ISSN: 2182-2069 / E-ISSN: 2182-2077

# Cardiac Waveform Inspired Optimized Key Generation Technique ROLE for SAFED to Secure Medical IoT Data Transmission

A.N. Sanjeev Kumar[1*], and B. Ramesh Naik[2]

[1*]Assistant Professor, Department of CSE, GITAM School of Technology, GITAM Deemed University, Nagadenehali, Doddaballapur Taluk, Bengaluru, Karnataka, India.
sanjeevitech82@gmail.com, https://orcid.org/0000-0003-0793-1345

[2]Associate Professor, Department of CSE, GITAM School of Technology, GITAM Deemed University, Nagadenehali, Doddaballapur Taluk, Bengaluru, Karnataka, India.
rbhukya@gitam.edu, https://orcid.org/0000-0002-9082-7364

Received: February 11, 2025; Revised: March 24, 2025; Accepted: May 05, 2025; Published: May 30, 2025

## Abstract

The Signal Apex Follower Encryption Decryption (SAFED) approach addresses the confidentiality issues of the IoT device data and employs a persistent security mechanism for the data under transmission. The adaptability of the SAFED approach is evident from the initial stage of cardiac waveform signal (ECG) processing with the Finite Impulse Response (FIR) filter to obtain the fine-tuned ECG signal. The obtained signal is subjected to generating a Binary Sequence, ECG features are extracted through DB4, and an enhanced binary sequence quality conversion mechanism empowered with a ROLE hashing technique to generate a hash value as the private key for the encryption. With this private key and the Binary sequence of P-peaks, the SAFED algorithm encrypts the patient's medical record to ensure secure data transmission across the network. The SAFED performance is articulated from Binary Sequence Generation to key employment for Encryption and Decryption. The technique's overall performance ensures greater data security over communication and ease of adaptability for resource-constrained real-time applications with optimized key size and reduced encryption and decryption time.

**Keywords:** Point of Care, Electrocardiogram, Signal Apex Follower, Right Odd Left Even, Daubechies DB4 Wavelet.

## 1 Introduction

The contemporaneity of healthcare has dramatically increased over the past decades to optimize labor costs and to enhance remote patient monitoring systems through Point of Care (PoC) and various wearable devices assisting human health monitoring Sumithra & Sakshi (2024). The advancements in technologies such as the Internet of Things (IoT) and Data Analytics furnish the requirements for the design of Advanced Healthcare Systems integrated with continuous monitoring Malhotra & Joshi (2025). The PoC's primary purpose is to minimize the traffic at the healthcare centres by treating the

*Journal of Internet Services and Information Security (JISIS)*, volume: 15, number: 2 (May), pp. 480-498.
DOI: *10.58346/JISIS.2025.I2.034*

*Corresponding author: Assistant Professor, Department of CSE, GITAM School of Technology, GITAM Deemed University, Nagadenehali, Doddaballapur Taluk, Bengaluru, Karnataka, India.

patients at their homes, where the remote doctors monitor the data generated by the various devices at PoC as depicted in Figure 1.

Faster data transmission and data security by protecting patient data from threats in the healthcare industry is major concern in real-time applications like PoC Menon & Patil (2023). The emergency circumstances are to be handled at PoC via rapid data transmission, and data security by ensuring the system dependability through the use of common cryptographic techniques and effective resource management. IoT in healthcare makes it possible for objects to coordinate and communicate to carry out activities collectively. Secure communication across the IoT network is important because IoT sensors generate vast amounts of sensitive and non-sensitive data, which needs to be communicated in the IoT Network Moosavi et al. (2016).

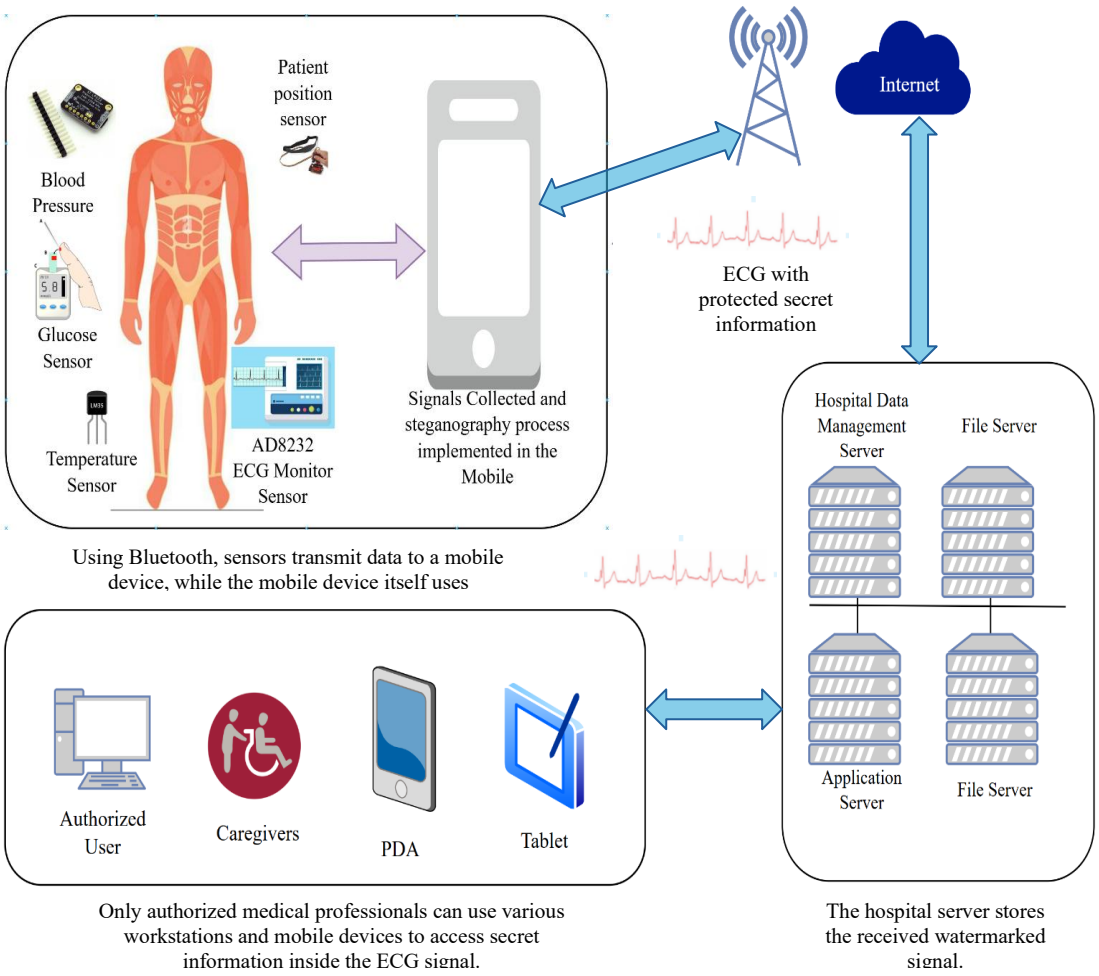


Figure 1: Patient Monitoring at PoC

The PoC collects the patient's bio-physiological data, which is then labelled with personally identifiable information and transferred over the internet by an IoT environment. The data must be protected against unwanted access during transmission. Data privacy is ensured by data concealing for secure communication. Patient Monitoring at PoC is depicted in Figure 1. By using public and private keys for secure communication through encryption and decryption procedures, cryptography enables data concealing during transmission. The creation of keys in a resource-constrained environment for

successful and efficient data transfer is a crucial component of cryptography. The generated key encrypts the patient's medical and personal data Moosavi et al. (2017).

One among the patient data the patient's cardiac waveforms, known famously as Electrocardiogram (ECG) signals are used as a cryptographic parameter for the optimization of the key size. The cardiac waveforms are the significant and unique feature of a human being in the healthcare data employable for the secured communication to enhance the performance with the distinctive biometric characteristics of a person Padmapriya et al. (2024).

