Chelonian Conservation And Biology

Vol. 18 No. 2 (2023) | https://www.acgpublishing.com/ | ISSN - 1071-8443

DOI: doi.org/10.18011/2023.10(2).608.619

Energy-Efficient ECG Data Security Using Sidechain Technology

Sonali Lohbare (Pakhmode)[1*]
Research Scholar, G H Raisoni University, Department of Electronics and Telecommunication Engineering
(Asst Prof, at VPP&VA Sion Mumbai), Amravati-444701, Maharashtra, India.
pakhmodesy@gmail.com

Swati Dixit[2]
Asst Prof, E&TC Department G H Raisoni Institute of Engineering and Technology,
Nagpur Maharashtra, India
swati.dixit@raisoni.net

ABSTRACT

Electrocardiogram (ECG) signals are classified into heart disease categories through the design of high-efficiency signal processing models. These models must be able to perform Pre-processing, Segmentation of signal, Extraction of Feature, Classification, and Post-Processing steps with high efficiency in terms of accuracy and power metrics. To attain this, researchers have proposed the use of reinforcement learning models, that assist in offloading computationally complex tasks on the cloud. Due to this offloading, there are communication vulnerabilities between the ECG sensing device and the cloud data center. To mitigate the different vulnerabilities, researchers have proposed the use of various data security mechanisms, which adds to the computational complexity of the underlying ECG model. This increases the delay needed for communication, thereby reducing the real-time performance capabilities. While maintaining high security, side blockchain-based systems were introduced, which possess characteristics like immutability, transparency, traceability, and distributed computing. However the delay needed for the main blockchain is directly proportional to the chain length, thus they are not suited for big data applications like ECG signal communication. The proposed design of a novel side chain high security and QoS model for energy-aware ECG classification deployments to overcome these issues. While improving security performance making the model highly applicable for extensive variation of health real-time IoT data in which Delay, Energy, Throughput, and PDR are evaluated.

Keywords: ECG, Low Power, WOA, Optimization, Delay, Splitting, Merging, Security, Attacks

I. INTRODUCTION

Secure and low-power ECG classification is multidomain and involves the design of low-power models for signal acquisition, pre-processing, segmentation, feature extraction, and classification, combining them with high-security communication interfaces. To design such a model, researchers [1] need to identify system thresholds in terms of maximum processing delay, communication delay, and energy network classified as heart diseases using the CNN model, to perform final classification [2], the handling of large generated IoT data and increase traffic while data transmission from wearable IoT devices application challenges like security, malicious attacks, and data transmission delay have become major issues [3]. Pre-trained CNN model with real-time continuous updates using an incremental learning process. The complexity of the model directly depends upon the encryption and classification methods [4], which limits the model's scalability. To reduce this complexity, while maintaining high security and QoS blockchain-based systems were introduced. But the delay needed to add new blocks to blockchains is directly proportional to the chain length, thus they are not suited for big data applications like ECG signal communication. A survey of similar models along with their advantages, limitations, and future research issues is discussed in the next section. This is followed by section 3, wherein the design of a novel side chain-based high side chain-based energy aware ECG classification deployments are discussed. This model is evaluated under different types of ECG signals, and different types of network attacks in section 4. The performance of the proposed model facilitates real-time deployment applicability. Finally, the proposed system concludes with observations and further improves patient data.

