Enhancing Security in IoMT: A Blockchain-Based Cybersecurity Framework for Machine Learning-Driven ECG Signal Classification

Aya Hamid Ameen[1], Mazin Abed Mohammed[1,*], Ahmed Noori Rashid[1]
[1]Computer Science Department, College of Computer Science & Information Technology, University of Anbar, Anbar, Iraq
Emails: aya21c1006@uoanbar.edu.iq; mazinalshujeary@uoanbar.edu.iq; rashidisgr@uoanbar.edu.iq

Abstract

The Internet of Medical Things (IoMT) revolutionizes healthcare, enhances patient care, and optimizes workflows. However, the integration of IoMT introduces concerns related to privacy and security. In addressing these issues and aiming to bolster privacy and data security, this study presents a novel cybersecurity framework based on blockchain (BC) technology. The primary goal is to ensure secure communication among IoMT devices, preventing unauthorized access and tampering with sensitive data. The proposed framework is implemented in a model designed for classifying electrocardiogram (ECG) signals, utilizing two datasets: a Medical Technology Database (MTDB) with a limited sample size and the Massachusetts Institute of Technology–Beth Israel Hospital (MITBIH) dataset with a more extensive sample size. The datasets are subsequently partitioned into training and testing data. Feature extraction and selection are performed using the Pan-Tomkins and genetic algorithms. To enhance security, BC technology is employed to encrypt the test data. Finally, signal classification is performed using the support vector machine (SVM) classifier. Thus, the model trained on the MITBIH dataset outperforms its small data counterpart, achieving an impressive accuracy rate of 99.9%. Additionally, the model exhibits a true positive rate (TPR) and true negative rate (TNR) of 100%, an F-score of 100%, and a positive predictive value (PPV) of 100%.

Key words: Internet of Medical Things; Blockchain; support vector machine; ECG; Cybersecurity.

1. Introduction

The Internet of Medical Things (IoMT) is crucial to developing long-term healthcare infrastructures. The IoMT significantly impacts healthcare since it allows for the monitoring and verification of patient medical information before its transfer to a cloud network for use in the future. Since the IoMT is a rapidly expanding big-data platform, all information must be kept safe and secure. Specifically, sensors and linked systems allow the healthcare industry to streamline administrative tasks, improve patient treatment quality, and keep tabs on their health from afar [1]. By bridging the gap between the digital and real worlds, IoMT improves patient health by reducing the time between diagnosis and treatment and allowing real-time behavioral and environmental adjustments to improve outcomes [2]. Significant effects on patients and healthcare providers are expected from the integration of medically relevant technology [3].

Due to the IoMT's fast expansion and diverse character, protecting it becomes a formidable problem, especially as new and more pervasive forms of cybercrime emerge [4]. To guarantee data consistency, validity, legality, and secrecy, data protection is defined as the capacity to store and convey data without permitting unwanted access [5]. The private data is only accessible to those who have been granted access. Cybercrime develops and routinely affects hospitals and sensors due to unauthenticated individuals and their unlawful access. Many parts of the healthcare business collect, transmit, and share a great deal of IoMT data [6]. Ensuring data transmission security is of utmost importance [7]. This enormous data processing mechanism is directly responsible for the cyberattack's meteoric rise. Therefore, a safe framework is required to protect medical information stored in the IoMT [8]. According to this research, blockchain (BC) technology may be used to create an IoMT more trustworthy and dependable architecture. BC is a decentralized database that allows for transactions and communications amongst entities whose reliability is questionable. Untrustworthy third parties can conduct cloud-based transactions using BC technology [9]. BC monitors and analyzes data from several sources via a decentralized database architecture.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

The distributed ledger uses cryptography to link its blocks. Information blocks recorded on the BC distributed ledger cannot be altered or removed [10], [11].

These days, many programs are moving away from being installed on a computer's hard drive and instead are being made available online [12]. For instance, in COVID-19 [13], many individuals prefer to keep tabs on their health without leaving the house. IoMT is a reliable system via which several healthcare apps and servers may provide various healthcare services to remote users. Live doctor-patient checkups, remote electrocardiogram (ECG) monitoring, and similar services are only a few examples [14]. Healthcare sensors, wireless networks, and the cloud are only a few examples of the technologies that comprise the IoMT mechanism [15]. IoMT technologies are separated into distinct levels, such as the user layer, which links application sensors; the wireless layer, which hosts numerous Internet-based technologies; and the cloud layer, which houses more servers and virtualization [16]. However, IoMT data processing between layers and technologies is only possible with adequate cybersecurity [17]. Various body area networks can connect to many medical care sensors in the framework and freely move around without any risk to their health, gratitude to the IoMT cloud-enabled BC [18].

Malware assaults, denial of service attacks (DoS), phishing, unauthorized data access, Structured Query Language (SQL) injections, and many other forms of cybercrime are severe. These challenges can significantly impact the quality of care provided to patients by medical apps in the IoMT architecture and system. These cyber security challenges are crucial and distinct from those that have previously arisen. The server, the wireless network, and the software must be secure against malicious software, viruses, and other threats, respectively. Information on known cyber assaults on data may be found with little effort in the network. However, when they are unknown and present at distinct levels of the IoMT mechanism for medicinal apps, they cause serious problems [19].

Several BC technologies exist, such as Ethereum Hyper-ledger [20], which improve the security performance of IoMT apps. There are substantial processing costs since no existing BC framework can handle the security and validation requirements of the IoMT. This study introduces a cybersecurity framework based on BC technology. It aims to improve the security and privacy of healthcare apps that use IoMT by creating a lightweight, adaptable, and intelligent framework that can spot and stop hackers and keep data safe through BC. The main contributions of this study are:

- To create an optimized framework for the IoMT that incorporates AI and is specifically designed for medical purposes, it is necessary to include blockchain technology to enhance data security and prevent unauthorized access.
- To propose a preprocessing stage using Pan Tompkins ECG QRS Detector and training dataset. Bandpass filtering (5-15 Hz) filters out non-heart-related frequencies, while another filter emphasizes the QRS complex, and the signal is squared.
- Recommend signal averaging and sample rate tuning for noise reduction in ECG data. Employ a Genetic Algorithm (GA) with random strategies to identify features, evaluating success through improved model accuracy.
- To propose that a Bitcoin timestamp server is used to mimic a peer-to-peer electronic currency system and store mock data. By gathering together and broadcasting recently processed transactions in the form of blocks, nodes ensure that all data is accurate and reliable
- To classify the ECG QRS data using a Support Vector Machine (SVM), the SVM is used to classify test transactions. The characteristics retrieved from the data will likely be used to categorize the transactions.

The rest of this study is organized as follows: **section 2** presents the related work, **section 3** presents the study methodology, **section 4** presents results and discussion, and **section 5** presents the conclusion and future works.

2. Related Work

The IoMT is at the forefront of emerging technologies such as wearable sensors, data analytics, and telemedicine. IoMT significantly impacts society by improving healthcare outcomes, reducing costs, and increasing access to healthcare services. Because IoMT systems are susceptible to cyberattacks, healthcare facilities and patients face privacy and security issues. The lack of strong security measures vs cyber-attacks has made healthcare equipment security and patient privacy persistent worries. Existing cyber-health solutions are less appealing due to security flaws. The detection of fraud and improving security in the IoMT have been the subject of numerous recent research studies. Lakhan et al. (2021) [1] introduced a framework for IoMT based on a deep neural network (DNN). and assumed that the mobile device, the wireless network, and fog are layers in the DNN that take data from the tasks and train them. The training model decides offloading based on the service's location and mobility. After that, the tasks are scheduled in two stages: the first is a topological sort, and then the tasks are scheduled. Results from the tests show an outperformance in response times and energy consumption. However, this research does not address resource allocation and security allocation. Lin et al. (2021) [21] proposed a scheme for securely offloading tasks and allocating resources by integrating BC into the virtual reality-enabled remote healthcare system. where the collective reinforcement learning (CRL) algorithm is used to maximize the long-run reward and to allocate resources adaptively based on requirements. The evaluated results are better in terms of security and stalling rate. However, this research does not solve network failure and mobility services for IoMT apps. Dinh C.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

Nguyen et al. (2021) [22] propose a new decentralized health architecture based on smart-BC technology with a mobile edge cloud for offloading and sharing privacy-aware data. The evaluations showed strong system security and low latency. but ignore security, such as timestamp reliance, server-caused authorization fake, and smart-contract reentrancy attacks. Lakhan et al. (2021) [22] Created a cost-effective task scheduling algorithm based on smart contracts for the IoMT system, consisting of stages: smart contract stage, task sequencing, resource matching, and task scheduling. Based on evaluation results, the proposed IoMT system is cost-effective and safe for distributed healthcare infrastructure. However, it fails to balance implementation costs and deadlines. Lakhan et al. (2021) [23] presented a BC-enabled framework for cost-effective task scheduling. The framework has three steps: function validation, deadline-based task scheduling, and app cost reduction using an iterative heuristic. Based on the test results, data validation and security improved by 10%, and app costs decreased by 30%.
However, neither mobility services nor resource failure were addressed. Furthermore, Lakhan et al. (2021) [24] provide a framework that supports a novel DRL and BC for the IoMT. It consists of offloading tasks based on the DRL policy and scheduling the BC tasks with the sequence of tasks and methods of matching the research. The simulation results reduced the communication/computation time for each system application. But ignore the identification of anomalies and security attacks. And cannot identify anomalies. Lakhan et al. (2021) [25] create robotic schemes inspired by the ankle joint in an IoMT environment supported by BC-enabled computing nodes. The deep reinforcement policy works to schedule all tasks at different periods, and the BC validates and secures transactions in the IoMT environment. The simulation results showed that the methods used reduced the service cost by 50% and the mining cost by 40%. but not focus on deadlines for tasks and not discover anomalies. Time, do not focus on deadlines of task scheduling, and do not discover anomalies. Lakhan et al. (2022) [19] Create an effective BC-enabled cybersecurity framework for medical apps where both types of malware, known and unknown, are detected. The cost of implementation and cyber security are the study's objectives. This framework reduces the cybersecurity data validation cost by 33% and cuts the security execution cost by 50%. This research considers numeric data cyberattacks only, while mobile, fog, cloud, and network cyberattacks are ignored. Lakhan et al. (2022) [26] devised an IoMT privacy and security framework based on novel federated learning (FL) and BC that can detect fraud for healthcare apps in the cloud-backed network to reduce security risks, delays, deadlines, and energy. According to the framework results, it reduced delays by 28% and energy usage by 41%. However, unknown attacks (run-time and dynamic) aren't considered. Lakhan et al. (2022) [27] introduced a secure and cost-effective scheduling system in a serverless computing environment for IoMT-enabled BC technology to detect real-time diseases via various sensors. The sensor tasks are offloaded to the system, which processes the request according to priority. Simulation results show that it decreases security risk by 33%, execution cost by 42%, and latency by 52%. However, it has not focused on energy-saving blockchain operations for healthcare apps. LIU et al. (2022) [28] provide an energy-saving and secure IoMT system. BC technology was adopted to address the security problem. In addition, the DRL algorithm was used to improve security performance and energy efficiency. Simulation results show that the proposed approach balances energy efficiency and security issues. However, latency and operation in real-time remain unaddressed. Lakhan et al. (2022) [29] provided a BC-enabled framework based on the programming of sockets for healthcare (e.g., heartbeat and teleconsultation). It encrypts and decrypts based on asymmetric rules as BC's Proof of Work (PoW) is integrated into socket programming and node validation. The simulation showed that the proposed socket reduced service costs by 40%, blockchain costs by 49%, and storage costs by 23% for healthcare apps. However, it did not address energy consumption within the frame of IoMT. Ahmed et al. (2022) [30] introduced a framework for IoMT apps based on the programming of sockets with a BC-enabled network. So, they introduced a hybrid offloading method to enable a PoW method and ensure security and privacy within the app framework. Simulation results show that the proposed socket reduces service and blockchain costs and meets deadlines and security requirements. However, it failed to deal with issues like power consumption within the IoMT frame. Lakhan et. al (2022) [31] presented a cost-effective and secure IoMT processing model based on a restricted Boltzmann machine (RBM). by using an algorithm based on Rivest Shamir Adleman (RSA). The results showed that the methods used are more secure and less expensive for apps compared to other methods. However, it fails to deal with protection against dynamic cyberattacks and mobility. Lastly, Lakhan et al. (2023) [32] They designed a framework for DRL-aware, BC-based task scheduling. An agent policy helps move work from mobile devices to fog and cloud nodes. PoW is used to verify data validation and security between different nodes. The statistical analysis results show that the algorithm used is flexible and meets configuration, privacy, and security requirements. But, not handling energy use, the cost of electricity. The summary on the related work summarized in Table 1.

