Alexandria Engineering Journal (2023) 73, 159–172

Alexandria University

Alexandria Engineering Journal

www.elsevier.com/locate/aej
www.sciencedirect.com

ORIGINAL ARTICLE

An efficient privacy-preserving control mechanism based on blockchain for E-health applications

Hanan Naser Alsuqaih [a], **Walaa Hamdan** [a], **Haythem Elmessiry** [b,c], **Hussein Abulkasim** [b,d,*]

[a] *Department of Libraries and Information, College of Arts, Princess Nourah bint Abdulrahman University, P. O. Box 84428, Riyadh 11671, Saudi Arabia*
[b] *College of Engineering and Technology, University of Science and Technology of Fujairah, Fujairah, United Arab Emirates*
[c] *Faculty of Computer and Information Sciences, Ain Shams University, Cairo, Egypt*
[d] *Faculty of Science, New Valley University, El-Kharga 72511, Egypt*

Received 15 December 2022; revised 4 April 2023; accepted 18 April 2023
Available online 4 May 2023

Abstract The development of the Internet of Things (IoT) has opened up new horizons in the field of remote health data analysis to obtain smart healthcare. However, protecting patients' data privacy seems challenging because medical files are so sensitive. There are significant risks to data confidentiality associated with storing patient health information on third-party servers. The covid-19 epidemic also enhanced the need for a temperature sensor-based respiratory monitoring device. Sharing electronic health records can aid with diagnostic accuracy when privacy and security protection are important system challenges. Due to the benefits of immutability, blockchain has been suggested as a possible option to enable personal health data exchange with privacy and security protection. This work suggests a safe and privacy-preserving diagnostic enhancement strategy for e-Health platforms based on blockchain technology, which addresses the inadequacy of previous work in these regards. The proposed work proposes an effective access control system that would let data owners specify their preferred access controls over their privacy-sensitive medical data. Users could utilize their user transactions for key generation to efficiently cancel or add authorized doctors. Experimental data and security analyses demonstrate the proposed Health-chain's suitability for use in smart healthcare systems. The thorough experimental investigation demonstrates the blockchain's effectiveness of computing and time consumption as well as its resistance to numerous security assaults.

* Corresponding author at: Faculty of Engineering and Technology, University of Science and Technology of Fujairah, United Arab Emirates.
E-mail address: hussein@scinv.au.edu.eg (H. Abulkasim).

Peer review under responsibility of Faculty of Engineering, Alexandria University.

https://doi.org/10.1016/j.aej.2023.04.037

1. Introduction

Through significant advancements in e-health records, account information and prescription drug data, the IoT paradigm has transformed the healthcare industry [1]. The IoT-based medical equipment could assist in the collection of priceless patient data, automate workflows, offer insights into the indications and patterns of diseases, make remote care easier, and give patients greater control over their lives and medicines [2]. Patients could be examined in real-time with IoT devices. Additionally, they might lessen the necessity of visiting hospitals for regular health examinations. Hospital stays or readmission expenses may be decreased with the aid of connected home health surveillance devices. Through warnings and trigger messages, IoT-enabled medical devices may assist with diagnosis before it gets serious. Sensors attached to various components of a patient's clinical tool could gather information and then transmit it to the clinic, where a medicinal professional could review it for any potential anomalies. Without a doubt, IoT advancements have sparked ongoing advances in the healthcare industry [3]. However, since this data is dispersed throughout numerous medical facilities, securely processing the electronic healthcare record (HER) has become exceedingly difficult. Most currently in use healthcare systems are generally centralized, making them susceptible to single points of failure and data loss. The disclosure of sensitive information about patients may result in con schemes. Additionally, in managing EHR, the present medical technologies fall short in providing transparency, dependable provenance, data integrity, audit, confidentiality, and security. Blockchain technology has the capacity to address these issues in the present healthcare systems. By 2025, it is predicted that blockchain technology's approval could save between $100 and $150 billion annually in expenditures associated with data breaches, frauds, and pirated items [4].

The WHO has reported a global epidemic caused by COVID-19, which was brought on by the severe, serious breathing illness. A temperature sensor-based respiratory tracking system became more necessary as a result [5,34]. Particularly following the COVID-19 epidemic shutdown, it may be expected that between 40 and 50 percent of individuals globally suffer from some sort of hypertension. Moreover, during this shutdown time, the development of new technologies, IoT, and E-health can assist the functioning of the health service without causing the virus to propagate via direct interaction with infected sufferers [6]. Due to various factors, people are more prone to get dangerous diseases. Therefore, it is important to check people's blood pressure levels as well [6]. Information about healthcare is essential to everyone. It keeps a concrete record of our bodies. It is crucial for the identification and management of illnesses [7]. As machine learning has fast developed, patient records have turned into a valuable asset. It has the potential to develop medical methods for artificial intelligence as well as to assist in diagnosis. Compared to paper documents, EHR were easier to access and maintain, but greater care still should be taken to guarantee that the data's confidentiality is preserved [8]. Many clinics and organizations have restricted data transmission and interchange in order to avoid information privacy breaches. As a result of medical information being spread throughout multiple medical facilities, data obstacles have emerged. Security and privacy issues with healthcare data also cause other issues. For security reasons, patients must, for instance, undergo a new examination each time they visit a different hospital. Energy and resources are wasted by this action. Medical data is not shared with research institutes due to patient privacy concerns, which hinders medical advancement. It has prompted the quest for safe data storage as well as transmission techniques, and blockchain is extensively utilized for sharing medical data since it is decentralized and tamper-proof [9]. To allow continuous scanning of international life science data, Innoplexus integrates blockchain with artificial intelligence. A system makes information available to research organizations and medicinal firms. A platform called BlockRx has been productively employed in actual applications. The system includes powerful digital ledger technologies from iSolve with blockchain. The platform incorporates health information from the research and biomedical organizations. BlockRx has made significant progress since it was first implemented in practice [10].

By delivering exceptional data efficiency and upholding trust, blockchain is a capable network, which has the possibility to improve healthcare processes and systems [11]. It provides a variety of noteworthy and integrated features, such as decentralized storing, accessibility, integrity of data, and authentication, flexibility in data access, connectivity, and safety, allowing broader use of blockchain- based for handling healthcare data. Blockchain makes use of the concept of "smart contracts," that define terms and regulations that are acknowledged by every medical system players and do away with the necessity for an intermediary[12]. It lowers wasteful administrative expenses. Peer-to-peer networking, public key encryption, and concurrency control, to name a few, are the three primary elements that underpin blockchain. The three components of public, private, and consortium blockchains are based on managing authorization. On blockchain networks, agreements could be reached by anybody with an Internet access. Public blockchains combine finance with encoded digit identification using proof-of-work or proof-of-stake methods. The identity of every participant is kept largely anonymous yet the entire public blockchain network is transparent. In a private blockchain, the network is under the control of just one company. As a result, for this particular blockchain architecture to reach agreement, a reliable agent is needed. The advantages of both private and public different blockchains are mutual in the consortium blockchain (see Fig. 1). Just specific organizations who want to improve communication with one another should use it. Healthcare firms can adopt any form of blockchain network, as each one has advantages and disadvantages that can be tailored to specific demands or use case situations[13].

