A Lightweight Blockchain-Based Framework for Medical Cyber Physical System

Ashish Kumar (ashishk.ph21.cs@nitp.ac.in)
National Institute of Technology Patna
Kakali Chatterjee
National Institute of Technology Patna

Research Article

Keywords: Blockchain, Medical cyber physical system, Consensus, IoT gateway, Actuator

Posted Date: September 22nd, 2022

DOI: https://doi.org/10.21203/rs.3.rs-2073666/v1

A Lightweight Blockchain-Based Framework for Medical Cyber Physical System

Ashish Kumar[1] and Kakali Chatterjeer[2]

[1]Department of Computer Science and Engineering, National Institute of Technology Patna, Patna, 800005, Bihar, India.
[2]Department of Computer Science and Engineering, National Institute of Technology Patna, Patna, 800005, Bihar, India.

Contributing authors: ashishk.ph21.cs@nitp.ac.in; kakali@nitp.ac.in;

Abstract

A medical cyber physical system(MCPS) combines intelligent medical devices with a network. Nowadays, MCPS is extensively used in the healthcare system. While sharing the patient data into MCPS, the data privacy of the MCPS is a significant challenge in healthcare as most of the devices are suffered from data leaking and data manipulation attack. In this current work, blockchain implementation ensures patient data security and privacy with no delay. The blockchain module controls unauthorized data access from illegitimate users. The result and performance analysis of the proposed framework shows the low latency in the data sharing, high transaction rate, and high throughput with an increasing number of users in the network.

Keywords: Blockchain, Medical cyber physical system, Consensus, IoT gateway, Actuator

1 Introduction

Cyber-Physical system is an emerging technology in the modern world and also attracts much attention to their key features of computing and communication capabilities with the cyber and physical world. Nowadays, Cyber-physical system is used almost in every sector, like electrical power

grids, transportation system, household appliances, healthcare devices. With the advancement in technology of wireless sensor networks, cloud computing, and medical sensors, CPS is capable of healthcare applications like remote patient care and taking action on the medical emergency for the patient. A medical cyber physical system is the integration of a network of medical devices and cyber-physical system. Moreover, used for many life support devices and critical units. In MCPS, medical sensors, implantable body devices, and wearable devices are responsible for sensing the patient body and sharing those data with the medical organization for patient treatment efficiently [1]. Wearable devices will track the patient's health records such as blood pressure, sleep cycle, heart rate, SPo2 monitoring, and body temperature to improve the patient's life. The medical data which is collected by the medical sensors shared via network connection like Bluetooth, ZigBee, or wi-fi, maybe at security risk of data leakage, data theft, data manipulation, and also vulnerable to many security attacks like man-in-the-middle attacks, false data injection, SQL injection [2]. MCPS generates a large amount of medical data in a short time and is stored on a cloud server that needs uncompromising security. Some solutions to enhance security and privacy (Shrestha et al., 2016; Filkins et al., 2016), fog computing(Bonomi et al., 2012; Yi et al., 2015), mobile edge computing(Abbas et al., 2017; Hu et al., 2015), are discussed. In the literature, most of the MCPS is based on the cryptographic algorithm in which medical data is secured using bilinear pair-based cryptography, a key control scheme, DNA-based encryption, and signature-based cryptography. The medical data is stored on the cloud using these techniques and accessed through the internet[3]. While accessing these data through the cloud, there is much overhead in terms of latency and network bandwidth, and also found some difficulties in scalability, throughput, the volume of the data, and the privacy of the medical data.[4].

While working in the collaborative model, data security and privacy are vital concerns as medical data are too confidential from ethical and legal perspectives. So, while designing an MCPS, exceptional attention is paid to data security and privacy. We also have to consider important issues like storing and managing the large volume of data collected through medical sensors[5]. Many solutions are proposed for the security issues like the Cryptographic algorithm(Kumar et al., 2014), Kalman filter and chaotic cryptosystem(Mekki et al., 2018), and PKI scheme(Ray et al., 2013), but they have not been considered the privacy for the critical data. Many solutions are proposed for data storage and management (Iwaya et al., 2017; Huang et al., 2017), but fail to provide privacy to the medical data.

The intelligent healthcare system is integrated with healthcare 4.0, which was introduced by industry 4.0. Industry 4.0 comprises key technologies like data mining, artificial intelligence, machine learning, blockchain technology, cloud computing, fog computing, etc[26]. An intelligent healthcare system uses a smart wearable device that will capture the health data like blood

pressure, temperature, glucose level, and heart rate for the real-time monitoring of a patient's health remotely. The data collected through the wearable device and implantable devices are stored on the cloud and made available to the caregivers[31]. The patient health data are shared through a network connection like Bluetooth, Zigbee, or COAP, which may be at security risk of data leakage, data theft, data manipulation, and also vulnerable to many security attacks like Man-in-the-middle attacks, phishing, and SQL injections.

1.1 Motivation

The motivation behind this paper is : Most cryptographic solutions are mainly focused on the security of medical data. However, data leakage, data tampering, and data traceability are not taken into consideration. Considering a hospital scenario, where the patient's data is shared with the organization. Here different stakeholders like medical practitioners, drug agencies, R & D, etc. In such an open environment, the possibility of data falsification and data tampering rises high. On the other hand, the direct storage of sensitive health data, such as data aggregated from body sensors, is prone to advanced attacks like ransomware attacks. Hence the privacy, integrity & confidentiality of health data must be maintained.

While working in the collaborative model, data security and privacy are vital concerns as medical data are too confidential from ethical and legal perspectives. So, while designing an MCPS, exceptional attention is paid to data security and privacy. We also have to consider important issues like storing and managing the large volume of data collected through medical sensors. Many solutions are proposed for the security issues like the Cryptographic algorithm(Kumar et al., 2014), Kalman filter and chaotic cryptosystem(Mekki et al., 2018), and PKI scheme(Ray et al., 2013), but they have not been considered the privacy for the critical data. Many solutions are proposed for data storage and management (Iwaya et al., 2017; Huang et al., 2017) but fail to provide privacy to medical data.

1.2 Research Problem and Contribution

Also, sharing the data in the network may lead to data or privacy leakage. For instance, a patient shares medical data with the caregivers. Somehow, attackers may be able to gain knowledge about the patient's name, location, and disease. Also, MCPS generates a large amount of data in a short time, named big data. In order to handle the privacy of big data, secure and efficient privacy preservation is required.

These two issues motivate us to work in these technologies like blockchain that can handle data tampering, data traceability and data privacy with no delay and low processing time. Hence, this paper identified two significant objectives in the MCPS. The first objective is to eliminate data tampering, and another one is to enhance data traceability with low processing time. To fulfill the

objectives, we have designed a blockchain-based framework as it delivers a trusted network for sharing information in insecure channels.
The key contributions of this research work are as follows:

- A framework has been proposed, which integrates blockchain for the MCPS that enhances the security and reduces the latency.
- The proposed blockchain-based ensures privacy with the clustering technique where the cluster head will authenticate every request of data retrieval. The trust of the cluster head depends upon the reward-punishment scheme.
- The proposed framework is demonstrated and analyzed by the various experiment and results in terms of several metrics like throughput, transaction time, latency, and a number of users. The Blockchain module controls the unauthorized access of the data from illegitimate users.

The rest of the paper is organized as follows: Section 2 presents Related Works; Section 3, provides Describes the proposed framework, section 4 presents the experimental setup and results, Section 5 presents the Performance and analysis of the proposed scheme ; finally, it concluded in Section 6.

2 Background

With the advancement in technology, the healthcare sector is also developed with new technology like cloud computing, machine learning, MCPS, blockchain, etc. The distributed systems simultaneously monitor and control various parts of the patient's physiology in place of standalone devices that can be created, approved, and utilized independently of one another to treat patients. Modern medical device systems are a unique class of cyber-physical systems due to the devices' embedded software, networking capabilities, and complex physical dynamics displayed by patient bodies (CPS). These are what we refer to as MCPS.