Table 1: Summary on the related works

Study/ Year	Method	Dataset	Objective	Strengths	Weaknesses
Lakhan et. al (2021)	DNN	General healthcare	Min. cost	Cost, Energy	One of the limitations is that sensitive medical data requires

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

[1]					privacy to be addressed. Additionally, integrating deep learning into systems of healthcare calls for expertise and resources. And, allocation of resources, Security, are not addressed in this research.
Peng Lin et.al (2021) [21]	CRL BC	General healthcare	Min stalling rate	Security.	Combining BC and reinforcement learning may require extensive expertise and resources, that might be difficult for some medical organisations. And network failure and mobility services for IoMT apps are not solved in this research.
Nguyen et. al (2021) [22]	BC	Cerebellar disease	Min. latency	Security, and latency	Healthcare systems may face difficulties implementing a decentralized architecture due to the high cost and complexity of doing so when utilising BC technology and mobile edge computing.
Lakhan et. al (2021) [33]	Smart-BC	ECG	Min. cost	Security	Some medical organisations may find it difficult to integrate BC, smart contracts, and fog computing into their systems since they may need extensive expertise and resources. Also, it fails to balance implementation costs and deadlines.
Lakhan et. al (2021) [23]	BC	ECG	Security. Min. cost	Security	It requires a lot of resources and experience to integrate BC technology and serverless computing. And, neither mobility services nor resource failure were addressed.
Lakhan et. al (2021) [24]	DRL BC	ECG	Min. makespan	Time. Security	The study handles data validation between nodes. However, no anomalies can be identified. and face difficulties in dealing with resource allocation and distribution. And, ignore the identification of anomaly being and security attacks. And cannot identify anomalies.
Lakhan et. al (2021) [25]	DRL BC	Heartbeat (HB)	Min blockchain cost	validation	The study still has difficulties striking a in discover anomalies.
Lakhan et. al (2022) [19]	BC	ECG	Min.cost	Security, Cost	Compared to traditional techniques, a system may have a greater latency rate, making it unsuitable for real-time applications in medical contexts. additionally, numeric data cyberattacks are considered only, while mobile, fog, cloud, and network cyberattack are ignored.
Lakhan et. al (2022) [26]	FL and BC	ECG	Privacy. Min. energy consumption and delay.	Security. Reduce energy consumption	Unknown attacks aren't taken into account.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

Lakhan et. al (2022) [27]	BC	ECG HB	Min. risk, and latency	Security. Min execution and latency	The study did not focus on energy-saving blockchain operations for healthcare apps. furthermore, increases energy consumption which reduces the IoMT system's overall cost-efficiency.
LIU et. al (2022) [28]	DRL BC	Covid-19	Security, energy consumption	Security Reduce energy consumption	Ignored latency. real-time operation unaddressed.
Lakhan et. al (2022) [29]	BC	ECG	Min the cost of services, and blockchain security.	Security	The use of socket RPC and BC technology increases resource consumption, such as energy and computational power, which have an influence on the overall efficiency, and environmental performance of the IoMT framework.
Ahmed et. al (2022) [30]	BC	ECG	Security.	Security	It proposed a serverless processing cost framework that bills clients based on the duration of execution, with monthly, weekly, hourly and on-demand prices available. While this unique technique has the potential to reduce processing costs for medical apps, but it emphasises the significance of careful monitoring and adjusting of the cost framework to ensure efficient and fair resource allocation.
Lakhan et. al (2022) [31]	RBM RSA	General healthcare	Min. services cost	Security	Training model typically necessitates significant computational resources and time. This is especially difficult in edge computing contexts with limited resources, especially when dealing with healthcare data real-time. additionally, there is lack of protection against dynamic cyberattacks.
Lakhan et. al (2023) [32].	DRL BC	General healthcare	Min. makespan	Security, and privacy.	The proposed system isn't always able to support real-time medical apps in their entirety due to possible delays in workflow execution among different computing nodes. Immediate processing is required for real-time healthcare, and combining BC with DRL could be difficult in terms of resources and complexity, making it difficult to apply in real-world healthcare settings. and not address energy consumption and cost.

A summary of previous studies' results, taken from Table 1: Each study successfully achieved a unique objective. To the best of our knowledge, no work has yet been done to present or recommend BC-based, cost-efficient, and cyber-physical systems (CPS) for IoMT healthcare apps. Many blockchain systems, such as Ethereum, Corda, and Fabric, have prioritized security as the main challenge. They should have considered saving expenses while still providing adequate healthcare. In addition to this, we were able to identify some shortcomings in the techniques

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

of earlier investigations, which were as follows: The studies [1] [21][24][25][26][28] [31] ,and [32] that utilized ML and DL did not take into account the process of discovering abnormalities and unknown attacks.

- The computational overhead of BC processing was ignored in previous research. However, the system is generally expensive because the BC procedure needs a great deal of resources. Key restrictions for running these apps over a distributed network are taken into account [21][22][33][27][29][30], and [32].
- Current studies have considered cybersecurity concerns at various Industrial Internet of Healthcare Things (IIoHT) mechanism levels. Existing studies have looked at cybersecurity problems, including DoS attacks, phishing, and malware at the user, wireless, and cloud levels, among other places.
- And every single study that uses BC achieves the highest confidentiality and privacy standards.

3. Methodology

The framework sequence that has been presented is critical in many areas of healthcare technology. Initially, the model significantly improves the processing of electrocardiogram (ECG) data by using the Pan Tompkins ECG QRS Detector and other preprocessing methods such as noise reduction and bandpass filtering. This improvement has made a big difference in ECG signal interpretation because it is crucial for diagnosing and monitoring heart problems. Furthermore, using the genetic algorithm (GA) for feature selection guarantees the recognition of the most critical data qualities, leading to more precise results with less computing complexity. Decisions can then be made based on the significant components of the electrocardiogram signal.

Employing a Bitcoin timestamp server for saving test data ensures data quality, dependability, and security, showcasing the resilience of a decentralized transaction architecture. Regarding medical applications, this feature is crucial for ensuring the authenticity and correctness of ECG data. By applying the SVM to identify test transactions, we can verify that the model's generated features adequately sort and categorize ECG data. There is much promise in classifying data to improve heart illness, pattern detection, and management. All steps of the process, from preprocessing data to picking characteristics and categorizing them, contribute to more accurate and efficient analysis of ECG data, which might lead to better diagnostic monitoring and faster detection of heart abnormalities. Furthermore, this method can streamline datasets by removing redundant information and focusing on what's essential for making decisions. The proposed paradigm may advance healthcare IT, improve diagnostics, ensure data integrity, and inspire innovation in healthcare research and practice. The dataset is first partitioned into a training set and a testing set. The former is used to train the model, while the latter is used to measure how well it performs. After that, the Pan Tompkins ECG QRS Detector is used to preprocess the data. The signal is squared, and a bandpass filter (5–15 Hz) removes noise that isn't connected to the heart. A second filter brings attention to the QRS complex.

By averaging the signal, we can remove spikes of high-frequency noise and tune the sample rate to match the characteristics of the ECG. During the modeling phase, a GA is used to identify relevant features. Crossover techniques (Double Point, Single Point, and Uniform) and Selection strategies (Tournament and Roulette) are chosen randomly during operations based on a binary system. The success of the GA is measured by how well it improves the model's accuracy. Next, a Bitcoin timestamp server mimics a peer-to-peer electronic currency system and stores mock data. By gathering together and broadcasting recently processed transactions in blocks, nodes ensure that all data is accurate and reliable. Finally, the SVM is used to classify test transactions. The features retrieved from the data will likely be used to classify the transactions. Figure 1 illustrates the proposed IoMT framework architecture. This section presents all the steps and procedures of the proposed framework.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

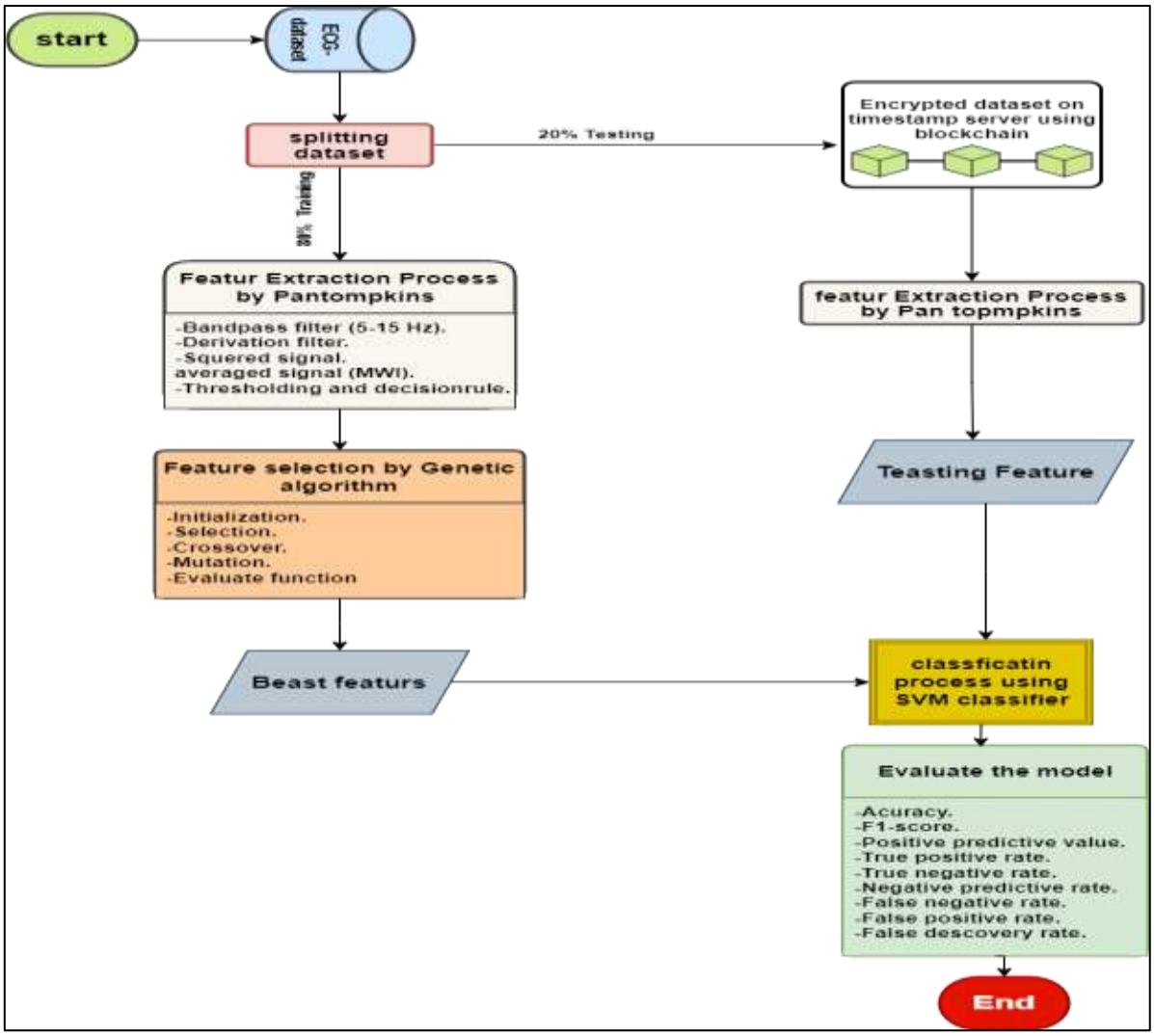

Figure 1: proposed framework architecture.