In smart healthcare where users' source documents are necessary for medical treatments, the conventional privacy-preserving strategies focused upon brief or producing distortion data are ineffective. Novel privacy-preserving strategies grounded on Blockchain (BC) technologies have recently been presented by study to overcome this problem [14–16]. A peer-to-peer network uses blockchain, a permanent timestamp record of blocks, to store and distribute data in a distributed way. There is no requirement for centralized power because blocks in BC are distributed by every network participant. The aspect of data protection and user confidentiality is one of the main challenges, nevertheless, in additional to the storage pressure brought on by the large amount of data. On the

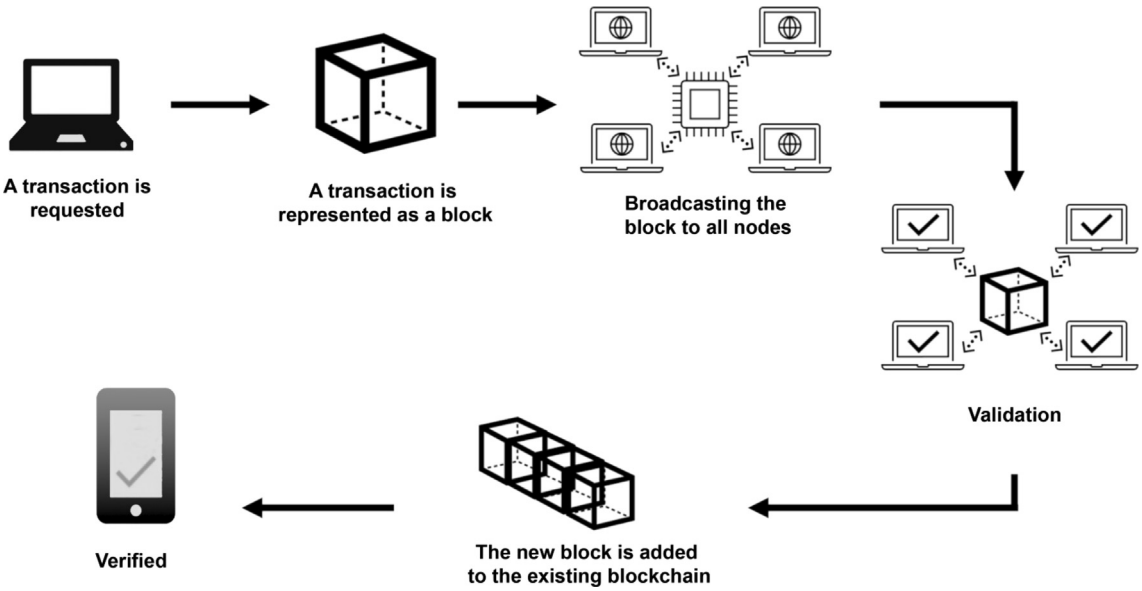

Fig. 1 A block diagram showing the structure of Blockchain.

one side, users' anonymity can be easily violated due to the open and visible structure of the blockchain. On the other hand, users' health data must be accessible to approved expert healthcare professionals, such as doctors or AI health analysts. Users' health information should be secured as a result, and the encrypted data must be subject to fine-grained network access. Only licensed healthcare professionals have access to a specific user's health information. Health-chain gives customers the ability to upgrade encryption keys, cancel, and add achieving high quality health professionals at any time for improving the adequate security of health data[17].

In this article, a BC-based access control architecture is proposed that protects patients' privacy. Instead of storing the original data, the patient's medical information is acquired. As the study clusters the miners to avoid redundant information and prevent their participation in the consensus operation, the study adapts the basic Blockchain framework to increase its effectiveness in the medical area. Additionally, the length of transmission is limited to be small for transmission over BC in order to avoid network overhead. Owners of sensitive data may specify access policies for those pieces of information with BCHealth. In contrary to the rest of BC-related activity, which publishes information on other servers and then implements access control mechanisms, the Blockchain health architecture forbids the distribution of patients on the BC network without the user's agreement. As with the idea of the edge of the network, blockchain health stores the data remotely on a device that is nearest to the patient rather than using the internet or a health information center. The resulting reduction in communication costs and delays would be significant.

The remainder of the paper is structured as follows. The required blockchain knowledge is covered in Section 2, along with an examination of similar work. The suggested architecture is presented in Section 3, while blockchain health privacy and security are assessed in Section 4. The findings of the study results are presented in Section 5, and the study is concluded and further research possibilities are suggested in Section 6.

2. Related work

To design a solution that effectively protects data stored in the Cloud without imposing a significant burden on processing and transmission. For better preserving the privacy of clinical data in hybrid servers, this work propose a contrasted clustering and geometric data disturbance strategy in this work. The K-mean clustering approach is utilized to first divide the high-dimensional data into distinct portions, with every split being treated as a cluster. The mean estimation for every cluster is then processed, and a comparison among the mean cluster and cluster member values is then calculated. In the subsequent stage, the grouped information is perturbed using the Geometric Data Perturbation (GDP) methodology, making it challenging to obtain the parameters. In contrast to these disturbed values, which are retained in the cloud platform, the crucial variables for randomizing and grouping are preserved in the private cloud. If they essentially store every sensitive data on private clouds, the technique would help reduce the amount of storing upon private clouds. The empirical findings demonstrate that the GDP procedure protects privacy more effectively than other approaches currently in use. The GDP methodology still needs to be improved for the study to achieve a higher level of privacy preservation. The goals of this work are to investigate privacy-aware, beneficial cloud scheduling of anonymized data sources by using privacy preservation as a measurement together with various metrics, such as stockpiling and calculating later. Data clustering using this approach is challenging when clusters fluctuate in size and density [18].

Smart healthcare attempts to create a framework to constantly monitor patient's health-related data depend on smart technology as the industrial Internet of Things (IIoT) develops. The advancement of secure intelligent healthcare is also supported by the development of blockchain as well as artificial intelligence technology. The data also are susceptible to attack as well as privacy leaks because they are kept on a cloud

server. Be aware that the security problem of private information intermingled with original information gathered from a sizable number of dispersed and heterogeneous smart wearable equipment has received little attention. The research suggests deep learning-based predictive analytics as well as privacy protection solution for IoT enabled healthcare to address such issue. Study get raw data from the users as well as segregate their personal information in a privacy-isolation zone. Study analyses health-related data in the cloud while knowing the personal details of the users and build a sensitive security module utilizing convolutional neural networks. Extensive studies show the prototype performance of this system and durability where also deploy as well as assess it. The proposed technique does not fully guarantee semantic privacy, such as differential privacy, but it does offer different privacy protection via user-defined confidentiality levels. Enhancing the recommended solution's semantic privacy assurance as well as mathematical validation is thus one possible future research direction. Furthermore, the proposed approach just sanitizes the delicate language. The detection and sanitizing of terms with semantic relationships is another possible research field. Due to its insufficient security, this approach is ineffective [19].

To permit algorithms to train on confidential material without sharing it, new advancements in privacy-preserving computer vision are required for Ai technologies for important healthcare images. PriMIA, a free, open-source software framework for privacy - preserving, securely aggregated learning algorithm and encrypted predictions on medical image data, is introduced. PriMIA was put through its paces by study who used an actual case scenario where a deep convolutional neural system trained by specialists was used to categories paediatric chest X-rays. The method's classification results in comparison to that of a locally trained insecurity classification model. Study empirically and theoretically evaluate the effectiveness as well as privacy assurances of the architecture, and they show that the safeguards put in place stop a gradient-based modeling inversion approach from reconstructing useful data. Considering the suggested protocol changes, the computing necessities for implementing the system are significant, as well as the delay resultant from encryption inferences remains extremely high in comparison to unencrypted reasoning. The fundamental remote execution framework presently provides limited GPU functionality; full support is anticipated for a later release. High quality of the data on the networks is a key factor in FL models' performance. The accuracy of the data is measured on how much each dataset contributes to the algorithm or to identify local overfitting, remain to be researched. In an honest-but-curious system, which they see as the norm in healthcare organizations, the library is intended to be utilized. As a result, despite the fact that study offer comprehensive data protection security protocols, they did not include any particular defensive measures against malware accomplishments of lower quality or adversarial information to the FL procedure or to ensure that the framework employed in the implication configuration is the one that had offered to the data controller. In addition, study emphasize that considerations of the con problem statement ceptual adversary model are an abstraction layer that does not adequately capture the complexities of actual events. For this strategy to work, a substantial of training data is required [20].