2.1 Medical cyber physical system

MeMedical cyber physical system consists of the medical device with the network system that will connect the medical devices and the cyber things, an intelligent control system that will take action based on the signal generated through actuator[1]. MCPS is interconnected, intelligent, safety-critical systems for medical devices. Patients serve as the "plants" in traditional clinical scenarios, which can be thought of as closed-loop systems with caregivers acting as the controllers, medical devices serving as the sensors, and caregivers acting as the actuators[11]. By integrating more computational entities that assist the caregiver in managing the "plant," MCPS changed this viewpoint. The conceptual overview of MCPS is shown in Figure 1. The devices used in MCPS can be divided into two main categories based on their primary uses: monitoring devices, such as bedside oxygen-level and heart-rate monitors and sensors, which provide various types of clinic-relevant information about patients; and delivery devices, such as infusion pumps and ventilators,

which actuate therapy capable of altering the patient's physiological state. The monitoring equipment in MCPS can transmit the data it accumulates to administrative support or decision support entities, each of which serves a different but complementary objective. Decision support entities can process the collected data and provide alarms for a number of medical emergencies[22]. Alarms are important to let medical professionals know when a patient's condition has gotten worse and what information is pertinent to treating them. But it is now obvious that we need to create intelligent alarm systems that go beyond the existing threshold-based approaches to deliver more precise, targeted alarms together with context data[9]. The analysis of the data and the deployment of delivery mechanisms by caregivers to start treatment place them in the patient's control loop. Alternatively, the decision support entities can close the loop by using a smart controller to assess the information gathered from the monitoring devices, determine the patient's state of health, and automatically begin therapy (such as a medicine infusion) by sending commands to delivery devices[11].

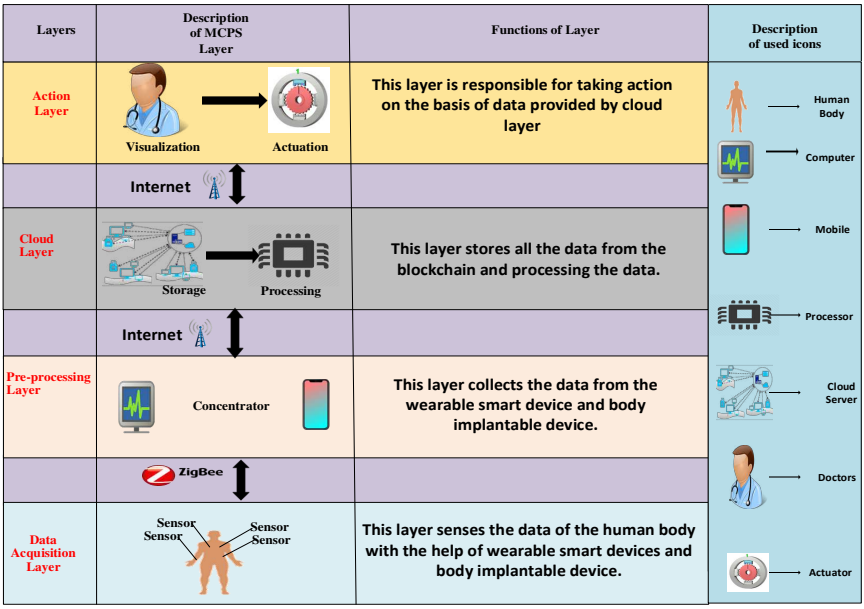

Fig. 1: Basic architecture of the MCPS

To address the security issues in IoT-based e-healthcare systems, several solutions were discovered. The primary goal of an IoT-based electronic healthcare system is to gather health information from multiple users and exchange it with them so that they can each receive different healthcare-related services. This system requires a variety of users; hence strong authentication methods

are required to manage user access.
The Basic architecture of the MCPS is:

- Data acquisition layer: This layer senses the data of the human body with the help of wearable smart devices and body implantable devices. And sends it to the mobile or any connected device for further process of data.
- Pre-processing layer: After sensing the data from the smart device, data is collected to any smartphone or system so that it can be sent to medical organizations and caregivers.
- Cloud layer: This layer stores all the medical data from the blockchain and processes the data and transfers the data to caregivers for taking action.
- Action layer: Based on the medical data received, the action will be taken by the caregivers or automatically by the smart device.

2.2 Related Works

The resources from the Internet can also be accessed by medical devices (or nodes) in MSNs. The networked gadgets enhance medical outcomes, cut healthcare expenses, and integrate the Internet into patients' daily lives. However, because such an ecosystem exchanges and stores such sensitive information, cybercriminals are very likely to compromise such a type of network for financial gain. A hardware module with four modules—attack scenario development, security enhancement, security evaluation, and platform management—that is developed for the security of cyber-physical systems was proposed by X Ning et al[33]. This module aids in attack detection and mitigation, hence minimising or eliminating cps loss.

B Jiang et al.[24] Differential privacy can be utilised to preserve privacy since data loss makes data sharing in the collaborative model require additional privacy. By using the Laplace and exponential mechanisms to introduce noise to the data, differential privacy can be established. Through the use of federated learning to create data models and the sharing of the data models rather than the raw data empowered by blockchain, Y Lu et al.[26] turned the challenge of data sharing into a machine learning problem. The two parts of this paradigm that are in charge of retrieving and storing data are the data requester and the data providers. Based on the quality of collaborative training, the chosen committee uses proof of training as a basis for execution.

Q yang et al.[34] utilized a TEE in their model, a hardware device called GB gmbTEE is used to isolate the execution of any programme or piece of code, preventing interference from other parties during the creation of a blockchain.

JPA Yaacoub et al. [27] discussed about the primary concerns in a cyber-physical system are security threats, attacks, and vulnerabilities. Various physical and cyberattacks, threats, and vulnerabilities are described, along with possible solutions including cryptographic and non-cryptographic techniques.

Table 1: Literature review

S.no.	References	Year	Title of the paper	Objective	Limitations
1	X Ning et al. [33]	2021	Design, analysis and implementation of a security assessment/enhancement platform for cyber physical system	A hardware module is designed for the security of cyber physical system and this module helps in detecting the attack, mitigating the attack so that loss in cps can be minimized or terminated.	There are limited no. of attacks, detection method and mitigation method.
2.	Y Lu [26]	2019	Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT	Integrated federated learning in the consensus protocol, so that computing work for consensus can be used for federated learning.	No discussion about the data utility and efficiency of blockchain for data privacy.
3.	Q yang et al. [34]	2021	Secure Blockchain Platform for Industrial IoT with Trusted Computing Hardware	Implemented a trusted execution environment for blockchain to safeguard blockchain against different attacking vectors	They have not considered the privacy protection of blockchain data.
4.	Shrestha et al. [35]	2016	Enhanced e-health framework for security and privacy in healthcare system	To improve data privacy and security	Failure at a single point, not robust.
5.	Kshteri et al.[25]	2017	Blockchain's roles in strengthening cyber security and protecting privacy	Described the functions of a blockchain to protect users' privacy from cyber security threats	Not suitable for large dataset.
6.	Banerjee et al. [13]	2018	A blockchain future for internet of things security: a position paper	Presented IoT security solutions with blockchain technology	Takes more time for small and large data set
7.	Gordon et al. [14]	2018	Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability	Offer a hand of assistance in the blockchain's journey to patient-driven interoperability.	Consume more power and computational power.
8.	Theodouli et al. [15]	2018	On the Design of a Blockchain-Based System to Facilitate Healthcare Data Sharing	Developed a blockchain-based healthcare data collaboration solution.	Not focussed on privacy issues of the healthcare data.
9.	Yang et al. [16]	2017	A reliable, searchable and privacy-preserving e-healthcare system for cloud-assisted body area networks	Designed a healthcare system	Not support dynamic data set
10.	He et al. [17]	2018	Privacy in the Internet of Things for Smart Healthcare	Developed a plan for a smart IoT healthcare system to protect privacy	Only suitable for medium range dataset, not for large dataset
11.	Sarwar et al. [18]	2012	Intelligent Naive Bayes Approach to Diagnose Diabetes Type-2	Early Prediction of diabetes-disease diagnosis with AIapproach	System evaluated with only few parameters.
12.	Ma et al. [19]	2018	Certificateless searchable public key encryption scheme for mobile healthcare system	Created a PKE scheme that can be searched for a mobile healthcare system	Not resist replay and MIM attack.
13.	Sharma et al. [20]	2018	Improved Classical Cipher for Healthcare Applications	Developed a WSN healthcare system that protects patient privacy	possible for Collision attack, not considering attacks on the data
14.	Mcleod et al. [21]	2018	Cyber-analytics: Modeling factors associated with healthcare data breaches	Provided a security model that included risk indicators for healthcare data breaches.	Limited practical significance
15.	Sathya et al. [22]	2017	Secured remote health monitoring system	Created a method for remote healthcare observation	Not resist brute force attack

Shanshan Zhao et al.[28] unveiled an industrial internet of things that uses blockchain technology to address concerns with interoperability, device reliability, security and privacy, and silo mentality.