The Proposed Framework Steps are:

1- Randomly splitting the database to two parts (80% training and 20% testing)
2- Preprocessing step (feature extraction) using Pan Tompkins ECG QRS Detector and training dataset
   a. Bandpass filter (5-15 Hz).
   b. Derivation filter to high light the QRS complex.
   c. Signal is squared.
   d. Signal is averaged (MWI) to remove high frequency noise (0.150 seconds length).
   e. Thresholding and decision rule.
3- Feature Selection Process using Genetic Algorithm
   a. Binary Genetic Algorithm
   b. Random Population Generation
   c. Selection Process Randomly selection between (Tournament Selection, Roulette Wheel Selection).
   d. Cross Over Process Randomly selection between (Double Point Crossover, Single Point Crossover, Uniform Crossover)
   e. Mutation Process
   f. Fitness function is Accuracy
4- Storing Best Features in dataset
5- Storing testing data in timestamp server using Bitcoin: A Peer-to-Peer Electronic ECG System in a network according to the following steps:
   - Broadcast a new transaction to all nodes.
   - New transactions are collected into a block of node.
   - Every node search for a difficult proof-of-work for its block.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

- A node broadcasts a proof-of-work to all nodes when finds it.
- The block is accepted only if all its transactions valid and not have been spent.

6- Classification the testing transactions using SVM.
7- Matrix evaluation for classification task.

3.1 Dataset Collection

The gathering of datasets is a fundamental component in any machine learning (ML) activity, and the quality and diversity of the data play a critical influence in determining model performance. This procedure entails obtaining a comprehensive set of examples that methodically represent the problem domain. To ensure that the trained model generalizes correctly, the dataset should include the variability found in real-world events. During this stage, consider factors such as data bias, completeness, and relevance to the objective task. In this step, we used two ECG datasets:

1. **MITDB**: MIT-BIH arrhythmia obtained from https://www.physionet.org/content/mitdb/1.0.0/ contains 48 half-hour excerpts of ambulatory ECG recordings(signal) from 47 people, each signal length is 650000 cells; it has three categories (tachycardia:1, bradycardia:2, Normal:3). The recordings are captured at 360 Hz and typically last about 30 minutes. The dataset includes various standard and rare arrhythmias, making it a complete resource for testing the robustness of arrhythmia detection systems. Table 2 illustrates the dataset details.
2. **MITBIH**: Physionet's arrhythmia dataset obtained from the Kaggle website: https://www.kaggle.com/datasets/shayanfazeli/heartbeat/ , which consists of 109446 samples (rows). Each row has a signal length of 188 cells. It has five categories' Classes (N: 0, S: 1, V: 2, F: 3, Q: 4), with a Sampling Frequency of 125Hz.

Table 2: The datasets detail.

Content	**MITBIH**	**MITDB**
Format	CSV	Header (.hea), Data File (.dat), and Annotation File(.atr).
No. Sample	109446-signals	47-signals
No. classes	5-class: [N: 0, S: 1, V: 2, F: 3, Q: 4]	3-class [tachycardia:1, bradycardia:2, Normal:3]
Frequency sample	125Hz	360Hz
Signal length	188-cells	650000-cells

3.2 Splitting the Dataset

It is a critical stage in the machine learning process for training and assessing models. This procedure breaks the gathered data into discrete subsets, usually test, validation, and training sets. The validation set aids in adjusting the model's parameters and preventing overfitting, and the training set is utilized to educate the model patterns and relationships found in the data. The test set, unseen by the model during training, is the final standard to judge the model's ability to generalize to new, unobserved data. Striking a suitable balance between the size of each split is crucial since an underfit model can be produced by the training set having too little data, and performance metrics can be unreliable by the test set having too little data. Building robust and efficient machine learning models requires careful thought and randomness during splitting.
In this stage, we were divided randomly into the training and test sets (or validated) by the train-test method. The training set is a subset of a dataset that is utilized to train a model. A test set is a subset of the dataset used for model testing. The dataset was divided into an 80:20 split. We trained the model for 80% of the data, while the remaining 20% is for testing, As illustrated in Figures 2 and 3.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

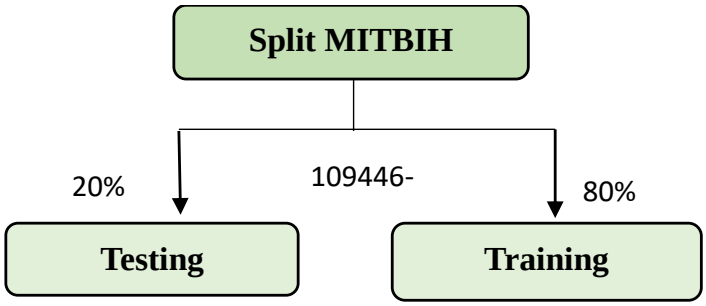

Figure 2: Split MITBIH dataset.

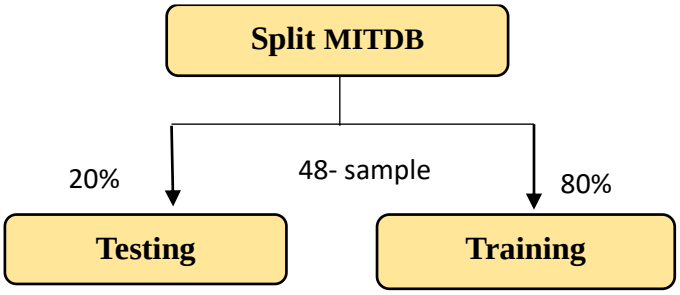

Figure 3: Split MITDB dataset.

3.1 Feature Extraction Stage

It is an essential preprocessing step that aims to convert unprocessed data into a more readable and understandable representation. Its clear, it entails picking or modifying the data's most pertinent features to incorporate into a model. When working with high-dimensional datasets, this procedure is incredibly crucial. The data's dimensionality is decreased by identifying and extracting important features, improving the interpretability and performance of the model. Feature extraction techniques vary depending on the type of data. We implement this step by using Pan Tompkin's algorithm for QRS-feature extraction by removing noise from the signal. Applying a series of filters to remove noises and frequency content highlights to depolarize the heart rapidly. Algorithm 1 illustrates the Pan Tompkins algorithm. Figure. 4 shows the Pan Tompkins stages.

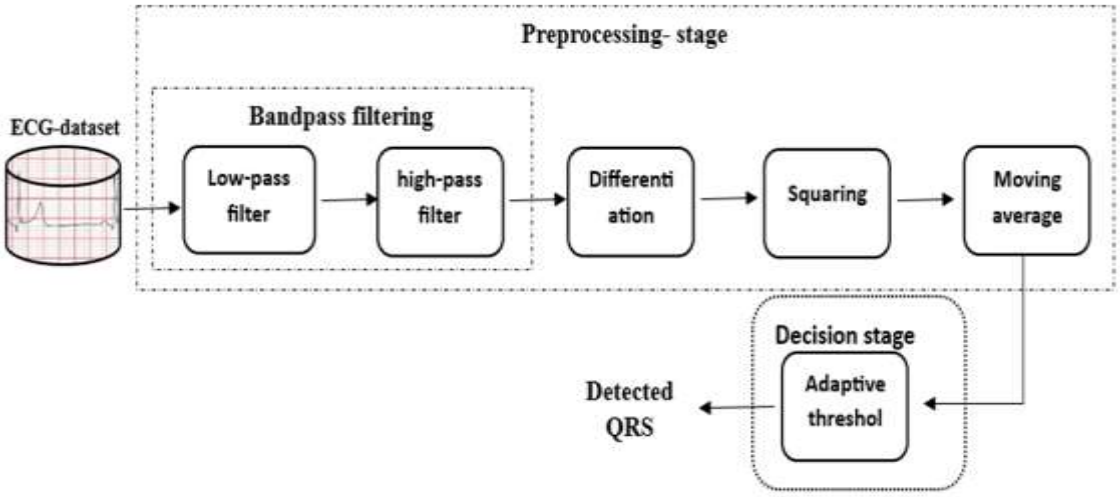

Figure 4: Pan Tompkins algorithm stages.

a- Bandpass filtering

It is applied to improve the ratio of signals to noise. Only electrical signals within a given frequency range are allowed to pass(5Hz-15Hz), while all others are blocked to maximize the QRS contribution while minimizing noise. This step uses A Butterworth filter to implement the bandpass filtering operation.

The **low pass filter** calculates the equation 1:

$$H_L(z) = \frac{(1-z^{-6})}{(1-z^{-1})}\frac{2}{2} \quad \text{..... (1)}$$

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

And, **high pass filter** calculates the equation 2:

$$H_H(z) = \frac{-\frac{1}{32}+z^{-16}-z^{-17}+\frac{1}{32}z^{-32}}{1-z^{-1}} \text{ …….. } \textbf{(2)}$$

b- Differentiation (a derivative filter)

It is a mathematical operation done on a signal (bandpass ECG signal) to improve slopes and rapid changes in the ECG wave to facilitate the detection of the QRS complex, which is comprised of rapid changes in the ECG signal. The discrete derivative of a signal x(n) at a particular point n is expressed mathematically in equation 3:

$$H_D(z)] = 0.1(-2z^2-z^{-1}+z+2z^2) \text{ …… } \textbf{(3)}$$

c- Signal is squared

It's a mathematical process in which each value in a signal is raised to the power of two. This process emphasizes the high-frequency components of the signal (maximizing QRS-complex contribution) while suppressing the lower-frequency components. The squaring process is applied to each data point of a discrete signal x(n), representing the outcome as x2(n). It is mathematically stated in equation 4:

$$Y(n)= (x(n))^2 \text{ ……. } \textbf{(4)}$$

d- Signal is averaged

It is applied to the signal squared. A moving average filter extracts information relating to the QRS complex's duration. The sample number to average is determined to average 0.15 s. The generated signal is known as an integrated signal and a smoothed signal. Moving average implemented in equation 5:

$$H_I(z) = \frac{1}{N}(z^{-1} + z^{-2} + \cdots + 2^{-N}) \text{ …… } \textbf{(5)}$$

Where, N is samples number.

e- Thresholding and decision rule

Thresholding distinguishes between truly QRS complexes (the R-wave peaks) and noise or other signal errors. THR_SIG and THR_NOISE, which represent the signal and noise thresholds, are initialized in this step. Within the first two seconds of the signal, the signal threshold (THR_SIG) is set to one-third of the maximum value of the smoothed signal (averaged signal). The noise threshold (THR_NOISE) is set to half the smoothed signal's mean value over the same period. The thresholds change adaptively. When a QRS complex is identified, the signal threshold (THR_SIG) is modified based on the amplitude of the detected QRS. These adaptive adjustments guarantee that the thresholds remain acceptable for detecting QRS complexes even when noise levels and R-R intervals alter. The relationship between the peak amplitudes and the thresholds is the basis for the decision rule. If the amplitude of a peak over the signal threshold (THR_SIG), it is considered to be part of a QRS complex and, updating the **LEV SIG** as equation 6:

$$\textbf{LEV}_{\textbf{SIG}} = 0.125 \times \textbf{CURRENT P EAK} + 0.875 \times \textbf{LEV}_{\textbf{SIG}} \text{ …… } \textbf{(6)}$$

And peaks below the noise threshold (THR_NOISE) are considered as noise, then updating $\textbf{LEV}_{\textbf{NOISE SIG}}$ as equation 7:

$$\textbf{LEV}_{\textbf{NOISE}} = 0.125 \times \textbf{CURRENT P EAK} + 0.875 \times \textbf{LEV}_{\textbf{NOISE.}} \text{ ….. } \textbf{(7)}$$

Based on updated signal and noise level estimates ($\textbf{LEV}_{\textbf{SIG}}$, $\textbf{LEV}_{\textbf{NOISE}}$), update the thresholds as follows equation 8 and 9:

$$\textbf{THR\_SIG} = \textbf{LEV}_{\textbf{NOISE}} + 0.25 \times (\textbf{LEV}_{\textbf{SIG}} - \textbf{LEV}_{\textbf{NOISE}}) \text{ …… } \textbf{(8)}$$

$$\textbf{THR\_NOISE} = 0.5 \times \textbf{THR\_SIG} \text{ ……..…... } \textbf{(9)}$$

If an abnormally long period passes without an above-threshold peak, the algorithm will believe a QRS was missed and execute a search back. The minimum time required to initiate a search back is 1.66 times the current R peak-to-R peak time interval (commonly referred to as the RR interval). The missing QRS complex is supposed to occur at the highest point in the interval between the adapted threshold levels. In addition, candidates for physiologically implausible QRS complexes that occur within 200 ms of a previously recognized one are discarded to minimize false positives. Finally, the algorithm identifies the QRS complexes that occur after 200 ms (refractory period) but within 360 ms of the previous QRS, if it is real QRS in the ECG signal or a T wave that is abnormally prominent based on the waveform's mean slope at that position.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

Algorithm 1: Pan Tompkins.

