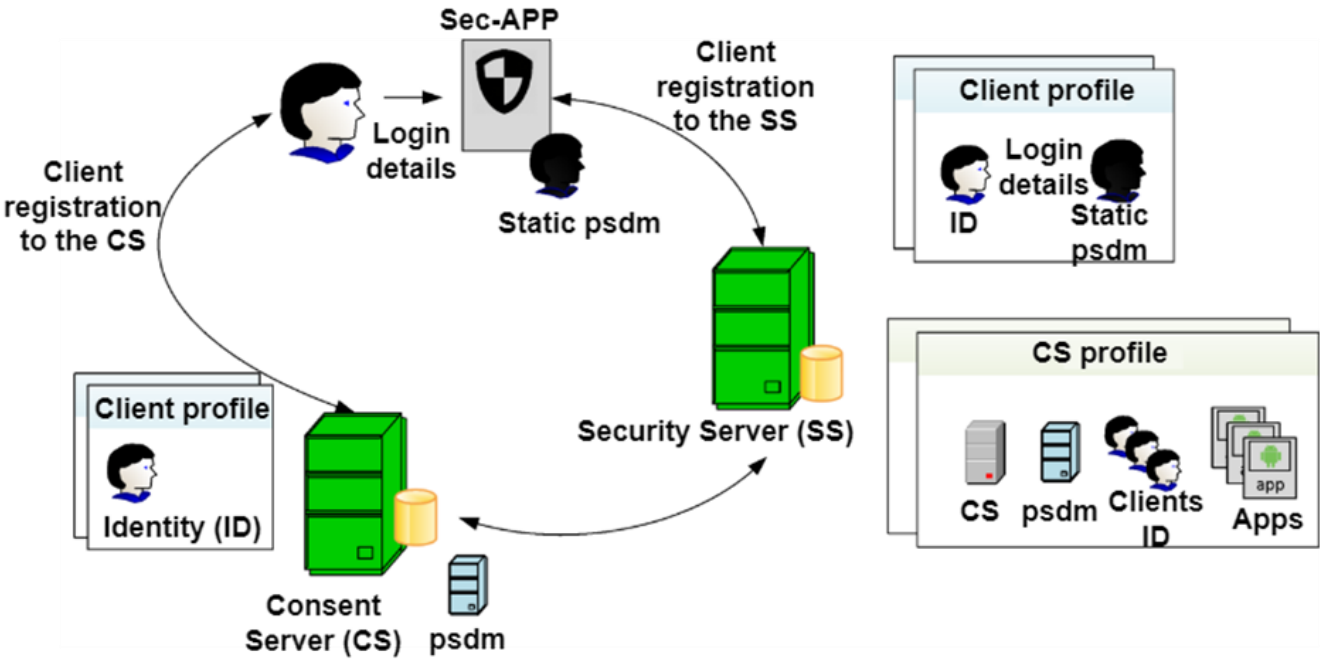

Figure 5 Registration Procedure between Clients and CSs

RESEARCH ARTICLE

3.4.2. Protocol Initialization

Parameter creation: The SS executes the below functions to get the collection of public parameters, which are then shared by the SS with the registered CSs and clients:

- Chooses 2 cyclic groups of prime order p, G_1 and G_2, where p refers to a prime of K bits, G_1 has points in an elliptic curve.
- Selects a point $P \in G_1$ as a creator.
- Chooses a bilinear map e such that $e: G_1 \times G_1 \rightarrow G_2$.
- Picks 2 cryptographic hash functions $H_1, H_2: \{0,1\}^* \rightarrow G_1$ depending on the SHA-256 algorithm.
- Chooses another hash function $H_3: \{0,1\}^* \rightarrow Z_p$.
- Selects randomly a secret value $s \in Z_p$ and creates a public key $W = sP$.
- Picks randomly a public value $Q_s \in G_1$ and gets a control key $W_s = sQ_s$.

Identity creation: The CS gets an identity after registration with the SS. For identity creation for the CS y, the SS executes the below processes:

- Chooses a value $\mu_y \in Z_p$.
- Determines a secret key $S_y = P\frac{1}{(s+\mu_y)}$.
- Forwards to the CS y, over a secure medium, the identity $I_y = (\mu_y, S_y)$. The CS y authenticates that $e(\mu_y P + W, S_y) = e(P, P)$ holds and accepts the identity.

Table 1. EOAuth 2.0 Protocol Initialization

Entity	Public values	Secret values
SS	$G_1, G_2, P, H_1, H_2, H_3, e(\cdot), W, W_s$	s
CS	$psdm_y$	I_y
Sec-APP (client)	-	$psdm_x$
Client	-	Name and secret code $(name_x, src_x)$

Static psdm creation: The CS y having a legitimate identity $I_y = (\mu_y, S_y)$ issued by the SS can create a static $psdm$ by executing the function $psdm_y = \mu_y Q_s$. This pseudonym is public and unique of the CS y. Likewise, a client x also gets a static $psdm$, $psdm_x = \mu_x Q_s$, where μ_x refers to the secret value obtained from the client values $name_x$ and $src_x: \mu_x = H_3(name_x \| src_x)$ in which $\|$ is the string concatenation. The value $psdm_x$ is accumulated in the Sec-APP. Table 1 summarizes the secret and public parameters generated during EOAuth 2.0 protocol initialization.

3.4.3. Trust Score Measure

The trust score of each client for authentication is measured based on the below steps:

- Initialize the trust score for the client x as $\epsilon = 0$;
- Get the API access requests from x;
- Check whether the API requests from x are limited (within the access limit of the client) or unlimited (beyond the access limit of the client);
- If limited requests are received from x, then ϵ is incremented; or else, ϵ is decremented;
- Trust score $= \frac{\text{Number of limited API requests by client}}{TotalNumber\ of\ API\ access\ requests\ from\ client}$;
- Threshold θ is sent as 0.9.

3.4.4. Client Authentication

In this EOAuth 2.0-based protocol, the pseudonym-based signs with the consent code grant type pattern are added to the transmitted message. It involves the following phases:

- *ClientAuthrequest1*: It is conducted by the CS. The CS y sends a verification request code to the client x. The broadcast data is consisting of the CS public pseudonym $psdm_y$, a pseudonym-based sign $sign_{psdm_y}(D)$ on a data D and a random value δ. In this phase, the CS y:

i. Gets $Q_i = H_1(app\_ID)$ from the app-specific identifier app_ID.

ii. Check trust score ϵ is whether greater than the threshold θ or not, i.e. $\epsilon > \theta$ or $\epsilon < \theta$.

iii. If $\epsilon > \theta$, then the verification reply code is immediately sent back to y; otherwise, the following steps are conducted.

iv. Gets an app-specific pseudonym $psdm_{y,i} = \mu_y Q_i$ and δ.

v. Signs D, where $D = \delta \| psdm_{y,i}$, with its public pseudonym $psdm_y$. It is conducted using a signing algorithm:

a) First, the y selects $\alpha, r, r' \in Z_p$.

b) Then, it gets a time slot $T = \alpha S_y, R_{G_1} = rQ_i$ and $R = e(Q_i, P)^{r'}$.

c) It gets $c = H_3(D \| T \| R_{G_1} \| R \| psdm_y)$.

d) After, it gets $z_1 = c\alpha + r'$ and $z_2 = c\mu_y + r$.