II. RELATED WORK

The proposed research work has discussed distributed cloud architecture based on blockchain IoT devices. A wearable IoT-cloud device has a flexible architecture used for data storing, classification, and analysis in one place and reduces end delay and computational energy. Blockchain keeps the patient's records and deals with the current time to each block, Identification, and hash code. Existing Deep Learning Algorithms and sidechain-based blockchain approach networking in the central place of data storage as a cloud environment are unable to meet the Quality of Service (QoS) like Recognition Verification, and security needs of healthcare wearable IoT devices and applications [5]. To improve healthcare data efficiency, Blockchain plays a vital role in handling IoT data quality and security to avoid the duplication of unique data storage forms [6]. The author has proposed a blockchain-based time tracking and monitoring of the location assuring the good quality of medicine using the supply chain [7]. Decentralized and distributed end-to-end security service provided by blockchain technology is secure and provides patient-related real-time data that can be accessed by multiple physicians at different locations. The author has discussed specific issues that arise from centralized data storage are increased computations of health data, slow access to medical data, and the lack of interoperability of the system, which provided security during the transmission of health information to the cloud. This reduces the data transmission delay during the analysis and validation process. In [8] this paper author has proposed a novel system called Bee Keeper based on the Ethereum blockchain, a cloud server processes the data to minimize delay and network traffic, of IoT. In [9], the authors proposed a blockchain-based architecture in the Fog Computing environment for the Internet of Everything. Fog Computing-based Blockchain Architecture Network (BFAN) proposed for the Internet of Everything. For data sharing in a trusted and secure way. The author has proposed the SETNet(Secure Networking) architecture network paradigm for storing real-time data storing and sharing with the help of Blockchain AI algorithm analysis of heart disease in the health care system [10]. Due to its reliability, blockchain technology has been widely used in a diversity of contexts, including the administration of data for insurance and financial transactions, as well as that of healthcare information. Med Rec, a blockchain-based access and authorization management system for medical data, was suggested by [11]. When it comes to the administration of Electronic Medical Records, authentication, confidentiality, accountability, and data exchange are among the most important factors. Due to the decentralized nature of blockchain technology, providing security of Electronic Medical Records (EMRs) is made possible. The authors highlight the benefits of employing blockchain technology for storing and administrating biological and healthcare data. On the other hand, the instances in which Internet of Medical Technology devices are used were not taken into account in the aforementioned publications [12]. The authors [13] presented different smart healthcare systems, based on the blockchain, each a unique WBAN that required maximum capacity and processing latency required to attain consensus, while the back end provides a trustworthy environment using blockchain technology. The proposed article offers a main blockchain IoT healthcare system with many stages. Here computational capacity increases while reducing processing time, but it also offers an environment that is trustworthy and secure for the transport and storage of data for intelligent healthcare systems [14]. A limited number of security models for ECG systems are elaborating on security performance. A design of a side-chain-based high-security model for energy-aware ECG classification deployment is proposed in this article.

III. METHODOLOGY

A. Proposed side-chain-based high-security model for energy-aware ECG classification

To improve QoS, most of the models discuss splitting the central blockchain into fixed or variable-sized length sidechains, which limits their scalability. This is because the formed sidechains are always increasing, and it becomes computationally complex to manage them after a certain point. For ECG-based storage and communication networks, instantaneous information is more relevant than temporal data. Thus, this section proposes the design of a WOA (Whale Optimization Algorithm) based sidechain generation model, that overcomes the limitation of static sidechain models.

Based on the model initialized the current blockchain's performance with reference to metrics of security and QoS, and based on this performance decisions are taken to either split or merge existing blockchains.

In Figure 1 the overall flow of the proposed side-chain model is depicted, wherein the WOA layer along with blockchain split and merge operations can be observed. The model analyses currently stored ECG data blocks and performs a wide variety of checks on them, which assists in continuous performance and security optimizations. The WOA model uses energy efficiency, delay for mining, and security metrics to estimate chain splitting and merging decisions. To further contemplate the model's design, and segregate it into multiple sub-parts. The model design is segregated into multiple subparts and each part is discussed in a different sub-section.