## 2 Related Works

Data confidentiality ensures access to the correct information by valid users. In protecting sensitive data from being exposed to malicious activities, the set of rules to impose on data access, encryption, and decryption serves the purpose. The lightweight cryptographic approach is in demand in a resource-constrained environment, and it may include XOR manipulations, hash computations, and so on.

The primary requirement of the cryptographic approach is a key management system addressing it Moosavi et al. (2017) proposed an ECG-based key generation for the body area networks. With the foundation of InterPulse Interval (IPI), a feature of the ECG, the approach provides two different key generation mechanisms. The first approach integrates the consecutive IPI sequences with Linear Feedback Shift Register (LFSR) for pseudo-random number generation, and implementing the Advanced Encryption Standard (AES) algorithm along with the IPI yields the second approach. The key generation mechanisms for security concerns are evaluated with the help of the MIT-BIH Arrhythmia dataset. As a result, the greater security is achieved. However, the computation time has yet to be optimized for key generation with AES Udayakumar et al., (2023).

González-Manzano et al. (2017) have proposed Encryption by Heart, a time-invariant symmetric key for wearable devices based on ECG for securing user data via encryption. The timely changing ECG signal adoption for decryption ensures higher security over the static keys generated simultaneously for both encryption and decryption. A real-time experiment was conducted over 24 hours for 199 users to evaluate the approach. It ensures that 95.97% of unique keys are generated with various lengths with optimized entropy. However, the training time optimization, re-encryption, key renewals, and more significant extended-period datasets are challenging.

Zheng et al. (2018) implement ECG-based security techniques for the Wearable and Implantable Medical Devices (WIMDs). The dual approach of cryptography using ECG-KD is fuzzy commitment and vault, where the polynomial computation and binary sequence generation are employed as the key distribution technique. The improved accuracy with the least false rejection rate is shown with the optimized cost for the wearable devices. The concern is that the enhanced precision and efficiency for the polynomial computations is a challenging one.

Janveja et al. (2020) proposed a lightweight version of Advanced Encryption Standard (AES) for low-powered IoT applications. The approach employs the modified version of AES architecture by a folded pipeline powered by time multiplexing for the encryption and decryption of the ECG data. The approach ensures the least computational power for the deployment, and ease of hardware implementation enables greater portability. Applicability to heterogeneous IoT applications is to be challenging.

The impact of IoT on the healthcare sector simplifies the living style of the patient through the Point of Care (PoC), but the private data on the IoT network has to be secure enough (Karimov & Sattorova

(2024). Addressing the security issues in healthcare, Ibaida & Khalil (2013) implement an ECG-based encryption technique that integrates wavelet-based steganography and scrambling techniques to ensure the confidentiality of patient data Shrivastav & Malakar (2024). The technique is evaluated based on the percentage residual variance and weighted PRD metrics to ensure efficient security. The ECG signal is watermarked in the approach, and the removal of the watermark leads to data utility issues.

Suggested a lightweight way to encrypt images using the ChaCha20 and Serpent algorithms with 16 rounds. It was shown that the system is quite secure and can withstand known and selected plaintext assaults.

The cypher was found to work well in places with limited resources, such as cloud systems and social media. We employed security indicators, including histogram analysis, entropy, and correlation, to judge.

It was claimed that the entropy value was 7.98 and the normalised pixel difference rate was more than 99.55%. The encryption approach has a high level of key sensitivity and unpredictability. It was found that the decryption method worked well, which meant that the data could be recovered.

Premkumar & Mohana (2020) employ the scrambling matrix integrated with the shared key to secure patient data via an ECG-based encryption mechanism. The same key decrypts patient-sensitive data and reconstructs the ECG signal on demand. The approach implements the Lyapunov exponent spectrum for the ease of extraction of the human ECG for the purpose of a secret key in encrypting the text and images. It also uses the chaotic cryptosystem for masking private keys. During masking, noise is added for safety purposes. The technique is highly reliable and quick due to its smaller key size, but misuse of the key leads to ECG signal exploration by hackers to steal the patient's sensitive data Karthik & Krishnan (2021).

Addressing the shortcomings of the existing technique in data confidentiality for resource-limited applications, an effort is made to use the Cardiac Waveform-based encryption and decryption for secure communication in Medical IoT applications. The contributions for secure communication are listed below:

(i) Generation of Fine-grained time-variant Cardiac Waveform (ECG) by employing an FIR filter.

(ii) Optimized Key Generation by processing and mapping the features from a finetuned Cardiac Waveform using DB4 and Private key generation by employing the ROLE hashing technique.

(iii) Security Booster is generated in parallel using DB4 with P-peaks of ECG signal as Binary Sequence.

(iv) Employing the Key generated and P-peaks for efficient data encryption and decryption of patient data based on SAFED.

The overall approach of the secured device data transmission, considering above listed contributions for Medical IoT applications for encryption and decryption, are provided below in forthcoming sections.

# 3 Low-Latency Cryptographic Approach Empowered with ROLE and SAFED

The automation of healthcare centres should maintain interoperability across medical devices for diagnostic monitoring between physicians and patients for treatments and therapy. The primary requirement for automation is secured and efficient data communication in the PoC ecosystem to

enhance patient life quality by mitigating patient data's from the adversaries. Although a wide range of techniques exists in communication security, a significant gap in addressing effective communication still exists. The exceptional challenge in the communication security literature is ensuring the end-to-end communication design with the efficient crypto-key generation technique with the available medical time-line ECG data to communicate beyond the local network boundaries.

The primary goal of the approach is to ensure the security of the patient data under communication by employing the optimized low-latency cryptographic approach built upon the ECG signal as the baseline. The approach mitigates data snooping and data tampering so that patients' medical records are securely communicated. The overall structural outline of the optimized low-latency cryptographic approach integrated with the ECG signal is pictorially represented in Figure 2. Which incorporates all the stages of the cryptographic approach for secured end-to-end communication. The proposed end-to-end communication technique is implemented in the three stages, which are as follows:

1. Cardiac Waveform Pre Processing for Binary Sequence and P-peaks Binary Sequence generation.
2. ROLE Hashing Technique for Private Key Generation.
3. SAF Encryption / Decryption Technique for secure communication.

