Received: November 14, 2024. Revised: December 18, 2024.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Secure Privacy-preserving Resolution Adaptive Data Sharing in Hybrid Blockchain Controlled Medical IOT Environment

Neelima Sahu[1]* **Indumathi Karthikeyan[2]**

[1]*Department of Information Science and Engineering, East Point College of Engineering and Technology, Bengaluru – 560049, Karnataka, India*
[2]*Department of MCA,Dr. Ambedkar Institute of Technology,Bengaluru, India*
* Corresponding author's Email: neelimasahu73@gmail.com

Abstract: Medical Internet of Things (IoT) will revolutionize healthcare industry by facilitating on demand medical assistance. Data collected from various sensor devices attached to patients are transmitted to various application servers which can monitor health and offer various medical assistance services. In this medical IoT era, to ensure data security and privacy of patients, it is necessary to mutually authenticate the communicating entities and deliver data at various resolutions between the entities based on the utilities. This work proposes a hybrid block chain controlled Medical IoT environment (HB-MIOT) for secure, privacy preserving data sharing from IoT devices. The solution proposes a novel multi resolution adaptive data sharing scheme using compressive sensing after consensus agreement between the IoT entities with combined block chain and hybrid cloud. The solution is secure against data leakage, data tampering and data compromise at public clouds. Through simulations, the computation complexity for data upload(encryption) and data retrieval (decryption) is 9% and 3.5% lower in proposed solution compared to most recent incremental update solution. Also, the block chain update cost is 13 times lower in proposed solution. Through experimental analysis with U.S Health dataset, the computation complexity for data upload and data retrieval is 10.3% and 3.2% lower in proposed solution compared to recent privacy-preserving and access control scheme for sharing EHRs using blockchain technology.

Keywords: Privacy preservation, Adaptive data resolution, Blockchain, Cloud storage, Medical data sharing.

1. Introduction

Medical Internet of Things (IoT) have facilitated offering high quality, convenient health care services on demand. Wireless sensor devices attached to patients and wearable devices collect various physiological data which are used to make important clinical health care decisions. The physiological data collected by the medical IoT devices are transmitted to health care data center, where data is stored and analyzed by various health care application services to make important decision on health care process, disease diagnosis and treatment. Though medical IoT brings many advantages like improved treatment outcomes, reduced healthcare costs, and enhanced patient satisfaction, it has significant security and privacy challenges [1, 2]. Internet is generally vulnerable to security threats. Intruders can gain access to network and launch various attacks. In medical IoT, risk is manifold as intruders can gain access to medical IoT devices and affect its operations. They can tamper the data from devices with malicious intentions of altering treatment and diagnosis process. The patient data is generally stored in cloud in medical IoT environment. This data can be compromised and privacy of patient can be breached. The security and privacy can be increased in medical IoT environment by tightening data confidentiality, authentication and access control procedures during data sharing. Various data sharing frameworks have been proposed using techniques like attribute-based encryption [3], key aggregate encryption [4] and blockchain [5]. Attribute based control systems have higher potential of information leakage through attributes and data related

information [6]. Blockchain provides consensus among distrustful parties before data sharing and can ensure secure fine grained data access. But for continuous IoT physiological data streams like Electro cardiogram (ECG), block chain storage is a huge overhead and not a scalable approach. Attribute based encryption schemes are not effective for resolution-based access over continuous IoTphysiological streams.Providing data at various resolutions depending on application utilities is necessary for physiological data-based services. Study by Kwon [7] illustrated the necessity of providing ECG signals at various resolutions in terms of adjusting sampling frequency for different applications. Besides this, computational complexity is higher for continuous IoT physiological streams for both storage and retrieval in existing works. Addressing these problems in secure and privacy preserving data sharing for continuous IoT physiological data streams, this work proposes a hybrid Medical IoT environment combining hybrid cloud with block chain. The physiological data streams are transformed and compressive sensed to multiple resolutions with joint light weight encryption and stored in public cloud. A mutual authentication procedure involving the data owner and data user is facilitated with blockchain. The data sharing consensus established between data owner and user is stored in blockchain and sharing is enabled with data sharing consensus guarantee by a private cloud. Even though data is public cloud is compromised, without cooperation between blockchain and private cloud, it is not possible for attacker to decipher the data. Transaction repudiation is facilitated using the blockchain. Following are the contributions of this work.

(i) A data sharing framework for medical streaming data combining hybrid cloud and block chain with increased sharing control by data owners and reduced computational/ communication overhead. The technique is secure against data compromise at public cloud.

(ii) A novel technique to provide data at various resolutions using compressive sensing. By this way, the data is offered to data user at the resolution depending on its utilities.

(iii) The problem of reconstruction error in compressive sensing process is solved by sampling with an optimized measurement matrix. This matrix is generated using a novel technique with particle swam optimization.

The rest of the paper is organized as follows. Section II provides the survey of existing works on private preserving data sharing in medical IoT environment. Section III presents the proposed hybrid blockchain controlled Medical IoT framework. Section IV presents the results of the proposed solution in comparison to most recent existing works. The concluding remarks and the future work scope is presented in Section V.

2. Related works

Oh et al [8] proposed a secure data sharing scheme combining key aggregate encryption with private set intersection technique. Data user and Data owner aggress on intersection results for data sharing and this is validated by a trusted authority. Using this intersection results, data user requests the encrypted data from cloud and decrypts it using aggregated key. Since aggregated key is transported on the network, attackers can capture and later use it for decrypting the data. The scheme provides data with same resolution. The computation complexity is higher for both storage and retrieval in this scheme. Bao et al [9] proposed light weight data sharing scheme based on linear secret sharing scheme. This scheme is designed for semi trust cloud storage with responsibility of key setups and trapdoor generation on trusted authority. Once the TA provides the trapdoor key to the data users, it has full control over the data and there is no control over the access resolution and duration in this scheme. Boumezbeuret al [10] proposed a secure electronic health record (EHR) sharing framework using blockchain and cloud. The data is encrypted and stored in cloud. The access control information are stored in blockchain. Through smart contracts access control is enforced. The cost for incremental update is higher in this approach due to block chain invocation for each update.Jastaniah et al [11] proposed a privacy preserving data sharing framework combining multi key Paillier homomorphic cryptosystem with cipher text policy-based encryption for access control. Though the scheme uses light weight Paillier encryption, the data is masked, decrypted multiple times in addition to one time encryption by data owner. This increases the computation complexity of continuous stream of IoT data. Also, there is no support for data requesters to get data at different resolutions. Data owners provide access control policies to service providers and SP can provide data to any number of data requesters satisfying the policy. This gives less control for data owners and non-transparency in data sharing. Further timed access control is also not supported during data sharing in this scheme. Yin et al [12] solved the problem of single point of failure of key authority node by distributing the key management to many attribute nodes. This improved the trust of key