RESEARCH ARTICLE

e) The sign $sign_{psdm_y}(D)$ has the tuple (T, c, z_1, z_2).

vi. Transmits D and sign $sign_{psdm_y}(D)$ to the client.

- *ClientAuthrequest2*: The browser on the client end accepts the verification request code which is transmitted to the Sec-App for validation. To confirm the code, the Sec-App applies the signature authentication scheme on the $sign_{psdm_y} = (D)$ of D, which is enclosed by the below processes:

i. Get $R'_{G_1} = z_2 Q_s - psdm_y c$ and $R' = e^{(Q_s,P)^{z_1}} / e^{(psdm_y + W_s,T)^c}$. Such functionalities need the public values Q_s and W_s accumulated in the Sec-App.

ii. Get $c' = H_3(D \| T \| R'_{G_1} \| R' \| psdm_y)$.

iii. Authentication is successful when equality $c' = c$ remains

Once the sign authentication is successful, the request code is certified and the Sec-App provides a client interface where x can use his/her login details to create the ClientAuthreply1. These login details must be used when there is a high level of trust within the client & Sec-APP and if many consent code grant types are not accessible.

ClientAuthreply1: The Sec-App requests x to add the username and secret code $(name_x, src_x)$ and gets the client's static pseudonym value $psdm_x = \mu_x Q_s$ where $\mu_x = H_3(name_x \| src_x)$. The Sec-App authenticates that the computed pseudonym equals the accumulated pseudonym acquired during the client registration with the SS. When the pseudonym equals, the Sec-App:

i. Utilizes the app ID to get the value $Q_i = H_1(app\_ID)$.

ii. Gets the app-specific pseudonym $psdm_{x,i} = \mu_{x,i} Q_i$, where $\mu_{x,i} = H_3(name_x \| src_x \| app\_ID)$.

iii. Check trust score ϵ is whether greater than the threshold θ or not, i.e. $\epsilon > \theta$ or $\epsilon < \theta$.

iv. If $\epsilon > \theta$, then the verification reply code is immediately sent back to y; otherwise, the following steps are conducted.

v. Signs a warrant w_x, where w_x is the tuple $(psdm_{x,i} \| \delta \| S)$ and S is the delegation scope with $psdm_{x,i}$. The sign $sign'_{psdm_{x,i}}(w_x)$ is achieved with a delegation signing scheme comprising $sign'_{psdm_{x,i}}(w_x) = \mu_{x,i} H_1(w_x)$.

vi. Creates the tuple $Del_{x,y} = \left(psdm_{x,i}, w_x, sign'_{psdm_{x,i}}(w_x)\right)$.

vii. The value $Del_{x,y}$ is transmitted back to y via the browser as the verification reply code. It is observed that it does not give significant data to recognize the client or to connect this client to another OAuth 2.0 verification of a similar client for other apps.

ClientAuthreply2: The CS y accepts the verification reply code, comprising the tuple $Del_{x,y} = \left(psdm_{x,i}, w_x, sign'_{psdm_{x,i}}(w_x)\right)$ and gets a delegated sign as:

i. Creates a request R, where the CS requests the SS for the original identity of the client maintaining $psdm_{x,i}$.

ii. Determines $Delsign'_{psdm_y, psdm_x}(R, w_x) = sign'_{psdm_x}(w_x) + \mu_y H_2(R \| w_x)$.

Client Verification: The CS contacts the SS to verify the client and recognize the client profile in the CS. Accordingly, the CS transmits the mutual sign with the request for the client identity to the SS, which comprises the following tuple: $R, w\_x,$ 〖$Delsign$〗_(〖$psdm$〗_(y,i), 〖$psdm$〗_(x,i))^' (R, w_x), 〖$psdm$〗_(x,i), 〖$psdm$〗_(y,i), 〖$psdm$〗_y, app_ID.
By receiving the data from the CS, the SS:

i. Authenticates that $psdm_y$ is a public pseudonym of a legitimate CS.

ii. Gets the app-specific value $Q_i = H_1(app\_ID)$ by app_ID.

iii. Check trust score ϵ is whether greater than the threshold θ or not, i.e. $\epsilon > \theta$ or $\epsilon < \theta$.

iv. If $\epsilon > \theta$, then the verification reply code is immediately sent back to y; otherwise, the following steps are conducted.

v. Authenticates that the app-specific pseudonym obtainable by the CS, i.e. $psdm_{y,i}$, is connected to the static pseudonym $psdm_y$ by authenticating that $e^{(Q_s, psdm_{y,i})} = e^{(psdm_y, Q_i)}$.

vi. Certifies the delegated sign $Delsign'_{psdm_{y,i}, psdm_{x,i}}(R, w_x)$ by verifying whether $e^{\left(Delsign'_{psdm_{y,i}, psdm_{x,i}}(R, w_x), Q_i\right)} = e^{(H_1(w_x), psdm_{x,i})} e^{(H_2(R \| w_x), psdm_{x,i})}$ remains.

vii. Recognizes x by connecting $psdm_{x,i}$ to the client's original identity. To achieve this, the SS gets the app-specific pseudonyms for every client involved in the list of clients of y, i.e. determines $psdm_{u,i} = \mu_{u,i} Q_i$ for all clients u and for $Q_i = H_1(app\_ID)$ and chooses the client for which $psdm_{u,i} = psdm_{x,i}$.

RESEARCH ARTICLE

Once the client is recognized, the SS transmits data over a secure medium to y with the client's identity.

To achieve reliable transmission, CoAP is applied, which helps to minimize the inactive latency for resource-constrained networks. This CoAP uses a Binary Exponential Backoff (BEB) technique to manage the congestion in the network. For reliable communication, a CON message is sent from a user to the server. When the message is not effectively sent in the initial trial, a retransfer is performed. The CoAP selects an arbitrary value of RTO for the initial communication ranging from 2-3sec. When the initial retransfer is unsuccessful, the BEB duals the RTO to prevent congestion. So, the current RTO ($RTO_{current}$) value is double the preceding RTO (RTO_{prec}) value based on equation (1).

$$RTO_{current} = 2 \times RTO_{prec} \quad (1)$$

Thus, it achieves an effective many-to-many transmission based on the RTO values in the resource-constrained IoT networks.