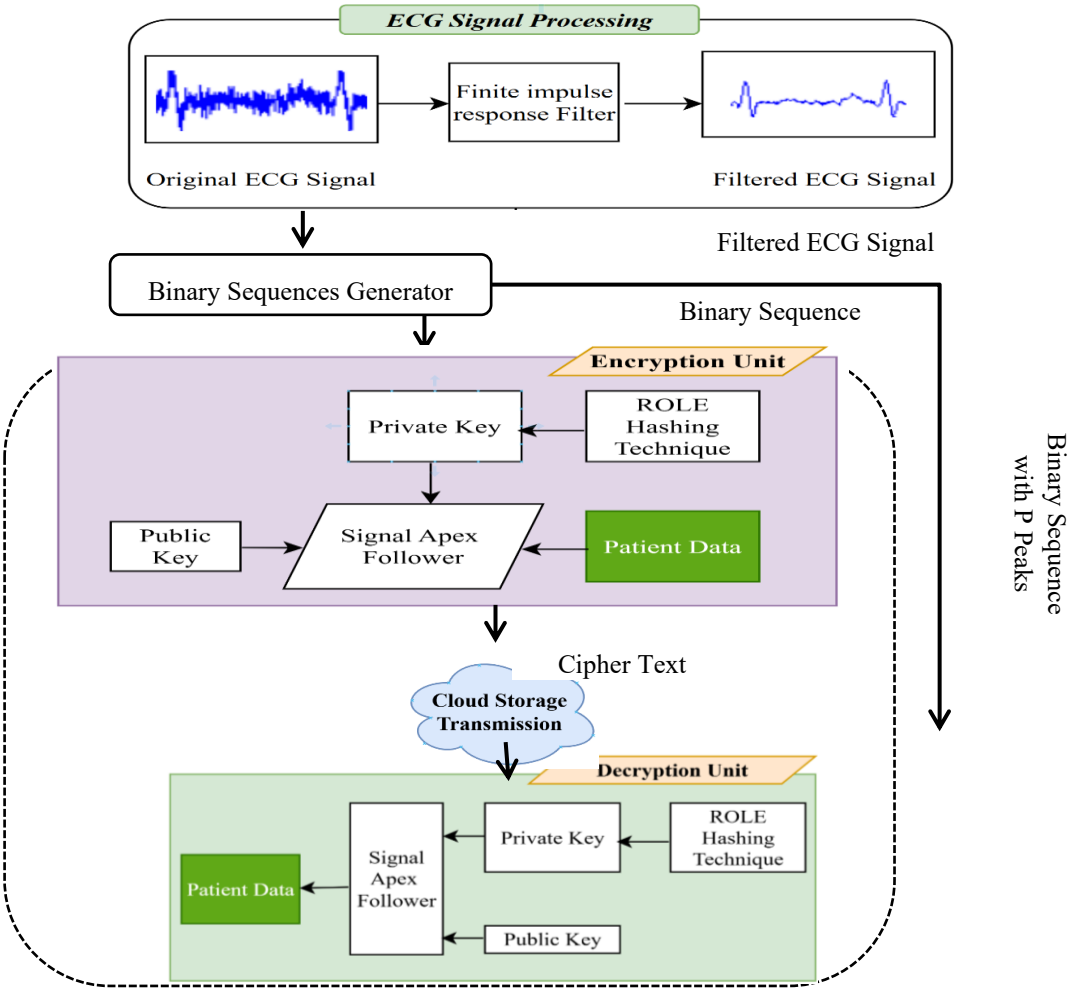


Figure 2: Structural Outline of Low-Latency Cryptographic Approach

In medical IoT, the patient's sensitive data, such as medical records, including diagnostic results and treatment, must be secured to ensure the data's confidentiality and authenticity. The devices that collect the patient's health data, such as blood sugar level, BP, etc., must be constantly protected from unauthorized access and securely transmitted to the required destinations. Structural Outline of Low-Latency Cryptographic Approach is depicted in Figure 2. SAF integration with the encryption and decryption methods ensures lightweight key generation from the ECG signal, as well as time and key size optimized encryption and decryption approach for the secured sensitive data transmission. The overall algorithmic approach is presented in the Signal Apex Follower Algorithm.

---

**Algorithm 1:** Signal Apex Follower Algorithm

**Input:** Medical Record (MR) and ECG Signal ('E')

**Output:** Encrypted Medical Record (ER)

---

1. Scan the ECG Signal ('E').
2. Extract 10 seconds of ECG signal with 500Hz as frequency.
3. Compute Number of Samples = frequency * time (5000 samples).
4. ECG Signal ('E') Pre-Processing with FIR
5. for n ⟵ 1 to 10 seconds do
6. $y[n] = \sum_{k=0}^{N-1} b[k].x[n-k]$
7. Obtained Filtered ECG Signal Subjected to Binary String Generation (Bs)
8. Bs = DB4 ($y[n]$)
9. Obtained Filtered ECG Signal Subjected to P-peak Binary String Generation (BP)
10. BP = DB4 ($y[n]$)
11. Feed the Bs to ROLE Hashing Technique to get Private Key (Pk)
12. Pk = ROLE( Bs )
13. Perform the data encryption with SAFE
14. ER = SAFE(MR, Pk, BP)
15. End

---

### 3.1 Cardiac Waveform Pre-Processing for Binary String and P-peaks Binary String generation.

ECG is one of the sensitive parameters in the medical field; removing unwanted noise from the ECG is very important in biomedical signal processing. The noise-biased ECG signal represents the critical points of ECG titled P, Q, R, S, and T waves uniquely for further processing. Eliminating the noise from the ECG Signal is the first step toward the optimized low-latency cryptographic method before the binary sequence generation. The most applied filters for the filtration of an ECG signal are digital filters. FIR digital filter works well for eliminating noise in low and high-frequency signals, as stated in the literature (Qiu et al., 2020).

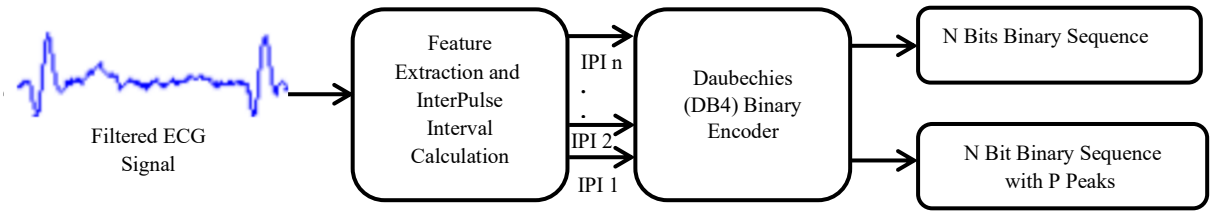


Figure 3: ECG Signal Pre-Processing and Binary Sequence Generation

The FIR filter eliminates the noise to enhance the signal quality through a sequence of steps for the original ECG signal input. It primarily focuses on noise identification from the input signal, which may be caused by baseline wander, powerline interface, and muscle artifacts. The FIR was equipped with a band-pass and Hamming window to enhance performance, reasoning regarding the main and side lobe attenuation, and consideration of the low-pass and high-pass frequency ranges Abdulbaqi et al. (2021). ECG Signal Pre-Processing and Binary Sequence Generation is depicted in Figure 3. The convolution of the ECG signal with the filter coefficients improves the performance, and the same is evaluated with the help of Signal-to-Noise Ratio (SNR), Power Spectral Density (PSD), and visual inspection of the ECG waveform. FIR Filter employs the Equation 1 for the computation and the same is given as:

$$y[n] = \sum_{k=0}^{N-1} \mathrm{b[k]}.\,\mathrm{x[n-k]} \quad (1)$$

Where:

(y[n]) is the output (filtered signal) at time (n).

(x[n]) is the input (ECG signal) at time (n).

(b[k]) are the filter coefficients [Fourier Transform of frequency transfer function].

(N) is the number of filter coefficients (filter order + 1).

The quality-enhanced ECG signal is considered for binary sequence generation. Daubechies wavelet transform is employed to extract the significant points P, Q, R, S, and T recorded under the unique cardiac waveform (ECG signal). The substantial nature of the Daubechies DB4 wavelet is its higher reliability and resemblance in its scaling function to the shape and identification of the features of ECG signals. The approach primarily relies on ECG signal conversion to a binary sequence with the help of Daubechies DB4 wavelet feature extraction functionality, and the P-peak location is extracted based on the fiducial points with the P feature. The DB4 has a total of four wavelet and scaling function coefficients. Suppose the primary dataset has N values; then the wavelet function needs to be computed and employed in the order of N /2 differences, reflecting the data change Moosavi et al. (2016). The DB4 scaling (a) and wavelet (c) functions are represented in Equations 2 and 3, respectively.

$$\mathrm{ai} = \mathrm{h0S2i} + \mathrm{h1S2i{+}1} + \mathrm{h2S2i{+}2} + \mathrm{h3S2i{+}3} \quad (2)$$

$$\mathrm{ci} = \mathrm{g0S2i} + \mathrm{g1S2i{+}1} + \mathrm{g2S2i{+}2} + \mathrm{g3S2i{+}3} \quad (3)$$

Where ‘h’ indicates the scaling function coefficients, and ‘g’ indicates the wavelet function coefficients. Equation 4, 5, 6, and 7 are employed for the computation of ‘h’ and ‘g’ values.

$$h_0 = \frac{1+\sqrt{3}}{4\sqrt{2}} = -g_3 \quad (4) \qquad h_1 = \frac{3+\sqrt{3}}{4\sqrt{2}} = g_2 \quad (5)$$

$$h_2 = \frac{3+\sqrt{3}}{4\sqrt{2}} = -g_1 \quad (6) \qquad h_3 = \frac{1-\sqrt{3}}{4\sqrt{2}} = g_0 \quad (7)$$

The DB4 oversees the calculation of the wavelet function and scaling function value for each iteration with an index increment of i. The heart rate and accompanying ECG recording are within the normal range in a typical sinus rhythm. Variations in the ECG signals caused by cardiac problems may occur when DB4 overheads are used to extract the required information from a single heartbeat wave. In these situations, features are detected and extracted, and calculations are carried out using the collected waves, the summed wavelet, and scaling functions. Once the dependable P peak spots with the greatest amplitude have been found, the remaining calculations are processed further. The type of ECG signal and the applications for which it is used determine how much intelligence is needed to extract the feature. This allows for the optimization of key generation techniques using efficient cardiac waveform-based cryptography systems. Because it requires fewer processing time and coefficients, DB4 is the most economical and time-efficient approach for extracting features from ECG signals.