management nodes. Authors proposed a decentralized cipher text policy-based encryption to encrypt the user's data for secure sharing. The computing complexity is higher in this approach for streaming data from IoT devices. Lai et al [13] proposed a secure medical data sharing scheme combining cloud assisted private set intersection with aggregation signature. Though the scheme provided secure authentication and access control, the computing complexity for storage and retrieval is higher for streaming IoT data. Pan et al [14] solved the problem of asymmetric access control from different parties over the medical data shared over cloud. Authors solved the access control conflict between policies of different owners by a balance score calculation using the mutual influence weight and intention between owners. But this problem could have been solved during the mutual authentication and storing the consensus in blockchain. Xu et al [15] proposed a blockchain based medical data sharing framework. The medical data stored in medical consortium chain is shared after two-way authentication. But this scheme is not scalable and overloads blockchain considering large volume of data generated by medical IoT devices. Wang et al [16] proposed a hybrid blockchain based data sharing scheme where two different blockchains are used to avoid interference in sharing across different entities. Though authors used B tree for indexing the stored items and efficient retrieval, the overhead is higher for continuous data streams of IoT devices.Xiaoyan et al [17]proposed a privacy preserving data sharing scheme using consortium blockchain. The data from IoT devices are encrypted with secret key this secret key is further encrypted by a group key. Both encrypted data and encrypted key are stored in consortium blockchain. The data requesters use their individual decryption key to decrypt the secret key and using it to decrypt the IoT device data. The group management is centralized at blockchain. There is no access revocation and access resolution control in this scheme. Peng et al [18] proposed a privacy preserving medical data sharing framework using dual blockchain. This framework provides more control for data owners using a tripartite authentication key agreement scheme. Unique key is provided for each portion of EMR for a fine-grained access control. The encrypted data is stored and shared via blockchain. But this scheme does not support delivering data at adaptive resolutions and not scalable for continuous data streams due to storage bottleneck on blockchain. Zhang et al [19] proposed a privacy preserving data sharing scheme combining block chain with attribute based searchable encryption. Access control is enforced using block chain. The encrypted data is kept in interplanetary file system to improve scalability of storage. The scheme does not support sharing data at different resolutions. Uddin et al [20] leveraged blockchain to realize a decentralized health care data sharing architecture. The architecture had three layers. Agents at each layer cooperatively authenticated each other for secure communication. Block chain was used for storing health care data. But the mechanism was not scalable for streaming data due to its overhead on blockchain. Also, this scheme does not support streaming data. Meisamiet al [21] proposed a block chain based decentralized data sharing architecture for e-health. The access control mechanism is kept in blockchain and enforced using smart contract. The data is stored in IPFS to improve scalability. But the solution does not support sharing data at various resolutions. Amanat et al [22] proposed a secure peer to peer decentralized framework for health care data sharing. Users are authenticated using a proof of stake cryptography consensus mechanism. Data is encrypted using Secure hashing algorithm (SHA-256) and shared using public clouds. The scheme does not support timely access revocation and sharing data at different resolutions. Yu et al [23] proposed Edge Blockchain Secure Data Sharing Scheme for data sharing in edge enabled IoT environment. The solution combines symmetric encryption with edge blockchain to guarantee data

Confidentiality. Edge blockchain constructed by edge servers and cloud, authenticate IoT devices and upload the encrypted data to public cloud.

Encrypted data are sent to data requesters. There is no resolution control on data shared to requesters. Also, the scheme provides limited control to data owner on whom he wants to share the data. Wang et al [26] proposed a user centered medical data sharing solution combining blockchain and trusted execution environment. The scheme is not scalable for streaming data as the entire data volume has to be kept in blockchain. Wang et al [27] combined blockchain with cloud for supporting incremental update of data. The access policy enforcement is done by blockchain. Public cloud stores the data.The scheme has higher computational complexity for streaming data due to frequent private key updates and block chain interaction.

The summary of the survey in given in Table 1. Based on the survey, the gaps identified in existing works are detailed in Fig. 1. From the survey, it can be seen that most solutions do not provide control to data owner over sharing data at various resolutions to requesters. Most of schemes have higher computational complexity during storage and

retrieval for streaming data due to complex cryptographic primitives and double encryptions. Along with other factors, block chain-based data storage/sharing makes the schemes not scalable for streaming data.

Table 1. Survey summary

Work	Solution	Gap
Oh et al [8]	Key aggregated based data encryption and sharing the keys for decryption	Data access with multiple resolutions is not supported. Computation complexity is higher for streaming data.
Bao et al [9]	Trusted authority for key setup and trapdoor generation.	Data access with multiple resolutions not supported. Data owner has less control over duration and number of times of sharing.
Boumezbeur et al [10]	Secure electronic health record (EHR) sharing framework using blockchain and cloud	Higher cost for incremental data update due to invocation of blockchain for each update.
Jastaniah et al [11]	Paillier homomorphic encryption with cipher text policy based encryption for access control.	Computation complexity is higher due to two level encryption. Data owner has limited control over data sharing. Data access with multiple resolutions not supported.
Yin et al [12]	Decentralized cipher text policy based encryption	Computation complexity is higher for streaming data. Data owner has less control over duration and number of times of sharing. Multi resolution-based access is not supported
Lai et al [13]	Private set intersection with aggregation signature	Computing complexity is high for streaming data. Multi resolution-based access is not supported
Xu et al [15]	Block chain-based data sharing with two-way authentication before data sharing	Not scalable as the data is stored on block chain. Multi resolution-based access is not supported
Wang et al [16]	hybrid blockchain based data sharing scheme with two block chains.	Not scalable for streaming data. Data access with multiple resolution not supported.
Xiaoyan et al [17]	Group key-based encryption with data storage in blockchain for sharing	Not scalable for streaming data. Data access with multiple resolution not supported. Data owner has limited control over duration and number of times of sharing
Peng et al [18]	Tripartite authentication with data storage and sharing via blockchain	Not scalable as data is stored on block chain. Multi resolution-based access is not supported
Zhang et al [19]	Block chain for access control with attribute based searchable encryption.	The scheme does not support sharing data at different resolutions
Uddin et al [20]	Data sharing via blockchain with access control by smart contract	Not scalable as data is stored on block chain. Multi resolution-based access is not supported
Meisami et al [21]	block chain for access control with data stored at IPFS.	Multi resolution-based access is not supported
Amanat et al [22]	Data is encrypted using Secure hashing algorithm (SHA-256) and shared using public clouds.	Data owner does not have timely access revocation and sharing data at different resolutions
Yu et al [23]	symmetric encryption with edge blockchain to guarantee data confidentiality	Not scalable as data is stored on block chain. Multi resolution-based access is not supported
Wang et al [26]	Combined blockchain and trusted execution environment for data sharing	Not scalable as data is kept in blockchain
Wang et al [27]	Blockchain based access control with data sharing via public cloud	The scheme has higher computational complexity for streaming data due to frequent private key updates. Multi resolution-based access is not supported