A significant category of medical data that includes rich spatially and temporally information is time-series medical imaging. These image sequences are typically subjected to state-of-the-art computer-aided diagnostic (CAD) methods to increase analytical precision. However, these CAD methods were frequently forced to upload medical photos to servers that are honest yet curios, which raises serious privacy issues. The available CAD algorithms do not permit evaluation of entire encryption consecutive frames in order to maintain privacy the results in the loss of crucial temporal information between frames. HE-CLSTM is presented for evaluating time-series clinical data that have been encrypted using a completely homomorphic encryption algorithm in order to address this difficulty. To be more precise, LSTM-based analysis software layers (HE-LSTM) are used to encode time-based dependencies from the encrypted image sequences while a number of convolutional blocks are built to retrieve discriminatory spatial information. Additionally, to enhance performance as well as lower the rate of missed diagnoses, weighting units as well as a sequential voting level are created to combine both temporal and spatial variables with distinct values. Compelling evidence that the framework could encode visual representations, as well as sequential interactions from encrypted clinical image sequences, is provided by the findings on two demanding benchmarks. The system obtained AUCs above 0.94 both on the Cervigram and BreaKHis sets of data, comprising a substantial margin of a quantitative impact compared over several existing techniques. The proposed approach still takes too long to analyses the encrypted images because it uses the BFV cryptosystem. Study determined to make the method's computations simpler in upcoming work. Another prospective difficulty stems from its adaptability to different kinds of medical picture data. It also requires more research to confirm how well HE-CLSTM performs on other databases. Web - based learning applications like classification and prediction when the input data is not a series aren't well suitable for this method [21].

The EHR technology that gathers a vast quantity of information every day has expanded the possibilities of data analysis on healthcare information to provide better healthcare care. In the current situation, the hospital keeps up its EHR system and preserves the specific patient data. Data from every EHR system, regardless of where it is situated, must be saved at the centralized data processing server in order for data mining to improve healthcare. Privacy risks arise from the accumulation of health information on an unreliable central data mining system. Patients' private data contained in healthcare data are shared for data analysis, which raises privacy concerns. The majority of prior studies either concentrated on the information-losing k-anonymity approach, which lowers data mining effectiveness, or on privacy-preserving data mining, which concentrates on a single data mining method. In this research, they describe a unique approach for healthcare data gathering and mining using source anonymization as a privacy-preserving method. The strategy collects data from all EHR systems without affecting its validity, stores it on a solitary, centralized information mining system, as well as ensures that privacy is protected. A central data mining system aids in the based on the obtained data utilizing various tools and techniques without the need for EHR systems. The plan is resistant to collaboration against EHR systems, including centralized data mining servers. The effectiveness of our plan in terms of calculation and communication costs is demonstrated by theoretical and experimental analysis. The experi-

mental findings utilizing a dataset for heart disease demonstrate the benefit of using the suggested approach in EHR systems in terms of disease predictive performance. The study must be altered nevertheless, to incorporate the constant joining and quitting of EHR systems. The dynamical joining and departing of EHR systems is not explained by this strategy [22].

The IoT has finished incredible strides in the distribution of medical data also activating the related appropriate measures within the modern world, with developing web frameworks automation and computerizing numerous industrial and household applications. Present-day difficulties include sharing healthcare-related information across destination node, protecting privacy, as well as maintaining data integrity. Particularly in the case of healthcare-related collected data, information should be encrypted to guarantee the privacy of the confidential material transferred among the networks. It might not be practically possible to implement traditional cryptographic techniques via the access point, and it is not recommended to place an excessive amount of load on them. The purpose of the study has concentrated upon numerous safety threats with the current system, existing security solutions for IoT-driven health checking architectures, and a state-of-the-art framework that is context-aware and predicated on Blockchain technology that was used to encode data between nodes in the infrastructure of a 5G network. The recommended approach succeeded in comparison to existing one when the proposed approach has been evaluated using a variety of performance evaluation indicators. Since the data uploaded to the network cannot yet be changed, an effective model must be developed to track the changes made to the blockchain network. The quantum blockchain system can accurately handle the storage capabilities across all of the administration nodes in the network and adequately allocate the load of ledger maintenance with decentralized activities. The storage proficiency of this research has to be increased [23].

Wireless sensor systems' suggested energy-efficient multisensor data sample and fusing with judgement for individual health risk assessment. Three processes make up the process multisensor data fusing, energy-efficient sampling rate modification, and judgement. Every biosensor performs samples, and it adjusts its rate according to the local hazard and the global hazard. The coordinating computes the global hazard, and the information is then combined. Lastly, judgements are made based on the patient's risk level. Whenever an emergency is identified, a choice is taken in accordance with the analysis of these tasks, which permits in real-time the implementation of the biosensor sampling rates depending on the dynamically riskiness of every biosensor. Utilizing real health datasets, the effectiveness of the proposed method is assessed, and several of its characteristics—such as the rates at which information is reduced and energy is consumed—are compared to those of an existing system. The obtained findings show a reduction in the amount of data collected, resulting in a large saving energy while maintaining the quality and integrity of the information. Additionally, by employing an advance warning rating system to offer a data fusion modeling at the coordinating levels, it was possible to evaluate the patients' state of health and make the right choice whenever spotting crises. Due to its lack of specificity and robustness, this approach is ineffective [24].

For minimising the sent EEG traffic from Patient Data Aggregator (PDA) to the destinations, a feasible EEG Fractals compressing model is suggested. The suggested paradigm facilitates the exchange of EEG patient information and enhances Wireless Body Sensor Network by lowering network activity. The chosen Fractals Block Size is discovered to be the crucial factor in providing greater Compression Ratio (CR) and driving the necessary Percentage Residue Differential (PRD) when the primary modeling parameters are examined. The suggested model has entirely surpassed existing strategies in terms of outcomes and effectiveness. The resulting CR might be as high as 160 while maintaining a PRD below 1. This approach is inefficient since it involves more lossy[25].

This study states a lossless electroencephalogram (EEG) data compression method with epileptic seizure identification for IoMT systems. Three functions are accomplished by the suggested strategy. Initially, it uses lossless EEG data compression depending on a hybrid technique of k-means cluster and Huffman encodes (KCHE) at the edge gateway to decrease the quantity of information transported from the edges to the fog gateway. The epileptic seizure detector-based Naive Bayes (ESDNB) method is used to determine the patient's epileptic seizure condition at the fog gateways. Utilizing the same lossless compression method used in the initial phase, it minimizes the size of IoMT EEG data sent to the cloud. The usefulness of the recommended technique has been demonstrated by a variety of measurements, and comparing findings reveal that the KCHE minimizes the quantity of EEG data supplied to the fog and cloud platforms and delivers an accurate epileptic seizure identification. For all EEG data, the average compression strength of the suggested KCHE is four times more than the average compression strength of previous approaches (Z,F,N,O, and S). Additionally, utilizing the set of data from Bonn University, the suggested ESDNB outperforms than the other approaches in terms of accuracy, with accuracy ranging from 99.53% to 99.99%. Since there is a loss in compressing, this approach is ineffective [26].

In order to assess patient health in periodical WBSNs while using less energy, this study proposes an AREDaCoT (adaptive rate energy-saving data collection method). Durations are used in the AREDaCoT's operation. Redundancy elimination and sample rate adjustment are the two processes of every period. The initial phase makes use of an enhanced LED to eliminate redundant measurements of the vital signs, while the second phase utilises 2 distinct methods to determine the risk rating in accordance with the patient's risk level and the calibrate sampling rate in order to adjust the detector sample selection ratio. The effectiveness of AREDaCoT has been assessed in comparison to conventional methods using many series of simulations using actual health datasets. The obtained findings demonstrate how AREDaCoT reduces the amount of data collected, resulting in a considerable energy reduction while maintaining data integrity and quality. Additionally, both the rating discrepancies among them and the percentage outcomes of data analysis over the original set of information are suitable. This methodology does not demonstrate how well it performs in terms of energy use, upholding integrity of data, or efficacy on overall decision correctness [27].