### 3.2 ROLE: Right Odd Left Even 2 – bit rotation Hashing Technique.

Cryptographic key generation and validation across the sender and receiver are carried out under ROLE hashing technique. The steps in the approach are diagrammatically represented in Figure 4.

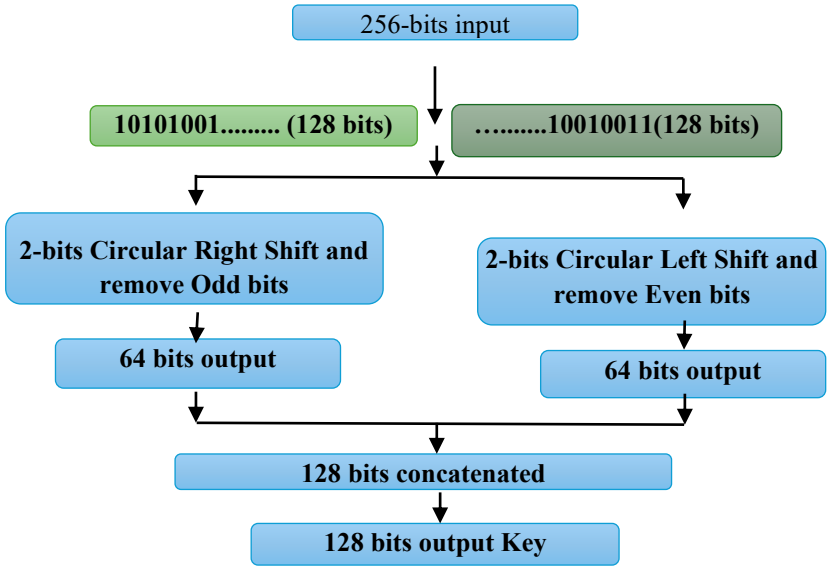


Figure 4: ROLE Hashing Technique for Key Generation

The technique is implemented on the binary sequence obtained from finetuned ECG signal is shown in Figure 4. The binary sequence entropy has to be enhanced by adding the randomness for critical cryptographic key generation. The generated cryptographic key ensures higher security levels with optimized key generation time. The ROLE technique integrates the mechanism of enhancing the randomness of the binary sequence with the low-cost shift and drop operation before generating the hash value in terms of base 64 representation.

Pre-processing of the binary sequence is carried out to meet the key properties of the cryptographic algorithms, such as randomness, sufficient length of the key generated, and uniform distribution. The obtained binary sequence is validated for its length, and randomness is enhanced through entropy for its unpredictability. The binary sequence obtained from the ECG signal may not always be the required length. The approach defines the binary sequence length to be processed as 256 bits; if the number of bits in the obtained binary sequence is more than the first 256 bits, it is considered. Otherwise, the '0' has been padded to the most significant side of the binary sequence.

---

**Algorithm 2:** ROLE Hashing Algorithm

**Input:** ECG Signal as Binary Sequence (Bs)

**Output:** Cryptographic Hash Key (CHK)

---

1. Analyse the Binary Sequence: Bs
2. Convert the Bs to Binary String B ss
3. Length = strlen (B ss)
4. if Length > 256 then
5. B ss = B ss [:255]
6. else
7. B ss = ('0'* (256 – Length)) + B ss
8. end if
9. Split B ss to 2 Equal parts of 128bits
10. B ssl - Left 128bits of B ss
11. B ssr – Right 128 bits of B ss
12. Apply Right 2 – bit Rotation on Odd removal to get UB ssl.
13. Apply Left 2 – bit Rotation on Even removal to get UB ssr.
14. CHK = UB ssl. $\oplus$ UB ssl.

---

The typically binary sequence generated from the ECG signal possesses less randomness due to the characteristic nature of the ECG signal. To ensure the unpredictability of the binary sequence employed for the key generation, additional entropy is added using the ROLE hashing technique for the improved randomness of the binary sequence and to optimize the risk to the cryptographic approach. The unpredictable binary sequence is processed by the hashing function ROLE to generate the cryptographic key. The processed fixed-length binary sequence ensures that it exhibits the cryptographic nature and properties as a secure way of communication. The generated 128 bits (Converted to Base 64) hash value is considered as the cryptographic key Ibaida & Khalil (2013).

### 3.3 Signal Apex Follower – Encryption / Decryption

The biometric characteristics and the uniqueness of the ECG signals play a significant role in incorporating them into the cryptographic systems. The highly individualistic nature of the ECG signal ensures greater distinguishability across the cryptographic keys generated for the encryption and decryption procedures. The cryptographic key generated on processing the ECG signal features is employed on medical data, which is applicable during encryption and decryption. Encryption is an encoding mechanism where the plain data is encoded so only authorized persons can access it. The encryption mechanism generally uses massive computational assets and abilities, whereas the optimized version of encryption and decryption can be quickly assured with the SAFED Premkumar & Mohana (2020).

SAFED integrates the Binary Sequence generated based on P-peaks of the ECG signal as Binary String, the cryptographic key generated with medical data to be encrypted and the same is applicable during the decryption with the encrypted data. The approach resembles the symmetric block cipher model structure that encrypts and decrypts a continuous block of data with 128 bits using a unique key. For ease of display, the base64 representation of the encrypted data is received Janveja et al. (2020).

Encrypted medical data transmitted securely across a network ensures that the right person receives it. In order to convert the encrypted data into a readable format once it has been received and reprocessed, interpretation must be applied. Decryption is the term used to describe the procedure used to do it. Using the encryption key, the device decrypts the data by analysing it and turning it into legible text. The same key that was used for encryption must be used for decryption in SAFED and the Binary String obtained based on the P-peaks of ECG signal. By using the ROLE Hashing process, SAFED makes it easier to regenerate the same cryptographic key at the destination by making the use of Binary Sequence generated from the ECG signal. After obtaining the private key, the encrypted data is processed to obtain the original data in a readable format.

# 4 Experimental Setup and Results

Low-latency cryptographic key generation for secure transmission of Medical IoT data based on ECG Signal features is implemented on the MIT-BIH Arrhythmia dataset with modifications. Tools such as MAT Lab and Python programming and its primary packages, such as pycryptodome and pywavelets, are used for the implementation. The comparative analysis of the SAFED approach is carried out with state-of-the-art cryptographic methods like AES, RSA, ECC, and Chaotic Systems.

## 4.1 Dataset

The MIT-BIH Arrhythmia database is publicly available through the PhysioNet platform. It consists of ECG raw images and processed values. The dataset has 48 half-hour ECG recordings, resulting in almost 24 hours of data. Every recording is captured across a 1 mV range at 360 Hz with an 11-bit resolution. Two channels are used to record the ECG signals; one lead of ECG data is provided by each channel. The MIT-BIH Arrhythmia Database is primarily considered for researching and detecting various types of prevalent arrhythmias like Normal sinus rhythm (N), premature ventricular contractions (PVC), premature atrial contractions (PAC), Atrial fibrillation (AF), Ventricular fibrillation (VF), Bradycardia and Tachycardia.