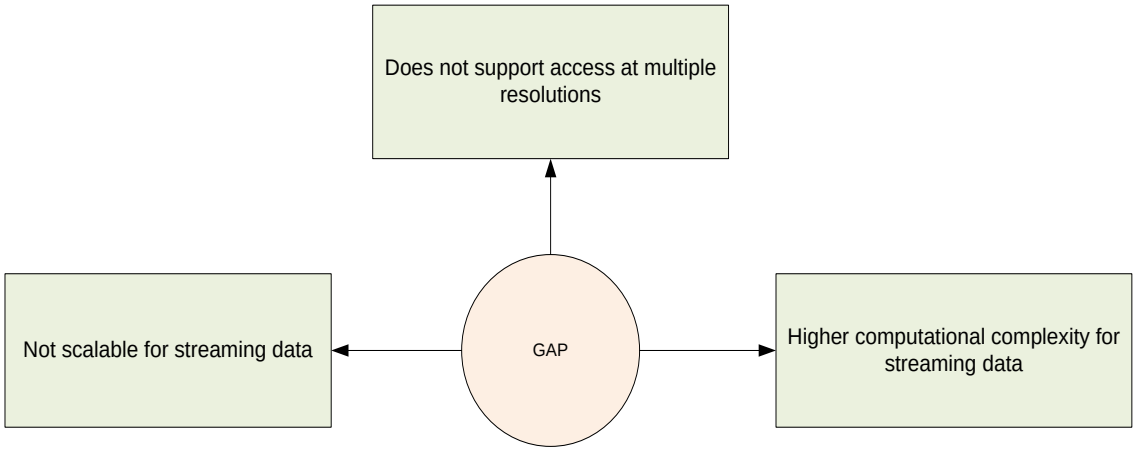

Figure. 1 Gaps in existing work

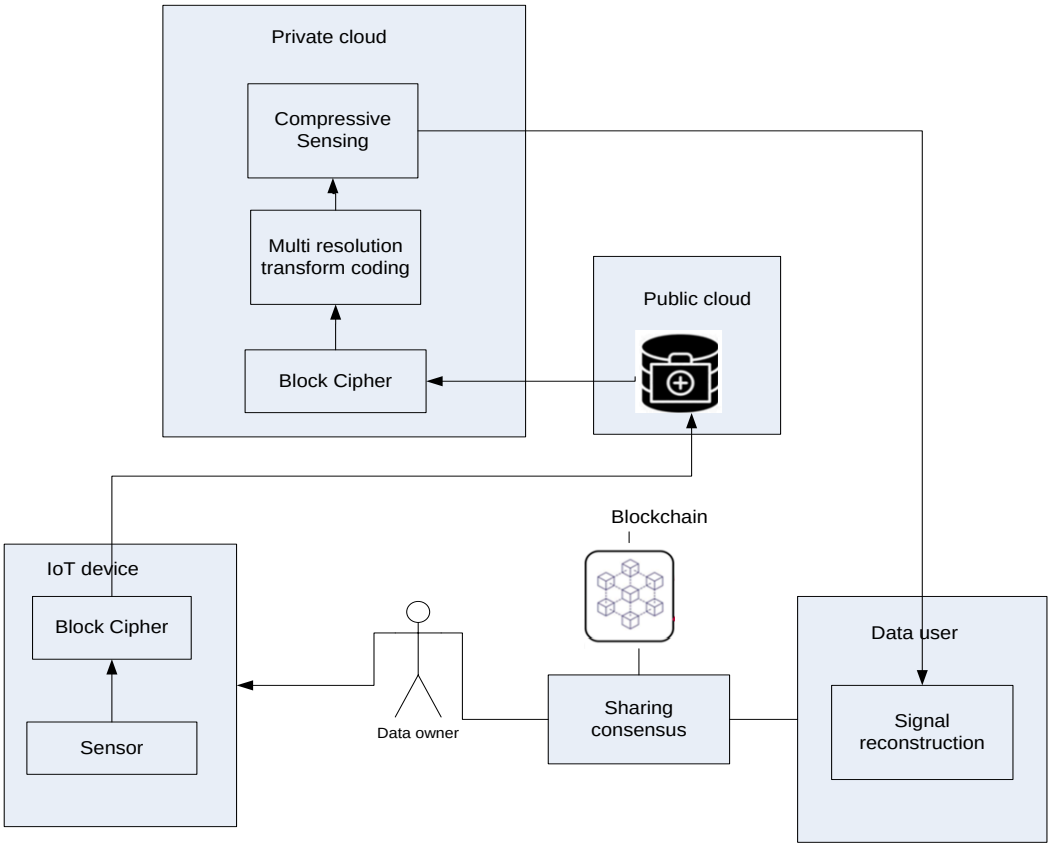

Figure. 2 HB-MIOT Architecture

3. Proposed method

This work proposes HB-MIOT framework combining hybrid cloud and blockchain to solve the three problems of (i) data resolution control, (ii) increased data ownership and (iii) reduced computational complexity for large volume streaming data. The architecture of the solution is given in Fig. 2. Compressive sensing with adaptive transform coding is implemented to provide data resolution control. Three party mutual authentications with blockchain for data sharing consensus and private cloud for sharing control is implemented for increased data ownership. Light weight cryptography combined with transform coding is implemented to reduce the computational complexity for large volume data streaming. The notations used in the equations are given in Table 2.