Input: ECG-Signal (**MITDB**, **MITBIH**).
Output: Detected-Peaks (binary ECG-Signal).
Begin
Step 1: **Bandpass-filter**:
filtered Signal = bandpass-Filter (ECG-Signal)
step2: **Squaring**:
Squared-Signal = square(filtered-Signal)
Step3: **Moving window integration**:
Integrated-Signal =integrate(squared-Signal)
Step4: **Find peaks in the integrated signal** (**threshold**)
peaks = find-Peaks(integrated-Signal)
step5: **Determine R-R intervals**
rr-Intervals = calculate RR-Intervals(peaks)
step6: **Filter out false positives**
Corrected Peaks = remove False Positives (peaks, rr-Intervals)
return Corrected Peaks.
End.

3.2 Feature Selection by Genetic Algorithm (GA)

It is an essential stage in data analysis and ML. It involves selecting a subset of relevant features from a large dataset (ECG dataset). Feature selection aims are to reduce computational complexity, improve model performance, increase interpretability, and reduce overfitting. GA is adapting heuristic algorithms for searching inspired by natural selection and genetic processes. Figure 5 illustrates the genetic algorithm stages. It can be utilized to find optimal feature subsets from a vast search space. Individuals in the GA are subsets of predictors stored as binary strings. The model's fitness scores are some measures of the model's efficiency, such as accuracy in classifying. Algorithm 4 illustrate feature selection based-GA.

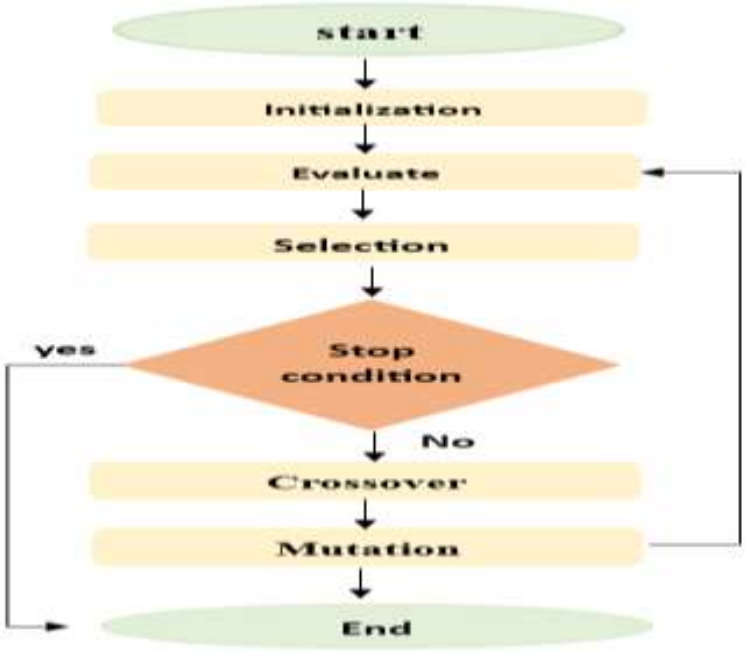

Figure 5: Genetic algorithm steps.

A. **Initialization:** Generate the initial population of (chromosomes) randomly in the ECG-feature subset.
B. **Selection:** is a better solution (chromosome) preferred over worse ones based on the accuracy (fitness value) to be parents, and we used two selection processes, roulette-wheel selection, and tournament selection, to achieve this goal.

- **Roulette-wheel selection**

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

It is a popular selection method used in GA to select the best individuals (feature) for the next generation. Algorithm 2 illustrates Roulette-wheel selection.

Algorithm 2: Roulette-wheel selection.

```
Begin
Step1   Evaluate Fitness for each population individual
step2   Total Fitness = sum of all individuals fitness values in the population
step3   Compute population probability p= individual's Fitness /total Fitness
step4   selected = an empty list to store selected individuals
step5   Repeat until a sufficient number of selections are made:
step6   Random value = random number between 0 and total Fitness
step7   Cumulative probability = 0
step8   For each individual in the population:
step9           Cumulative probability += individual's probability
step10          If cumulative probability >= random value:
step11          selected.add(individual)
step12  Break;
Step13 Return selected;
END.
```

- **Tournament selection**

It is a selection method used in GA. A chromosome (ECG- feature) with the best fitness is selected. Algorithm 3 illustrates Tournament selection steps.

Algorithm 3: Tournament selection.

```
BEGIN
Step1   Evaluate Fitness for each population individual.
Step2   Selected = a blank list for storing individuals.
Step3   Repeat until a sufficient number of selections are made:
Step4   Tournament Participants = Selecting individuals at random from the population.
Step5   Best Individual = the participant with the highest fitness among 'tournament
Participants'
Step6   Selected.add (best Individual);
Step7   Return selected;
End.
```

C. **Crossover:** Following selection, new, hopefully improved offspring where the ECG-individuals from the mating pool are crossed by Applying random selection between (Double Point Crossover, Single Point Crossover, and Uniform Crossover).

- **Single - Point Crossover**

Child 1 It is created by taking the gens of parent1 until the crossover point is reached, then taking the gens of parent2.

Child 2 It is created by taking the gens of parent2 until the crossover point is reached, then taking the gens of parent1. Figure 6 illustrates the Single-Point Crossover.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

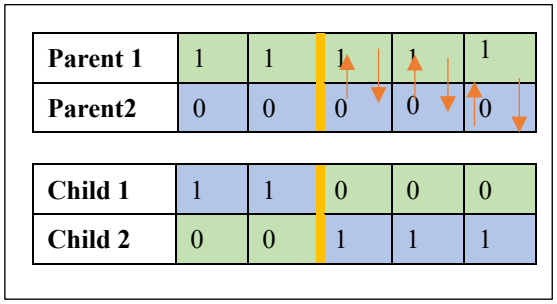

Figure 6: Single - Point crossover

- **Double - Point Crossover**

The child is created by exchanging the parents' genes between the two crossover points. Figure 7 illustrates Single-Point Crossover.

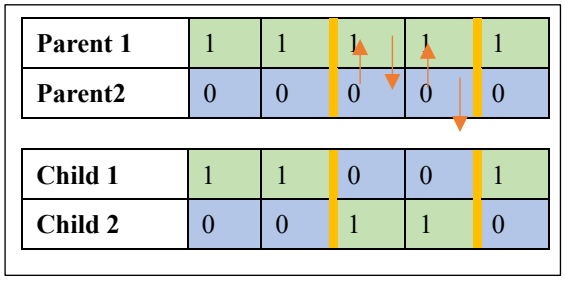

Figure 7: Double - Point crossover

- **Uniform Crossover**

The child is created by generating a binary mask (each gen consists of random 0s and 1s) with the same parents' size.

Child 1 = gen's mask * parent1 + (1 - gen's mask) * parent2. (In other words, taking a gene from parent one is indicated if a mask value is 1, and taking a gene from parent two is 0).

Child 2= = gen's mask* parent2 + (1 - gen's mask) * parent1. In other words, taking a gene from parent two is indicated if a mask value is 1, and taking a gene from parent one is 0). Figure 8 illustrates a uniform Crossover.

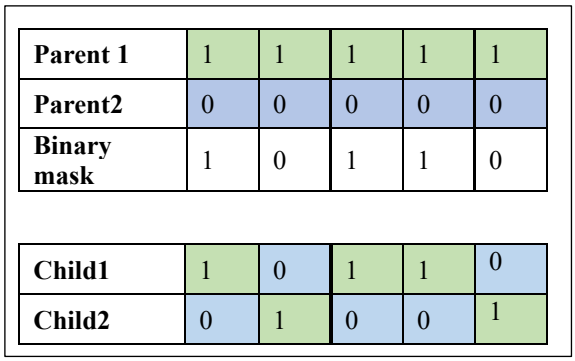

Figure 8: Uniform Crossover

D. Mutation

We may get better chromosomes with a crossover, but the issue is that a gene always carries a matching allele (such as a single-point crossover). The mutation solves this problem, increasing population diversity and ensuring that the entire space of searches will be examined. Figure 9 illustrates mutation process.

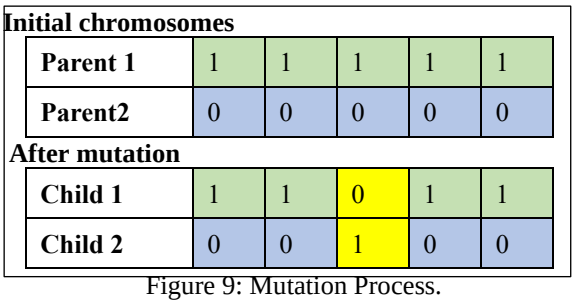

Figure 9: Mutation Process.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

E. **Evaluation**

Evaluate candidate solutions' fitness values(accuracy). Where, performed the following steps for each chromosome in the population:

Extract the features from the ECG-signal.
Train an SVM classifier using ECG-features extracted.
Calculate the chromosome fitness value based on the SVM-classifier performance(accuracy). The extracted and selected features output presented in table 3:

Table 3: the extracted and selected features

	MITBIH	MITDB
ECG signal length	188	650000
Features number	177	3000
Selected features count	11	1518

Algorithm 4: Feature selection based-GA

Input: ECG-train samples (**MITBIH, MITDB**).
Output: ECG-selected feature.
Performance-values: accuracy.
Best-iteration: max accuracy.
BEGN
Step1: Generations number (GN):
Step2: Population size (PZ):
Step3: Crossover Rate: 0.5
Step4: Mutation Rate: 0.5
Step5: **INITIALSE** population**;**
Step6: **REPEAT**
Step7: **SELECT** parent based on fitness value;
Step8: **CROSSOVER** selected parents;
Step9: **MUTATE** crossover parents;
Step10: **EVALUATE** Fitness values(accuracy);
Step11: **SAVE** best chromosomes of current population.
Step11: **Until** the stop criterion is reached (GN).
END.

3.3 Encrypt by Blockchain (BC)

It is an important tool for securing sensitive information and is an essential procedure in data protection and cybersecurity. It entails converting plaintext data to ciphertext via an algorithm, making the original data illegible to anyone who doesn't have a valid key. Encryption's primary goal is to ensure confidentiality by preventing unauthorized access to or interception of sensitive data during transmission or storage. The BC technology enables cybersecurity and data protection in a distributed healthcare system. The stages of implementing a peer-to-peer system are:

- Creating a chain of digital signatures.
- Utilizing a timestamp server for building a chain of timestamps.
- Implementing a proof-of-work system.
- Designing a network of nodes for verifying transactions.
- Supplying incentives for nodes to aid the network.
- Running simplified verification.

The peer-to-peer system steps in detail are:

a. Transactions

Every patient transmits data (ECG signal) by digitally signing a hash of the previous transaction and the next patient's public key and appending these to the end of the data. The recipient (hospital server) can validate the chain of patients by verifying the signatures.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

b. Timestamp Server

It operates by timestamping a block's hash and then broadcasting it extensively to prove that data existed at that time to get into a hash. Each timestamp includes the previous timestamp in its hash, which produces a chain where each timestamp verifies the ones that came before it.

c. Proof-of-Work (PoW)

A PoW system is used to create a distributed timestamp server on a peer-to-peer basis. To show PoW, one must search for a value such that, when hashed (using Secure Hash Algorithm (SHA-256)), the hash starts with a zero-bit count. One hash can be used to verify that the average work required is exponential in the number of required zero bits. The mining machine is designed in this research as shown in the algorithm 5. A hash algorithm is a mapping algorithm that transforms a string of characters into another fixed-length string.

Algorithm 5: SHA-256 implementation.

```
Set parameters
        Method = 'SHA–256';
        Input = 'ascii';
Create a hash with the given parameters.
        newhash = DataHash (' x650000 ECG-string', Method, Input)
```

Finding a potential input string is necessary when selfHash 's first three digits begin with 000. Several inputs can satisfy this condition because we just provided the first three digits of self Hash. In case the hash value of 'ECG-signal' cannot be determined, proceed to try with the next integer until the first three digits of self Hash equal 000—algorithm 6 Blockchain mining.