4. SIMULATION RESULTS

This section analyzes the performance of the presented eHealthChain-based healthcare system called enhanced eHealthChain is analyzed by implementing it using iFogSim. iFogSim allows simulating real-world IoT systems, implementing them in a fog/edge scenario, and analyzing network measures including latency, cost, processing period, etc. In Table 2, the parameters used for simulating the proposed model are presented.

The efficiency is evaluated using iFogSim for the healthcare system with the enhanced eHealthChain model and analyzed different performance metrics to compare the efficiency with the existing blockchain models. The existing blockchain models are eHealthChain [13], TR-mHealthChain [19], FHIRChain [20], and BEdgeHealth [24]. Also, the considered metrics are a percentage of unsuccessful transmission, mean service time, mean network delay, mean server usage, and mean QoE. Likewise, the security analysis is performed to evaluate EOAuth 2.0 with the CoAP scheme in terms of data integrity, authorization, and confidentiality. Figure 6 depicts the high-level blockchain-edge model for healthcare systems implemented in the iFogSim simulator.

The suggested blockchain-edge model is split into 3 essential stages. The initial stage of the iFogSim enables the arrangement of resource-limited and edge nodes, as well as the integration of lightweight blockchain. Information observed and collected at nodes is transferred to edge nodes for local analysis and decision-making.

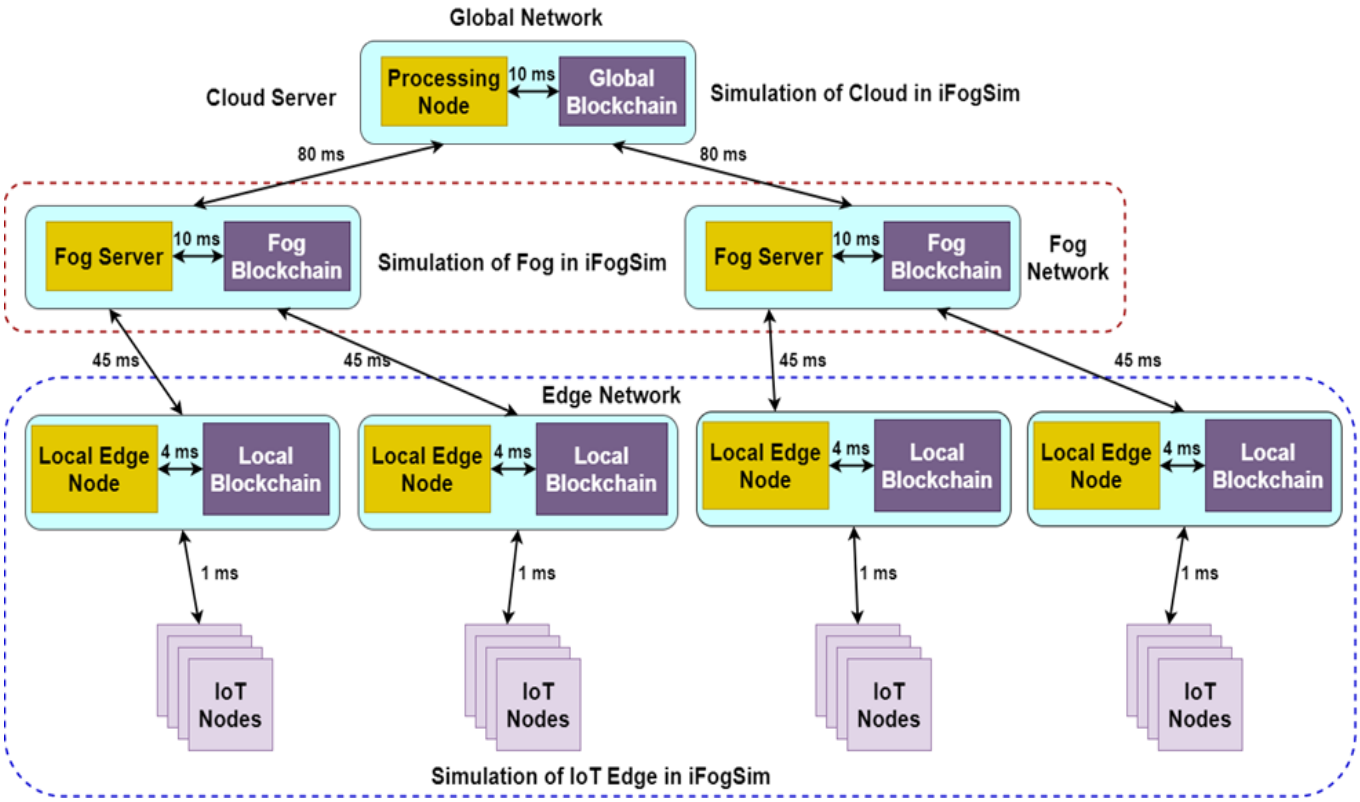

Figure 6 High-Level Design of Blockchain-Edge Model for Healthcare Systems in iFogSim

RESEARCH ARTICLE

Table 2 Simulation Parameters for the Blockchain-Edge Model

Parameters	Global networks	Fog networks	Edge networks	IoT devices
Upstream bandwidth (Mbps)	150	75	30	12.5
Downstream bandwidth (Mbps)	80	37.5	18	6
Storage abilities/RAM (GB)	16	8	4	1
Processing abilities/CPU (Million Instructions Per Second (MIPS))	13000-20000	8000-11000	4000-8000	500-1500
Transmission delay (ms)	145	45	5	1
Blockchain instructions (M)	20	11	5	-
Blockchain processing power (Watts)	20-80	12-40	1.4-20	-

Then, the local blockchain allows for trustworthy data exchange with other edge nodes. The subsequent phase permits the arrangement of fog nodes with increased computing capability. A single fog node connects to several IoT-edge nodes and offers the necessary resources (processing/storage) as well as network monitoring. The last phase is the arrangement of the cloud which has the most resources and is in charge of overall application administration. As a result, the blockchain-edge model's execution model strategy is bottom-up, i.e. from local to global networks.

4.1. Scalability Analysis

In this study, scalability is defined in terms of the number of failed transmissions, average service time, network delay, and throughput for different numbers of transmissions in the healthcare blockchain.

4.1.1. Percentage of Unsuccessful Transmission

It is the fraction of failed transmissions in the network. Table 3 shows the results of a percentage of unsuccessful transmissions under a varying number of transmissions for different healthcare blockchain models.