Table 2. Notations in equations

Variable	Equation	Description
P_{pm}	1	Master public key
E_i	2	Private key for user
h_1	2 to 10	Hash function
x	15	Physiological signal data to be shared by the data owner to data user
ϕ	16	Measurement matrix
∅	16	Signal measurement vector
M	17	Number of measurements to be done for optimal reconstruction of original signal
$X_i(t)$	20	Position of particle at time t
$V_i(t)$	20	Velocity of particle at time t
$p_{besti}(t)$	21	Position of locally best particle at time t
$g_{besti}(t)$	21	Position of globally best particle at time t
$\bar{x}$	22	Reconstructed signal
f	22	Optimization function used for PSO

3.1 System model

The proposed system is designed for an untrusty public cloud and network where attackers can get access to the data and attempt to compromise any private information. IoT devices owned by data owner or the patient can stream data which needs to be stored in the cloud. The data user (or the applications) can request access for the data from IoT devices at various resolutions. The data owner provides access to the data after a sharing consensus established through mutual authentication between data owner and data user with transaction guarantee and de-refutation provided by blockchain. The data owner is provided necessary controls over the means of sharing as established through sharing consensus by the private cloud in cooperation with block chain.

3.2 Proposed methodology

The sensing data from IoT devices managed by data owner is encrypted with blockcipher and stored in public cloud. The key for blockcipher is generated by the data owner and set in the IoT device. A lightweight blockcipher mechanism is used in this work which is secure and suited for low resource constraints of IoT devices.

The encrypted data in public cloud can be shared at different resolution securely to the data requesters after mutual authentication involving data owner, data requester with use of smart contract at blockchain. Each of the entities of data owner and data requesters register to blockchain via a smart contract to receive the private keys. The smart contract named initialize() generates the master privatekey for itself. It also generates master public key and creates a transaction containing public key and hash functions. The initialize() function selects a bilinear map $e = G_1 \times G_1 \rightarrow G_2$ with two cyclic additive (G_1) and multiplicative (G_2) group. The two groups are of same prime order$q$. It selects a random number R as the master private key. The master public key is then generated as

$$P_{pm} = R.P \tag{1}$$

Where P is the generator for the cyclic additive group G_1. It also generates a one-way hash function h_1 of prime order q. A transaction block containing $\{P_{pm}, h_1, G_1, G_2, P, q\}$with identifier $G$is created and added to blockchain. Each of the entities (data owner or data user) register to blockchain to get their private key using a smart contract named registerEntity(). The smart contract generates private key for entity(E_i) with identifier ID as

$$E_i = \frac{1}{R+h_1(ID)}\ P \tag{2}$$

The private key is returned to the entity.

A data user (ID) who wants to request data at a particular resolution over a time period wraps the access request into a message $ReqM$, It then calculates two number $d_1$and d_2 as

$$d_1 = x.(P_{pm} + h_1(G).P) \tag{3}$$

$$d_2 = h_1([e(P,P)]^x, G) \oplus (ID, y) \tag{4}$$

Where x, y are two random numbers. Data user sends $\{d_1, d_2, AES\_Encrypt(ReqM, y)\}$ to data owner. Data owner does the following to extract ID and y.

$$k = e\left(\frac{1}{d_1+h_1(G)}.P, d_1\right) \tag{5}$$

$$v = h_1(k, G) \tag{6}$$

$$(ID, y) = d_2 \oplus v \tag{7}$$

It then decrypts $ReqM$ message using y and checks if it can satisfy the requirements of data user. If it cannot satisfy the requirements, it rejects with negative response.If it can satisfy the requirements, it

creates the conditions for acceptance as $ResM$ it computes two numbers m_1, m_2

$$SK = y.d_1 \quad (8)$$

$$m_1 = y.(h_1(G).P + P_{pub}) \quad (9)$$

$$m_2 = y.(h_1(h_1(ID), h_1(G), y, ID, G, SK)) \quad (10)$$

$ResM$ also has the server identifier in the private cloud to access the device sensing data. It then invokes share_aggreement_start() contract with $ReqM$, $ResM, d_1$, ID, m_2 on the blockchain. Blockchain creates a sharing consensus block with information of $ReqM$, $ResMd_1$,$ID, m_2$and responds. After the response, the data owner sends a response message containing $\{m_1, m_2, AES\_Encrypt(ResM, y)\}$ to the data user.

The data user authenticates the data owner by calculating $\bar{m}_2$ as

$$K = H_1(y.m_1) \quad (11)$$

$$\bar{m}_2 = H_1(h_1(h_1(ID), h_1(G), y, ID, G, SK)) \quad (12)$$

If $\bar{m}_2$equals m_2, data owner is authenticated and it computes

$$d_3 = \left(y + H_1(ID, SK, m_2, d_1)\right) \times \left(\frac{P}{d_1 + h_1(ID)}\right) \quad (13)$$

as it's agreement to conditions of the data owner and and send it data owner. On recovering it, data owner invokes share_aggreement_finish() contract on blockchain. Blockchain on receiving d_3, verifies if the following relation holds

$$e\left(d_3.\left(P_{pm} + h_1(ID).P\right)\right) = k.g^{h_1(ID, SK, m_2, d_1)} \quad (14)$$

If the relation holds, then the sharing consensus is established and a transaction block is added to the block chain. The blockchain ensures the irrefutability of sharing agreement established between data owner and data user.

The data user requests for the streaming data by sending requests to server identifier in the private cloud with signature computed using its private key. Private cloudcalls a smart contract called verify() on the blockchain with the signature of the data requester. Verify checks the signature of data requester, retrieves the transaction block and provides the $ReqM$ to the private cloud. Private cloud collects the block ciphered streaming data from public cloud and decrypts it. It applies multi resolution transfer coding according to resolution in the $ReqM$.

The multi resolution transfer coding reduces the streaming data to the resolution in terms of sampling frequency set in the $ReqM$. The multi resolution transfer coding generates a binary encoding matrix (EM) based on the sampling frequency. This EM is encrypted with public key of data user and sent to the data user. The EM is thus secure and can only be decrypted by the data user. The EM is used in the compressive sensing (CS) process to get encoded streaming data. The encoded streaming data is sent to the data user. Without EM, it is not possible to reconstruct the streaming data and thus streaming data is secure from any deciphering attacks. CS is technique used in signal processing to reconstruct original signals from fewer observations. CS works by utilizing the sparsity in the signal and sampling it below the Nyquist limit. As most physiological signals are sparse in either time or frequency domain, CS is used in this work to adapt the resolution. In addition encoding is fast in CS due to its use of non-adaptive linear projections. CS samples to acquire important information and get reduced representation. From this reduced representation, projection is done using various optimization methods to get the original signal. Due to sampling below Nyquist limit, the compressive gain is higher and this also reduces the communication overhead in sending data from private cloud to data user. The compressive gain is higher with increased sparsity in the signal. A physiological signal (x) can be represented in terms of its N sparse representation ($\varphi = \{\varphi_1, \varphi_2, .. \varphi_N\}$) and K linear basis functions for $K < N$ as