Mohammad Wazid et al.[29] discussed a tutorial with the goal of creating a standardised safe authentication key management method for the IoIT environment based on blockchain technology. In order to build a security protocol for such communication settings, they have described a network and attack models for blockchain-based IoIT communication environments. They discovered that the cost of computation rises with the number of users because an increase in users results in the creation and addition of more blocks in the blockchain, and that an increase in blocks results in an increase in computation cost because an increase in blocks results in the creation and addition of more blocks in the blockchain.
Huang et al. [30] presented an eHealth system built on Blockchain that would enable consumers to audit health data and spot data manipulation. To track data change, hospitals, patients, and healthcare professionals log all types of operations on health data on the Blockchain. To further provide precise access control of medical data, they also used attributes-based proxy re-encryption.
The present healthcare system has problems with security, privacy, inconsistent data, and easy access to health records. A Blockchain-based health system that employs smart contracts to handle data storage and access management was created by Zhuang et al. [31] to address these problems. This approach delivers patient-centric HIE by personalising data segmentation and creating a "authorised list" for doctors to access their data.
The availability, integrity, and privacy of IoT data collection and processing in a traditional centralised system are at risk. "PrivySharing" was the solution put up by Makhdoom et al.[32] for smart cities to share health data. They provided guidance on how to protect the privacy of health data segments and various channels. Additionally, a system of rewards was created for disclosing user data to stakeholders and other parties.

The authors [30] suggested a secure Blockchain system for cloud-based EHR. Transaction logging ensures data integrity and access control, and patient EHRs are stored and managed on a cloud server. They employed elliptic curve cryptosystems to secure cloud health data (ECCs).
The privacy protection of EHRs is addressed by authors in [2] using a Blockchain technology-based framework named "Healthchain." The security, scalability, privacy, and integrity of healthcare data may all be maintained via this system. This "Healthchain" framework is created by the authors using Hyperledger Composer and the InterPlanetary File System (IPFS). The healthcare data is strengthened further by using a novel cryptographic public-key encryption approach to store encrypted data on the IPFS.
When EHR records are compromised, patient privacy is put in danger. Blockchain technology may be used to protect the integrity of health data and to facilitate data interchange. In [2], the authors described an EHR encryption system built on the Blockchain that makes use of intricate logic expressions to enable users to search the data using a specific set of indexes kept on the Blockchain. This procedure guarantees the integrity, anti-tampering, and

traceability of the index.
From the above discussion, following challenges have been identified:

- Data storing and data accessing time is too high, that must not be in the healthcare system.
- While increasing in the number of users, throughput is decreasing.
- In the existing model, block creation, block validation takes too much time.
- In the existing model, data processing and data query with authentication is a time consuming process.

3 Proposed Model

Based on the research problem discussed above, the proposed architecture is designed, which is shown in Fig.2
Based on the above research problem, a blockchain based framework is designed for the electronic healthcare system. The description of the proposed system is given below: The detailed proposed architecture is discussed in the subsequent subsections.

3.1 Description of proposed system architecture:

The MCPS contains a medical sensor, an IoT gateway, a decision support system, and an actuator. In MCPS, the device used can be categorized into two groups based on the service: monitoring or sensing device, that will sense the data from the patient body and also monitor the health data like heart-rate, oxygen-level of the patient body; transporting device like infusion pumps, ventilators, and pacemakers, that actuate the therapy of patient that can change the physiological state of the patient. An MCPS ensures the smart operations executed by the actuator with the help of a decision support system. The medical data collected by the MCPS is uploaded to the cloud through a permissioned blockchain. The MCPS has different entities for sensing the data, collecting the health data, storing the health data, and accomplishing the instruction as directed by the decision support system. The architecture of MCPS is shown in figure-2. The description of each entity in MCPS is discussed below:

- Patient: The medical data will be collected from the patient body with the help of medical sensors like pressure sensors and oxygen sensors.
- Medical sensor: Medical sensors or monitoring devices like BP monitoring, body temperature sensors, airflow sensor, thermistor, etc. are deployed in the patient body. It will capture the patient's health data as well as provides support to the doctors for managing the medical device.
- IoT gateway: IoT gateway is responsible for data collection from the medical sensor. It receives the sensed data, pre-process the data, and filters and

cleans the unfiltered data. It transports the sensed data into standard protocols for communication. It will share the data with the decision support system and to the cloud also.

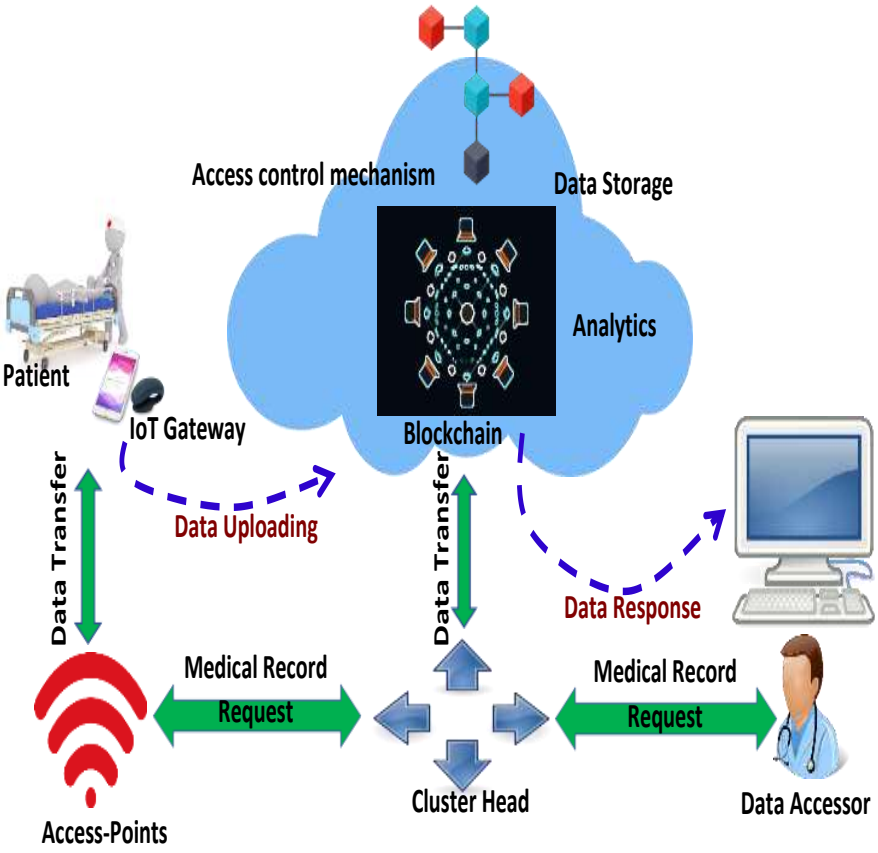

Fig. 2: Proposed Framework

- Decision support system: DSS will be responsible for analyzing the captured data. Based on the analysis, it will generate an alarm for medical emergencies and send instructions to the actuator.
- Transporting device or Actuator: The actuator is responsible for accomplishing the instruction given by the decision support system on the smart medical device. It will deliver the medical service through medical devices like dialysis machines, infusion pumps, oxygen concentrators, etc.