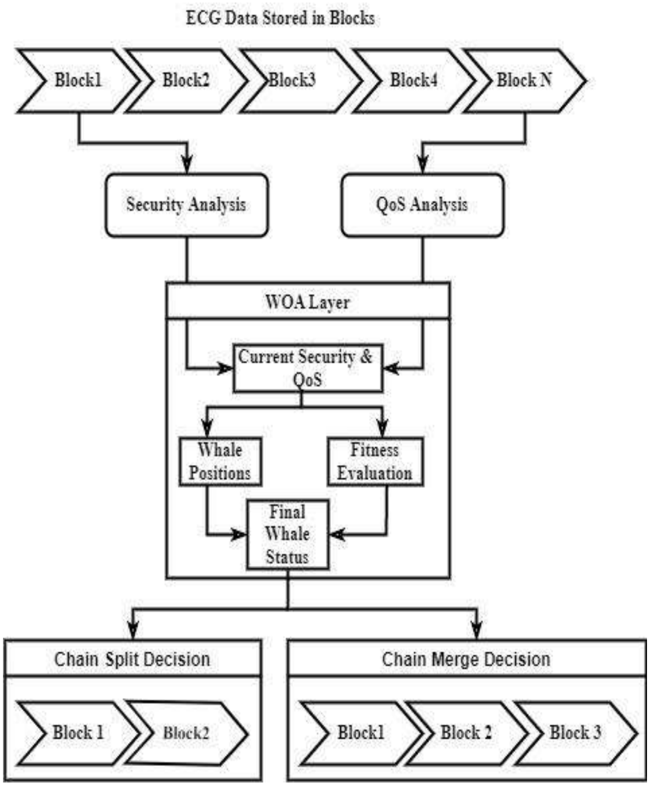


Figure 1 Overall Flow of the proposed sidechain model

B. Initial QoS and Security performance evaluation layer

Before making decisions about merging or splitting the blockchain, the security and QoS metrics are analyzed. This analysis involves the initiation of honeypot requests, which do not affect the actual blockchain but assist in estimating the QoS and security performance. To accomplish this the following process is used. A group of N honeypot ECG data storage is initiated, with random ECG signals. These are divided into normal (N_r) and malicious (M_r)

using a Markovian process, that uses for the generation of random numbers using Equation (1)

$$Nr=RAND(L), Mr=RAND(L) \qquad (1)$$

Where L represents the current length of the blockchain. The malicious requests are segregated into, Distributed Denial of Service (DDoS), Man-in-the-middle (MiTM) attacks, Sybil attacks, Wormhole attacks, Spoofing attacks, and Masquerading attacks.

This is performed by use of the Markovian process, which assists in depicting real-time attack behavior. These attacks are performed on the blockchain, and the performance of Quality of Service (QoS) is evaluated in terms of computational Delay, residual Energy for communication, PDR (Packet Delivery Ratio), and performance of throughput. These metrics are evaluated under attack, and non-attack scenarios to estimate the performance of the blockchain model.

For instance, communication delay under attack requests D(A_r), and communication delay under normal requests D(N_r) is evaluated using Equations (2) and (3) as follows,

$$D(A_r) = \frac{\sum_{i=1}^{M_r} ts_{e_i} - ts_{s_i}}{M_r} \qquad (2)$$

$$D(N_r) \quad = \quad \frac{\sum_{i=1}^{N_r} t_{e_i} - t_{s_i}}{N_r} \qquad (3)$$

Similarly, the energy required to store these blocks for normal and attack requests is evaluated using Equation (4) and (5) as follows

$$E(A_r) = \frac{\sum_{i=1}^{M_r} E_{s_i} - E_{e_i}}{M_r} \qquad (4)$$

$$E(N_r) \quad = \frac{\sum_{i=1}^{N_r} E_{s_i} - E_{e_i}}{N_r} \qquad (5)$$

Continuing on the same principle, throughput during storage is evaluated using Equation (6) and (7) as follows,

$$T(A_r) \ = \sum_{i=1}^{M_r} \frac{P_i(Rx)}{M_r * D(A_r)} \qquad (6)$$

$$T(N_r) = \sum_{i=1}^{N_r} \frac{P_i(Rx)}{N_r * D(N_r)} \qquad (7)$$

While, packet delivery ratio for these requests is evaluated using Equation (8) and (9) as follows,

$$PDR(A_r) = \sum_{i=1}^{M_r} \frac{P_i(Rx)}{P_i(Tx) * M_r} \qquad (8)$$

$$PDR(N_r) \; = \sum_{i=1}^{N_r} \frac{P_i(Rx)}{N_r * P_i(Tx)} \qquad (9)$$

Where, t_s, t_e represents timestamp values during start and end of storage operations, E_s,E_e represents residual start and end energy levels of nodes that have initiated the requests, P(Tx) and P(Rx) represent number of transmitted and received block packets during storage of these blocks. Using these metrics, a QoS to Security rank (QSR) is evaluated using Equation (10), where performance under attack is correlated with performance for normal blockchain operations.