3. Problem statement

Given the constrained data processing and storage capability of IoT devices, users' health data is often maintained in a cen-

tralized third party, such as a patient's medical record or clouds. As a result, consumers have less control over their health information, which increases the likelihood of illegal exposure and single-point bottlenecks. Thus, smart healthcare apps encounter a number of significant issues, including privacy and security of data. One of major security challenegs is protecting the privacy of healthcare systems. For clarity, Privacy-sensitive healthcare data are typically kept on a web-server and handled remotely. People start to worry about the security and privacy of their information as a result. This is because a variety of security assaults are feasible under such circumstances. For instance, an auhtrized user may intercept healthcare data over the Internet, change it, and then insert incorrect facts into healthcare information center, or it could steal information from distant servers. In healthcare systems where consumers' original data are necessary for medical therapies, the conventional privacy-preserving techniques focused on summarizing or producing noisy data are ineffective. Academic researchers have recently proposed new privacy-preserving protocols based on BC technology as a possible solution to the problem of secure healthcare data management. Due to its immutability and transparency attributes, Blockchain has been viewed as a promising alternative for the secure management of healthcare records. However, there is a trade-off between the openness of the system and the privacy of user information, which has hindered the widespread implementation of Blockchain in medical systems. While some studies have considered patient privacy protection and offered alternatives, recent models have not well-taken data owners' desires for access control into account. In general, Blockchain is utilized to store data hashes and access controls to improve the availability and integrity of users' information. By storing this information in a Blockchain, it can guard against Denial of Service (DoS) attacks and single failure points. Therefore, the authors suggest an efficient system for access control that uses Blockchain technology for e-health applications. They also proposed a framework to address the issue of balancing transparency with network access by allowing patients to choose their preferred access controls while preserving the privacy of their medical information.

4. Methodology

Blockchain is utilized in the suggested architecture to store hashes of users' healthcare information as well as users' access control policies for their data[28]. Who can acquire the users' data is determined by the policies. The following major modules make up the system architecture. Fig. 2 depicts the proposed system model.

Every patient is equipped with numerous sensors that are fastened to their body and used for monitoring the patient's vital signs like blood pressure and heart rate. Such sensors have limited resources, including computing power, electricity, and storage. Taking into account these restrictions, sensors transmit the data they have gathered utilizing short-range communications, includes Zigbee or Bluetooth, to a more capable device, like a smartphone or a Personal Digital Assistance (PDA) that acts as a gateway to transport the information to the medical servers [29].

In comparison to sensors, PDA and smartphones get more computational power and battery life. They can perform demanding activities, including cryptographic operations including packet transmission across long-distance networks like cellular one for IoT Health Manager (IHM) [30].

IHM may simply be a PC that stores health information and does the following tasks, including such receiving and maintaining data from smartphone devices carrying out cryptographic processes such as hashing transferring information, and policy hashes to the Blockchain network of the health center.

All of a country's health centers may be included to the hospitals and health centers section. They oversee the BC network, mining, and user information. They get user data and policy hashes from IHMs and store them. They are in charge of registration users data (patients, medical personnel, etc.) and assigning a health wallet (HW) and a cluster mining to every one of them so that they may interact with the BC network.

Basic controls and information hashes are maintained in BC to improve the reliability and integrity of user information [31]. Effective data maintenance in a BC is protected from DoS attacks and singular areas of failure. User information and policy are hashed and kept in two distinct ledgers. It would be easier to maintain such two distinct structures for transactions.

Every hospital and health center in the architecture has a number of miners. New transactions are verified by the miners before being added to the BC ledger. Although there are difficulties, including how to persuade and inspire miners outside the clinic to save data, miners outside the health centers could also be utilized. Adopting proof of the staffs is not feasible given the enormous amount of IoT devices are dealing with.

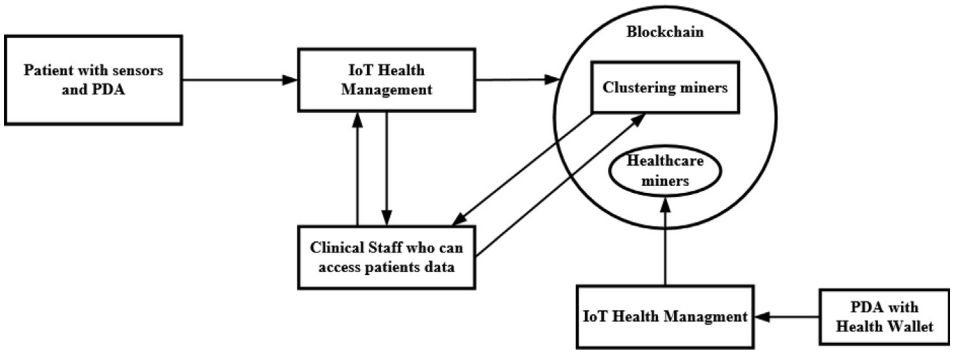

Fig. 2 Healthcare framework based on Blockchain.

In order to achieve this, a novel technique known as Practical Byzantine Fault Tolerance (PBFT) voting-based consensus [32], is employed that calls for numerous levels of voting from each network node. It aids in improving network security and efficiency while lowering network costs, such as bandwidth and processing utilization.

For the purpose of maintaining data integrity within the conventional blockchain, every node must hold redundant information that is the similar instance of the ledger. Although this is beneficial for financial systems like crypto currencies, it dramatically lowers network throughput. It is because every transaction needs to be spread throughout the network's nodes. The miners are grouped into clusters and keep the medical records of every patient in a single cluster to prevent this overhead. While they all run simultaneously, each cluster is autonomous. This equalizes the load across several clusters.

4.1. Data access policy

Through Health Wallet, the data controller in BCHealth establishes specific access policies. The patient registers the required access control policies in blockchain as an exclusive form of transmission known as a policy transmission that is recorded within the BC network's policy chain [33]. In order to accomplish this, the data owner could search up the ID of the clinical staff member in the database of their registered health center and authorize them access. In addition to giving access policies immutability, this will accelerate every chain's search process. It goes without saying that each user can create and implement a single policy at a time for a set of data. For instance, one can declare in a policy transmission, which a doctor has access to every one of their health information or that access is only permitted for a certain amount of time. A 7-tuple could have been used to specify each policy, as shown below:.$\langle O_{id}, R_{id}, T, E_t, \langle s_D, e_D\rangle, V\rangle$

- O_{id} specifies the Patients ID.
- R_{id} is the ID for the user who has access to the information.
- T is the kind of information that is accessible to authorized users.
- E_t is the expiration date of the policy.
- $\langle s_D, e_D\rangle$ it outlines the time frame for the data's accessibility. For example, a clinician can only view patient information that has been recorded on a specific date.
- V is a binary number that shows the policy's integrity, with value "1″ denoting policies which are acceptable and value "0" those that are invalid.

Users are unable to modify a policy that before expire period since the BC ledger is immutable. When a patient requests that a specific user rescind their access, HW creates the same policy transactions in BC with the value "$V = 0$. " Algorithm 1 explains the specifics.

Table 1 displays two illustrations of policies. For two years, from 20 May 2016 to 20 May 2018, the patient whose ID X gave the clinical personnel having ID A permission for reading their heartbeat data. The policy is in effect until November 20, 2020. The second policy states that the similar patient has cancelled the clinician staff's authorization to view every one of their data from July 6 through July 7 from the identifier B.

4.2. Data storage and retrieval

4.2.1. Interaction between PDA to IHM

The patient's PDA categorizes the sensory information it receives based on the sort of data it contains, ECG, heartbeat, temperature, sensor, EEG. Such data is encrypted using a symmetric encryption technique, such as AES, using a key that is first shared among the PDA as well as the IHM. A schematic illustrating how the smartphone (or PDA) and IoT health management communicate is shown in Fig. 3. The IHM uses the accept message as an acknowledgement that it has received data.

4.2.2. Interaction between IHM and blockchain

The IHM creates a hash of the data after obtaining the health information from the sensors as well as supplies the information. After that, a transaction with this hash value is shared to blockchain and kept in the "Data Chain." As given in Eq.1:

$$Hash = H(D\|S\|T) \tag{1}$$

Here, D is the received data from the sensors, S is the date of received data; T is the data type.

The interaction between the health managers (IHM) and the Blockchain is given in Fig. 4. In this process, O_{id} is the id of the patient that developed the transaction. O_{enc} corresponds the asymmetric encryption method, which utilizes the private key of the data owner.

A binary value called emergency determines whether the input is urgent or not. IHM analyses information based on the kind of data after it receives it if the data value falls or rises outside of the expected range. If an emergency occurs, the value will be set to 1; otherwise, it'll be zero.