## 4.2 Performance Analysis

The performance record of the SAFED for the Low-latency cryptographic approach on the Modified MIT-BIH Arrhythmia dataset is articulated in the following sections by considering the Quality of the Binary Sequence Generated, Encryption, and Decryption as the primary concerns. Mean Equal-Error Rate (MEER), Standard Deviation Equal-Error Rate (SD-EER), and Entropy are the metrics for method comparison of Binary Sequence. Encryption approaches are measured by Encryption Time, Reconstruction Time, and Encryption Size Naik (2023).

The accuracy and dependability of the approach improve with a lower MEER value. The Mean Equal-Error Rate (MEER) percentages across five indices (Abdulbaqi et al., 2021; Malhotra & Joshi, 2025; Premkumar & Mohana, 2020; Naik, 2023; Janveja et al., 2020) are compared and represented in Figure. 5. An increase in performance is indicated by the linear congruential generator (LCG) approach,

which shows a declining trend in MEER from 2.5% to 1.8% throughout the indices. A notable improvement in accuracy and dependability over the indices is indicated by the MACE Filtering method's MEER, which starts at 2.5% and drops to 1.2%. Mersenne Twister's MEER values, which range from 1.8% to 1.2%, demonstrate steady progress and strong performance. With MEER values between 1.7% and 1%, the Bio-convolving Approach consistently and significantly improves performance across all indices. With the lowest MEER values (varying from 1.3% to 0.8%) of all the approaches examined, the SAFED method appears to perform the best in terms of accuracy and dependability showing that it gives the most balanced and accurate outcomes in terms of error minimization.

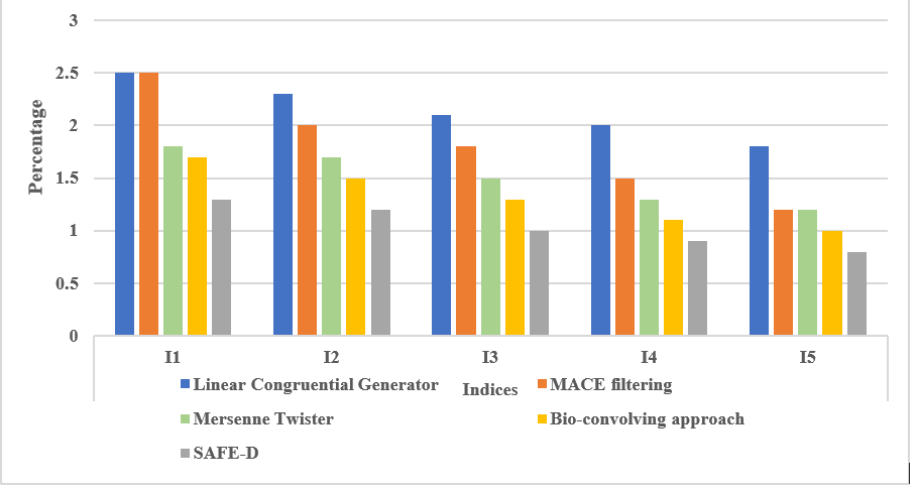


Figure 5: Mean Equal-Error Rate (MEER) (%) Comparison

The SD-EER percentages for different techniques across five indices (I1 to I5) are compared and the difference in error rates when erroneous rejections and false acceptances are equal is displayed in SD-EER Figure 5. When the SD-EER value is smaller, the approach's performance is more reliable and consistent. As evidenced by the SD-EER going lower from 0.3% to 0.2% across the indices utilizing the LCG technique, consistency and dependability have improved.

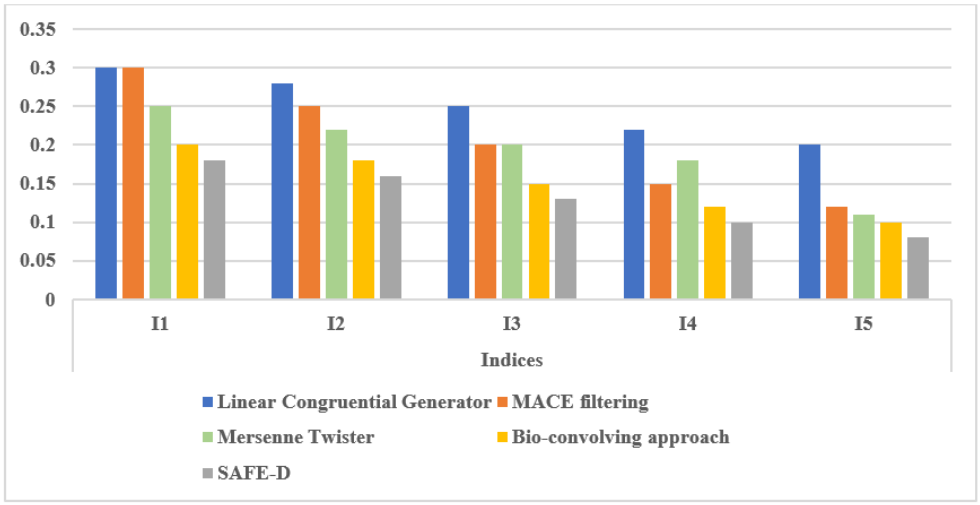


Figure 6: Standard Deviation Equal-Error Rate (SD-EER) (%) Comparison

Starting at 0.3% and falling to 0.12%, the SD-EER of the MACE Filtering technique indicates a significant improvement in consistency over the indices. The stability and dependability of Mersenne Twister are continually improved, with SD-EER values ranging from 0.25% to 0.11%. The bio-convolving technique consistently and significantly improves consistency across the indices, with SD-EER values ranging from 0.2% to 0.1%. The SAFED technique's lowest SD-EER values, which vary from 0.18% to 0.08% among the methods offered, demonstrate that it performs better than all indices in terms of consistency and reliable results in terms of error variability minimization. Standard Deviation Equal-Error Rate (SD-EER) (%) Comparison is shown in Figure 6.

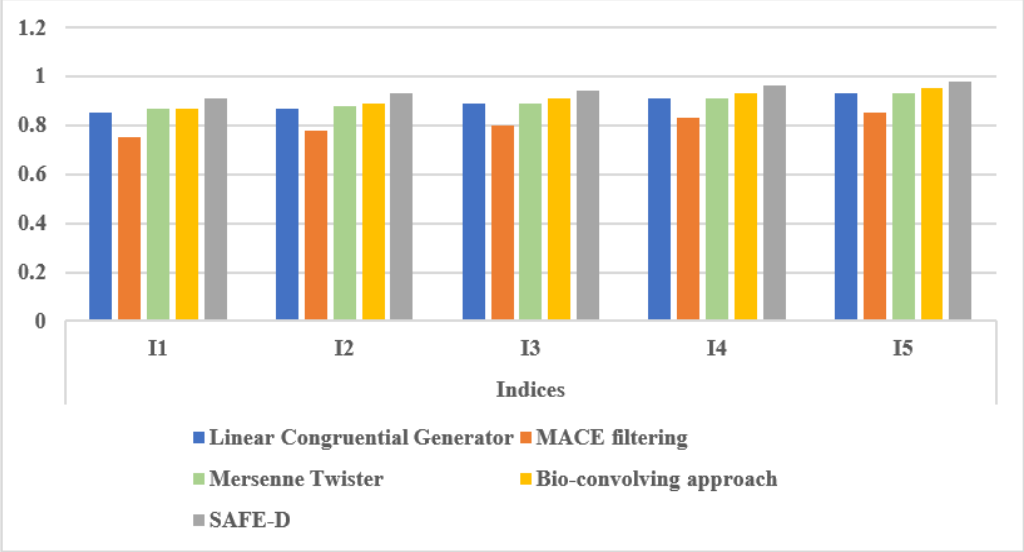


Figure 7: Entropy Table Analysis (in bits)

The entropy measures of Twister Mersenne, which are similar to LCG and range between 0.87 and 0.93, indicate a very high degree of randomness and are widely known for their better pseudo-random numbers. The Bio-convolving Approach is slightly more unpredictable than the LCG and Mersenne Twister and has entropy values ranging from 0.87 to 0.95. With entropy values between 0.91 and 0.98, the SAFED method produces the most random and non-deterministic data among all the strategies discussed. Compared to the rest of the techniques in the Figure 7, the SAFED technique outperforms the other methods in creating random data based on the nature of the ECG signal on embedding the ROLE method.