$$QSR = \frac{1}{4} * \left[\frac{D(N_r)}{D(Ar)} + \frac{E(N_r)}{E(Ar)} + \frac{T(Ar)}{T(N_r)} + \frac{PDR(A_r)}{PDR(N_r)}\right] \qquad (10)$$

For a secure blockchain with high QoS performance, the $QSR \cong 1$ condition must be satisfied. If this condition is fulfilled, then ECG data is stored on the current blockchain, else WOA model is initiated for either merging or splitting existing blockchain with previously stored sidechains. Design of this model is discussed in the next subsection.

C. The WOA layer for optimization of sidechains

The WOA layer is activated whenever QSR performance is not satisfactory. This indicates that either the currently used blockchain needs to be split into two different parts, or it needs to be merged with existing blockchains. To estimate this decision, the following WOA model is used, Initialize WOA parameters, Number of rounds (NR), Number of whales (NW), Circling rate (CR),Current Number of sidechains(Nsc), Length of each side chain(Lsc).Generate initial whale population by repeating the following process for NW rounds. Select a random sidechain from the current list of sidechains, and generate a random number of requests (NRANDOM) for block addition to this chain. Separate these requests into normal and malicious ones, and evaluate security and QoS performance for each request using Equation (2) to (10) . Based on these metrics, evaluate Whale fitness using Equation (11)

$$f_w = \frac{\left[\sum_{i=1}^{N_{RANDOM}} QSR_i - \sum_{j=1}^{N_{RANDOM}} \frac{QSR_j}{N_{RANDOM}}\right]}{N_{RANDOM}} * \left[\frac{D(N)-D(A)}{D(A)} + \frac{E(N)-E(A)}{E(A)} + \frac{T(A)-T(N)}{T(N)} + \frac{PDR(A)-PDR(N)}{PDR(N)}\right] \quad (11)$$

Based on this process, initial whale population is generated and iterated over different rounds. To perform this task, initially a Whale fitness threshold is estimated using Equation (12)

$$f_{\ th} = \frac{\sum_{i=1}^{N_R} f_{w_i} * C_r}{N_W} \quad (12)$$

Once the threshold f_{th} is evaluated, then perform each round in 1 to $\mathrm{N_R}$ and each whale in 1 to N_W . If this whale's fitness is lower than f_{th}, then this whale is near to an optimum solution, thus it can be skipped. Else, Modify this whale's circling capability via the following process,

Replace the existing sidechain with a stochastic sidechain from the current list of sidechains, and generate a stochastic number of requests (N_{stoch}) for block addition to this chain. Segregate these requests into normal and malicious, and update this Whale's fitness levels. Whale with minimum fitness is marked as a 'Hunter' whale, and based on this whale's fitness, circling rate is modified as per Equation (13)

$$New(C_r) = Old(C_r) * N_w \frac{Min\left(\cup_{i=1}^{N_w} f_{w_i}\right)}{\sum_{i=1}^{N_w} f_{w_i}} \quad (13)$$

If decision to split the chain is recommended by WOA, then, current sidechain is divided into two equal parts. Value of QSR is evaluated for these chains using Equation (10), and is used to select the sidechain with higher QoS and better security performance.

Using these QSR levels, a selection threshold is evaluated using Equation (14) as follows.

$$Sel_{th} = \frac{QSR_{SC1}}{QSR_{SC2}} \quad (14)$$

Where, SC1 and SC2 represent equal sized sidechains 1 and 2 respectively. If $Sel_{th} > 1$, then sidechain 2 is used as the current sidechain, while existing sidechain is merged with the main blockchain, else the same process is followed for sidechain 1, and it used to add future ECG storage blocks. Using these split and merge operations, blockchains are created for ensuring optimum QoS and security performance for ECG storage applications.