The interaction between the IoT health management and blockchain to transmit policy transmission is depicted in Fig. 5.

4.2.3. Accessing the healthcare data

Medical personnel or any other user who requires access to the patient's information should submit a request to the BC network after the information has been stored in BC. Clinical staff makes a request for permission to the BC with the necessary details, such as the patient's ID, data type, the beginning dates of the data, in order to access patient information,

Table 1 Data of two policies.

Patient ID	Request ID	Type	Expiration date	Data availability (s_D)	Data availability (e_D)	Valid
X	A	All	May 9, 2020	Jun 7, 2018	Jul 7, 2018	0
X	B	Heartbeat	Nov 11, 2020	May 20, 16	May 20, 18	1

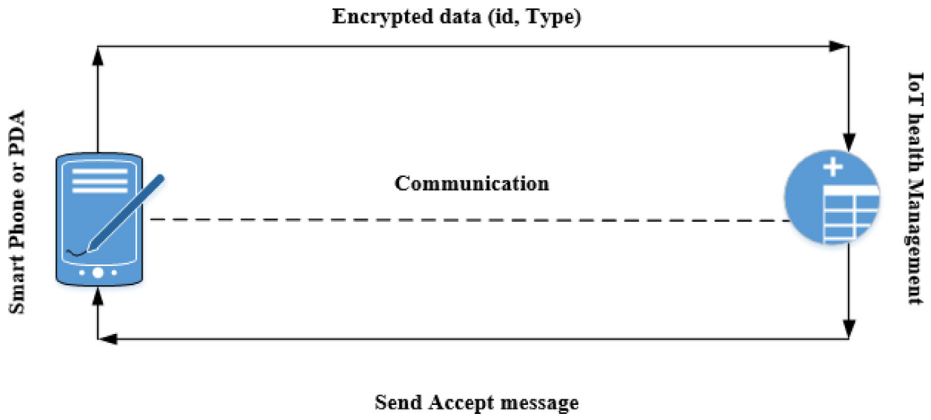

Fig. 3 Communication between PDA and IHM.

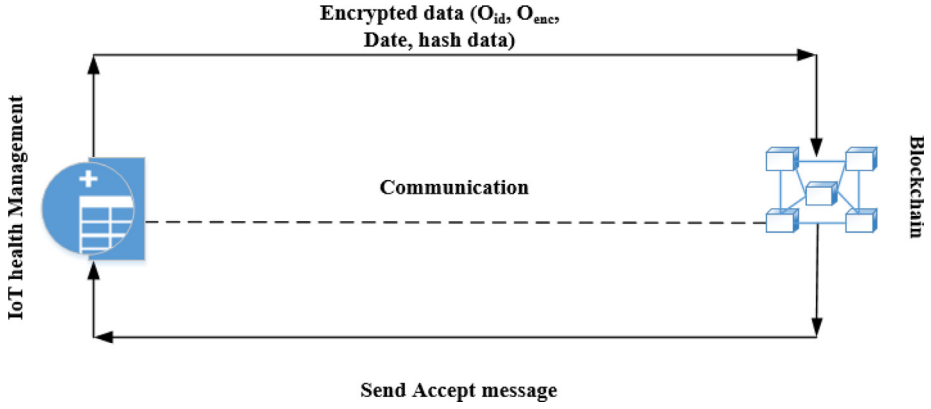

Fig. 4 Data transaction interaction between the health managers (IHM) and the Blockchain.

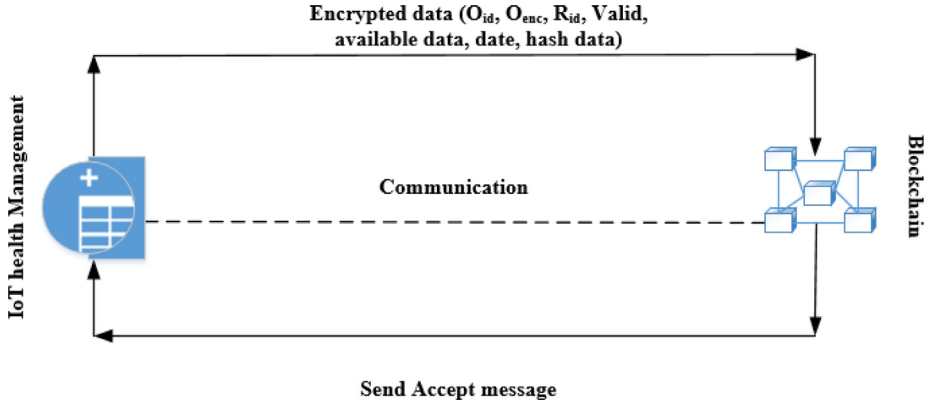

Fig. 5 Communication between IHM and Blockchain for policy transaction.

including EEG. Every mining in the BC that receives such request shows up the requester's authorization in the policy chain (i.e., the medical staff) before proceeding. The miner would submit a request transmission to the IHM with the hash data and ID of the requester if the requester is permitted. The IHM then verifies the demand; if it is legitimate, it forwards the patient's raw information to the clinical team.

4.2.4. Alerting healthcare staff

By transmitting the variable "1″ within the emergency feature of the transmission process, the IHM could indicate if a data transmission is an emergency. A miner that accepts an emergency transmission looks up the healthcare staff members that are permitted access towards this patient's information in the policy chain. The miner notifies the medical personnel of the

patient's emergency by sending an emergency request to them all.

4.2.5. Mining with access control

Controlling requester accessibility for the patient's information based on particular policy transmissions is among the key responsibilities of miners in BCHealth. A miner should validate any request transactions it receives from users that include the patient's ID, the type of data, the beginning time, as well as the length of the data.

If the transaction is acceptable, the miner looks for policies, which are specified for the required data inside the policy chain. The hash data would have been provided for the IoT health management if the requester is valid. Fig. 6 depicts the process of access control procedure.

4.3. Analysis of privacy and security

The Confidentiality, Integrity, and Availability (CIA) security trial is used to examine the security and privacy of the proposed framework aspects in order to demonstrate how robust it is to various threats.

Only users with permission can access the communications because of their confidentiality. For protecting the privacy of the acquired information, the communications between the smartphone and the IHM is transferred using symmetric key encryption. Additionally, the IHM and Block-Chain's communication is protected by public-key encryption. Additionally, the IoT Health Management will be the only entity with accessibility to the patient's information, which is kept in a safe, encrypted format.

Data integrity makes sure that no one may alter the data that has been stored without authorization. Due to BC's inherent irreversibility, it is immune to illegal data change. Data hashes are kept in IHM and BC. Because these two-hash codes still wouldn't match in the event of an unauthorized modification, manipulation would be detected.

In contrast to its centralized competitors, Blockchain health does not experience the typical single source of failure or assault since the decentralized nature of Blockchain. Furthermore, since the accessibility of the policy and data hash within that group is ensured by the fact that they are maintained throughout all miner nodes belonging to the same group as the patient provides enough amount of miner nodes occur in every group. The IHM stores user healthcare data, which might be duplicated on other devices connected or kept remotely in the servers of the related hospital to guarantee availability and prevent data loss because of an attack.

5. Result and discussion

The majority of research works on the use of blockchains use open-source programs already in existence, including Hyperledger and Ethereum, to execute and assess the effectiveness of their recommendations. However, because the fundamental BC structure is significantly changed in BCHealth (clustering the nodes, taking into account various topologies, adopting the PoA Consensus Algorithm among the nodes in every cluster, and using various chains. The existing study and findings were unable to conduct the experimental evaluation using the available tools.