The architecture of permissioned blockchain in this model is discussed below:

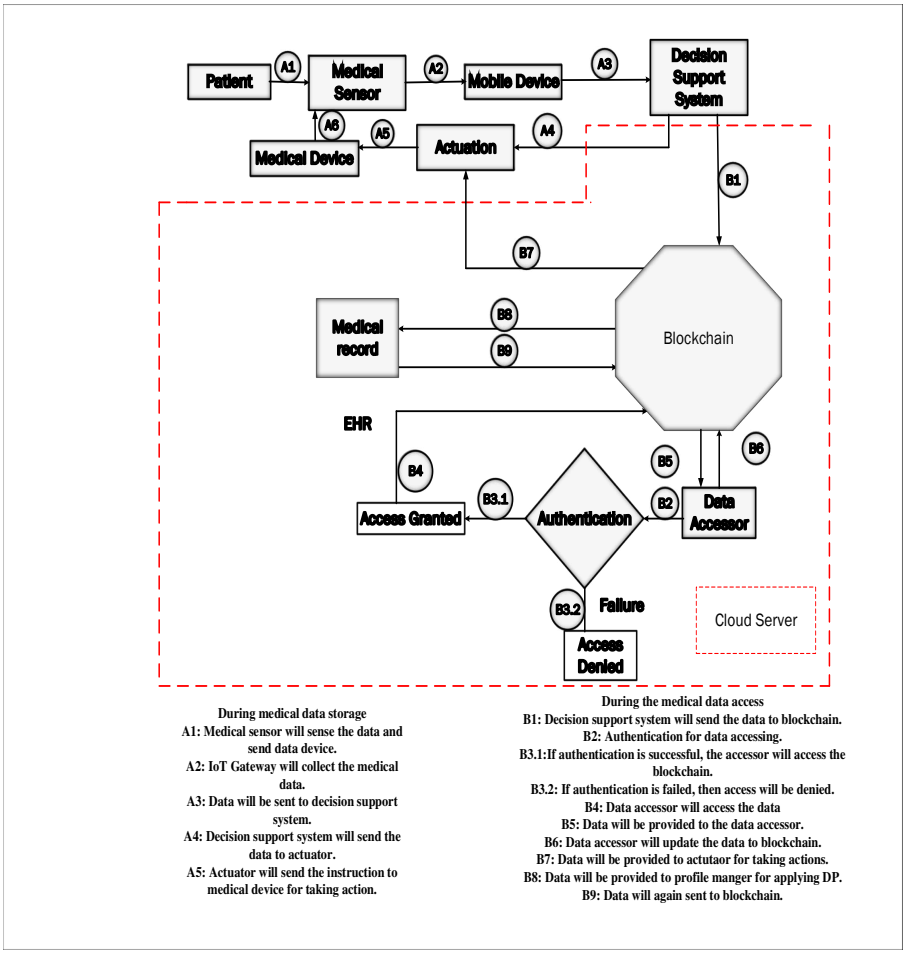

Fig. 3: Working of Proposed Framework

In this section, each entity of the permissioned blockchain is described. The selection of the permissioned blockchain over the permission-less blockchain is on the basis of the following issues of the permission-less blockchain:

1. Open Network: In an open network, anyone can join the network, which may be a security issue for the network.

2. Weak information privacy: As permission-less blockchain is transparent to every entity, each piece of information has to be shared with every entity. So there is less privacy related to the shared information.
3. Slow network: Permission-less blockchain is slow as there are more nodes to manage the transaction. However, a faster network is a vital component of healthcare.

3.2 Blockchain Module

The permissioned blockchain module ensures the tamper-proof, secure, and traceable transaction in the network. In the permissioned blockchain, data will be shared after the authentication process. In the permissioned blockchain, there are two entities: cluster head and data accessor. The functional model depends upon two operational blocks, which are known as the EHR generation and storing block; is EHR accessing block.

1. **EHR generation and storing block**
   In this operational block, EHR is generated through the collection of the patient's data and also storing those data in the blockchain. For storing the data, the selection of cluster head will be taken place. The description of the cluster head is discussed below:
   (a) **Cluster head Selection:** The cluster head is the supervisor of this permissioned blockchain. It is responsible for the execution of all the transactions. The selection of the cluster head is based on the mining of the transaction in the network. Compared with the bitcoin network, in this permissioned blockchain, the miner of the block will be the cluster head. It will manage all the transactions and maintain the ledger. There will be two types of the ledger; one is for successful transactions, and another is for unsuccessful transactions. Here, a successful transaction means the authentic transaction between the authentic entities. There is a reward for each successful transaction and a penalty for the unsuccessful transaction. For the reward system, each successful transaction adds one point to the corresponding miner and deducts one point for the unsuccessful transaction. In this way, the authenticity and utility of the permissioned blockchain remain reliable.

   The role of the cluster head is:
   - Adding or removing the entity from the blockchain.
   - Adding, verifying or removing the transaction.
   - Authentic the participated user or unauthorized user.
   - Update the database locally as well.

Algorithm 1 Algorithm for selecting cluster head

```
procedure Input:(Consensus, Patient's data(P_D),Hospital's data(H_D),
Doctor's data(D_D))
Output:A cluster head for the blockchain network
BEGIN
    while i to n do
        Mine(Block)
        patient_dataCollect(data_p)
        hospital_dataCollect(data_h)
        doctors_dataCollect(data_d)
        execute(Consensus)
        block_mined
        Data_added_to_blockchain
    end while
end procedure
```

The selection of cluster head follows the steps explained below:

- Step 1: The Patient's data(P_D),Hospital's data(H_D), Doctor's data(D_D) will be provided to the participated nodes.
- Step 2: The participated nodes will execute the consensus Mine(Consensus), that who execute the consensus first, that will be the cluster head.
- Step 3: Data will be collected by the cluster head for
  patient_dataCollect(data_p),
  hospital_dataCollect(data_h),
  doctors_dataCollect(data_d).
  After the collection of the data, all the data will be added to the block.

(b) **Block Creation and Block validation**

The steps for block creation and block validation in the proposed framework is explained below: The block creation process in the proposed framework follows the steps explained below:

- Step 1: Calculate the hash of the patient's data(P_D), hospital's data(H_D), and doctor's data(D_D) by applying SHA-256. It will return a hash of the data.
- Step 2: Calculate the block header of the block(P_B_H) by hashing the previous block hash, gas limit, gas used, timestamp and the transaction list.
  If Block_No.==1, Then prev_block==new_block,
  Otherwise,
  calculate_Header=calculateHash(blockheader(prev_hash, Gas_limit, gas_used, timestamp, tx_list))
- Step 3: Add all the hash generated for the entities data into the block(prev_hash, Gas_limit, gas_used, timestamp, tx_list), calculate the hash again.

If the calculated hash and set hash is equal then block is create otherwise calculate hash again with these data(B_N, T_P, P_D, H_D, D_D, P_B_H).

- Step 4: Then data will be added into the blockchain by cluster head.