IV. RESULT AND DISCUSSION

The proposed Side Chain Based High Security Model for Energy Aware ECG Classification (SCHSE2CG) model uses a combination of WOA with continuous QoS and security analysis to improve attack flexibility while storing ECG data. To evaluate its performance, simulation on standard ECG dataset storage was needed. To obtain the standard ECG datasets MIT-BIH and PTBXL were used, and incrementally stored using the proposed sidechain-based model.

Table I. ECG Storage Delay performance for different nodes over 1000 ECG blocks

Num. of Storage Blocks	***Delay (ms)***	***E (mJ)***	***Thr. (kbps)***	***PDR (%)***
100	0.22	4.42	656.82	98.75
150	0.28	4.70	676.61	98.95
200	0.36	4.91	695.41	99.10
300	0.44	5.08	702.92	99.18
400	0.51	5.31	709.37	99.25
500	0.59	5.65	687.99	99.35
600	0.66	5.97	695.41	99.45
800	0.71	6.22	702.92	99.57
1000	0.79	6.45	709.37	99.65

For each storage request, standard QoS and security parameters evaluation was done in terms of End-to-End storage Delay, Energy consumption during each storage, PDR (Packet Delivery Ratio) and throughput obtained for all storage requests. Each of these computations were done for storing 100 to 1000 different blocks. For varying number of storage nodes, based on these conditions. Table I represents delay, Energy, Throughput, PDR performance for five different storage nodes.

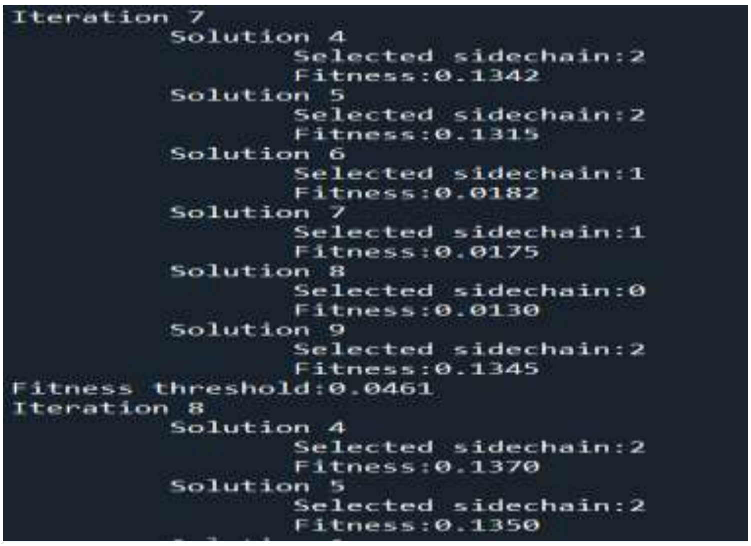
Table I, shows that end-to-end delay has been reduced. Energy required for storing the blocks has been reduced. This is due to use of end-to-end delay metrics and use of residual energy metrics while selection of hunter whales for splitting and merging the sidechains.

This improvement allows the system to be applied for real-time use like low-powered ECG storage applications. Similarly, Performance evaluation in terms of throughput and Packet Delivery Ratio metrics is managed. The performance shows that the proposed model is capable of high QoS and high security ECG storage applications. Similar evaluations were done for the storage model under different attack types. Evaluation of security performance is done as follows. In Healthcare sector data security is possible using blockchain, the model is capable of mitigating different storage attacks. To test these capabilities, QoS performance, evaluations were done for energy and delay, for different with-attack and without-attack. The results are calculated in Table II by varying the number of nodes for the following different scenarios.