Table 1: Encryption Time Consumption (in ms)

| Data samples (in bits) | Methods | | | | |
|---|---|---|---|---|---|
| | RSA | CS | ECC | AES | SAFED |
| DS1 | 30 | 5 | 10 | 2 | 1.8 |
| DS2 | 32 | 5.5 | 10.2 | 2.1 | 1.9 |
| DS3 | 35 | 6 | 10.5 | 2.2 | 2 |
| DS4 | 60 | 12 | 20 | 4 | 2.3 |
| DS5 | 65 | 12.5 | 20.5 | 4.1 | 2.5 |

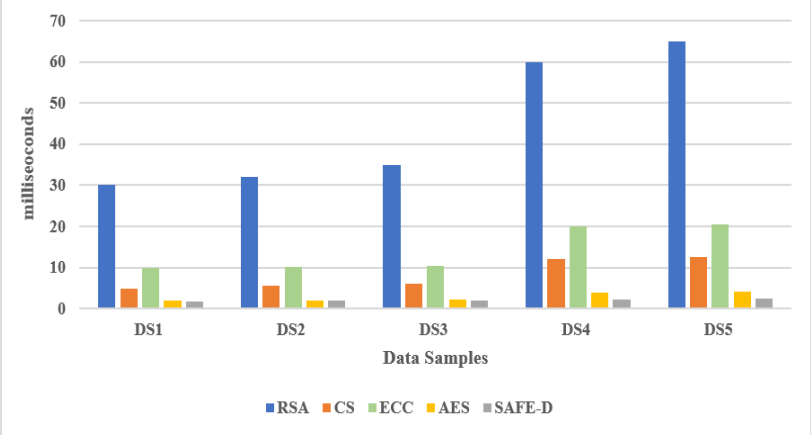


Figure 8: Encryption Time Consumption (in ms)

The largest encryption sizes are achieved by the RSA approach, which ranges from 2048 bytes for DS1 (1024 bits) to 4096 bytes for DS5 (2048 bits) in Table 1. The CS technique's encryption sizes, which range from 128 to 256 bytes, are substantially less than those of RSA, suggesting a markedly improved storage efficiency. The AES technique also demonstrates increased efficiency with encryption widths between 128 and 256 bytes, which are similar to CS. The ECC technique has mediocre efficiency with encryption sizes ranging from 86 to 174 bytes. It requires less storage than RSA, CS, and AES. Because SAFED has the smallest encrypted length—between 48 and 98 bytes—it requires the least amount of storage out of all the techniques that were examined. In conclusion, because the SAFED technique has the lowest encryption size values compared to the other methods shown, it performs better and uses less storage space. Encryption Time Consumption is depicted in Figure 8.

Table 2: Reconstruction Time Consumption (in ms)

| Data samples (in bits) | Methods | | | | |
|---|---|---|---|---|---|
| | RSA | CS | ECC | AES | SAFED |
| DS1 | 25 | 10 | 8 | 1 | 0.8 |
| DS2 | 27 | 11 | 8.5 | 1.1 | 0.9 |
| DS3 | 30 | 12 | 9 | 1.2 | 1 |
| DS4 | 55 | 25 | 18 | 2 | 1.2 |
| DS5 | 60 | 26 | 18.5 | 2.1 | 1.3 |

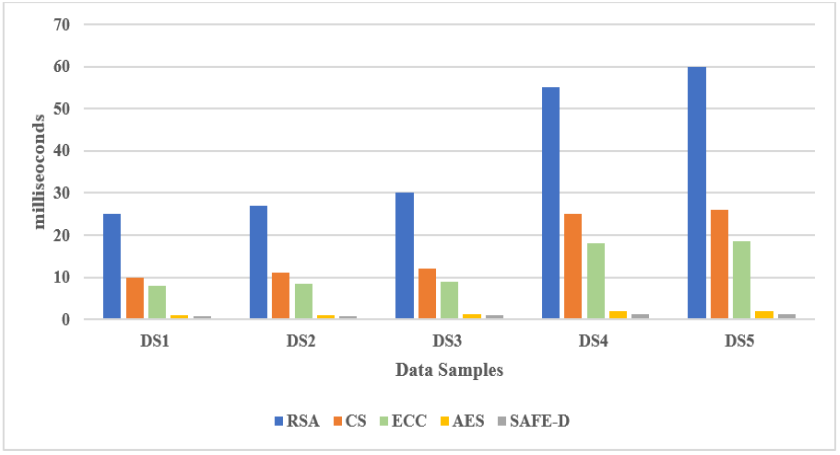


Figure 9: Reconstruction Time Consumption (in ms)

The RSA method's reconstruction time rises with sample bit size, from 25 ms for DS1 (1024 bits) to 60 ms for DS5 (2048 bits) in Table 2. Out of all the techniques shown, RSA requires the longest time to reconstruct. Since the CS approach's reconstruction timeframes are shorter (10–26 ms), it is more effective than RSA. The ECC technique has reconstruction times of 8–18.5 ms, indicating a reasonable level of efficiency. It is less effective than AES and SAFED, but more effective than RSA. The AES approach is much faster at reconstructing data samples, with reconstruction periods ranging from 1 ms to 2.1 ms. With reconstruction times ranging from 0.8 to 1.3ms, the SAFED approach is the most efficient of the methods examined. Because the SAFED approach requires the least amount of rebuilding time, it is therefore superior and more effective than the other methods. SAFED is the fastest method for reconstructing data samples. Reconstruction Time Consumption is depicted in Figure 9.

Table 3: Encryption size analysis (in bytes)

| Data samples (in bits) | Methods | | | | |
|---|---|---|---|---|---|
| | RSA | CS | AES | ECC | SAFED |
| DS1 | 2048 | 128 | 128 | 86 | 48 |
| DS2 | 2080 | 130 | 130 | 88 | 66 |
| DS3 | 2112 | 132 | 132 | 90 | 86 |
| DS4 | 4000 | 250 | 250 | 170 | 92 |
| DS5 | 4096 | 256 | 256 | 174 | 98 |

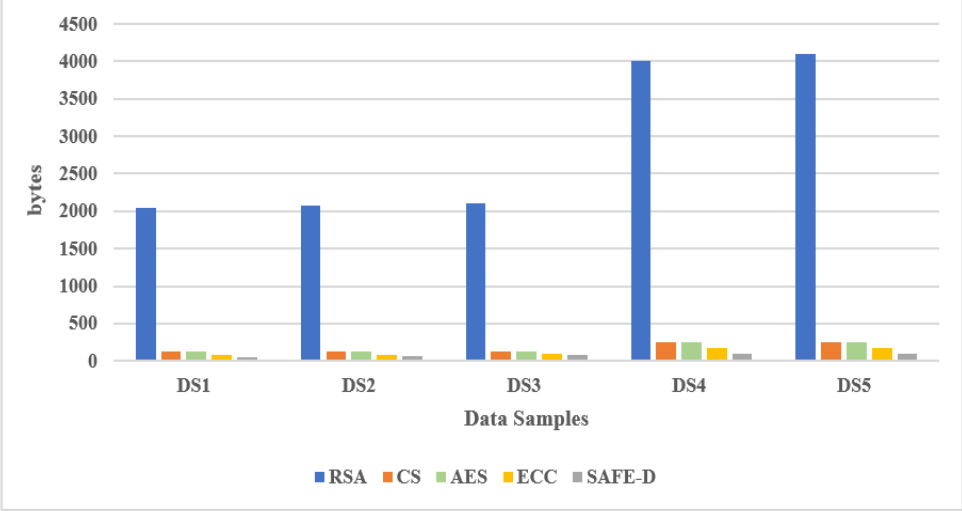


Figure 10: Encryption Size Analysis (in bytes)