The algorithm for the creation of blocks in the proposed framework is explained below

Algorithm 2 Algorithm for Block creation

```
procedure Input:(Block_no.(B_N), Timestamp(T_P), Previous_Block_Header(P_B_H), gas_limit, gas_used, Patient_data(P_D), hospital's_data(H_D)), Doctor's_data(D_D)
Output:Block Creation

    BEGIN
    while i to n do
        function calculateHash(B_N, T_P, P_D, H_D, D_D, P_B_H)
            hash=SHA-256(dataset)
            return hash
        end function
        function Calculateblockheader(P_B_H)
            calculateBlockheader()
            if Block_No.==1 then
                Then prev_block==new_block
            elsereturn Header=calculateHash(blockheader(prev_hash, Gas_limit, gas_used, timestamp, tx_list))
            end if
        end function
        function Block_creation(calculatedHash())
            if CalculatedHash==sethash then return block
            elsecalculateHash(B_N, T_P, P_D, H_D, D_D, P_B_H)
            end if
            Block_creation()
            Add data into Blockchain
            return Block
        end function
    end while
end procedure
```

The algorithm for the validation of blocks in the proposed framework is explained below:

Algorithm 3 Algorithm for Block Validation

procedure **Input:**((previous_hash(P_H), parent's_hash (Pa_H), Block_no.(B_N), Parent's_Block(Pa_B), gas_limit(G_L), total_gas(T_G), timestamp(T))
Output: Block validated
  BEGIN
  while true **do**
    if If (P_H==Pa_H),
      B_N==successorof(Pa_B)
      G_L==gaslimitof(Pa_B)
      T_G $\ll$ gaslimitof(Pa_B)
      T $\gg$ timestampof(Pa_B) $\ll$ 15minutes **then**
      Then block is valid
    elseValidation rejected
    end if
  end while
end procedure

The steps for the validation of blocks in the proposed framework is explained below:

- Step1: Verify the equality of previous hash value(P_H) of the block to parent's hash value,
  $(Pa\_H), (P\_H == Pa\_H)$
  Block no.(B_N) must be the successor of the parent's block(Pa_B),
  $B\_N == successor\_of(Pa\_B)$
  Gas limit(G_L) of the current block to the gas limit of parent's block.
  $G\_L == gaslimitof(Pa\_B)$
- Step 2: Verify the amount of total gas(T_G) used in the current block is less than the block's gas limit.
  T_G $\ll$ gaslimitof(Pa_B)
- Step 3: Verify the timestamp(T) of current block is more than the parent's block and not more than 15 minutes
  T $\gg$ timestampof(Pa_B) $\ll$ 15minutes.
- Step 4: Validate the block and add the block into the blockchain.

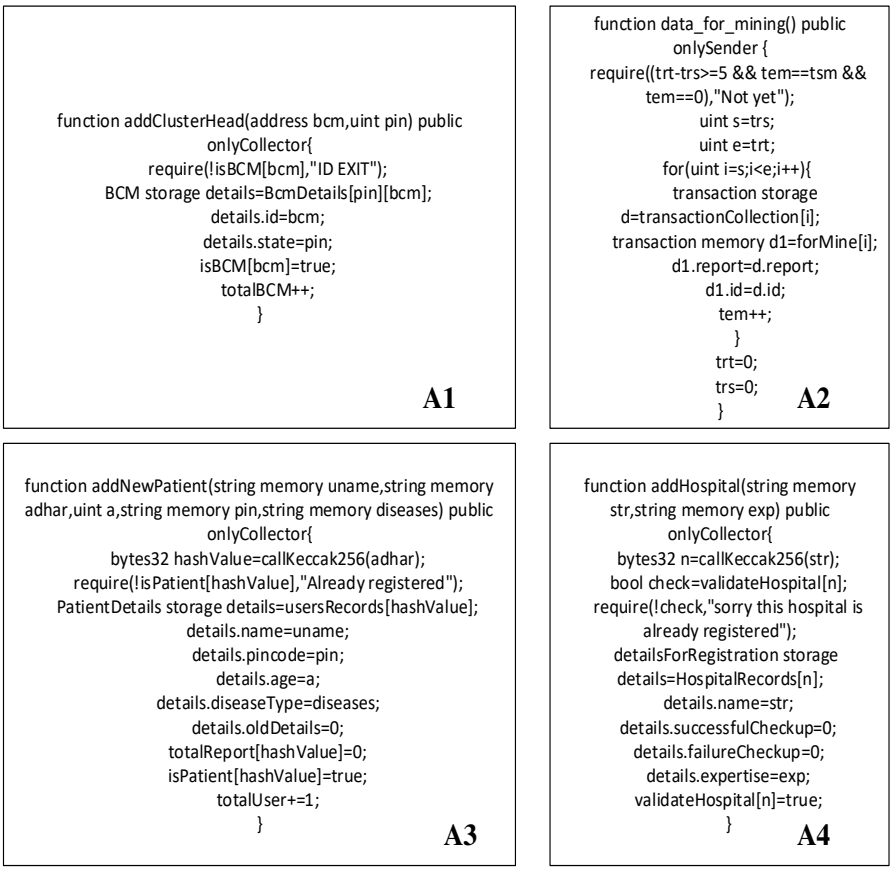

Fig. 4: Functions with the attributes in the proposed scheme

Functions associated with the proposed framework: In this proposed framework, there are some functions associated with the algorithm. The description of the some functions is discussed below:

- addCluster Head(): The block A1 of figure-4 explains the function of selecting cluster head in the proposed scheme. This function will select the Cluster Head on the basis of location. The function will ask for the parameters like their id and address pin. And then most of the participating node will select the cluster head.
- data_for_mining(): The block A2 of figure-4 explains the adding and validating the blocks in the proposed scheme.
- addNewPatient(): This function will add new patient into the blockchain network. The function will ask for the parameteres like thier name, aadhar details, pincode etc,. Then cluster head will verify those data and add them to blockchain network. It is shown in block A3 in figure-4.

- addHospitals(): The main purpose of this function is, adding of new hospitals into the blockchain. So it will be asked for the hospitals details like, hospital's name and it's pin code. Then, cluster head will verify and then add it into the blockchain network. It is shown in block A4 in figure-4.

Algorithm 4 Algorithm for Registration of Hospitals, Doctors, Patient

```
procedure Input:((Hospital_data(H_D), Patient's_data(P_D),Doctor's data(D_D)))
Output:(Registration ID(R_id) and password(R_pw) of hospitals, patient, doctors )
    BEGIN
    while true do
        function ADD(new_registration(N_R))
            Add ()
            Provide (H_D, P_D, D_D)
            Verify (H_D, P_D, D_D)
            Verify ()
            Cluster_head will verify
            if verification ==successful then
                then add ()
            elseremove
            end if
        end function
    end while
    Provide(registration_id, pw)
end procedure
```

- Step 1: Entities like hospitals(H_D), doctors(D_D), patients(P_D), request for the registration(N_R).
- Step 2: Cluster head will ask for the data to be added in the blockchain Provide (H_D, P_D, D_D).
- Step 3: Cluster head will verify the data and register them with the blockchain network.
  Verify (H_D, P_D, D_D).
- Step 4: Cluster head will provide the register id and password to entities.
  Provide(registration_id, pw)

2. **Data Accessing Block**
   In this block, EHR is generated, and there will be a data accessor of the medical data. The data accessor will send the request for the data accessing, and authorization will be done before the data sharing to the data accessor. The description of this block is discussed below in detail:

- Data Accessor: Data accessor who wants to access the data from the blockchain. Data accessors may be hospitals, patients, and doctors. Some rules are defined for the data accessed in this blockchain network. Data accessor must be a part of this blockchain network. The cluster head will authenticate the new participants in the network. Authentication will be done on the basis of the id and password provided by the cluster head. After authentication, data will be provided to the data accessor.

Algorithm 5 Algorithm for Data Accessor

```
procedure Input:(Login_id, Password)
Output:data_published
BEGIN
    while i to n do
        request_to_CH(id,pw)
        function APPROVE(verify)
            BEGIN
            function VERIFY(id,pw)
                isequals==(data_provided_by_CH)
                if Yes then
                    Then Success
                elserejected
                end if
            end function
        end function
    end while
end procedure
```

- accessdata(): The block A5 of figure-5 shows the code of for accessing data. This function will provide the data to the data accessor. Before providing data to the data accessor, first, it will verify, and only the manager will verify and allow the data accessor to retrieve the data.
- getPatientdata(): This function will provide the data to the data accessor. The function will ask for the hospital's details, patient id, age, pin code, etc. The parameter is checked, and if passed, then data is provided to the data accessor. The code is shown in block A6 of figure-5.
- updateNewpatient(): This function will update the patient details with the updated data to the blockchain network.