Algorithm 6: Blockchain mining

```
Not found = true;
iter = 1;
tic
while(not_found)
Combine block data and iteration (iter):
        Data to hash = ([strcat (newBlock.getCombined()), num2str(iter))];
For hashing, use the given parameters:
        Selfhash = DataHash (Data to hash, Method, Input)
 Check that the hash satisfies the criteria:
        if (strcmp (selfHash (1: 3), '000'))
If the criteria are met, update the parameters of the block and add it to the blockchain:
                New-Block. Nonce = iter;
                New-Block. SelfHash = SelfHash;
                AddBlock (New-Block);
Exit the loop when not found = false
                        end
Increase iteration:
                iter = iter + 1;
toc
end
```


Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

a- Network

The steps to follow for running the network are:

- Broadcast a new transaction to all nodes.
- New transactions are collected into a block of node.
- Every node search for a difficult proof-of-work for its block.
- A node broadcasts a proof-of-work to all nodes when finds it.
- The block is accepted only if all its transactions valid and not have been spent.
- Nodes indicate their acceptance of a block by working on the next block in the chain, with the accepted block's hash as the previous one. Nodes always assume the longest chain to be correct and will work to enlarge it. Algorithm 7 illustrates a class of BC implementation.

Algorithm 7: A class of BC implementation

```
Parameters
index;
data;
previousHash;
selfHash;
nonce;
function obj = Block (index, data, previousHash)
if nargin = =2 is genesis block
        obj. index = index;
        obj.data = data;
        else if nargin == 3
                obj. index = index;
                obj.data = data;
                obj. previousHash = previousHash;

        end
        function str = get Combined(obj)
        str = strcat ([num2str (obj. index), obj. previousHash, join(obj.data)]);
end
```

The ECG peer-to-peer system involves a blockchain server to secure, store, and share data(selfhash). The BC server stores the ECG signals in a timestamp, server owner's public key, and hash form. The system validates requests for access using the owner's public key. If the verification succeeds, the access process continues with the verification access request. After successful validation, the ECG signals can be made public. Figure 10 illustrates the ECG peer-to-peer system.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

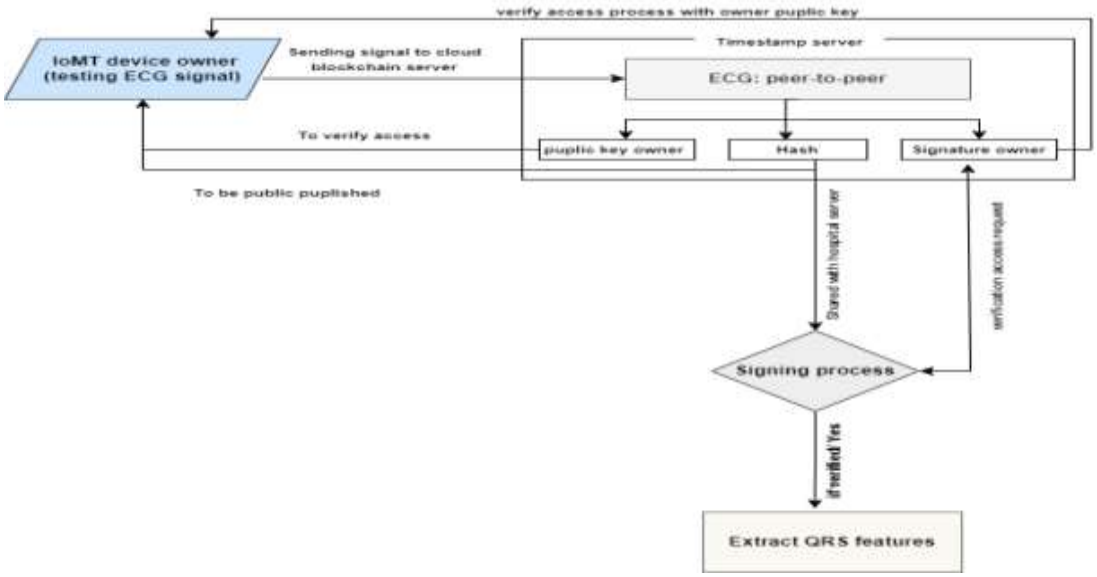

Figure 10: ECG peer-to-peer system.

3.4 Support Vector Machine Classification Model

The classification process is classifying items or points of data into predetermined groups or classes based on specific features or features. This is an essential concept in ML and data analysis. The SVM algorithm selects the best hyperplane in an N-dimensional space for separating data points into different classes in the feature space. The hyperplane attempts to optimize the distance between the closest points of various classes. This stage involves Loading and dividing the ECG dataset into training and testing sets. The data is then mapped to a high-dimensional feature space, allowing data points to be categorized even when they are not otherwise linearly separable. Following that, train the SVM classifier by locating the best hyperplane in the feature space that can split data points into distinct classes. Finally, evaluate the SVM classifier to see how it performs. Figure 11 and Algorithm 8 shows the SVM- classifying approach.

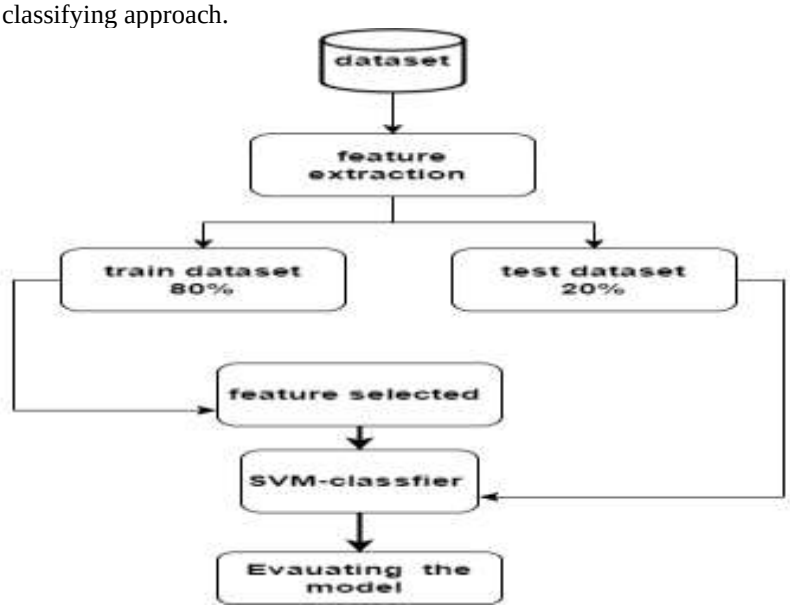

Figure 11: The SVM- classifying approach.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

Algorithm 8: SVM- classification approach

BEGIN

Input: **CHOOSE** ECG-dataset (**MITBIH**, or **MITDB**).

Output: The accuracy, and other metrics of built model

BEGIN

Step1: **IMPORT** the Dataset.

Step2: **Feature extraction** for ECG-dataset (Pan Tompkins).

Step3: **Feature selection by** (**GA**)

Step4: **TRAIN** the SVM-model using feature selection.

Step5: **EVALUTE** the model metrics (such as accuracy).

Step6: **RETURN** Evaluation metrics.

END.

3.5 Evaluation Model

Various techniques and measurements can be employed to evaluate a model based on the kind of model and the issue being addressed. In this search, we used confusion matrices [True Positive (TP), True Negative (TN), False Positive (FP), True Negative (TN)] are a table that describes an ML model's performance on a set of test data. TP is the model's true positive prediction number, while TN is the true negative prediction number. FP is the model's false positive prediction number, and FN is a false negative prediction in several models. Confusion matrices are explained in Table 4.

Table 4: The Confusion matrices.

		Actual class	
		Positive	**Negative**
Predicate class	**Positive**	TP	FP
	Negative	FN	TN

The accuracy (ACC) of a model is a measure of how effectively it predicts actual values. It is the ratio of the number of correct predictions to the total predictions provided by the model, the ACC calculated as equation 10:

$$\textbf{ACC}= \frac{TP+TN}{TP+TN+FP+FN} \dots\dots\dots (\mathbf{10})$$

F1-score takes the harmonic mean of two metrics, recall, and precision, and combines them into a single score. The F1-score calculated as equation 11:

$$F1-SCOR = \frac{2TP}{2TP+FP+FN} \dots\dots\dots (\mathbf{11})$$

Precision, or [positive predictive value (PPV)], denotes the percent of true positive predictions out of all positive predictions made by the model. It is calculated as equation 12:

$$\textbf{PPV}= \frac{TP}{TP+FP} \dots\dots (\mathbf{12})$$

Recall, or [true positive rate (TPR)], denotes the percent of true positive predictions of all actual positive in the dataset. It is calculated as equation 13:

$$\textbf{TPR}=\frac{TP}{TP+FN} \dots\dots\dots (\mathbf{13})$$

Specificity [true negative rate (TNR)] denotes the percent of true negative predictions of all dataset negative actuals in the dataset. It is calculated as equation 14

$$\textbf{TNR}= \frac{TN}{TN+FP} \dots\dots\dots (\mathbf{14})$$

Negative predictive value (NPV), is calculated as equation 15

$$\textbf{NPV} =\frac{TN}{TN+FN} \dots\dots\dots (\mathbf{15})$$

Miss rate [false negative rate (FNR)] is a measure used to evaluate a cache system's performance. It indicates the proportion of cache misses out of all memory requests performed to the cache. It is calculated as equation 16

$$\textbf{FNR} =\frac{TN}{TN+FN} \dots\dots\dots (\mathbf{16})$$

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

Fall-out [false positive rate (FPR)] is the proportion of false positive predictions out of all negative predictions. It is calculated as equation 17

$$\mathbf{FPR}=\frac{FP}{FP+TN} \quad \ldots\ldots\ldots (\ \mathbf{17})$$

False discovery rate (FDR) is determined by dividing the total number of discoveries by the number of false discoveries. It is calculated as equation 18

$$\mathbf{FDR}=\frac{FP}{FP+TP} \quad \ldots\ldots\ldots (\ \mathbf{18})$$

False omission rate (FOR) complements the negative predictive value and estimates the percentage of false negatives that are incorrectly rejected. It is calculated as equation 19

$$\mathbf{FOR}=\frac{FN}{FN+TN} \quad \ldots\ldots\ldots (\ \mathbf{19})$$

These measures aid in determining how well the model performs and whether it makes accurate predictions.

4. Results and discussions

The outcomes of evaluating the model's performance utilizing BC-based ECG-signal samples from MITDB and MITBIH are discussed in this section, which details the outcomes for each of the model's iterative steps.

4.1 Feature extraction by Pan Tompkins Results

Table 5 displays the results of the Pan-Tompkins method on the MITDB dataset. It includes a detailed examination of the number of false negatives, false positives, and missed beats for records with ten samples. This demonstrates the algorithm's efficacy in accurately identifying QRS complexes in ECG signals while maintaining low false positives and negative rates throughout the dataset. The algorithm has proven reliable and resilient in practical settings by decreasing false positives and missing beats.

Table 5: Pan Tompkins performance [34].

Record (No.)	Total (No. Beats)	FP (Beats)	FN (Beats)	Failed (Beats)	Failed (%)
100	2274	0	0	0	0
101	1874	0	6	6	0.32
102	2187	0	0	0	0
104	2230	1	2	3	0.13
105	2572	48	32	80	3.11
108	1824	61	71	132	7.24
200	2601	1	3	4	0.15
202	2146	0	6	6	0.279
219	2312	0	0	0	0
222	2634	131	2	133	5.04

4.2 Experiments with a Designed Classifier

Each generation of the GA, which used a Crossover Ratio (CR) of 0.5 and a Mutation Ratio (MR) of 0.5, produced a new set of characteristics. The GA was applied across generations (GN) ranging from 5, 10, 15, 20, 25, …. 75, 80, with population sizes (PS) ranging from 5, 10, 15, ..., 95, 100. The performance of the algorithm was evaluated using accuracy, true positive rate or recall (TPR), true negative rate or Specificity (TNR), positive predictive value or Precision (PPV), and F_Score, which compared the predicted accuracy of each dataset. As the GA progressed through generations, the findings demonstrated the precise efficiency of the model.