The encryption size (in bytes) for various techniques is contrasted in Table 3 for five data samples (DS1 through DS5) with varied bit sizes. Reduced encryption sizes suggest faster transmission speeds and more effective storage use. The graphical representation is given in Figure 10. The RSA technique represents the largest encryption sizes, ranging from 4096 bytes for DS5 (2048 bits) to 2048 bytes for DS1 (1024 bits). Among the methods discussed, huge encryption sizes are utilized. Compared with RSA, the encryption sizes of the CS technique are much smaller, ranging from 128 to 256 bytes, indicating significantly higher storage efficiency. With encryption sizes comparable to CS, from 128 bytes to 256 bytes, the AES method also shows improved efficiency. With encryption sizes between 86 and 174 bytes, the ECC method shows average efficiency. Compared to RSA, CS, and AES, it uses less storage. SAFED is the least storage-intensive among the investigated methods as it has the least encrypted length, varying between 48 and 98 bytes. Encryption Size Analysis is shown in Figure 10.

### 4.3 Security Analysis

Standard threat models were used to see how well SAFED could handle both active and passive threats. The algorithm was first tested for its ability to withstand IND-CPA-style assaults by checking its uniform entropy and its ability to resist key reconstruction.

Table 4: Comparison of Hash Functions: ROLE vs. SHA-3 and BLAKE2

| Hash Method | Entropy (bits) | Avalanche % | Collision Rate ($10^6$ samples) |
|---|---|---|---|
| SHA-3 | 0.98 | 49.80% | 0 |
| BLAKE2 | 0.97 | 49.50% | 0 |
| **ROLE** | **0.95** | **48.70%** | **2** |

We compared the suggested ROLE hashing algorithm to well-known cryptographic hash functions as SHA-3 and BLAKE2 (Upadhyay et al., 2022). The examination looked at entropy, the avalanche effect, and how well it resists collisions. ROLE had a little less avalanche power and entropy than SHA-3/BLAKE2, but it still worked well in settings with minimal latency. Minor collisions in inputs with a lot of data signal that more strengthening may be done. Comparison of Hash Functions: ROLE vs. SHA-3 and BLAKE2 is depicted in Table 4.

Although ROLE slightly trails standard hashes in some metrics, it offers superior speed and storage efficiency suited for low-power environments.

Table 5: Entropy Validation Table

| Index | LCG | MACE | Twister | Bio-Convolving | SAFED (ROLE) |
|---|---|---|---|---|---|
| I1 | 0.87 | 0.87 | 0.89 | 0.91 | **0.93** |
| I2 | 0.88 | 0.88 | 0.9 | 0.92 | **0.94** |
| I3 | 0.89 | 0.89 | 0.91 | 0.93 | **0.96** |
| I4 | 0.9 | 0.91 | 0.92 | 0.94 | **0.97** |
| I5 | 0.93 | 0.95 | 0.93 | 0.95 | **0.98** |

We examined the entropy of binary sequences made by several approaches, such as the Linear Congruential Generator (LCG), MACE filtering, the Mersenne Twister, Bio-convolving, and the proposed SAFED, spanning five data indices (I1–I5). Entropy Validation Table is depicted in Table 5. SAFED had the greatest entropy values (0.91 to 0.98), which means it was more random and better for cryptography than the others National Institute of Standards and Technology (2022).

Table 6: Randomness Results

| NIST Test | p-Value (ROLE) | Result |
|---|---|---|
| Frequency (Monobit) | 0.483 | Pass |
| Approximate Entropy | 0.517 | Pass |
| FFT | 0.612 | Pass |
| Serial | 0.475 | Pass |
| Linear Complexity | 0.489 | Pass |

To ensure that the ROLE hash function is statistically sound by utilising the NIST SP 800-22 test suite National Institute of Standards and Technology (2022). ROLE passes all the main tests in the NIST suite, with p-values that are within acceptable limits. Randomness Results is shown in Table 6. This shows that it can create statistically random sequences that can be used for cryptography.

# 5 Case Study: ECG Signal Encryption

The SAFED is employed to encode/decrypt the ECG signal to be transmitted over the IoT ecosystem. Every step of the SAFED is used on the ECG Signal to generate the private key and to communicate over the network. The base 64 representation of the private key is graphically represented in the graphs (Figure 11) when converted to binary. The overall approach, performance, and efficiency are justified by this comparison analysis.

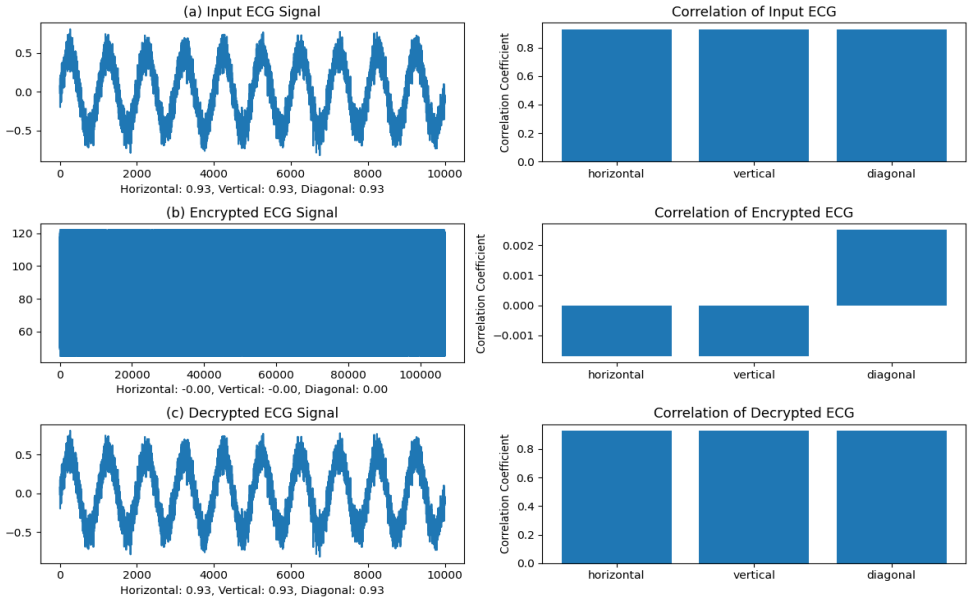


Figure 11: Analysis of Correlation Tests. (a) The Original Electrocardiogram (ECG) Signal, (b) its Horizontal and Vertical Correlations, (c) its Vertical and Diagonal Correlations, (d) its Encrypting Using ECC, (e) its Correlations, (f) its Horizontal and Vertical Correlations, (g) and its Diagonal and Diagonal Correlations, (h) it's Encrypting Using ECC

The correlation distribution before and after encryption in all three directions (horizontal, vertical, and diagonal) illustrates the results of the correlation study. Because electrocardiogram (ECG) waveforms are smooth and continuous, the unencrypted signal shows a strong correlation between neighbouring data points. On the other hand, encrypted electrocardiogram signals show correlation coefficients close to zero or slightly negative, suggesting successful scrambling and eliminating discernible patterns.

The correlation coefficients for the original and encrypted ECG signals and benchmark values from earlier encryption approaches Karthik & Krishnan (2021) are shown in Figure 11. Proving that the suggested approach effectively obfuscates any structural continuity and improves data security by generating neighbouring values at random, the encrypted ECG signal has low correlation coefficients.