$$x = \sum_{i=1}^{K} \emptyset_{ni}\, \varphi_{ni} \quad (15)$$

Where $\varphi_{ni} \in \varphi$. Let $\emptyset = [\emptyset_1, \emptyset_2, ... \emptyset_N]^T$ be the vector of coefficients vector of the basis function φ for the physiological signal x and it with measurement over signal is represented as

$$y = \phi\emptyset \quad (16)$$

$$\phi: M \times N \quad (17)$$

$$K < M < N \quad (18)$$

ϕ is the uniform random measurement matrix, y is measurement vector of signal x . $\emptyset$ is the coefficients for the signal x and $M = cK(c < 1)$ is the number of measurements to be done for a successful reconstruction of the signal. The signal reconstruction is done by multiplying the CS output

signal with measurement matrix and then applying optimization methods to reconstruct the original signal. Out of many optimization methods, l_1 norm minimization [25] is the most used which works by finding the vectors with smallest l_1 norm subject to condition

$$min||x||_n \; subject \; to \; \phi x = y \tag{19}$$

l_1 norm minimization is used for signal reconstruction in this work due to its reduced computation complexity compared to other signal reconstruction algorithms.

The measurement matrix used for sampling the signal is generally constructed using Gaussian distribution in the CS process. But the computational complexity is higher with this matrix due to its real values. This can be reduced by generating binary random measurement matrix. The size of the binary random measurement matrix is $M \times N$ where M is set as sampling frequency value in the $ReqM$ message. The binary measurement matrix can be generated using the binary matrix generation procedure given in [24]. But the measurement matrix is not optimized for all physiological signals and it can introduce large error in signal reconstruction. This work models the problem of binary matrix generation for physiological signals as an optimization problem and uses particle swarm optimization (PSO) to solve the problem.

PSO algorithm is based on bio forging behavior of swarms. The algorithm relies on collective behavior of all particles in swarm to find the location of the food. This behavior of swarms is used in PSO and the search for food in PSO context is the search for optimal solution in a solution space. Though there are many swarm algorithms for finding optimal solution in search space like artificial bee colony optimization, fish swarm optimization, firefly optimization etc. PSO is selected as it is simple to realize and it converges quickly compared to other algorithms. PSO algorithm initially starts with random candidate solutions in the search space. Each random solution is a particle. At each iteration, fitness function is calculated for every particle and the particles with maximum value of fitness function are selected as globally best solution (g_{best}) and locally best solution (p_{best}). After finding the best solutions, each particle modifies its solution (in some of dimensions) based on p_{best} and g_{best}. The rate at which particle updates its solution (number of dimensions in the solution) is called as velocity. Particle updates the solution at time at time $t+1$ as below

$$X_i(t+1) = X_i(t) + V_i(t+1) \tag{20}$$

$$V_i(t+1) = wV_i(t) + c_1 r_1\big(p_{besti}(t) - X_i(t)\big) + c_2 r_2\big(g_{besti}(t) - X_i(t)\big) \tag{21}$$

In the above equation the parameters c_1 and c_2 are the acceleration control parameters influencing how much of locally best and globally best solution affects the solution update of the particle. r_1 and r_2 are the random bias parameters. Once the particle updates the solutions, iteration is repeated. The iteration is stopped when there is no change in fitness value or maximum count of iterations is reached.

The initial binary random measurement matrix is generated using [24]. This binary measurement matrix is optimized with the optimality criteria of minimizing the reconstruction error. The optimization function is given as

$$f = \frac{1}{|x - \bar{x}|} \tag{22}$$

Where $\bar{x}$ is the reconstructed signal using l_1 norm minimization. PSO is applied for optimizing the binary measurement matrix as follows. P particles of PSO are initialized with P binary matrix found using [24]. For each of P particles, fitness function f is calculated and the particle with highest value for f is set as best particles. Other particles move towards the best particle by replacing any row with large deviation to other rows with a row in the binary measurement matrix of best particle. The iteration process is repeated till there is no change in f. Once the iteration ends, the particle with highest value of f is the selected and its measurement matrix is the optimal matrix to be used in the compressive sensing process.

The overall interaction for data sharing is summarized in Fig. 3. Two smart contracts are invoked for establishing sharing consensus and one smart contract for verifying sharing consensus before data sharing session between private cloud and the data user.

4. Results

The performance analysis of proposed solution was conducted in two modes of experimental and simulation.