1- Experiments over MITDB Dataset

The experiments of the classifier on the MITDB dataset in terms of GN and PS were tested on several models, beginning with five generations and ending with 80 generations. PS started with 10 to 100 in each generation. The results of these models and their full model setups are listed in each row in Table 6 while the columns of this table show the following: The first column is model no.; the second column represents the number of GN in the model, which is between 10 and 80 generations; and the third column represents the PS between 5 and 100) in each generation. The fourth-eight columns include evaluation metrics (accuracy, TPR, TNR, PPV, and f_score).

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

Table 6: Results over MITDB dataset using CR=0.5 and MR=0.5

No. Model	GN	PS	Accuracy	TPR	TNR	PPV	f_score
1	5	5	75.51%	78%	73%	78%	78%
2	10	10	85%	89%	80%	89%	89%
3	10	45	85%	89%	80%	89%	89%
4	10	75	87.23%	89%	85%	89%	89%
5	10	80	87.23%	89%	85%	89%	89%
6	15	20	87.23%	89%	85%	89%	89%
7	15	50	87.23%	89%	85%	89%	89%
8	15	85	87.23%	89%	85%	89%	89%
9	20	25	87.23%	89%	85%	89%	89%
10	20	95	87.23%	89%	85%	89%	89%
11	25	10	87.23%	89%	85%	89%	89%
12	25	20	87.23%	89%	85%	89%	89%
13	30	90	87.23%	89%	85%	89%	89%
14	35	10	87.23%	89%	85%	89%	89%
15	35	55	87.23%	89%	85%	89%	89%
16	35	75	87.23%	89%	85%	89%	89%
17	35	95	87.23%	89%	85%	89%	89%
18	40	25	87.23%	89%	85%	89%	89%
19	40	50	87.23%	89%	85%	89%	89%
20	40	55	87.23%	89%	85%	89%	89%
21	40	70	87.23%	89%	85%	89%	89%
22	45	5	87.23%	89%	85%	89%	89%
23	45	95	87.23%	89%	85%	89%	89%
24	45	100	87.23%	89%	85%	89%	89%
25	50	35	87.23%	89%	85%	89%	89%
26	55	40	87.23%	89%	85%	89%	89%
27	55	95	87.23%	89%	85%	89%	89%
28	60	15	87.23%	89%	85%	89%	89%
29	60	25	87.23%	89%	85%	89%	89%
30	65	85	87.23%	89%	85%	89%	89%
31	70	50	87.23%	89%	85%	89%	89%
32	70	70	87.23%	89%	85%	89%	89%
33	70	75	87.23%	89%	85%	89%	89%
34	75	25	87.23%	89%	85%	89%	89%
35	75	30	87.23%	89%	85%	89%	89%
36	75	50	87.23%	89%	85%	89%	89%
37	75	70	87.23%	89%	85%	89%	89%
38	75	90	87.23%	89%	85%	89%	89%
39	80	5	100%	100%	100%	100%	100%
40	80	10	100%	100%	100%	100%	100%

After selecting the GN setting from the experiment explained in Table 6, this configuration was examined on a finite number of PS using the MITDB dataset for training and testing the models mentioned below; the confusion metrics are explained in Table 7.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

Table 7: The confusion metrics of MITDB dataset

0	**0**	**0**
1	**2**	**0**
0	**0**	**6**

The evaluation metrics are accuracy, and accuracy rate is 87%, Figure 12 depicts the relation between total population size (GN *PS) and model accuracy on the MITDB dataset using Crossover Ratio=0.5 and mutation Ratio=0.5. The x-axis shows the overall population, while the y-axis represents the accuracy. The figure depicts the accuracy of the models as the population size increases to 100%. This allows for examining the effect of population size on model performance.

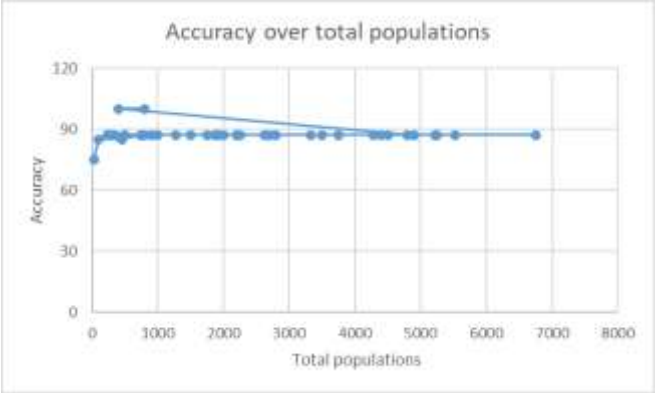

Figure 12: Accuracy Vs total Populations over MITDB Dataset

Meanwhile, Figure 13 depicts the relationship between the number of generations and accuracy in the MITDB dataset using Crossover Ratio=0.5 and Mutation Ratio=0.5. It shows how GN influences the accuracy of the models, where the x-axis denotes the GN, and the y-axis represents the accuracy. This chart indicates that as the number of generations increases, so does the accuracy.

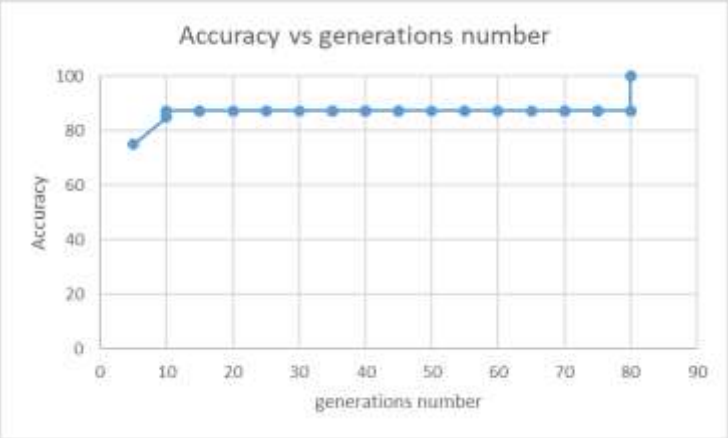

Figure 13: Accuracy Vs Generation Number over MITDB Dataset

Also, Figure 14 depicts the accuracy vs population size relationship in the MITDB dataset using CR=0.5 and MR=0.5. The x-axis represents the population size, while the y-axis represents the accuracy. The chart indicates that as the population size grows with the accuracy.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

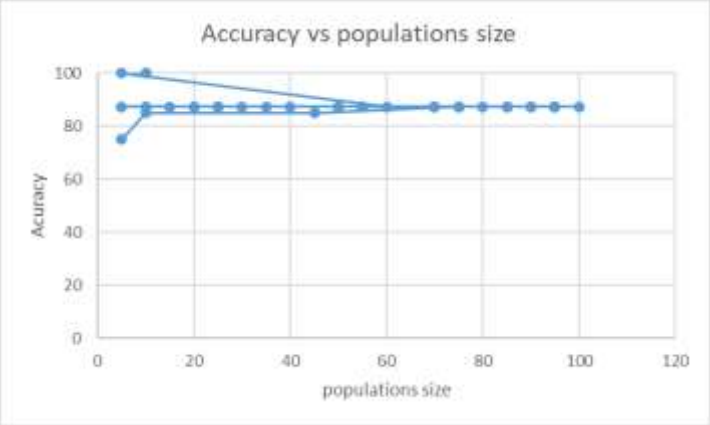

Figure 14: Accuracy Vs Population Size over MITDB Dataset

2- Results over MITBIH Dataset

Table 8 displays the findings of a study performed on the MITBIH dataset with a crossover ratio of 0.5 and a mutation ratio of 0.5. There are 8 columns and 39 rows in the table. The columns are as follows:

Table 8: Results over MITBIH dataset using CR=0.5 and MR=0.5

No. model	GN	Ps	Accuracy	TPR	TNR	PPV	f_score
1	5	10	99.99%	100%	100%	100%	100%
2	5	15	99.99%	100%	100%	100%	100%
3	5	25	99.98%	100%	100%	100%	100%
4	5	40	99.99%	100%	100%	100%	100%
5	5	50	99.97%	100%	100%	100%	100%
6	5	55	99.98%	100%	100%	100%	100%
7	5	70	99.98%	100%	100%	100%	100%
8	5	90	99.97%	100%	100%	100%	100%
9	10	5	99.97%	100%	100%	100%	100%
10	10	15	99.99%	100%	100%	100%	100%
11	10	20	99.96%	100%	100%	100%	100%
12	10	30	99.98%	100%	100%	100%	100%
13	10	30	99.98%	100%	100%	100%	100%
14	10	35	99.96%	100%	100%	100%	100%
15	10	55	99.98%	100%	100%	100%	100%
16	10	60	99.97%	100%	100%	100%	100%
17	10	65	99.97%	100%	100%	100%	100%
18	10	70	99.98%	100%	100%	100%	100%
19	10	75	99.97%	100%	100%	100%	100%
20	15	20	99.99%	100%	100%	100%	100%
21	15	75	99.99%	100%	100%	100%	100%
22	20	25	99.99%	100%	100%	100%	100%
23	20	50	99.99%	100%	100%	100%	100%
24	20	60	99.99%	100%	100%	100%	100%
25	20	65	99.99%	100%	100%	100%	100%
26	20	85	99.99%	100%	100%	100%	100%
27	20	100	99.99%	100%	100%	100%	100%

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

28	20	100	99.99%	100%	100%	100%	100%
29	25	15	99.99%	100%	100%	100%	100%
30	25	15	99.99%	100%	100%	100%	100%
31	25	25	99.99%	100%	100%	100%	100%
32	25	25	99.99%	100%	100%	100%	100%
33	25	30	99.99%	100%	100%	100%	100%
34	25	35	99.99%	100%	100%	100%	100%
35	25	40	99.99%	100%	100%	100%	100%
36	25	40	99.99%	100%	100%	100%	100%
37	25	45	99.99%	100%	100%	100%	100%
38	25	60	99.99%	100%	100%	100%	100%
39	30	25	99.99%	100%	100%	100%	100%

Thirty-nine rows and eight columns make up the. The columns are discussed. Each row represents one of the models used in the study, with different options for GN, PS, and other characteristics. The results demonstrate that all models obtained very high accuracy, achieving an accuracy of 99.96% or greater. The true positive rate, true negative rate, positive predictive value, and F1 score were all very high for all models. In comparison, the confusion metrics are changed slightly by the number of correct and incorrect predictions. The evaluation metrics are accuracy is 99.9%, TPR is 100%, TNR is 100%, PPV is 100%, and f_score is 100%. Figure 15 depicts the degree of accuracy across the total population (population size* generation number) for the MITBIH dataset using CR=0.5 and MR=0.5. The x-axis shows the general population, while the y-axis displays the accuracy. The chart indicates that as the population grows with the accuracy.

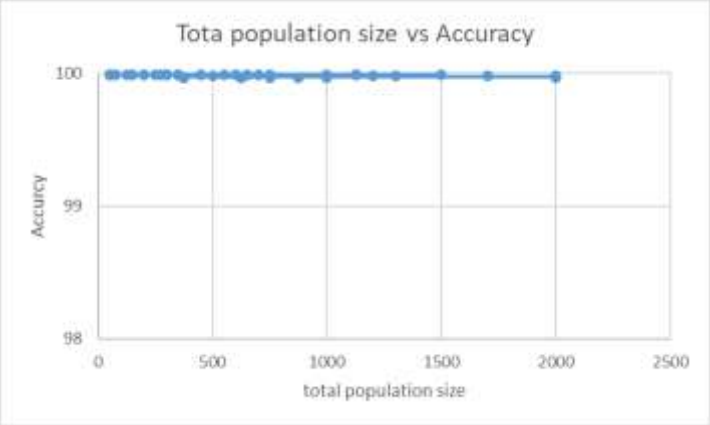

Figure 15: Accuracy Vs total Populations over MITBIH Dataset

Meanwhile, Figure 16 depicts the relation between accuracy and generation number in the MITBIH dataset using CR=0.5 and MR=0.5. The x-axis represents the generation number, while the y-axis represents the accuracy. The chart indicates that as the generation number rises, the accuracy also rises.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

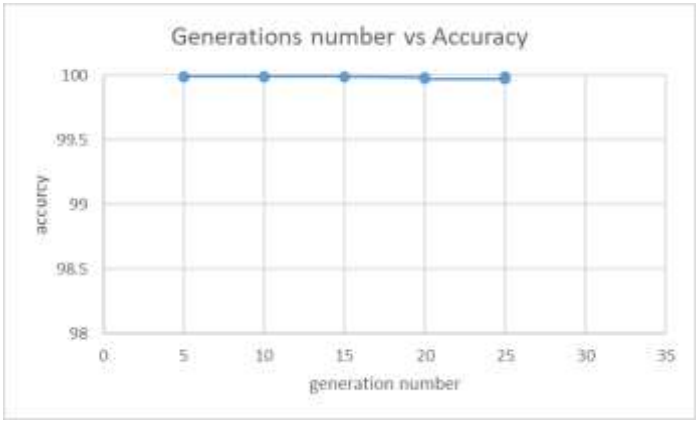

Figure 16: Accuracy Vs Generation Number over MITBIH Dataset

Also, Figure 17 depicts the accuracy vs population size relation for the MITBIH dataset using CR=0.5 and MR=0.5. The x-axis shows the population size, while the y-axis displays the accuracy. The chart indicates that as the population size grows, consequently does the accuracy.