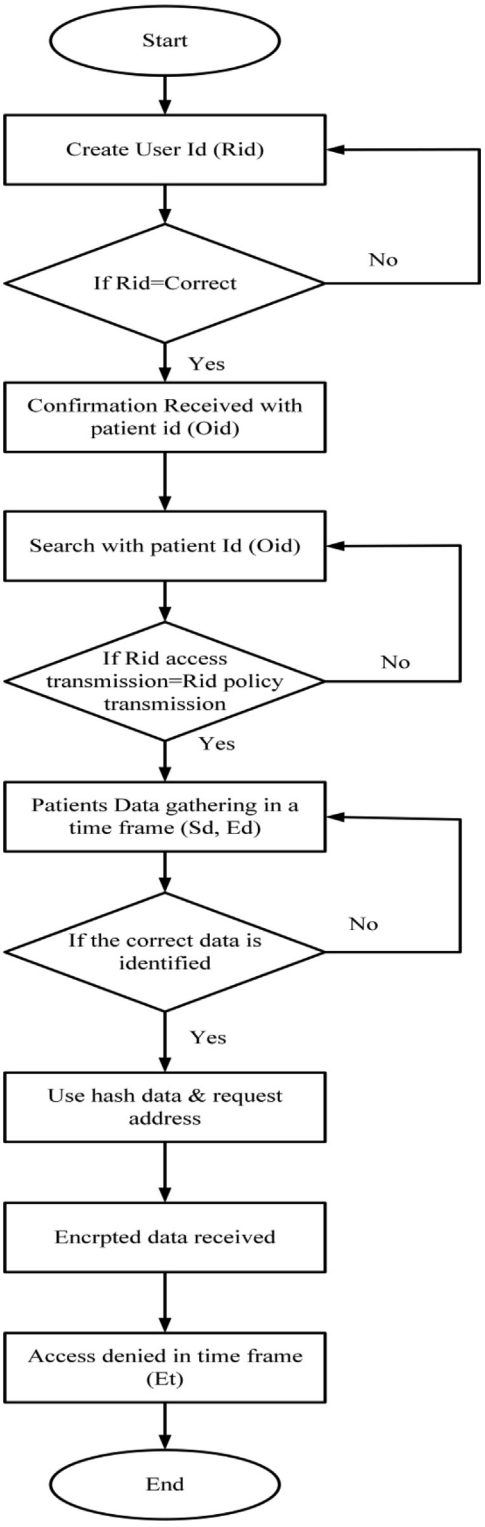

Fig. 6 Flowchart for process of access control.

To create user applications, or HW, for producing transactions, Python is used. On the BC network, the miners' program is setup for receiving and archiving transactions along with block mining, as well as applications for transmitting user access transactions. The Mininet network emulator is utilized

to create the BC network topology. With the computer that has a dual-core CPU as well as 4 GB of RAM, Mininet was run. A network of 12 different miner nodes with the same capabilities also processing capacity as the BC network layout. Also it evaluated and recorded both policy and data transactions on this network. Four nodes were also taken into account as the IHM for creating user healthcare transmissions as well as sending them to the BC network.

Concerning the data that is available in the IHM, it can be taken into account multiple selection for backing up data if there are emergency cases such as the patient's IHM, which includes guardians, whose location is indicated using the patient during the initialization stage, and (2) centrally storing it in the healthcare facility. The latter runs counter to the entire notion of decentralization. In light of the first possibility, one would contend that such backup data is vulnerable to assaults and misuse. Adopting Secret Sharing techniques might be one answer to that.

Health information has historically been regarded as sensitive information, making its storage on the Blockchain problematic from a privacy and security perspective. Anonymizing and access control techniques are just two of the options that have been put out in the blockchain to resolve this concern. These techniques can be classed as cryptographic or non-cryptographic procedures. Elliptic Curve Cryptography is used on a blockchain-based infrastructure to encrypt personal information. A blockchain-based Healthcare Data Gateway (HDG) program that estimates and saves the encoded data immediately upon the private blockchain cloud network without disclosing the original information. Although they don't offer mechanisms for controlling access and the patient has no control over their data, these solutions promote data security and privacy.

The two primary approaches for storing EHRs in blockchain are off chain storage and direct storage of the medical data (raw or hash). A significant computing and storage cost is imposed by the first method. Additionally, because the replicated information has been archived in every node, the likelihood of data leakage grows. The metadata is kept within the blockchain for validation and reliability, while the underlying information will be encoded as well as held by a reliable server, including Cloud.

5.1. Efficiency of the access control procedure

The time it takes for the health workers to obtain the information from the time the request is submitted to the BC until the information is received is referred to as the access time and includes the following:

- The amount of time needed to request access to the blockchain
- The duration of the data and policy chains' searches
- The duration of time needed to send data from the blockchain to the IoT Health Management
- The amount of time needed for the clinician to receive the information from the IHM.

Because the data is not accessed while the policy chain is lost, it is not necessary to seek the data chain, which drastically reduces the access time. Additionally, it is evident that adding more clusters will reduce access time in instances with two clusters.

In BCHealth, policy transactions are recorded via a policy chain. To prevent illegal access to the patient's information, every miner must confirm the request after obtaining an access request transaction. As a result, in order to locate relevant policy transactions, miners must look for policy in the policy chain. The search duration is accessed, or the access control algorithm's processing time. To do this, network with a set of random interactions is tested, and measured how long it took to identify the appropriate policy. According to various clustering methods, the outcomes of the search time for varying amounts of transactions are shown in Fig. 7. The time it takes to find the desired transactions grows together with the volume of transactions. Due to the spread of policy transactions over more clusters, a significant reduction in this time will result from doing so.

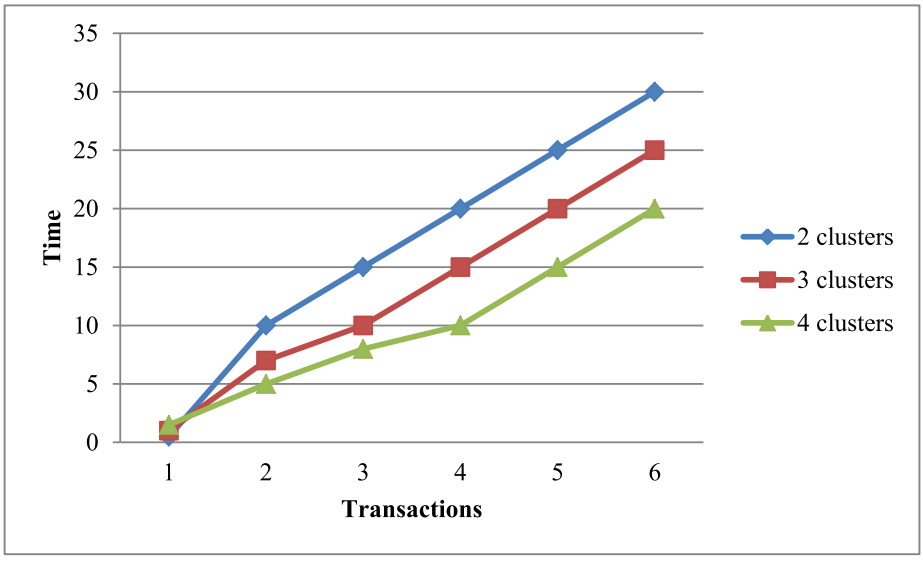

Fig. 7 Amounts of excuted transactions in various clusters.

5.2. Transaction time process

On an Android smartphone and a computer, the processing speed is measured, correspondingly. For a number of significant cryptographic algorithms, the detail processing time can be calculated, as shown in Table 2. Table 2 demonstrates that the RSA signature takes substantially longer to perform than a number of other cryptographic algorithms. The patient and staff's time to execute the transaction is then rigorously tested. TxIoT, TxKey, and TxDiag are generated in 4.567, 0.025, and 0.025 ms, respectively. The fact that every processing durations are the median of 10,000 repeated trials should also be highlighted.

Table 2 Transaction time process.