4.1 Experimental analysis

The performance of the proposed solution is

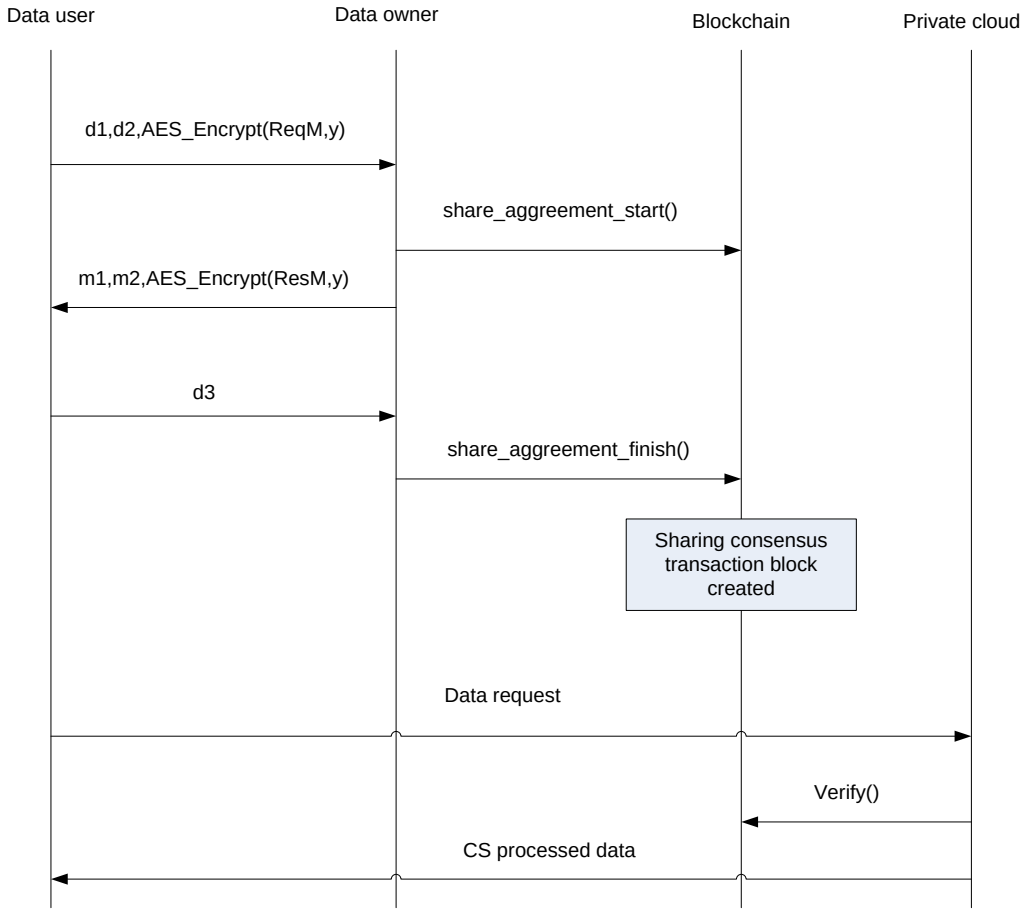

Figure. 3 Sharing consensus flow

compared against blockchain based secure data sharing solutions proposed in Boumezbeur et al [10], Wang et al [29] and Thwin et al [30]. The experiments are conducted in the same environment setting of Boumezbeur et al [10] for electronic health records (EHR) of varying sizes (128KB to 128 MB) downloaded from US Department of Health and Human Services (HealthData.gov, 2022). The data upload time (or encryption time) and data retrieval time (or decryption time) is measured for varying EHR file sizes and the results are given in Tables 3 and 4.

The data upload time is atleast 10.35% lower in proposed solution. The data retrieval time is atleast 3.2% lower in proposed solution. Use of low complexity cipher along with reduced number of interactions with blockchain has reduced the data upload and data retrieval time in proposed solution.

The real gas costs and the fees in Ethereum blockchain are calculated for document upload, update and delete functionalities and the result is given in Table 5.

From the results, it can be seen that there is no difference between the proposed solution and the Boumezbeur et al [10] for add and delete operations. The major difference is in the update operation. The proposed solution avoids block chain update by handling necessary operations in the private cloud and thus there is no gas and ether cost for update operation in proposed solution.

Table 3. Data upload time comparison

	Data upload time (seconds)			
File Size	Wang et al. [29]	Thwin et al [30]	Boumezbeur et al [10]	Proposed
128 KB	0.36646	0.0918	0.0012	0.0010
512 KB	0.37069	0.094	0.0158	0.0137
2 MB	0.37585	0.101	0.0452	0.0383
8 MB	0.42311	0.142	0.0615	0.0591
32 MB	0.59305	0.303	0.2064	0.1935
128 MB	2.24242	1.828	1.4149	1.3012
Average	0.384	0.107	0.0309	0.028

Table 4. Data retrieval time comparison

File Size	Data retrieval time (seconds)			
	Wang et al. [29]	Thwin et al [30]	Boumezbeur et al [10]	Proposed
128 KB	0.16169	0.00319	0.0013	0.0012
512 KB	0.17001	0.0064	0.0027	0.0021
2 MB	0.17967	0.01662	0.0157	0.0143
8 MB	0.22602	0.05919	0.048	0.033
32 MB	0.40503	0.23833	0.20123	0.1983
128 MB	1.95048	1.81479	1.6284	1.5879
Average	0.515	0.356	0.316	0.306

Table 5. Blockchain cost comparison

Operations	Gas used		Cost (ether)	
	Proposed	Boumezbeur et al [10]	Proposed	Boumezbeur et al [10]
Add	105222	106285	0.00010309645	0.000106285
Update	0	27094	0	0.000027
Delete	17141	17141	0.000017	0.000017

4.2 Simulation analysis

The performance of the proposed solution was measured by simulating in a computer with Intel(R) Core (TM) i5-7500 CPU @ 3.40 GHz 3.41 GHz, with 8 GB RAM on an Ubuntu 18.04 LTS 64-bit operating system. Ethereum blockchain platform was used. The coding was realized using Python 3.8. The performance of the proposed solution was compared against incremental update scheme proposed in [27] as this was the only recent scheme designed for streaming data with combinedblockchain and cloud storage use similar to proposed solution. The simulation was conducted in the same test environment used in [27] by executing data upload and retrieval for data file size variance from 50KB to 300 KB. Though simulation was conducted in both Intel SGX and non-Intel SGX environment, this work tests only in non-Intel SGX environment due to resource unavailability.

The computational complexity for data update and data decryption for various data sizes were measured and the result is given in Figs. 4 and 5.

The computation time for data decryption at data user end is on average 3.5% lower compared to Incremental update [27] in the proposed solution. The decryption time has reduced in proposed solution due to use of low complexity block cipher along with compressing sensing reconstruction. Fetching the key for the incremental update and data from block chain frequently has increased the computation time for data decryption in [27].

The computation time for data update from data owner end is on average 9% lower compared to Incremental update [27]. The computation time for data upload is less in proposed solution due to low complexity block ciphering without involvement of any blockchain operation during data upload. In addition to the cryptographic primitive'sinvolvement of blockchain for every incremental update has increased the data update in [27] but in proposed solution transaction update is made only during user entity registration.

The cost of execution of smart contracts in proposed solution is measured for three stages of data upload, access control and key authorization in terms of Eth feeand compared against [27]. The cost in terms of Eth fee is available in [27] for each sub operations of data upload, access control and key authorization. They are summed up to get total cost for the operations. The results are given in Table 6.

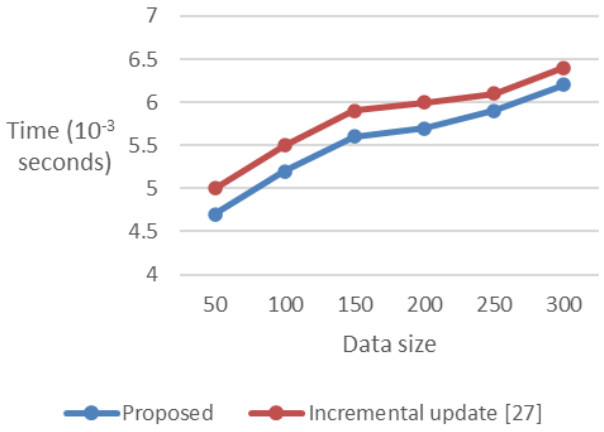

Figure. 4 Decryption time

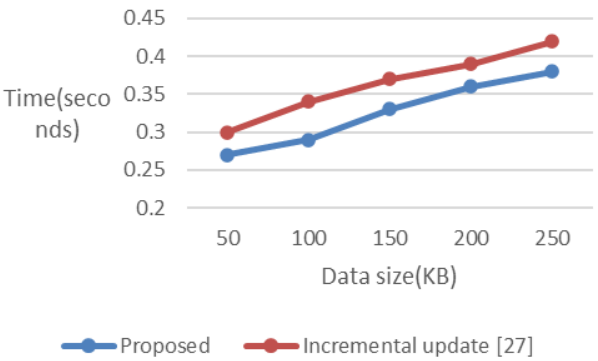

Figure. 5 Data upload time

Table 6. Smart contract cost

Stages	Eth free in Proposed	Eth fee Incremental update [27]
Data upload	0.012	0.189(0.01706772+ 0.001895)
Access control	0.017	0.0166 (0.01509572+ 0.00090984+0.0006072)
Key authorization	0.013	0.01322 (0.01106774+0.00215998)