Algorithm 6 Algorithm for Adding a new data

procedure **Input:**((Patient's_ID(Pa_id) and password(Pa_pw), Doctor's_ID(D_id) and password(D_pw), Hospital's id(H_id)and password(H_pw)))
Output:(New data is added to block)
  BEGIN
  while true **do**
    function AUTHENTICATION(R_id,R_pw)
      Authentication()
      if (R_ID==Pa_ID ‖ R_pw==Pa_pw,
        R_ID==H_ID‖ R_pw==H_pw,
        R_ID==D_ID ‖ R_pw==D_pw) **then**
        Then authenticated
      elserejected
      end if
    end function
    add_Data()
    Update the blocks
  end while
end procedure

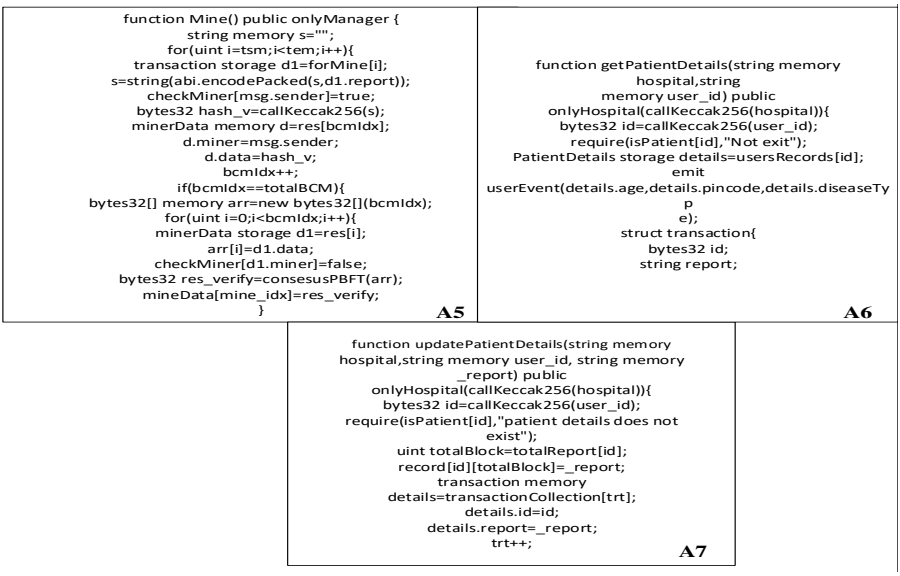

Fig. 5: Functions with the attributes in the proposed scheme

4 Experimental Results

In this section, we have analyzed the performance of the proposed BCF for the latency time, throughput, transaction time, and the number of users. Also, we have discussed the different platforms suitable for the proposed architecture.

4.1 Experimental setup and results

In this section, we have discussed the experimental setup, analysis, and results of the proposed model and also system performance for the proposed model. A secure BCF-smart healthcare prototype executable designed for Android is created. The android application makes the data collecting for healthcare available. The aggregation of health data has been done using the deployed prototype. The setup is depicted in Fig YY. The Arduino Nano V3.0 ATMEGA328 was utilized to collect the patient's health information. Through the general-purpose I/O pins, it provides an interface for sensors and actuators. The patient data will be operated on and collected. Python has been utilized with Google Cloud Platform (GCP), which is appropriate for offering a strong foundation. The Google Cloud Platform uses E2 machines for virtual machines. These machines have 128 GB of RAM and a maximum of 8 GB per vCPU. It supports 32 vCPUs in total. E2 computers have a 64-bit Linux operating system with a dual-core Intel i7-2500 CPU running at 2.8 GHz with 8GB of RAM.
We have implemented blockchain technology using Meta Mask, Remix IDE, Ethereum Virtual Machine, and Visual Studio and evaluated the effectiveness. Meta Mask is a well-known cryptocurrency wallet that is known for its ease of use, compatibility with the desktop and mobile platforms, ability to buy, send, and receive cryptocurrencies directly from the wallet, and ability to collect non-fungible tokens (NFTs) across two blockchains. Experienced cryptocurrency users will value the speed and ease of the transactions, but those who are new to the space face a greater risk of losing their tokens to scam websites, stolen secret words, and other cryptocurrency frauds. Remix IDE is a desktop and web program that is open source. It supports short development cycles and offers a wide range of plugins with straightforward user interfaces. Remix acts as a platform for the entire process of building Solidity contracts as well as an educational and training tool for Ethereum. An integrated development environment (IDE) for producing different types of software, such as mobile apps, websites, web apps, and computer programmers, is called Microsoft Visual Studio. It is equipped with tools to facilitate the software development process, such as compilers and completion tools.

We have computed the time and gas amount for the functions that are present in the proposed scheme. The results are shown in the table-2. The functions are addPatient(), addclusterHead(), addHospital(), adddoctors(), etc,. The table shows the amount of time and gas consumption for the execution of the functions. The results show that the time taken to add a patient and add a

cluster head will take 0.0001856 seconds and 0.0001864 seconds, respectively. The consensus PBFT will take approx one minute to execute in the proposed scheme. Another result shows the transaction time in the proposed scheme is low as compared with the previous scheme. The transaction time is linearly increased with the number of users and is lowest from the existing scheme. We have used the number of users from 200-2000 for measuring the throughput, and the result shows that throughput is increasing as the number of users increases.

Table 3: Time consumption and Gas cost for executing a funtion

Functions	**Time (in sec)**	**Gas Cost(Wei)**
addPatient	0.0001856	173976
addClusterHead	0.0001864	223441
addHospital	0.0002560	243652
addDcotors	0.0002368	23987
updateData	0.23456	753654
getData	0.00254	135678
consensusPBFT	30 sec to 1 min	1026568

5 Performance Analysis

After the experimental setup, the performance of the proposed scheme BCF is discussed in this section. The analysis is mainly in comparison with the existing Blockchain scheme with
1.) Average execution time
2.) Average transaction time
3.) Throughput
4.) Average latency

5.1 Comparison with the existing blockchain scheme

In the proposed scheme, PBFT is used as a consensus algorithm in our proposed architecture. The result is analyzed for with the proposed blockchain framework in terms of latency in adding a record, fetching a record, and how large amount of gas is consumed in executing a function. Table 1 shows the detailed analysis of the record. In the proposed framework, the throughput and latency are simulated by using METER. The smart contract of the suggested framework's framework includes a number of functions that are explained by algorithms. With the aid of Meter, we were able to simulate a range of users—from 200 to 2000—using the system and to carry out its various activities. The throughput in Meter is expressed as Data/Time, i.e., units of KB/sec. We have simulated the above-mentioned number of users during the experiments in order to assess the system's effectiveness. The proposed

framework is used to conduct these simulations, and throughput is examined at the conclusion. The reason for selecting PBFT as the consensus algorithm is the low latency in executing the transactions in the blockchain network. Also, PBFT provides more throughput in the context of a user. The figure-6 shows a detailed comparison between different types of consensus protocols.

- Average execution time: Execution time will grow as the number of transactions rises. The smart contract's features are used to carry out the transaction. When there is only one user, all the functions will execute more quickly; for example, adding a user, selecting a cluster head, and adding records would take 2.3, 5.67, and 2.1 seconds, respectively.
- Average transaction time: With the increase of the users in the network, the transaction time is increasing linearly in PBFT as compared with the other consensus algorithm. With comparing to the other consensus, algorithm POW takes a lot of time to execute one transaction. While comparing with PoB, a very small difference is analyzed in the latency for low number of users. A large difference in transaction time is analyzed with the increasing number of users. The main reason for the selection of PBFT is the high transaction rate with a large number of users.