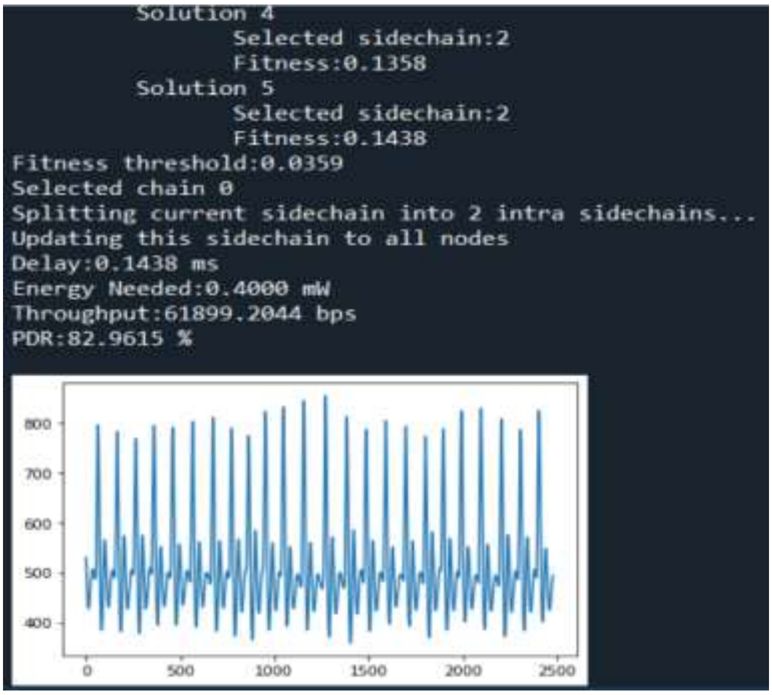
Table II. QoS Performance for 1000 and 10K ECG storage blocks for different types of attacks

Types of Attacks*	**1000 ECG storage blocks**		**10k ECG storage blocks**	
	Delay (ms)	***Energy (mJ)***	***Delay (ms)***	***Energy (mJ)***
MT	0.2	70.93	3.64	10.16
SpT	0.35	40.93	2.5	16.65
SpyT	0.26	31.28	4.35	8.93
NT	0.7	19.81	3.61	11.99
MA	0.3	652.53	2.66	46.12
SpA	0.74	184.26	3.04	15.2
SpyA	1	692.29	2.89	15.14
NA	3.77	91.3	3.14	109.66

*Note: T sands for with attack and A for without attack of proposed model.



```
Iteration 7
          Solution 4
                  Selected sidechain:2
                  Fitness:0.1342
          Solution 5
                  Selected sidechain:2
                  Fitness:0.1315
          Solution 6
                  Selected sidechain:1
                  Fitness:0.0182
          Solution 7
                  Selected sidechain:1
                  Fitness:0.0175
          Solution 8
                  Selected sidechain:0
                  Fitness:0.0130
          Solution 9
                  Selected sidechain:2
                  Fitness:0.1345
Fitness threshold:0.0461
Iteration 8
          Solution 4
                  Selected sidechain:2
                  Fitness:0.1370
          Solution 5
                  Selected sidechain:2
                  Fitness:0.1350
```



```
          Solution 4
                  Selected sidechain:2
                  Fitness:0.1358
          Solution 5
                  Selected sidechain:2
                  Fitness:0.1438
Fitness threshold:0.0359
Selected chain 0
Splitting current sidechain into 2 intra sidechains...
Updating this sidechain to all nodes
Delay:0.1438 ms
Energy Needed:0.4000 mW
Throughput:61899.2044 bps
PDR:82.9615 %
```

Observations

Figure 2 screen shots of console of proposed model

The above Figure 2 shows that how to split the blockchain, based on selecting parameters like number of iteration and fitness function. Select the sidechain for storing the health data in particular chain number. The proposes a novel healthcare data of patients are stored at center place location. The scalability and interoperability of side Blockchain technology will allow the doctors to view the details of patients' data records and to provide instant healthcare services. Blockchain provide safety in health data and addresses valid medication and the require QoS guarantees.