The data upload cost is 13 times lower compared to existing work. The data upload cost is low in proposed solution as it involves only one interaction with blockchain during upload but there are frequent interactions in [27]. Access control and key authorization cost is almost same in both the works.

The communication overhead in delivering data from private cloud to data user is measured for various resolutions in the proposed solution. ECG data from PhysioNet [28] was used for experimentation by sampling at 250 Hertz, 100 Hertz and 50 Hertz. The original dataset was available at frequency of 500 Hertz.

By reducing the resolution, the communication overhead is reduced in the proposed solution. The gain with 250 Hz is 1.2 times, gain with 100 Hz is 1.9 times and gain with 50 Hz is 2.5 times. The gain increases due to compressing sensing efficiency in handling the sparsity in the physiological signals.

The data owner has more control over the way the data is offered. Owner confirms data sharing only when the conditions provided by $ReqM$ are acceptable and only sharing consensus is established. This is facilitated by the block chain. At private cloud, the access history is maintained allowing auditing all access by different users.

The security strength of compressed data is measured in terms of predicting the binary measurement matrix from the encrypted binary measurement matrix sent from private cloud to the data user. The difficulty level in predicting the binary measurement matrix is measured in terms of a measure called variance of difference (VOD).

Let X_i be a random variable representing the binary measurement matrix value i, X_i' be the estimated result of X_i and difference $D_i = X' - X$. Let mean of D be $E(D_i)$ and variance be $Var(D_i)$. VOD for column i is $Var(D_i)$. VOD is measured for each of N columns and average VOD ($\overline{VOD}$) is calculated as

$$\overline{VOD} = \frac{\sum_{i=1}^{N} VOD_i}{N}$$

The guess is launched for 1 hour for various resolutions and the result is given below

The difficulty is very high for higher resolutions as the size of the binary measurement matrix is higher for higher resolutions. The average VOD increases by 100% for data resolution change from 50 Hz to 250 Hz.

4.3 Discussion

The proposed solution addresses three important gaps (Fig. 1) (i) data access at multiple resolutions, (ii) higher computational complexity for streaming data(iii) scalability for streaming data.

4.4 Data access at multiple resolutions

Through use of compressive sensing, the data is delivered from cloud to data user at the resolution as agreed in data sharing consensus. While existing works delivered the same data uploaded by data owner irrespective of utility to data user, the proposed solution solved this issue by delivering the data to user at the resolution depending on the utility of the user. While providing data at various resolutions, the proposed solution does it without compromise of security and at lower communication overhead as seen from results of Figs. 6 and 7. To the best of our knowledge, providing data at fine grained resolutions without compromising security and communication costs has not been considered in previous works.

4.5 Computational cost and blockchain cost

Most of the existing works encrypted data with complex cryptographic primitives and used block chain for data storage. This increased the computational complexity for streaming data. The proposed solution solved this problem by using

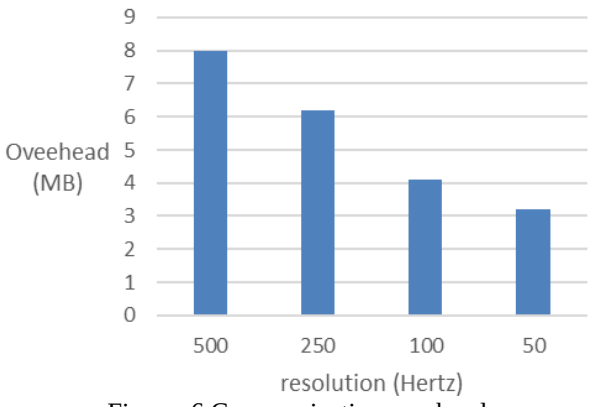

Figure. 6 Communication overhead

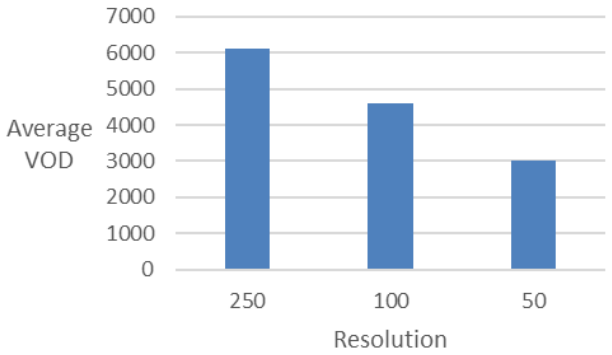

Figure. 7 Security strength

simple block cipher for encryption and keeping the data in cloud. The number of block chain transaction were reduced and this has in turn reduced the computational complexity in proposed solution. As reveled from results in Tables 3 and 4, Figs. 4 and 5, the computational complexity is reduced significantly in proposed solution compared to existing works. In addition, the proposed solution has also reduced the gas cost and Ethereum cost compared to existing work by managing update operations in private cloud instead of blockchain.

4.6 Scalability for streaming data

The proposed solution is scalable by moving the data storage to public cloud instead of keeping the data in blockchain. Also, it reduces the number of transactions needed for streaming update thereby reducing the block chain cost. From the results of Table 2, the block chain cost for data update in proposed solution is almost 13 times lower compared to [27].

5. Conclusion

This work proposes a secure, privacy preserving medical data sharing framework combining hybrid cloud with blockchain. The framework provides more control to data owner in sharing the data at various resolutions to the data user. The sharing consensus is made involving three parties using a light weight authentication mechanism. The computation complexity is atleast 9% lower for data upload and 3.5% lower for data access compared to incremental update solution. The block chain update cost is almost 13 times lower in proposed solution compared to incremental update solution. The communication overhead is also lower in produced solution at 2.5 times for resolution at 50Hertz compared to signal at original resolution of 250 Hz.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Ms.Neelima is the primary author conceptualized, implemented and documented the paper. The second authors guided and reviewed the work.