Table 3 Comparison of Percentage of Unsuccessful Transmissions (%)

No. of transmissions	TR-mHealthChain	FHIRChain	BEdgeHealth	eHealthChain	Enhanced eHealthChain
500	28.02	27.05	26.11	25.34	23.86
1000	29.96	28.41	27.83	26.51	25.73
1500	29.75	28.64	28.00	26.30	24.95
2000	30.44	29.82	28.04	27.08	26.34
2500	31.68	30.03	28.99	27.10	25.91

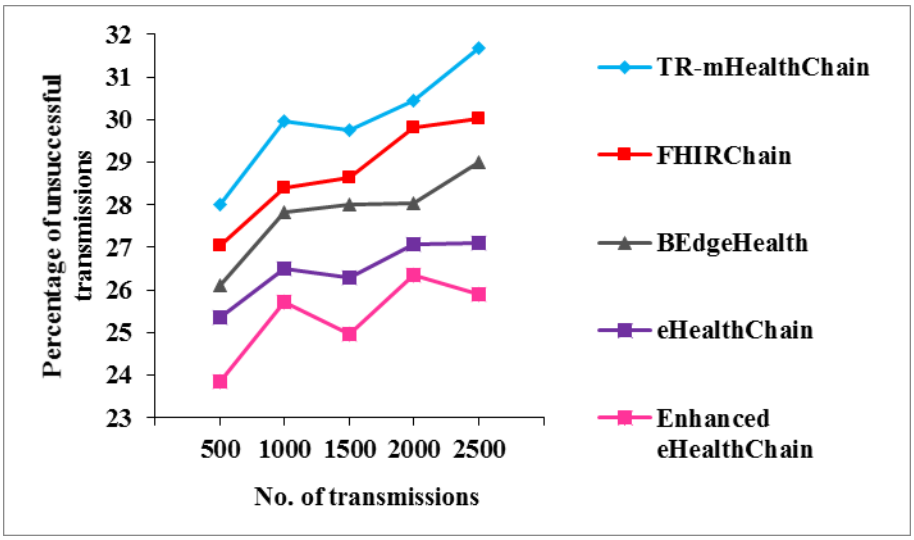

Figure 7 Percentage of Unsuccessful Transmissions vs. No. of Transmissions

RESEARCH ARTICLE

Figure 7 depicts the percentage of unsuccessful transmissions for the different blockchain-based healthcare systems under the number of transmissions. It analyzes that the enhanced eHealthChain model reduces the percentage of unsuccessful transmissions compared to the other models. For instance, when there are 500 transmissions, the percentage of unsuccessful transmissions for enhanced eHealthChain is 14.85% less than the TR-mHealthChain, 11.79% less than the FHIRChain, 8.62% less than the BEdgeHealth and 5.84% less than the eHealthChain. This is because of ensuring the client's identity by using the EOAuth 2.0 protocol that verifies the client requests based on their trust scores.

4.1.2. Average Service Time

Average service time is computed as equation (2).

$$Avg.service\ time = \frac{\sum total\ processing\ time + \sum total\ network\ time}{Number\ of\ transmissions} \quad (2)$$

Table 4 shows the results of average service time under a varying number of transmissions for different healthcare blockchain models.

Figure 8 illustrates the average service time (in sec) for the different blockchain-based healthcare systems under the number of transmissions. It analyzes that the enhanced eHealthChain model decreases the average service time compared to the other models. For example, when there are 500 transmissions, the average service time of enhanced eHealthChain is 22.9% less than the TR-mHealthChain, 19.5% less than the FHIRChain, 13.6% less than the BEdgeHealth and 5.7% less than the eHealthChain. This is because of using the trust level and adaptive backoff to minimize the authentication time and inactive latency, respectively.

Table 4 Comparison of Average Service Time (sec)

No. of transmissions	TR-mHealthChain	FHIRChain	BEdgeHealth	eHealthChain	Enhanced eHealthChain
500	4.28	4.10	3.82	3.50	3.3
1000	4.80	4.36	4.20	3.97	3.5
1500	4.90	4.76	4.49	4.10	3.9
2000	5.36	5.00	4.90	4.64	4.1
2500	5.61	5.48	5.10	4.90	4.5

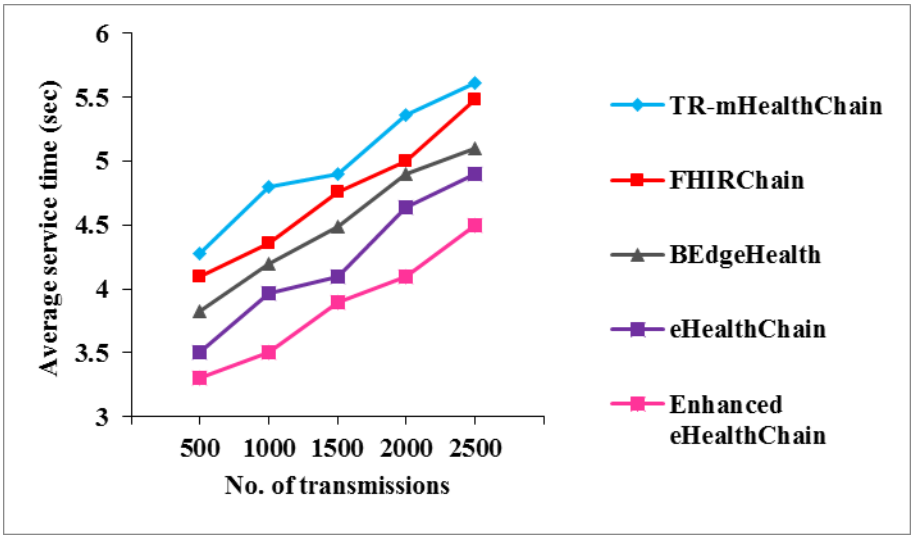

Figure 8 Average Service Time vs. No. of Transmissions

4.1.3. Average Network Delay

It is the average time between the client and server to transmit and access the data over a network. Table 5 shows the results of average network delay under a varying number of transmissions for different healthcare blockchain models.

Figure 9 portrays the average network delay (in sec) for the different blockchain-based healthcare systems under the number of transmissions. It observes that the enhanced eHealthChain model decreases the average network delay compared to the other models. For example, when there are 500 transmissions, the average network delay of enhanced

RESEARCH ARTICLE

eHealthChain is 20.75% less than the TR-mHealthChain, 17.73% less than the FHIRChain, 10% less than the BEdgeHealth and 4.49% less than the eHealthChain. This is due to the minimization of the authentication time and inactive latency in dynamic network configurations.