V. CONCLUSION AND FUTURE SCOPE

The proposed sidechain model uses a combination of QoS and security analysis, with WOA for optimization of ECG storage applications. Due to the use of these models, the proposed SCHSE2CG method is able to reduce End-to-End Delay, and consumption of energy, while improving throughput, and PDR (Packet Delivery Ratio) performance. This performance was evaluated under different attack scenarios, which makes the model highly applicable for a large variety of ECG storage deployment scenarios. It was noticed that the proposed model was able to mitigate Spoofing, Spying and MiTM like different attacks with high QoS performance. Evaluations done for PDR and energy consumption showcased a similar trend. Due to this improvement, the proposed sidechain base security model is deployable for a wide variety of clinical applications, that require higher QoS and better security for storing ECG signals. This performance is further improved using of a single central blockchain for archival, which assists in lowering computational complexity while searching older records. In the future, performance of model can be validated multiple types of blockchains, which will assist in estimating its deployment capabilities. Moreover, existing model performance via the use of deep learning and Q-Learning-based approaches for covering large-scale deployment scenarios.

VI. REFERENCES

[1] Tyagi A., Mehra R., “Intellectual heartbeats classification model for diagnosis of heart disease from ECG signal using hybrid convolutional neural network with GOA”. Appl. Sci. 3,265 (2021). DOI:10.1007/s42452-0210-4185-4.

[2] Lohbare Sonali, Dixit Swati “Elimination of Noise from Ambulatory ECG Signal using DWT” International Journal of Engineering Trends and Technology Volume 70 Issue 5, 266-273, May 2022 ISSN: 2231-5381/IJETT-V70I5P229 © 2022 Seventh Sense Research Group® DOI:10.14445/22315381/IJETT-V70I5P229

[3] Lohbare Sonali, and Swati Dixit. "Wearable Heart Disease Identification with Convolution Neural Networks." Journal of Optoelectronics Laser 41.7 (2022): 289-298.

[4] C. Ju, D. Gao, R. Mane, B. Tan, Y. Liu and C. Guan, "Federated Transfer Learning for EEG Signal Classification," 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), 2020, pp. 3040-3045, DOI: 10.1109/EMBC44109.2020.9175344.

[5] Lohbare Sonali P., Swati Dixit, “End-to-End Supporting System for IoT Applications:Survey." ICCCE 2021. Springer, Singapore, 2022. 931-939.

[6] Thomas McGhin, Kim-Kwang Raymond Choo, Charles Zhechao Liu, Debiao He. "Blockchain in healthcare applications: Research challenges and opportunities”, Journal of Network and Computer Applications, 2019

[7] Xinlai Liu “Blockchain-based smart tracking and tracing platform for drug supply chain” Computers & Industrial EngineeringSeptember2021-107669

[8] Lijing Zhou et.al. BeeKeeper: “A Blockchain-Based IoT System with Secure Storage andHomomorp-13hicComputation”.2169-353IEEEdoi 10.1109/access .2018.2847632.

[9] Saurabh Shukla, Subhasis Thakur, Shahid Hussain, John G. Breslin, Syed Muslim Jameel, “Identification and Authentication in Healthcare Internet-of-Things Using Integrated Fog Computing Based Blockchain Model”,Internet of Things,Volume 15,2021,100422,ISSN 542-6605.

[10] Kai Wang *et. al*. Securing Data with Blockchain and AI, IEEE Volume 7, 2019 DOI:2169- 9 10.1109/ACCESS.2019.2921555

[11] Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Accessand Permission Management," 2ndInternational Conference on Open and Big Data, pp.25- 30, DOI:10.1109/.2016

[12] J. Wang et al., "A Multistage Blockchain- Based Secure and Trustworthy Smart Healthcare System Using ECG Characteristic,"in IEEE Internet of Things Magazine, Vol4, no.3,pp.4858,September 2021,DOI:10.1109 /IOTM. 101.2000182.

[13] M. S. Pioner, L. Ignaczak, B. L. Dalmazo, E. d. S. Júnior and J. C. Nobre, "An Electrocardiogram-based Authentication Implementation Integrated with the Blockchain", 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 974-979.

[14] Zdravkovi Nemanja and Kumar, Vijay and Pavithraa, S and Harithaa, S. “A Web Deployment of Secured ECG Signal Medical Record Transactions using Blockchain” Annals of the Romanian Society for Cell Biology.25 19937 – 19951PP-2021