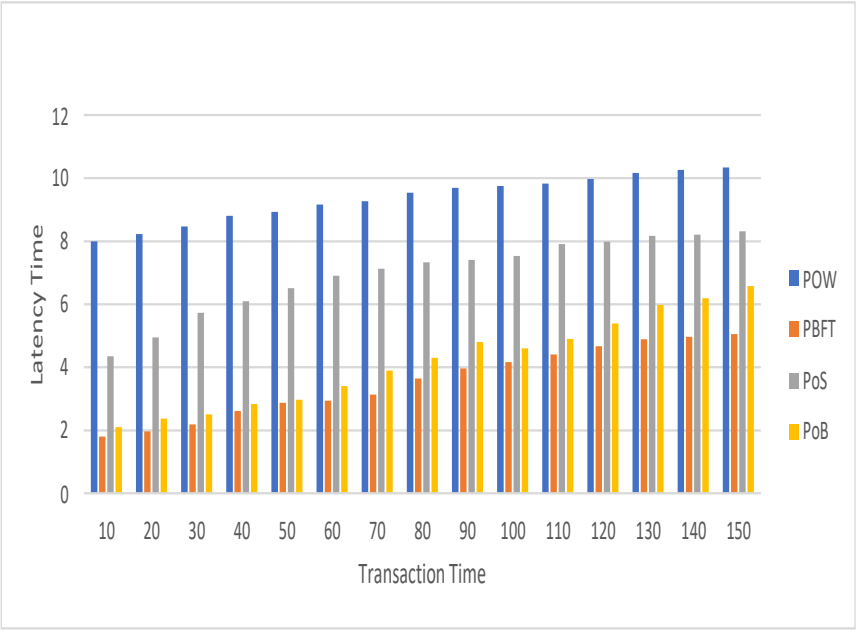

Fig. 6: Comparison of consensus algorithm

- Throughput: For calculating the throughput, JMeter is used, simulating a user base of 200 to 2000 users operating the system and carrying out operations. The throughput is expressed in units of data/time or KB/sec. The evaluation of the system's performance included a simulation of the users' numbers, as stated above. Throughput is assessed once the simulations are done on the suggested framework. The detailed analysis of the throughput is displayed in figure-7. It is observed that throughput is increasing linearly as the number of users increases. In other existing scheme[7], throughput decreases when the number of users increases.

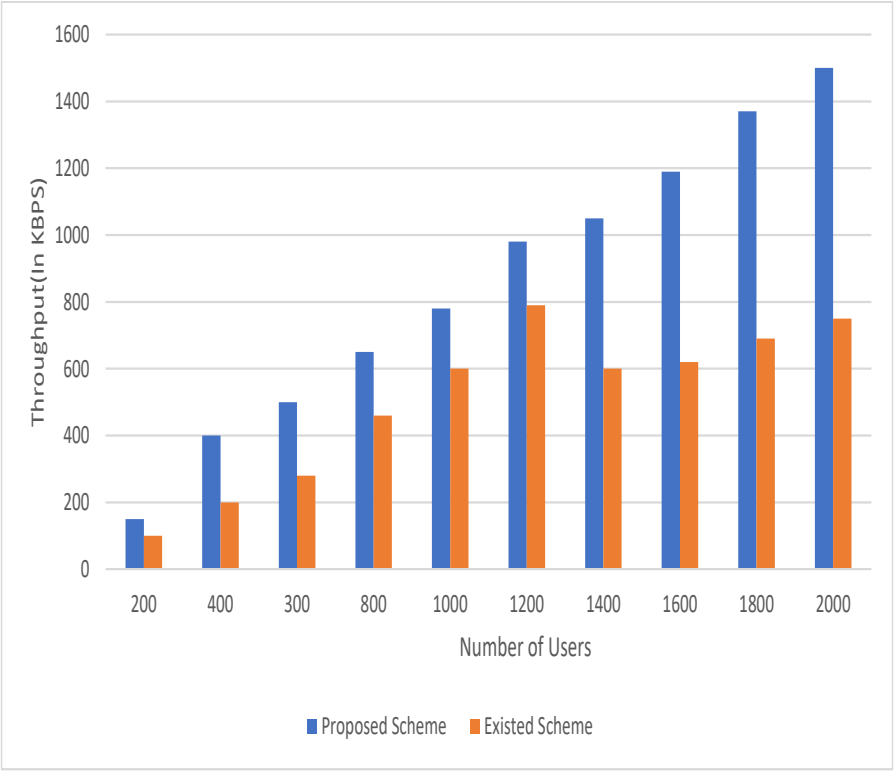

Fig. 7: Throughput of the proposed scheme

- Average Latency: Latency is defined as the time difference between the two actions. The time difference between the request of one component of the system and the response of that request. We have used the JMeter to calculate the latency between two actions. The latency is measured in milliseconds. The latency is analyzed between the throughput and the time in which it the task is completed. For this result, 2000 records have been taken into consideration and compared with the existing scheme. For 200-1400 records, the

graph comes out is nearly the same, but as the number of users is increasing, latency decreases in the proposed scheme as compared with the existing scheme[8].

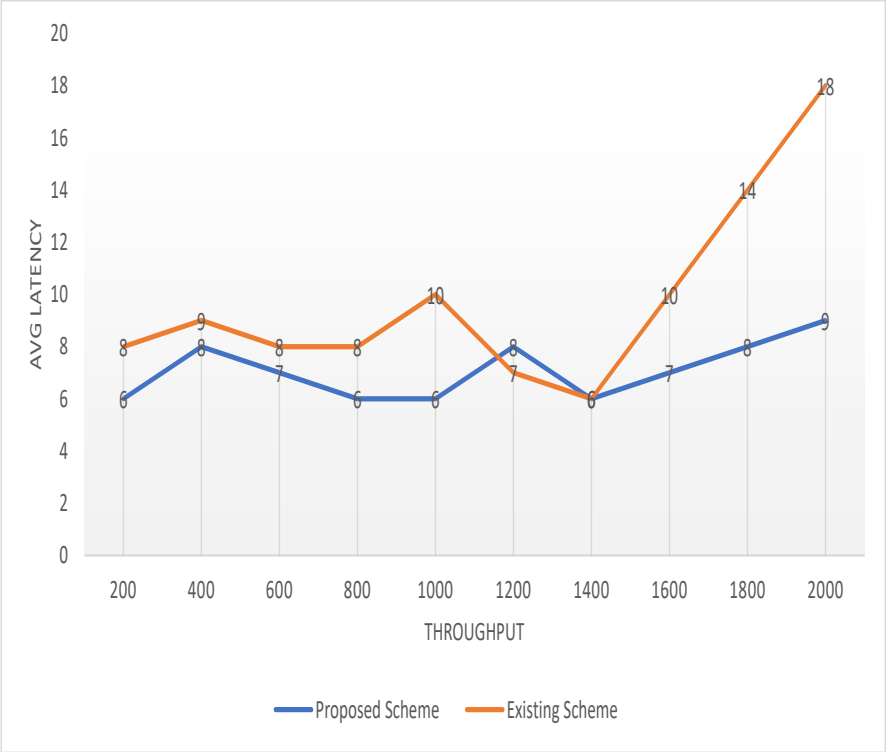

Fig. 8: Latency Graph

6 Conclusion

In the healthcare system, privacy and security is the main concerning issue. There are several solutions of security discussed, but most of the solutions are not feasible for the healthcare system in relation to automation, transparency, latency, throughput, security, data tampering, and distributed. The first objective of the proposed model is to enhance security and reduce service time for the healthcare system. Also, throughput is increased in the proposed model as compared to the existing model. This is possible because of the lightweight architecture of the proposed model, where only the main server is not responsible for all the necessary actions. Also a cluster head will manage all the actions. The experimental results and analysis have shown the identified

research problem is solved. While maintaining privacy, latency and transaction time is reduced, and throughput is increased. Along with that, this model also controls unauthorized access.