Process	Patient	Staff
RSA	4.567	0.025
RSA encryption	0.190	5.1
AES encryption	0.140	6.4
HASH-256	0.015	6.8

5.3. Comparison with the traditional approach

For the production of user transactions using the system, the computation cost and communication cost are contrasted with those of the conventional approach. In the conventional approach, the sender uses a symmetric key to encode the data. The symmetric key is then transferred and encoded using the recipient's public key, as well as the encrypted data. But keep

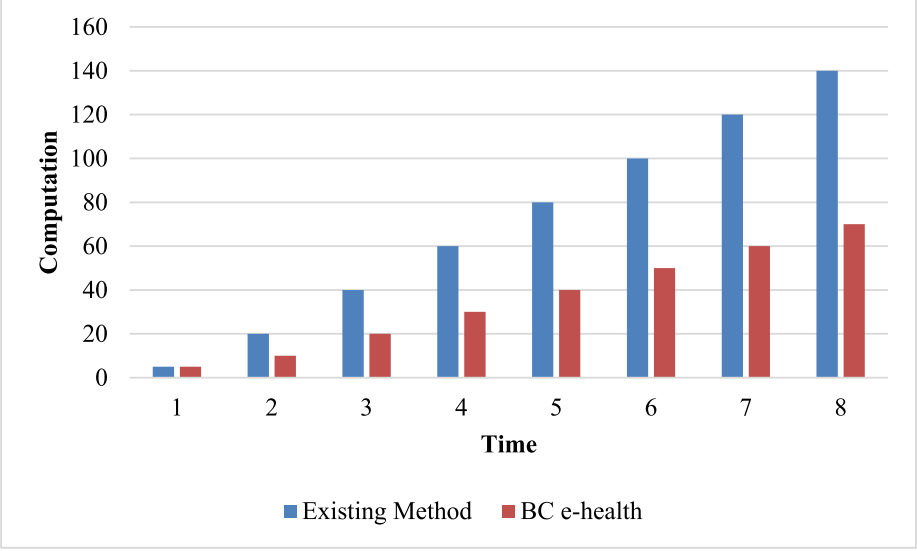

Fig. 8 Costs of computation for the processing of user transactions.

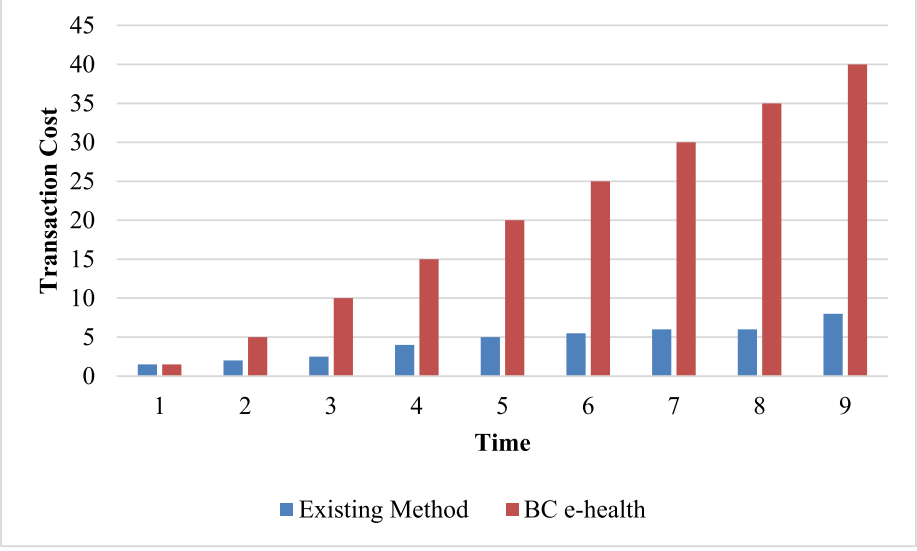

Fig. 9 Communication cost of user transactions.

Table 3 Comparison of proposed system processing time.

Technique	processing time (Sec)
Wearable Sensors based system	8
Kernel methods	16
IoT-based monitoring	12
Exploratory data analysis	10
Proposed Blockchain based healthcare system	5

in mind that IoT data updates could happen considerably more regularly than critical updates. Rather than changing the key every time the IoT transaction is changed, users could modify key transactions as needed under our method. The contrast between the method and the conventional scheme's computational time overhead for the production of user transactions is shown in Fig. 8. Fig. 9 compares the communication costs associated with creating user transactions using the system with the conventional system.

As seen in Figs. 7 and 8, as the system utilization time increases, both calculation cost and communication cost rise. According to Fig. 7, it only takes 96 s for a person who has been around for six months, whereas the conventional solution takes 130 s. The time it takes for users to produce transactions is shorter with Health-chain than it is with the conventional system.

As depicted in Fig. 8, when the system has been in place for six months, user-generated transactions in Health-chain are 3 MB in size, compared to 26 MB for the previous method. On the one hand, this suggests that Health-chain can significantly reduce the communication burden placed on users when sending transactions compared to the conventional system. It also shows that the plan could cut down on the level of user-developed transactions and thus further cut down on blockchain storage.

5.3.1. Processing time

The amount of time needed to complete a computing operation is called the computing time. Table 3 depicts the comparison of the proposed system computation time and Fig. 10 represent the performance evaluation based on computation time. The calculation duration is inversely correlated with the number of rule applications when computing is represented as a series of rule operations.

6. Conclusion

Due to the IoT significantly increased adoption, remote health data analysis for the purpose of smart healthcare has recently attracted a lot of attention. With the growth of the IoT, e-health is now the most important areas of study (IoT). Due to the sensitive nature of medical records, it appears to be challenging to secure patients' privacy. Patient data is frequently achieved in the cloud in healthcare, which reduces the amount of control customers have over their personal information. As per the General Data Protection Regulation, the data owner does have a right to decide when and how their data was stored, who could access it, and to what extent. As a result, the study presented an efficient access control system and suggested a framework to address the challenge of balancing openness with access control. According to the reuslts, the processing time of the proposed system has 5 s which is high efficiency compared to other conventional approaches. Health-chain also prevents medical conflicts by making changing or removing IoT data or doctor diagnoses hard. The suggested experimental data and security evaluations demonstrate Health-chain's potential for application in smart healthcare systems. The extensive experimental examination reveals the block chain's efficiency in terms of computing and time consuming as well as its ability to fend off various security attacks. This study will implement the design in the upcoming and conduct an exploratory method to assess how well the suggested architecture performs. Although the proposed method shows

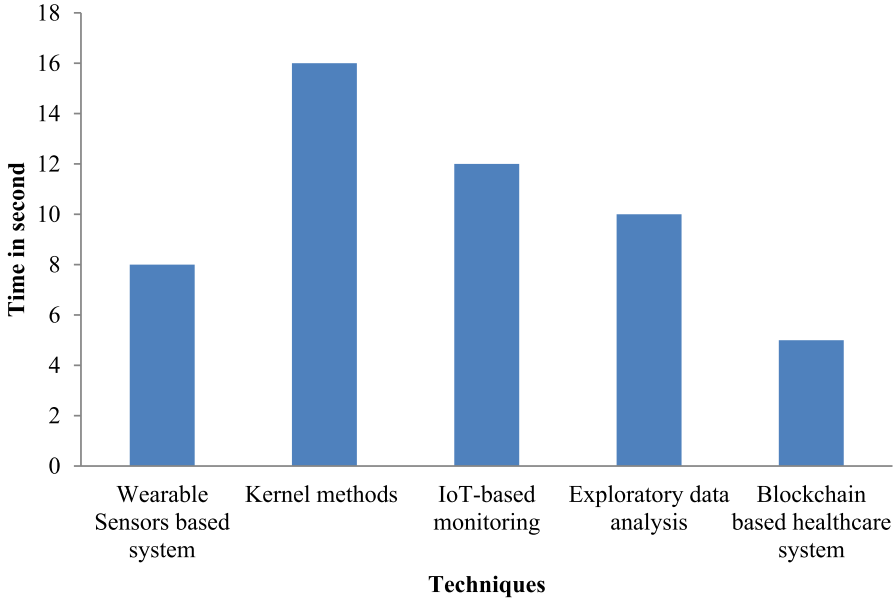

Fig. 10 Performance evaluation based on the processing time.

promising results, there are potential limitations in its ability to resist future quantum attacks that may arise in the future with the development of quantum computing. Future work should focus on developing quantum-resistant cryptography techniques.

Funding Statement.

Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R269), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Declaration of Competing Interest

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

Acknowledgements

The authors acknowledge Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R 269), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

References

[1] K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, J. Med. Syst. 42 (2018) 1–7, https://doi.org/10.1007/s10916-018-0982-x.