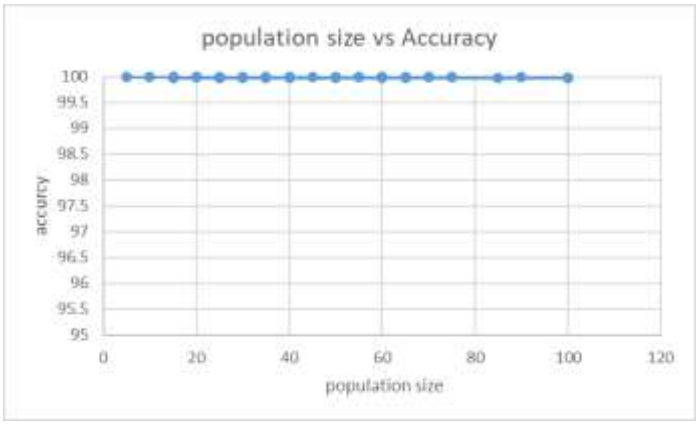

Figure 17: Accuracy Vs Population Size over MITBIH Dataset.

Overall, the statistics imply that expanding the population, GN, and PS can improve the accuracy of both datasets.

4.3 Encrypt by Blockchain Results

The result of the mining machine in this research is shown in Figure 18. It is found as a potential input string when selfHash's first three digits begin with 000; Mining gets more challenging and takes longer the stricter the restrictions are for the first characters of the selfHash.

```
itr= 3332
selfHash= '000cae98712d5ad33cbfd51f3fc6b05e'
```

Figure 18: The first three digits in newHash starts with 000.

In the BC, the mining process is maintained, which saves the block in Figure 19. The mining process is an array of arrays, and each array is a block. The first block is called the Genesis block and has a selfhash, while the second block is the first block in the network that contains an ECG signal(data) containing a previous hash of the Genesis block and a selfhash. as explained in Figure 20.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

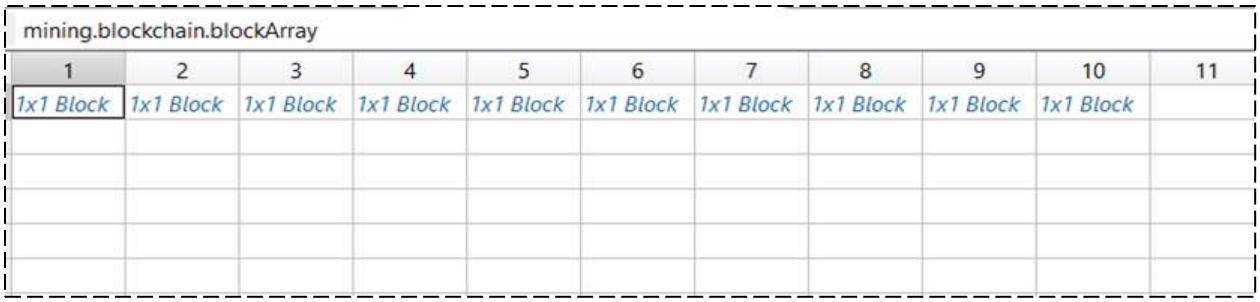

Figure 19: mining blockchain array

There is more than one block in the mining BC array; each block connects with the previous block by previous hash, and to the next block by self-hash.

Figure 20: Blockchain network.

The selfhash is distributed online to health centers. The centers receive the patient's data in the form of an encrypted file, and it is retrieved through the selfhash, where an access request is sent from the institution to the patients. The selfhash is sent to them until the request sent to him is proven, and thus, the data is accessed.

4.4 Classifying Test Data

This section presents the results of the model's performance with MITDB and MITBIH ECG signals. When testing the model classifier on MITDB using CR, MR=0.5, the results are summarized in Tables 9 and 10.

Table 9: MITDB confusion matrices testing

0	0	0
1	2	0
0	0	6

Table10: SVM based on GA classifier model over MITDB

Metrics\Dataset	**MITDB**
Accuracy (ACC)	87%
F1-score	88%
positive predictive value (PPV)	88%
True positive rate (TPR)	88%
True negative rate (TNR)	85%
Negative predictive value (NPV)	85%

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

False negative rate (FNR)	0.1
False positive rate (FPR)	0.15
False discovery rate (FDR)	0.1
False omission rate (FOR)	0.15

The results of comparing the model's performance with MITBIH ECG signal to evaluate the effect of several datasets on the classifier with the same parameters. The results obtained are summarized in table 11 and 12.

Table 11: MITBIH -Confusion matrices testing

18464	0	0	0	0
0	516	0	0	0
0	1	1187	0	0
0	0	1	152	0
0	0	0	2	1566

Table 12: SVM based on GA classifier model over MITBIH

Metrics\Dataset	**MITBIH**
Accuracy (ACC)	99.9%
F1-score	100%
positive predictive value (PPV)	100%
True positive rate (TPR)	100%
True negative rate (TNR)	100%
Negative predictive value (NPV)	100%
False negative rate (FNR)	9.13
False positive rate (FPR)	0.001
False discovery rate (FDR)	9.13
False omission rate (FOR)	0.0001

4.5 Results discussions

The study aims to improve healthcare applications' security and privacy by providing intelligent and lightweight frameworks to stop hacker attacks and maintain data security using blockchain technology. The proposed model protects medical data from tampering and then classifies it using the SVM algorithm based on GA, where two datasets, MITDB and MITBIH, were used for the ECG signal. The MITDB dataset consists of 47 samples, characterized by a length of up to 650,000 cells. In comparison, the MITBIH consists of 109,446 samples, described by many signals, to compare the effect of the signal length and the number of samples on the model's performance. After collecting and identifying samples, features are extracted using the Pan-Tomkins algorithm by applying a series of filters to remove noise and then squaring the signal to facilitate the identification of the QRS complex. Finally, thresholds are used to detect the peaks of the filtered signal. The results proved that it is suitable for evaluating the heart state, but it has some limitations, such as seeing false negatives and positives. After that, the GA algorithm was used to select features using CR = 0.5 and MR = 0.5 and different generations and population sizes. After two feature extraction and selection processes, then training the model using the SVM classifier. In the MITDB dataset, the classification results achieved an accuracy rate is 87%.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

In the MITBIH dataset, the classification results achieved an acc of 99.9%, TPR of 100%, TNR of 100%, f-score of 100%, and PPV of 100%. Table 13 shows results for each dataset.

Table 13: The datasets result

Dataset	Parameters	Acc	TPR	TNR	F-score	PPV
MITDB	MR=0.5 CR=0.5	87%	89%	85%	89%	89%
MITBIH	MR=0.5 CR=0.5	99.99%	100%	100%	100%	100%

The study's findings demonstrate the entire procedure for acquiring and training a model for cardiac rhythm categorization. Following the first training phase, the model is subjected to a security process that uses BC technology using MATLAB simulations. The mining process in this technology uses the SHA-256 algorithm, which generates a self-hash according to specific parameters, focusing on ensuring that the first three bits are zero. The study found that mining became more complex and time-consuming when initial character limits were imposed more strictly on the self-hash. The next step is transmitting the encrypted model to the data source so institutions can verify it online. This verification procedure guarantees the authenticity and integrity of the model. After the safety precautions are taken, the model is tested on two separate datasets, the MITDB and MITBIH.

The results obtained from the MITDB dataset, which achieved an accuracy rate 87%, show a thorough performance. Several other metrics are also included, such as an FNR of 0.1, FPR of 0.15, FDR of 0.1, and FOR of 0.15. The model's performance across several assessment criteria may be understood in depth with the help of these measures. However, the results from the MITBIH dataset, which show an extraordinarily high accuracy of 99.9%, highlight the model's effectiveness in this particular dataset. Accuracy, precision, negative predictive value, false negative, false positive, false discovery, and false omission rates all show that the model performs exceptionally well with few mistakes. Details include an FNR of 9.13, an FPR of 0.001, an FDR of 9.13, and a FOR of 0.0001. The model's sensitivity, accuracy, and precision in classifying the MITBIH dataset are high.

Considering each dataset's unique features and intricacies is essential for making sense of these findings. The decreased accuracy rate in the MITDB dataset raises concerns about possible data issues or subtleties that may affect the model's performance. The MITBIH dataset, however, shows that the model is great at correctly identifying cardiac rhythm patterns thanks to its almost flawless accuracy and low error rates. In light of the implications of sensitive medical data, the study's findings highlight the significance of executing strong security measures and training and testing a model. Models must be flexible and able to respond to the specific features of the data they encounter, as their performance might vary across various datasets. The results shed light on the complex cardiac rhythm classification model construction, security, and performance assessment areas.

Findings from the experiments show that the suggested model performs far better on the MITBIH dataset than on the MITDB dataset. The results achieved on the MITBIH dataset are remarkable, even if there were a few mistaken predicates during training on the MITDB dataset. Overfitting, which happened throughout training, is to blame for this performance gap. The problem of overfitting arises when the model is too optimized for the training data and starts to pick up on outliers or noise that only reflects part of the dataset. Here, it shows that the MITDB dataset needs to give the model more variety or coverage to generalize well, even though the signal length is high. Given the signal length, the training data isn't adequate for demonstrating outcomes higher than 95%," suggesting that a more varied and inclusive dataset is necessary for training purposes. Despite the considerable signal length in the MITDB dataset, the model could need more variety to do well on new data. The results highlight the importance of diverse and high-quality datasets to achieve reliable model performance. In the future, it recommended boosting the model's effectiveness across datasets and increasing its dependability in real-world applications, including improving dataset variety or utilizing regularisation approaches.

4.6 Benchmarking with state-of-the-art

Benchmarking with state-of-the-art refers to comparing an evaluation of a system, process, or approach to the most well-known and effective methods and technologies in a particular industry. When discussing methods now

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

considered at the forefront of their field, the term "state-of-the-art" describes the most cutting-edge and efficient methods. Organizations, researchers, and practitioners can use benchmarking to see how their systems, innovations, or work stack up against the best in their field. Various parameters might be encompassed in practice when benchmarking with state-of-the-art. When we compare our processes and tools to the most advanced ones, we also measure their efficiency, accuracy, and quality. In addition, this benchmarking tool helps determine how innovative a new approach is. By drawing comparisons to state-of-the-art methods, researchers and practitioners may highlight the distinctive aspects of their work. One of the most important parts of competitive analysis is benchmarking with state-of-the-art to understand better how a product or service compares to the competition. This adds to the field's continuous advancement and confirms the importance of research. Essentially, comparing results to those of the most advanced practices may be a map to help find the way to excellence, innovation, and progress in several areas.
This section compares the proposed framework with other methods using the same datasets, as illustrated in Table 14 and Figure 21.

Table 14: The comparison evaluating model with other works using MITDB dataset.

Study/ Year	Accuracy	Recall (TPR)	TNR	PPV	F1-score
Roland et.al 2022 [35]	84%	88%	78	86%	87%
Liu et.al 2019 [36]	92.5%	84.9%	84.9%	47.7%	-
Our Proposed	87%	87%	85%	89%	89%

Table 15: The comparison evaluating model with other works using MITBIH dataset.