Declarations

- Ethical approval: Not applicable
- Competing interests: The authors declare that they have no known competing financial interests or personal relationship that could have appeared to influence the work reported in this paper.
- Authors' contributions: The authors confirm contribution to the paper as follows: **Ashish Kumar** : Data curation, Formal analysis, Writing-original draft, Writing-review & editing, Validation. **Kakali Chatterjee**: Conceptualization, Writing-original draft, Writing-review & editing, Validation
- Funding: Not applicable
- Availability of data and materials: Not applicable

References

[1] Lee, Insup, Oleg Sokolsky, Sanjian Chen, John Hatcliff, Eunkyoung Jee, BaekGyu Kim, Andrew King et al. "Challenges and research directions in medical cyber–physical systems." Proceedings of the IEEE 100, no. 1 (2011): 75-90.

[2] Xu, Jie, Kaiping Xue, Shaohua Li, Hangyu Tian, Jianan Hong, Peilin Hong, and Nenghai Yu. "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data." IEEE Internet of Things Journal 6, no. 5 (2019): 8770-8781.

[3] Lu, Yunlong, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT." IEEE Transactions on Industrial Informatics 16, no. 6 (2019): 4177-4186.

[4] Kshetri, Nir. "Blockchain's roles in strengthening cybersecurity and protecting privacy." Telecommunications policy 41, no. 10 (2017): 1027-1038.

[5] Singh, Ashish, Kakali Chatterjee, and Suresh Chandra Satapathy. "TrIDS: an intelligent behavioural trust based IDS for smart healthcare system." Cluster Computing (2022): 1-23.

[6] Lu, Yunlong, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT." IEEE Transactions on Industrial Informatics 16, no. 6 (2019): 4177-4186.

[7] Ismail, Leila, Huned Materwala, and Sherali Zeadally. "Lightweight blockchain for healthcare." IEEE Access 7 (2019): 149935-149951.

[8] Shahnaz, Ayesha, Usman Qamar, and Ayesha Khalid. "Using blockchain for electronic health records." IEEE Access 7 (2019): 147782-147795.

[9] Hathaliya, Jigna J., and Sudeep Tanwar. "An exhaustive survey on security and privacy issues in Healthcare 4.0." Computer Communications 153 (2020): 311-335.

[10] Singh, Ashish, and Kakali Chatterjee. "Securing smart healthcare system with edge computing." Computers and Security 108 (2021): 102353.

[11] Kumar, Adarsh, Rajalakshmi Krishnamurthi, Anand Nayyar, Kriti Sharma, Vinay Grover, and Eklas Hossain. "A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes." IEEE Access 8 (2020): 118433-118471.

[12] Ning, Xirong, and Jin Jiang. "Design, analysis and implementation of a security assessment/enhancement platform for cyber-physical systems." IEEE Transactions on Industrial Informatics 18, no. 2 (2021): 1154-1164.

[13] Banerjee, Mandrita, Junghee Lee, and Kim-Kwang Raymond Choo. "A blockchain future for internet of things security: a position paper." Digital Communications and Networks 4, no. 3 (2018): 149-160.

[14] Gordon, William J., and Christian Catalini. "Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability." Computational and structural biotechnology journal 16 (2018): 224-230.

[15] Theodouli, Anastasia, Stelios Arakliotis, Konstantinos Moschou, Konstantinos Votis, and Dimitrios Tzovaras. "On the design of a blockchain-based system to facilitate healthcare data sharing." In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 1374-1379. IEEE, 2018.

[16] RSPP: Yang, Lei, Qingji Zheng, and Xinxin Fan. "RSPP: A reliable, searchable and privacy-preserving e-healthcare system for cloud-assisted body area networks." In IEEE INFOCOM 2017-IEEE conference on computer communications, pp. 1-9. IEEE, 2017.

[17] He, Daojing, Ran Ye, Sammy Chan, Mohsen Guizani, and Yanping Xu. "Privacy in the internet of things for smart healthcare." IEEE Communications Magazine 56, no. 4 (2018): 38-44.

[18] Sarwar, Abid, and Vinod Sharma. "Intelligent Naïve Bayes approach to diagnose diabetes Type-2." International Journal of Computer Applications and Challenges in Networking, Intelligence and Computing Technologies 3 (2012): 14-16.

[19] Ma, Mimi, Debiao He, Muhammad Khurram Khan, and Jianhua Chen. "Certificateless searchable public key encryption scheme for mobile healthcare system." Computers abd Electrical Engineering 65 (2018): 413-424.

[20] Mohan, Maya, M. K. Kavithadevi, and V. Jeevan Prakash. "Improved classical cipher for healthcare applications." Procedia Computer Science 93 (2016): 742-750.

[21] McLeod, Alexander, and Diane Dolezel. "Cyber-analytics: Modeling factors associated with healthcare data breaches." Decision Support Systems 108 (2018): 57-68.

[22] Sathya, Duraisamy, and Pugalendhi Ganesh Kumar. "Secured remote health monitoring system." Healthcare Technology Letters 4, no. 6 (2017): 228-232.

[23] Ning, Xirong, and Jin Jiang. "Design, analysis and implementation of a security assessment/enhancement platform for cyber-physical systems." IEEE Transactions on Industrial Informatics 18, no. 2 (2021): 1154-1164.

[24] Jiang, Bin, Jianqiang Li, Guanghui Yue, and Houbing Song. "Differential privacy for industrial internet of things: Opportunities, applications, and challenges." IEEE Internet of Things Journal 8, no. 13 (2021): 10430-10451.

[25] Lu, Yunlong, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT." IEEE Transactions on Industrial Informatics 16, no. 6 (2019): 4177-4186.

[26] Yang, Qing, Hao Wang, Xiaoxiao Wu, Taotao Wang, Shengli Zhang, and Naijin Liu. "Secure Blockchain Platform for Industrial IoT with Trusted Computing Hardware." IEEE Internet of Things Magazine 4, no. 4 (2021): 86-92.

[27] Yaacoub, Jean-Paul A., Ola Salman, Hassan N. Noura, Nesrine Kaaniche, Ali Chehab, and Mohamad Malli. "Cyber-physical systems security: Limitations, issues and future trends." Microprocessors and microsystems 77 (2020): 103201.

[28] Zhao, Shanshan, Shancang Li, and Yufeng Yao. "Blockchain enabled industrial Internet of Things technology." IEEE Transactions on Computational Social Systems 6, no. 6 (2019): 1442-1453.

[29] Wazid, Mohammad, Basudeb Bera, Ankush Mitra, Ashok Kumar Das, and Rashid Ali. "Private blockchain-envisioned security framework for AI-enabled IoT-based drone-aided healthcare services." In Proceedings of the 2nd ACM MobiCom workshop on drone assisted wireless communications for 5G and beyond, pp. 37-42. 2020.

[30] Huang, Haiping, Xiang Sun, Fu Xiao, Peng Zhu, and Wenming Wang. "Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments." Journal of Parallel and Distributed Computing 148 (2021): 46-57.

[31] Zhuang, Yu, Lincoln Sheets, Zonyin Shae, Jeffrey JP Tsai, and Chi-Ren Shyu. "Applying blockchain technology for health information exchange and persistent monitoring for clinical trials." In AMIA Annual Symposium Proceedings, vol. 2018, p. 1167. American Medical Informatics Association, 2018.

[32] Makhdoom, Imran, Ian Zhou, Mehran Abolhasan, Justin Lipman, and Wei Ni. "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities." Computers and Security 88 (2020): 101653.

[33] Benil, T., and J. J. C. N. Jasper. "Cloud based security on outsourcing using blockchain in E-health systems." Computer Networks 178 (2020): 107344.

[34] Yang, Qing, Hao Wang, Xiaoxiao Wu, Taotao Wang, Shengli Zhang, and Naijin Liu. "Secure Blockchain Platform for Industrial IoT with Trusted Computing Hardware." IEEE Internet of Things Magazine 4, no. 4 (2021): 86-92.

[35] Shrestha, N. M., Abeer Alsadoon, P. W. C. Prasad, L. Hourany, and A. Elchouemi. "Enhanced e-health framework for security and privacy in healthcare system." In 2016 Sixth international conference on digital information processing and communications (ICDIPC), pp. 75-79. IEEE, 2016.