Table 5 Comparison of Average Network Delay (sec)

No. of transmissions	TR-mHealthChain	FHIRChain	BEdgeHealth	eHealthChain	Enhanced eHealthChain
500	0.2284	0.2200	0.2011	0.1895	0.181
1000	0.2500	0.2291	0.2185	0.2000	0.186
1500	0.2587	0.2504	0.2411	0.2300	0.210
2000	0.2705	0.2593	0.2440	0.2373	0.214
2500	0.2810	0.2662	0.2576	0.2490	0.235

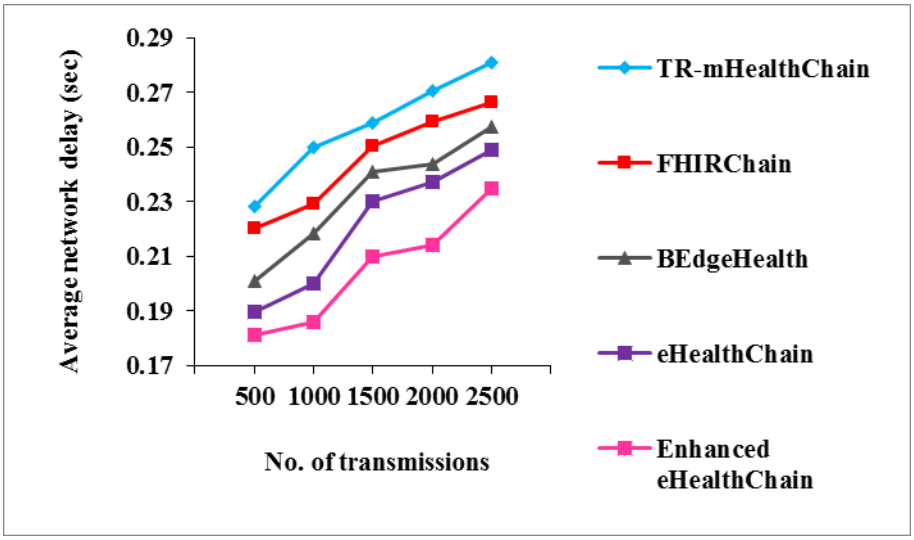

Figure 9 Average Network Delay vs. No. of Transmissions

4.1.4. Average Server Usage

It is the mean utilization of the server during data transmission, authentication, and authorization processes. Table 6 shows the results of average server usage under a varying number of transmissions for different healthcare blockchain models.

Figure 10 displays the average server usage (in %) for the different blockchain-based healthcare systems under the number of transmissions. It observes that the enhanced eHealthChain model decreases the average server usage compared to the other models. For example, when there are 500 transmissions, the average server usage of enhanced eHealthChain is 2.2% less than the TR-mHealthChain, 1.3% less than the FHIRChain, 0.8% less than the BEdgeHealth and 0.4% less than the eHealthChain. This is achieved because of decreasing in network delay and mean service time while increasing the number of transmissions, resulting in less usage of the server by the enhanced eHealthChain model compared to other models.

Table 6 Comparison of Average Server Usage (%)

No. of transmissions	TR-mHealthChain	FHIRChain	BEdgeHealth	eHealthChain	Enhanced eHealthChain
500	97.30	96.38	95.97	95.50	95.16
1000	97.96	97.50	96.68	96.40	95.62
1500	97.01	96.24	96.00	95.10	94.60
2000	97.86	97.40	96.50	96.00	95.70
2500	98.48	98.20	97.80	96.56	95.50

RESEARCH ARTICLE

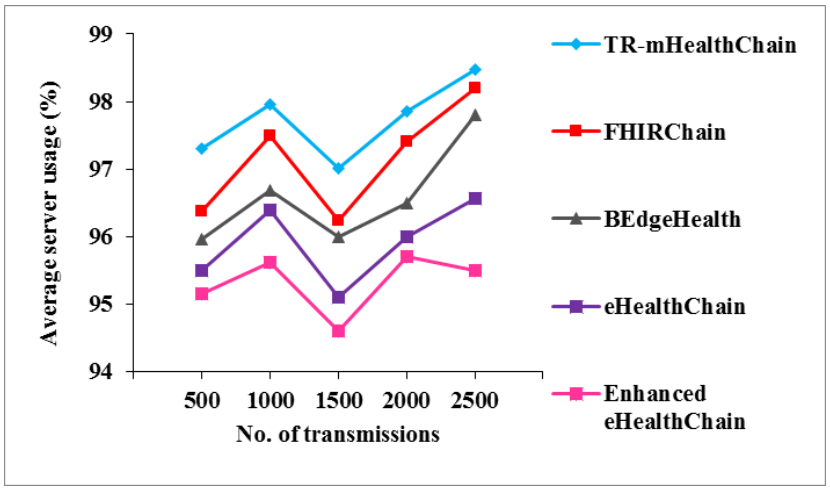

Figure 10 Average Server Usage vs. No. of Transmissions

4.1.5. Average QoE

It is the mean QoE experienced by all clients in the network. Table 7 shows the results of average QoE under a varying number of transmissions for different healthcare blockchain models. Figure 11 shows the average QoE (in %) for the different blockchain-based healthcare systems under the number of transmissions. It indicates that the enhanced eHealthChain model decreases the average QoE compared to the other models. For example, when there are 500 transmissions, the average QoE of enhanced eHealthChain is 29.5% greater than the TR-mHealthChain, 22.5% greater than the FHIRChain, 16.2% greater than the BEdgeHealth and 7.1% greater than the eHealthChain. This is due to the reduction in the percentage of failed transactions, service time, network delay, and server usage by authenticating user identity using EOuth2.0 and CoAP protocols during data transmission via cloud-edge networks.

Table 7 Comparison of Average QoE

No. of transmissions	TR-mHealthChain	FHIRChain	BEdgeHealth	eHealthChain	Enhanced eHealthChain
500	10.5	11.1	11.7	12.7	13.6
1000	11.3	12.2	12.6	14.0	16.2
1500	10.8	11.3	12.5	13.8	14.7
2000	11.7	12.7	13.1	13.5	15.0
2500	12.4	12.9	14.0	15.0	16.1

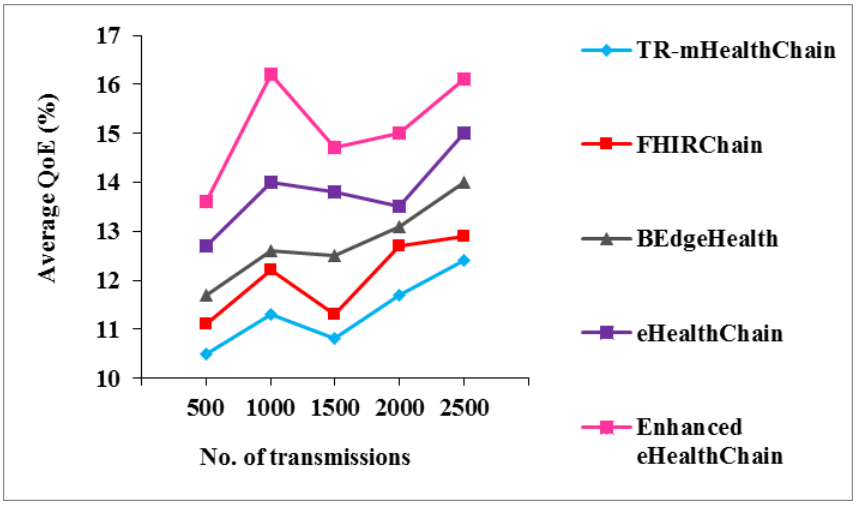

Figure 11 Average QoE vs. No. of Transmissions

RESEARCH ARTICLE

4.1.6. Throughput

It is the number of successful transmissions of healthcare records that the system handles in a second. Table 8 shows the results of throughput under a varying number of nodes for different healthcare blockchain models. Figure 12 shows the throughput (in transmissions per second) for the different blockchain-based healthcare systems under the number of transmissions. It indicates that the enhanced eHealthChain model increases the throughput scalability while increasing the number of nodes compared to the other models. For example, when there are 250 nodes, the throughput of enhanced eHealthChain is 85.7% greater than the TR-mHealthChain, 52.9% greater than the FHIRChain, 32% greater than the BEdgeHealth and 13% greater than the eHealthChain. The obtained results proved that the enhanced eHealthChain model is highly scalable in increasing the number of nodes and the number of healthcare records. This has no significant impact on efficiency because requests are processed securely by authenticating the user's identity based on the user's trust score.