The correlation study proves that the suggested encryption method successfully breaks the ECG signal's intrinsic continuity. The poor correlation coefficients of the encrypted ECG signal across all directions confirm the algorithm's capacity to conceal critical medical data, which indicates this disruption. The predicted behavior of a strong encryption approach is better security, which is why these results make sense. When data points are encrypted, they are no longer linked.

The substantial drop in correlation coefficients demonstrates that the suggested ECG encryption technique successfully scrambles nearby data points. These results lend credence to this method's potential usage in medical applications for the secure transmission of electrocardiogram (ECG) signals, which would prevent the unauthorized access or manipulation of sensitive patient data.

# 6 Conclusion

The adaptability of the SAFED approach to the resource-constrained environment is evident from the initial stage of ECG signal processing with the FIR filter. The obtained signal is subjected to the generation of the Binary Sequence from the ECG features and P peaks as the prerequisites for the Key Generation. The generated Binary Sequence consumes less time pointing to the ECG features, and the sequence quality is enhanced using DB4 as the conversion mechanism. The applicability of the ROLE as a hashing technique ensures high randomness and the periodic nature of the sequence with greater throughput. The smaller-sized private key of 128 bits boosts the performance of encryption. With this private key, the SAFED algorithm encrypts the patient's medical record to ensure secure data transmission across the network. The decryption is reliable enough to meet the critical aspects of the Medical IoT environment by employing the same private key. The overall approach ensures a secure, low-latency, optimized resource utilization cryptographic approach with higher performance.

### Conflicts of Interest

The authors declare no conflict of interest.

### Author Contributions

Conceptualization, methodology, software, validation, writing, original draft preparation, Mr. Sanjeev Kumar A N; review and editing, supervision, Dr. Ramesh Naik B.

# References

[1] Abdulbaqi, A. S., Obaid, A. J., & Abdulameer, M. H. (2021). Smartphone-based ECG signals encryption for transmission and analyzing via IoMTs. *Journal of Discrete Mathematical Sciences and Cryptography*, *24*(7), 1979-1988.

[2] González-Manzano, L., de Fuentes, J. M., Peris-Lopez, P., & Camara, C. (2017). Encryption by Heart (EbH)—Using ECG for time-invariant symmetric key generation. *Future Generation Computer Systems*, *77*, 136-148.

[3] Ibaida, A., & Khalil, I. (2013). Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems. *IEEE Transactions on biomedical engineering*, *60*(12), 3322-3330.

[4] Janveja, M., Paul, B., Trivedi, G., Vijayakanthi, G., Agrawal, A., Jan, P., & Němec, Z. (2020, April). Design of efficient AES architecture for secure ECG signal transmission for low-power IoT applications. In *2020 30th International Conference Radioelektronika (RADIOELEKTRONIKA)* (pp. 1-6). IEEE.

[5] Karimov, N., & Sattorova, Z. (2024). A systematic review and bibliometric analysis of emerging technologies for sustainable healthcare management policies. *Global Perspectives in Management, 2*(2), 31–40.

[6] Karthik, M. G., & Krishnan, M. M. (2021). Securing an internet of things from distributed denial of service and Mirai botnet attacks using a novel hybrid detection and mitigation mechanism. *Int. J. Intell. Eng. Syst*, *14*(1), 113-123.

[7] Malhotra, A., & Joshi, S. (2025). Exploring the Intersection of Demographic Change and Healthcare Utilization: An Examination of Age-Specific Healthcare Needs and Service Provision. *Progression Journal of Human Demography and Anthropology*, 8-14.

[8] Menon, K., & Patil, S. (2023). Assessing Terminology Gaps in Global Health Guidelines: AWHO Terminology Audit. *Global Journal of Medical Terminology Research and Informatics*, *1*(1), 5-8.

[9] Moosavi, S. R., Gia, T. N., Nigussie, E., Rahmani, A. M., Virtanen, S., Tenhunen, H., & Isoaho, J. (2016). End-to-end security scheme for mobility enabled healthcare Internet of Things. *Future Generation Computer Systems*, *64*, 108-124.

[10] Moosavi, S. R., Nigussie, E., Levorato, M., Virtanen, S., & Isoaho, J. (2017). Low-latency approach for secure ECG feature based cryptographic key generation. *IEEE Access*, *6*, 428-442.

[11] Moosavi, S. R., Nigussie, E., Virtanen, S., & Isoaho, J. (2017, January). Cryptographic key generation using ECG signal. In *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (pp. 1024-1031). IEEE.

[12] Naik, R. (2023). Bilateral Hashing model of ECG signal encryption system using Downhill Peak Follow (DPF) based Encryption technique.

[13] National Institute of Standards and Technology. (2022, January). Proposed decision to revise SP 800-22 Rev. 1a in response to public comments.

[14] Padmapriya, V. M., Thenmozhi, K., Hemalatha, M., Thanikaiselvan, V., Lakshmi, C., Chidambaram, N., & Rengarajan, A. (2025). Secured IIoT against trust deficit-A flexi cryptic approach. *Multimedia Tools and Applications*, *84*(9), 5625-5652.

[15] Premkumar, S., & Mohana, J. (2020). A novel ECG based encryption algorithm for securing patient confidential information. *International Journal of Electrical Engineering & Technology (IJEET)*, *2*(11), 35-43.

[16] Qiu, H., Qiu, M., & Lu, Z. (2020). Selective encryption on ECG data in body sensor network based on supervised machine learning. *Information Fusion*, *55*, 59-67.

[17] Shrivastav, P., & Malakar, U. (2024). Exploring Barriers to Medication Adherence Among Patients with Chronic Diseases. *Clinical Journal for Medicine, Health and Pharmacy*, *2*(3), 21-31.

[18] Sumithra, S., & Sakshi, S. (2024). Exploring the factors influencing usage behavior of the digital library remote access (DLRA) facility in a private higher education institution in India. *Indian Journal of Information Sources and Services*, *14*(1), 78-84.

[19] Udayakumar, R., Pansambal, S. Y., Gajmal, Y. M., Vimal, V. R., & Sugumar, R. (2023). User Activity Analysis Via Network Traffic Using DNN and Optimized Federated Learning based Privacy Preserving Method in Mobile Wireless Networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14*(2), 66-81. https://doi.org/10.58346/JOWUA.2023.I2.006

[20] Upadhyay, D., Gaikwad, N., Zaman, M., & Sampalli, S. (2022). Investigating the avalanche effect of various cryptographically secure hash functions and hash-based applications. *IEEE Access*, *10*, 112472-112486.

[21] Zheng, G., Shankaran, R., Yang, W., Valli, C., Qiao, L., Orgun, M. A., & Mukhopadhyay, S. C. (2018). A critical analysis of ECG-based key distribution for securing wearable and implantable medical devices. *IEEE Sensors Journal*, *19*(3), 1186-1198.

## Authors Biography

**Sanjeev Kumar**, an Assistant Professor at GITAM University, specializes in Computer Science & Engineering with a significant focus on "Security." His research extends to Internet of Things (IoT) applications within healthcare, particularly evident in his work on diabetic patient monitoring devices. This directly intersects with the realm of the Internet of Medical Things (IoMT). His contributions to network security, including cryptographic systems and malicious node detection, provide a strong foundation for addressing the critical security challenges inherent in IoMT devices. Thus, his major research interests encompass developing robust security measures and frameworks for connected healthcare technologies, aiming to ensure the integrity and privacy of patient data in digital health ecosystems

**Dr.B. Ramesh Naik** has over a decade of experience in teaching and research. He completed his Master's degree from JNTU Kakinada in Computer Science and Engineering. His PhD was awarded by Jawaharlal Nehru Technological University, Hyderabad. His research interest in Machine Learning, Image processing, Pattern recognition, and Analysis of Algorithms helped him to publish research articles in various national and international journals. He has substantial practical background knowledge in data sciences, information retrievals from databases, and machine learning approaches, and he has guided several undergraduate and postgraduate students.