[2] M. Aazam, S. Zeadally, K.A. Harras, Health fog for smart healthcare, IEEE Consum. Electron. Mag. 9 (2) (2020) 96–102, https://doi.org/10.1109/MCE.2019.2953749.

[3] M.G.R. Alam, S.F. Abedin, S.I. Moon, A. Talukder, C.S. Hong, Healthcare IoT-based affective state mining using a deep convolutional neural network, IEEE Access 7 (2019) 75189–75202, https://doi.org/10.1109/ACCESS.2019.2919995.

[4] I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, Blockchain for healthcare data management: opportunities, challenges, and future recommendations, Neural Comput. Appl. 34 (14) (2022) 11475–11490.

[5] S.S. Mahdi et al, New design of temperature sensor-based breathing monitoring system, AIP Conference Proceedings 2660 (1) (2022), https://doi.org/10.1063/5.0109347 020142.

[6] T. Al-Sharify et al, IoT and E-learning with the Impact of COVID 19 Pandemic Lockdown on the Undergraduate University Student Blood Pressure Levels, CEUR Workshop Proceedings 3149 (2022) 73–86.

[7] M.H. Stanfill, D.T. Marc, Health information management: implications of artificial intelligence on healthcare data and information management, Yearb. Med. Inform. 28 (01) (2019) 056–064, https://doi.org/10.1055/s-0039-1677913.

[8] J. Adamu, R. Hamzah, M.M. Rosli, Security issues and framework of electronic medical record: A review, Bull. Electr. Eng. Inform. 9 (2) (2020) 565–572, https://doi.org/10.11591/eei.v9i2.2064.

[9] S. Paul, M. Riffat, A. Yasir, M.N. Mahim, B.Y. Sharnali, I.T. Naheen, A. Rahman, A. Kulkarni, Industry 4.0 applications for medical/healthcare services, J. Sens. Actuator Netw. 10 (3) (2021) 43.

[10] P. Xi, X. Zhang, L. Wang, W. Liu, S. Peng, A review of Blockchain-based secure sharing of healthcare data, Appl. Sci. 12 (15) (2022) 7912, https://doi.org/10.3390/app12157912.

[11] N. Islam, Y. Faheem, I.U. Din, M. Talha, M. Guizani, M. Khalil, A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services, Future Gener. Comput. Syst. 100 (2019) 569–578.

[12] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, M. Imran, An overview on smart contracts: Challenges, advances and platforms, Future Gener. Comput. Syst. 105 (2020) 475–491.

[13] C.C. Agbo, Q.H. Mahmoud, J.M. Eklund, Blockchain technology in healthcare: a systematic review, Healthcare 7 (2) (2019) 56, https://doi.org/10.3390/healthcare7020056.

[14] M. Yang, T. Zhu, B. Liu, Y. Xiang, W. Zhou, Machine learning differential privacy with multifunctional aggregation in a fog computing architecture, IEEE Access 6 (2018) 17119–17129, https://doi.org/10.1109/ACCESS.2018.2817523.

[15] G. Zhang, Z. Yang, W. Liu, Blockchain-based privacy preserving e-health system for healthcare data in cloud, Comput. Netw. 203 (2022), https://doi.org/10.1016/j.comnet.2021.108586 108586.

[16] H. Abulkasim, A. Mashatan, S. Ghose, Quantum-based privacy-preserving sealed-bid auction on the blockchain, Optik 242 (2021), https://doi.org/10.1016/j.ijleo.2021.167039 167039.

[17] K.M. Hossein, M.E. Esmaeili, T. Dargahi, and others, "Blockchain-based privacy-preserving healthcare architecture", in, IEEE Canadian conference of electrical and computer engineering (CCECE) 2019 (2019) 1–4, https://doi.org/10.1109/CCECE.2019.8861857.

[18] A.I. Taloba, A. Elhadad, R.M.A. El-Aziz, O.R. Shahin, Prediction of data threats over web medium using advanced blockchain based information security with crypto strategies, J. Ambient Intell. Humaniz. Comput. (2021) 1–17.

[19] H. Bi, J. Liu, N. Kato, Deep learning-based privacy preservation and data analytics for IoT enabled healthcare, IEEE Trans. Ind. Inform. 18 (7) (2021) 4798–4807, https://doi.org/10.1109/TII.2021.3117285.

[20] G. Kaissis, A. Ziller, J. Passerat-Palmbach, T. Ryffel, D. Usynin, A. Trask, I. Lima, J. Mancuso, F. Jungmann, M.-M. Steinborn, A. Saleh, M. Makowski, D. Rueckert, R. Braren, End-to-end privacy preserving deep learning on multi-institutional medical imaging, Nat. Mach. Intell. 3 (6) (2021) 473–484.

[21] S.S.I. Ismail, R.F. Mansour, R.M. Abd El-Aziz, A.I. Taloba, A. D. Doulamis, Efficient E-mail spam detection strategy using genetic decision tree processing with NLP features, Comput. Intell. Neurosci. 2022 (2022) 1–16.

[22] N. Domadiya, U.P. Rao, Improving healthcare services using source anonymous scheme with privacy preserving distributed healthcare data collection and mining, Computing 103 (1) (2021) 155–177, https://doi.org/10.1007/s00607-020-00847-0.

[23] P.N. Srinivasu, A.K. Bhoi, S.R. Nayak, M.R. Bhutta, M. Woźniak, Blockchain technology for secured healthcare data communication among the non-terminal nodes in IoT architecture in 5G network, Electronics 10 (12) (2021) 1437, https://doi.org/10.3390/electronics10121437.

[24] A.S. Jaber, A.K. Idrees, Energy-saving multisensor data sampling and fusion with decision-making for monitoring health risk using WBSNs, Softw. Pract. Exp. 51 (2) (2021) 271–293, https://doi.org/10.1002/spe.2904.

[25] K.K. Al-Nassrawy, D. Al-Shammary, A.K. Idrees, High performance fractal compression for EEG health network traffic, Procedia Comput. Sci. 167 (2020) 1240–1249, https://doi.org/10.1016/j.procs.2020.03.439.

[26] A.K. Idrees, S.K. Idrees, R. Couturier, T. Ali-Yahiya, An edge-fog computing-enabled lossless EEG data compression with epileptic seizure detection in IoMT networks, IEEE Internet Things J. 9 (15) (2022) 13327–13337, https://doi.org/10.1109/JIOT.2022.3143704.

[27] A. Shawqi Jaber, A. Kadhum Idrees, Adaptive rate energy-saving data collecting technique for health monitoring in

wireless body sensor networks, Int. J. Commun. Syst. 33 (17) (2020) e4589.
[28] P. Sharma, N.R. Moparthi, S. Namasudra, V. Shanmuganathan, C.-H. Hsu, Blockchain-based IoT architecture to secure healthcare system using identity-based encryption, Expert Syst. 39 (10) (2022) e12915.
[29] F. Sallabi, F. Naeem, M. Awad, and K. Shuaib, "Managing IoT-based smart healthcare systems traffic with software defined networks," in *2018 international symposium on networks, computers and communications (ISNCC)*, 2018, pp. 1–6.
[30] O.A. Khashan, R. Ahmad, N.M. Khafajah, An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks, Ad Hoc Netw. 115 (2021) 102448.
[31] G. Ali, N. Ahmad, Y. Cao, M. Asif, H. Cruickshank, Q.E. Ali, Blockchain based permission delegation and access control in Internet of Things (BACI), Comput. Secur. 86 (2019) 318–334.
[32] M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M. H. Rehmani, Applications of blockchains in the Internet of Things: A comprehensive survey, IEEE Commun. Surv. Tutor. 21 (2) (2018) 1676–1717.
[33] R. Mukta, H. Paik, Q. Lu, S.S. Kanhere, A survey of data minimisation techniques in blockchain-based healthcare, Comput. Netw. 205 (2022) 108766.
[34] H. Onyeaka, C.K. Anumudu, Z.T. Al-Sharify, E. Egele-Godswill, P. Mbaegbu, COVID-19 pandemic: A review of the global lockdown and its far-reaching effects, Science progress 104 (2) (2021), 00368504211019854.