Table 8 Comparison of Throughput (Transmissions per Second)

No. of nodes	TR-mHealthChain	FHIRChain	BEdgeHealth	eHealthChain	Enhanced eHealthChain
250	700	850	985	1150	1300
500	968	1200	1320	1700	2100
750	1203	1400	1900	2500	3000
1000	1948	2300	2700	3000	3410

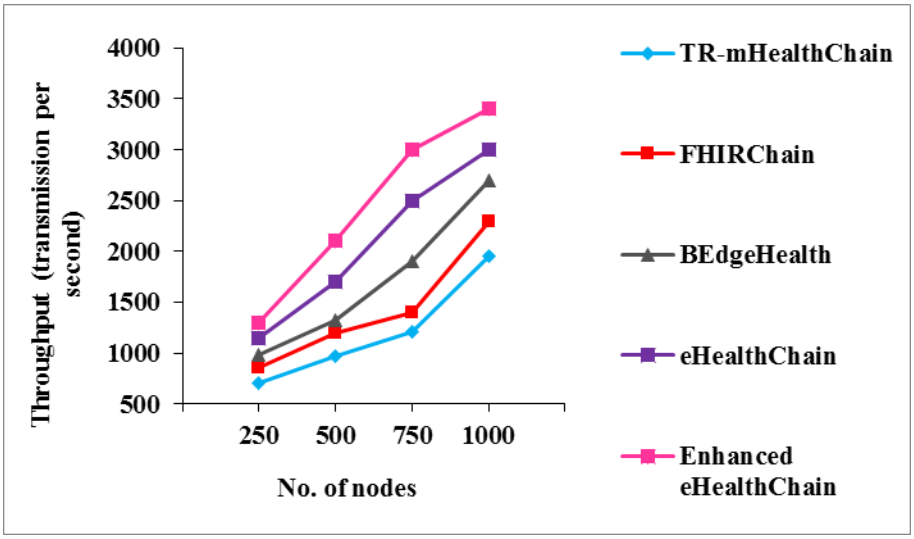

Figure 12 Throughput vs. No. of Nodes

4.2. Security Analysis

- Confidentiality: Any uncertified node is rejected from the data access with the help of this security service.
- Authorization: All nodes provide a unique key pair to perform cryptographic processes with the help of this security service. It is realized by applying the public key when any suspicious node desires to interact with network nodes; it requires the public key pair of the certified node.
- Integrity: It guarantees that data accepted by the target node have not been modified during transmission either by conflict or tampering by an untrustworthy node.

Figure 13 shows the confidentiality (in %) achieved by the OAuth 2.0+MQTT, OAuth 2.0+CoAP, and EOAuth 2.0+CoAP with varying the number of transmissions. It indicates that the EOAuth 2.0+CoAP can increase the confidentiality of data storage and access in healthcare systems compared to the other protocols. For instance, when there are 2500 transmissions, the confidentiality of EOAuth 2.0+CoAP is 3.8% greater than the OAuth 2.0+MQTT and 1% greater than the OAuth 2.0+CoAP. This is because of enhancing client security by measuring their trust levels and achieving reliable data transmission.

Table 9 shows the results of confidentiality under a varying number of transmissions for different authentication algorithms. Table 10 shows the results of authorization under a varying number of transmissions for different authentication algorithms.

RESEARCH ARTICLE

Figure 14 shows the authorization (in %) attained by the OAuth 2.0+MQTT, OAuth 2.0+CoAP, and EOAuth 2.0+CoAP with varying the number of transmissions. It realizes that the EOAuth 2.0+CoAP can improve the authorization to access sensitive information in healthcare applications compared to the other protocols. For example, if 2500 transmissions are considered in the network, then the authorization of EOAuth 2.0+CoAP is 3.8% higher than the OAuth 2.0+MQTT and 2.1% higher than the OAuth 2.0+CoAP. This is due to the consideration of trust measure and adaptive backoff period, which reduce the authentication period and inactive latency, correspondingly.

Table 11 shows the results of integrity under a varying number of transmissions for different authentication algorithms.

Figure 15 shows the data integrity (in %) obtained by the OAuth 2.0+MQTT, OAuth 2.0+CoAP, and EOAuth 2.0+CoAP with varying the number of transmissions. It observes that the EOAuth 2.0+CoAP can maximize the data integrity of data storage and access in medical systems more than the other protocols. For the case of 2500 transmissions, the data integrity of EOAuth 2.0+CoAP is 6.4% greater than the OAuth 2.0+MQTT and 1.7% greater than the OAuth 2.0+CoAP by enhancing the confidentiality of accessing sensitive information in the clinical systems.

Table 9 Comparison of Confidentiality

No. of transmissions	OAuth 2.0+MQTT	OAuth 2.0+CoAP	EOAuth 2.0+CoAP
500	76.0	77.0	79.4
1000	78.6	80.0	83.0
1500	79.4	81.0	82.5
2000	83.1	85.7	88.0
2500	86.0	88.4	89.3

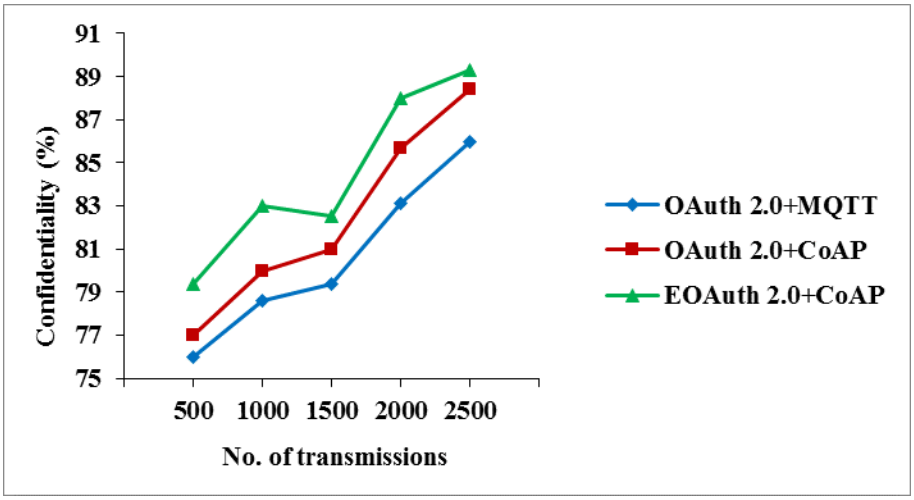

Figure 13 Confidentiality vs. No. of Transmissions

Table 10 Comparison of Authorization

No. of transmissions	OAuth 2.0+MQTT	OAuth 2.0+CoAP	EOAuth 2.0+CoAP
500	71.0	72.6	75.3
1000	71.6	74.0	75.0
1500	73.0	74.9	77.4
2000	76.3	79.5	80.9
2500	79.0	80.3	82.0