References

[1] F. Kamalov, B. Pourghebleh and M. Gheisari, “Internet of Medical Things Privacy and Security: Challenges, Solutions, and Future Trends from a New Perspective”, *Sustainability*, Vol. 15, No. 4, p. 3317, 2023.

[2] M. Elhoseny, N. Thilakarathne and M. Alghamdi, “Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions”, *Sustainability*, Vol. 13. No. 21, 2021.

[3] H. Wang, J. Liang and Y. Ding, “Ciphertext-policy attribute-based encryption supporting policy-hiding and cloud auditing in smart health”, *Comput. Stand. Interfaces*, Vol. 84, 2023.

[4] J. Oh, J. Lee and M. Kim, “A secure data sharing based on key aggregate searchable encryption in fog-enabled IoT environment”, *IEEE Trans. Netw. Sci. Eng*, Vol. 9, pp. 4468-4481, 2022

[5] J.Lee; J.Oh andD.Kwon, “Blockchain-enabled key aggregate searchable encryption scheme for personal health record sharing with multi-delegation”, *IEEE Internet Things J*., Vol.11, pp.17482-17494,2024

[6] C.Lai,H.Zhang and R.Lu, “Privacy-preserving medical data sharing scheme based on two-party cloud-assisted PSI”, *IEEE Internet Things J.*,Vol.11, pp.15855-1586, 2024.

[7] O. Kwon, J. Jeongand, B. Kim, “Electrocardiogram Sampling Frequency Range Acceptable for Heart Rate Variability Analysis”, *Healthc Inform Res*, Vol. 24, No. 3, pp. 198-206, 2018.

[8] J. Oh, S. Son and D. Kwon, “Design of Secure and Privacy-Preserving Data Sharing Scheme Based on Key Aggregation and Private Set Intersection in Medical Information System”, *Mathematics*, Vol. 12, No. 11, p.1717, 2024.

[9] Y. Bao, W. Qiu, and X. Cheng, “Secure and lightweight fine-grained searchable data sharing for IoT-oriented and cloud-assisted smart healthcare system”, *IEEE Internet Things J.*, Vol. 9, 2513-2526, 2022.

[10] I. Boumezbeur and K. Zarour, "Privacy Preservation and Access Control for Sharing Electronic Health Records Using Blockchain Technology", *Acta Informatica Pragensia*, Vol. 11, pp. 105-122, 2022.

[11] K. Jastaniah,. N. Zhang and A. Mustafa, "Efficient user-centric privacy-friendly and flexible wearable data aggregation and sharing ", *IEEE Transactions on Cloud Computing*, Vol. 12, pp. 967-982, 2024.

[12] H. Yin.; Y. Zhao and L. Zhang. "Attribute-based searchable encryption with decentralized key management for healthcare data sharing", *J. Syst. Architect*, Vol. 148, 2024.

[13] C. Lai, H. Zhang and R. Lu, "Privacy-preserving medical data sharing scheme based on two-party cloud-assisted PSI", *IEEE Internet Things J*, Vol. 11, pp. 15855-15868, 2024.

[14] H. Pan, Y. Zhang and X. Si, "*MDS*^{2}-*C*^{3}*PF*: A Medical Data Sharing Scheme with Cloud-Chain Cooperation and Policy Fusion in IoT", *Symmetry*, Vol. 14, No. 12, 2022.

[15] C. Xu, C. Fulong and X. Dong, "Design of a Secure Medical Data Sharing Scheme Based on Blockchain", *J. Med. Syst*, Vol. 44, 2020, No.52, 2022.

[16] T. Wang, Q. Wu and J. Chen, "Health data security sharing method based on hybrid blockchain", *Future Gener. Comp. Syst*., Vol. 153, pp. 251-261, 2024.

[17] H. Xiaoyan, S. Xiaoyi and C. Guang, "Efficient sharing of privacy-preserving sensing data on consortium blockchain via group key agreement", *Computer Communications*, Vol. 194, pp. 44-54, 2022.

[18] G. Peng, A. Zhang and X. Lin, "Patient-centric fine-grained access control for electronic medical record sharing with security via dual-blockchain", *IEEE Trans. Netw. Sci. Eng.*, Vol. 10, pp. 2908-3921, 2023.

[19] K. Zhang, Y. Zhang and Y. Li, "A blockchain-based anonymous attribute-based searchable encryption scheme for data sharing", *IEEE Internet Things J*, Vol. 11, pp.1685-1697,2024.

[20] A. Uddin, A. Stranieri and L.Gondal, "Blockchain leveraged decentralized IoTeHealth framework", *Internet Things*, Vol. 9 ,2020.

[21] S. Meisami, Y. Sadafand, A. Melina,"Combining Blockchain and IOT for Decentralized Healthcare Data Management", *International Journal on Cryptography and Information Security*, Vol. 13, No. 1, 2023.

[22] A. Amanat, M. Rizwan and C. Maple, "Blockchain and cloud computing-based secure electronic healthcare records storage and sharing", *Front Public Health*., 2022

[23] J. Yu, B. Yan, H. Qi, Sand W. Cheng, "An Efficient and Secure Data Sharing Scheme for Edge-Enabled IoT", *IEEE Transactions on Computers*, Vol. 73, No. 01, pp. 178-191, 2024

[24] S. A. Sankar and S. Sathidevi, "A scalable speech coding scheme using compressive sensing and orthogonal mapping based vector quantization", *Heliyon*, Vol. 5, No. 5, 2019.

[25] K. Usman, H. Gunawan and A. Suksmono, "Compressive Sensing Reconstruction Algorithm using L1-norm Minimization via L2-norm Minimization", *International Journal on Electrical Engineering and Informatics*, Vol. 10. pp. 37-50, 2018.

[26] L. Wang, L. Meng and F. Liu, "A User-Centered Medical Data Sharing Scheme for PrivacyPreserving Machine Learning", *Secur. Commun. Netw*., 2022.

[27] L. Wang, X. Liu, W. Shao, "A Blockchain-Based Privacy-Preserving Healthcare Data Sharing Scheme for Incremental Updates", *Symmetry*. Vol. 16, No. 1, 2024.

[28] https://physionet.org/about/database/

[29] H. Wang and Y. Song, "Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain", *Journal of Medical Systems*, Vol. 42, No. 8, 2018.

[30] T. Thwin and S. Vasupongayya, "Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems", *Security and Communication Networks*, Vol. 5, pp. 1-15, 2019.