Study/ Year	Accuracy	Recall (TPR)	TNR	PPV	F1-score
Ahamed et.al 2020 [37]	97.58%	-	-	-	-
Our Proposed	99.99%	100%	100%	100%	100%

5. Conclusion

Integrating BC into the IoMT has enormous promise for improving cybersecurity inside healthcare systems. BC's decentralized and tamper-resistant nature can dramatically strengthen the security and integrity of sensitive medical data transferred and stored by IoMT devices. Blockchain's public and immutable ledger provides the traceability and accountability of every transaction, promoting consumer confidence in the healthcare ecosystem. This study has explored the advantages of using blockchain in IoMT cybersecurity, such as reducing the risk of data breaches, protecting patient privacy, and establishing a resilient framework against harmful assaults. The implementation of BC in healthcare settings is fraught with difficulties and complications. Where BC networks must handle a vast number of transactions without compromising speed and efficiency, a model that was pre-trained using a large dataset (MITBIH) has better predictive power than a model trained with a small dataset, where the model's sensitivity, accuracy, and precision in classifying the MITBIH dataset are high, which show an extraordinarily high accuracy of 99.9%, with a 99.9% accuracy rate, true positive rate (TPR) of 100%, true negative rate (TNR) of 100%, f-score of 100%, and positive predictive value (PPV) of 100%.

***Funding Statement*:** The authors received no specific funding for this study.
Conflict of Interest Statement: The authors declare no conflict of interest.

References

[1] A. Lakhan, Q. U. A. Mastoi, M. Elhoseny, M. S. Memon, and M. A. Mohammed, “Deep neural network-based application partitioning and scheduling for hospitals and medical enterprises using IoT assisted mobile fog cloud,” *Enterp Inf Syst*, vol. 16, no. 7, 2022, doi: 10.1080/17517575.2021.1883122.

[2] A. A. Mutlag *et al.*, “MAFC: Multi-agent fog computing model for healthcare critical tasks management,” *Sensors (Switzerland)*, vol. 20, no. 7, Apr. 2020, doi: 10.3390/s20071853.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

[3] A. Lakhan, M. A. Mohammed, A. N. Rashid, S. Kadry, and K. H. Abdulkareem, "Deadline aware and energy-efficient scheduling algorithm for fine-grained tasks in mobile edge computing," *International Journal of Web and Grid Services*, vol. 18, no. 2, pp. 168–193, 2022, doi: 10.1504/IJWGS.2022.121935.

[4] A. Lakhan, A. H. Sodhro, A. Majumdar, P. Khuwuthyakorn, and O. Thinnukool, "A Lightweight Secure Adaptive Approach for Internet-of-Medical-Things Healthcare Applications in Edge-Cloud-Based Networks," *Sensors*, vol. 22, no. 6, Mar. 2022, doi: 10.3390/s22062379.

[5] F. Mosaiyebzadeh *et al.*, "Privacy-Enhancing Technologies in Federated Learning for the Internet of Healthcare Things: A Survey," Mar. 2023, [Online]. Available: http://arxiv.org/abs/2303.14544

[6] A. Lakhan *et al.*, "Dynamic application partitioning and task-scheduling secure schemes for biosensor healthcare workload in mobile edge cloud," *Electronics (Switzerland)*, vol. 10, no. 22, Nov. 2021, doi: 10.3390/electronics10222797.

[7] A. A. Mutlag *et al.*, "Multi-agent systems in fog–cloud computing for critical healthcare task management model (CHTM) used for ECG monitoring," *Sensors*, vol. 21, no. 20, Oct. 2021, doi: 10.3390/s21206923.

[8] M. A. Mohammed *et al.*, "Adaptive secure malware efficient machine learning algorithm for healthcare data," *CAAI Trans Intell Technol*, 2023, doi: 10.1049/cit2.12200.

[9] D. J. Hemanth, J. Anitha, and G. A. Tsihrintzis, Eds., *Internet of Medical Things*. Cham: Springer International Publishing, 2021. doi: 10.1007/978-3-030-63937-2.

[10] M. Jmaiel, M. Mokhtari, B. Abdulrazak, H. Aloulou, and S. Kallel, Eds., *The Impact of Digital Technologies on Public Health in Developed and Developing Countries*, vol. 12157. in Lecture Notes in Computer Science, vol. 12157. Cham: Springer International Publishing, 2020. doi: 10.1007/978-3-030-51517-1.

[11] A. Lakhan, M. A. Mohammed, S. Kadry, S. A. AlQahtani, M. S. Maashi, and K. H. Abdulkareem, "Federated Learning-Aware Multi-Objective Modeling and blockchain-enable system for IIoT applications," *Computers and Electrical Engineering*, vol. 100, May 2022, doi: 10.1016/j.compeleceng.2022.107839.

[12] S. Razdan and S. Sharma, "Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies," *IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India)*, vol. 39, no. 4. Taylor and Francis Ltd., pp. 775–788, 2022. doi: 10.1080/02564602.2021.1927863.

[13] K. Hameed Abdulkareem *et al.*, "Smart Healthcare System for Severity Prediction and Critical Tasks Management of COVID-19 Patients in IoT-Fog Computing Environments," *Comput Intell Neurosci*, vol. 2022, 2022, doi: 10.1155/2022/5012962.

[14] K. Alatoun, K. Matrouk, M. A. Mohammed, J. Nedoma, R. Martinek, and P. Zmij, "A Novel Low-Latency and Energy-Efficient Task Scheduling Framework for Internet of Medical Things in an Edge Fog Cloud System," *Sensors*, vol. 22, no. 14, Jul. 2022, doi: 10.3390/s22145327.

[15] Q. U. A. Mastoi, T. Y. Wah, R. G. Raj, and A. Lakhan, "A novel cost-efficient framework for critical heartbeat task scheduling using the internet of medical things in a fog cloud system," *Sensors (Switzerland)*, vol. 20, no. 2, Jan. 2020, doi: 10.3390/s20020441.

[16] A. Lakhan *et al.*, "Delay Optimal Schemes for Internet of Things Applications in Heterogeneous Edge Cloud Computing Networks," *Sensors*, vol. 22, no. 16, Aug. 2022, doi: 10.3390/s22165937.

[17] A. A. Mutlag, M. K. Abd Ghani, N. Arunkumar, M. A. Mohammed, and O. Mohd, "Enabling technologies for fog computing in healthcare IoT systems," *Future Generation Computer Systems*, vol. 90, pp. 62–78, Jan. 2019, doi: 10.1016/j.future.2018.07.049.

[18] M. A. Mohammed *et al.*, "Energy-efficient distributed federated learning offloading and scheduling healthcare system in blockchain based networks," *Internet of Things*, p. 100815, May 2023, doi: 10.1016/j.iot.2023.100815.

[19] A. Lakhan, M. A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, and N. Kumar, "Blockchain-Enabled Cybersecurity Efficient IIOHT Cyber-Physical System for Medical Applications," *IEEE Trans Netw Sci Eng*, 2022, doi: 10.1109/TNSE.2022.3213651.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

[20] A. Ayub Khan, A. A. Wagan, A. A. Laghari, A. R. Gilal, I. A. Aziz, and B. A. Talpur, "BIoMT: A State-of-the-Art Consortium Serverless Network Architecture for Healthcare System Using Blockchain Smart Contracts," *IEEE Access*, vol. 10, pp. 78887–78898, 2022, doi: 10.1109/ACCESS.2022.3194195.

[21] P. Lin, Q. Song, F. R. Yu, D. Wang, and L. Guo, "Task Offloading for Wireless VR-Enabled Medical Treatment with Blockchain Security Using Collective Reinforcement Learning," *IEEE Internet Things J*, vol. 8, no. 21, pp. 15749–15761, Nov. 2021, doi: 10.1109/JIOT.2021.3051419.

[22] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "BEdgeHealth: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain," *IEEE Internet Things J*, vol. 8, no. 14, pp. 11743–11757, Jul. 2021, doi: 10.1109/JIOT.2021.3058953.

[23] A. Lakhan *et al.*, "Cost-efficient service selection and execution and blockchain-enabled serverless network for internet of medical things," *Mathematical Biosciences and Engineering*, vol. 18, no. 6, pp. 7344–7362, 2021, doi: 10.3934/mbe.2021363.

[24] A. Lakhan, M. A. Mohammed, S. Kozlov, and J. J. P. C. Rodrigues, "Mobile-fog-cloud assisted deep reinforcement learning and blockchain-enable IoMT system for healthcare workflows," *Transactions on Emerging Telecommunications Technologies*, 2021, doi: 10.1002/ett.4363.

[25] A. lakhan, M. A. Mohammed, D. A. Ibrahim, and K. H. Abdulkareem, "Bio-inspired robotics enabled schemes in blockchain-fog-cloud assisted IoMT environment," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 1, pp. 1–12, Jan. 2023, doi: 10.1016/j.jksuci.2021.11.009.

[26] A. Lakhan *et al.*, "Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare," *IEEE J Biomed Health Inform*, vol. 27, no. 2, pp. 664–672, Feb. 2023, doi: 10.1109/JBHI.2022.3165945.

[27] A. Lakhan, M. A. Mohammed, M. Elhoseny, M. D. Alshehri, and K. H. Abdulkareem, "Blockchain multi-objective optimization approach-enabled secure and cost-efficient scheduling for the Internet of Medical Things (IoMT) in fog-cloud system," *Soft comput*, vol. 26, no. 13, pp. 6429–6442, Jul. 2022, doi: 10.1007/s00500-022-07167-9.

[28] L. Liu and Z. Li, "Permissioned Blockchain and Deep Reinforcement Learning Enabled Security and Energy Efficient Healthcare Internet of Things," *IEEE Access*, vol. 10, pp. 53640–53651, 2022, doi: 10.1109/ACCESS.2022.3176444.

[29] A. Lakhan, T. Morten Groenli, A. Majumdar, P. Khuwuthyakorn, F. Hussain Khoso, and O. Thinnukool, "Potent Blockchain-Enabled Socket RPC Internet of Healthcare Things (IoHT) Framework for Medical Enterprises," *Sensors*, vol. 22, no. 12, Jun. 2022, doi: 10.3390/s22124346.

[30] S. Ahmed, A. Lakhan, O. Thinnukool, and P. Khuwuthyakorn, "Blockchain Socket Factories with RMI-Enabled Framework for Fine-Grained Healthcare Applications," *Sensors*, vol. 22, no. 15, Aug. 2022, doi: 10.3390/s22155833.

[31] A. Lakhan *et al.*, "Restricted Boltzmann Machine Assisted Secure Serverless Edge System for Internet of Medical Things," *IEEE J Biomed Health Inform*, vol. 27, no. 2, pp. 673–683, Feb. 2023, doi: 10.1109/JBHI.2022.3178660.

[32] A. Lakhan, M. A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, and N. Kumar, "DRLBTS: deep reinforcement learning-aware blockchain-based healthcare system," *Sci Rep*, vol. 13, no. 1, Mar. 2023, doi: 10.1038/s41598-023-29170-2.

[33] A. Lakhan *et al.*, "Smart-contract aware ethereum and client-fog-cloud healthcare system," *Sensors*, vol. 21, no. 12, Jun. 2021, doi: 10.3390/s21124093.

[34] H. Sedghamiz, "Matlab Implementation of Pan Tompkins ECG QRS Detector," 2014.

[35] G. Roland, J. Dhana Sony, S. N. Padhi, S. Kayalvili, S. Cloudin, and A. Kumar, "An Automated System for Arrhythmia Detection using ECG records from MITDB," in *International Conference on Automation, Computing and Renewable Systems, ICACRS 2022 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 26–33. doi: 10.1109/ICACRS55517.2022.10029289.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023

[36] J. Liu, S. Song, G. Sun, and Y. Fu, "Classification of ECG Arrhythmia Using CNN, SVM and LDA," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer Verlag, 2019, pp. 191–201. doi: 10.1007/978-3-030-24265-7_17.

[37] M. A. Ahamed, K. A. Hasan, K. F. Monowar, N. Mashnoor, and M. A. Hossain, "ECG heartbeat classification using ensemble of efficient machine learning approaches on imbalanced datasets," in *2020 2nd International Conference on Advanced Information and Communication Technology, ICAICT 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020, pp. 140–145. doi: 10.1109/ICAICT51780.2020.9333534.

Doi: https://doi.org/10.54216/FPA.140117
Received: July 21, 2023 Revised: October 15, 2023 Accepted: December 05, 2023