RESEARCH ARTICLE

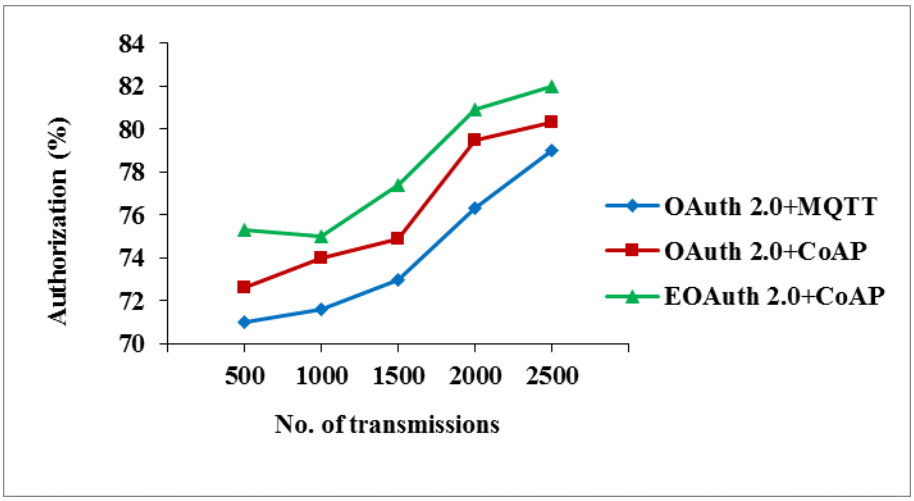

Figure 14 Authorization vs. No. of Transmissions

Table 11 Comparison of Integrity

No. of transmissions	OAuth 2.0+MQTT	OAuth 2.0+CoAP	EOAuth 2.0+CoAP
500	79.3	81	83.8
1000	80	84	87
1500	83.1	84.5	86.3
2000	85.4	87	90.3
2500	86	90	91.5

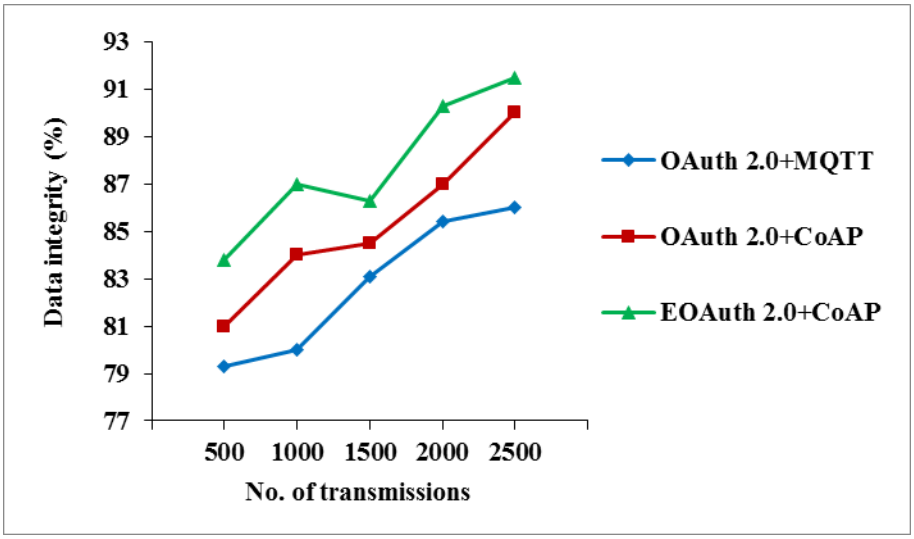

Figure 15 Data Integrity vs. No. of Transmissions

4.3. Discussion

The proposed EOAuth 2.0-based protocol and CoAP are relatively enhanced authentication protocols for blockchain technology in the healthcare sector. This enhanced eHealthChain model is well-suited for storing and sharing health records because the trust of each stakeholder in the medical sector is increased in the absence of any intermediary. This model focused on enhancing security and interoperability by achieving reliable data sharing between multiple stakeholders using EOAuth 2.0 and CoAP protocols. Thus, this enhanced eHealthChain model solves the network interoperability issue by guaranteeing secure health data

RESEARCH ARTICLE

sharing, resulting in it will be adopted in other systems like smart homes, transportation, etc.

The enhanced eHealthChain model can only be developed for healthcare industries, where cloud-edge networks have been used to share multiple health records and enhance the security of data sharing. As a result, this model does not need additional costs in terms of hardware and software requirements for execution, maintenance, and upgrades. This model can be a promising blockchain technology in healthcare organizations to improve the client's security from different vulnerabilities and attacks due to the consideration of the trust score of each client. Based on the trust scores, highly trusted clients are shared or access data without further authentication.

The proposed enhanced eHealthChain model is that the patient's health information is collected from multiple healthcare IoT devices and this information is accessible securely and privacy-sensitively by the patients and physicians. In this model, rather than the hospital, clients are the data providers or owners and are responsible for managing their health records. To ensure data privacy and consent, many privacy-preserving algorithms have been developed by earlier researchers that allow clients to securely use and share data across multiple stakeholders. This study only focused on the enhancement of the authentication protocol during data sharing in healthcare systems, whereas future work will consider the challenges in data privacy and design a novel privacy-preserving protocol for health record information privacy against unauthorized access.

5. CONCLUSION

In this paper, the EOAuth 2.0-based protocol was initially designed to improve client security by integrating the pseudonym-based sign and sign delegation policies. The trust value of each client was measured by the data owner to ensure the client's identity and reduce the authentication time since highly trusted clients were not needed to consider for the authentication process. Besides, the Sec-App was designed which involves a robust UI layer to protect the client's entry with the help of cryptographic procedures. Moreover, the CoAP was employed to establish secure broadcast in cloud-edge IoT applications. To conclude, the implementation findings proved that the enhanced eHealthChain model using EOAuth 2.0 and CoAP achieves higher efficiency than the standard protocols.

REFERENCES

[1] O. Ali, A. Jaradat, A. Kulakli, A. Abuhalimeh, "A comparative study: Blockchain technology utilization benefits, challenges and functionalities," IEEE Access, vol. 9, 2021, pp. 12730-12749.

[2] M. A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, "A survey on the adoption of blockchain in iot: challenges and solutions," Blockchain: Research and Applications, vol. 2, no. 2, 2021, 1-49.

[3] A. Al Sadawi, M. S. Hassan, M. Ndiaye, "A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges," IEEE Access, vol. 9, 2021, pp. 54478-54497.

[4] M. I. Rojo-Rivas, D. Díaz-Sánchez, F. Almenarez, A. Marín-Lopez, "Kriper: A blockchain network with permissioned storage," Future Generation Computer Systems, vol. 138, 2023, pp. 160-171.

[5] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, ... Y. Cao, "A survey on blockchain technology: evolution, architecture and security," IEEE Access, vol. 9, 2021, pp. 61048-61073.

[6] A. Verma, P. Bhattacharya, N. Madhani, C. Trivedi, B. Bhushan, S. Tanwar, ... R. Sharma, "Blockchain for Industry 5.0: vision, opportunities, key enablers, and future directions," IEEE Access, vol. 10, 2022, pp. 69160-69199.

[7] E. Mbunge, B. Muchemwa, J. Batani, "Sensors and healthcare 5.0: transformative shift in virtual care through emerging digital health technologies," Global Health Journal, vol. 5, no. 4, 2021, pp. 169-177.

[8] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, M. Omar, "The role of blockchain technology in telehealth and telemedicine," International Journal of Medical Informatics, vol.148, 2021, pp. 1-10.

[9] A. Haleem, M. Javaid, R. P. Singh, R. Suman, S. Rab, "Blockchain technology applications in healthcare: an overview," International Journal of Intelligent Networks, vol. 2, 2021, pp. 130-139.

[10] M. Soni, D. K. Singh, "Blockchain-based security & privacy for biomedical and healthcare information exchange systems," Materials Today: Proceedings, 2021, pp. 1-7.

[11] P. Pandey, R. Litoriya, "Securing and authenticating healthcare records through blockchain technology," Cryptologia, vol. 44, no. 4, 2020, pp. 341-356.

[12] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, G. Dhiman, "Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives," Journal of Food Quality, vol. 2021, 2021, pp. 1-20.

[13] P. Pawar, N. Parolia, S. Shinde, T. O. Edoh, M. Singh, "eHealthChain – a blockchain-based personal health information management system," Annals of Telecommunications, 2021, pp.1-13.

[14] X. Xu, X. Wang, Z. Li, H. Yu, G. Sun, S. Maharjan, Y. Zhang, "Mitigating conflicting transactions in hyperledger fabric-permissioned blockchain for delay-sensitive IoT applications," IEEE Internet of Things Journal, vol. 8, no. 13, 2021, pp. 10596-10607.

[15] https://hyperledger-fabric.readthedocs.io/en/release-2.0/blockchain.html

[16] S. Hong, H. Kim, "VaultPoint: A blockchain-based SSI model that complies with OAuth 2.0," Electronics, vol. 9, no. 8, 2020, pp. 1-20.

[17] D. Dinculeană, X. Cheng, "Vulnerabilities and limitations of MQTT protocol used between IoT devices," Applied Sciences, vol. 9, no. 5, 2019, pp. 1-10.

[18] M. Q. Nguyen, D. Loghin, T. T. A. Dinh, "Understanding the scalability of Hyperledger Fabric," arXiv preprint arXiv:2107.09886, 2021, pp. 1-10.

[19] D. Ichikawa, M. Kashiyama, T. Ueno, "Tamper-resistant mobile health using blockchain technology," JMIR mHealth and uHealth, vol. 5, no. 7, 2017, pp. 1-10.

[20] P. Zhang, J. White, D. C. Schmidt, G. Lenz, S. T. Rosenbloom, "FHIRChain: applying blockchain to securely and scalably share clinical data," Computational and Structural Biotechnology Journal, vol. 16, 2018, pp. 267-278.

[21] H. Huang, P. Zhu, F. Xiao, X. Sun, Q. Huang, "A blockchain-based scheme for privacy-preserving and secure sharing of medical data," Computers & Security, vol. 99, 2020, pp. 1-13.

[22] T. Benil, J. J. C. N. Jasper, "Cloud based security on outsourcing using blockchain in E-health systems," Computer Networks, vol. 178, 2020, pp. 1-45.

[23] U. Chelladurai, S. Pandian, "A novel blockchain based electronic health record automation system for healthcare," Journal of Ambient Intelligence and Humanized Computing, 2021, pp. 1-11.

[24] D. C. Nguyen, P. N. Pathirana, M. Ding, A. Seneviratne, "BEdgeHealth: a decentralized architecture for edge-based IoMT

RESEARCH ARTICLE

networks using blockchain," IEEE Internet of Things Journal, 2021, pp.1-15.
[25] M. Ejaz, T. Kumar, I. Kovacevic, M. Ylianttila, E. Harjula, "Health-BlockEdge: blockchain-edge framework for reliable low-latency digital healthcare applications," Sensors, vol. 21, no. 7, 2021, pp.1-22.
[26] T. Kumar, E. Harjula, M. Ejaz, A. Manzoor, P. Porambage, I. Ahmad, M. Ylianttila, "BlockEdge: blockchain-edge framework for industrial IoT networks," IEEE Access, vol. 8, 2020, pp.154166-154185.

Authors

Thakur Saikumari is in 3rd year of her Ph.D. program at M.G.R Research Deemed to be University. She is currently an Assistant Professor in the Information Technology Department, Complier Design at Malla Reddy Institute of Technology and Science. Her research interest is Blockchain Technology and the Internet of Things. She has also published a paper on a survey of Blockchain technology Integrated with the Internet of Things. She holds her Master's Degree from Shadan Womens College of Engineering and Technology Affiliated with the University of JNTUH. Before starting her Ph.D., she was Head of the Department of Information Technology at Shadan Womens College of Engineering and Technology for 4 years.

Dr. G. Victo Sudha George currently working as a Professor in the Department of Computer Science and Engineering at Dr.M.G.R Educational and Research Institute, Chennai-95. She is having more than 25 years of academic experience. She received B.E (CSE) in 1993, M.Tech(CSE) in 2007, and Ph.D. in 2016. Her area of interest includes Bio-Informatics, Big Data Data Mining, Cloud Computing, and Computational Intelligence.

How to cite this article:

Thakur Saikumari, G. Victo Sudha George, "An Enhanced Authorization Protocol in Blockchain for Personal Health Information Management System", International Journal of Computer Networks and Applications (IJCNA), 10(3), PP: 277-295, 2023, DOI: 10.22247/ijcna/2023/221885.