Received: October 20, 2022. Revised: November 17, 2022.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Securing Data Transmission and Privacy Preserving Using Fully Homomorphic Encryption

Areej Abdulmunem Ahmed[1, 2]* **Magda Mohamed Madboly**[1] **Shawkat Kamal Guirguis**[1]

[1]*Department of Information Technology, Institute of Graduate Studies and Research,*
Alexandria University, Alexandria, Egypt
[2]*Research and Development Center, Ministry of Electricity, Baghdad, Iraq*
* Corresponding author's Email: areej_abdulmunem@yahoo.com

Abstract: The Cloud computing is a repository that stores massive amounts of data that is accessible online. There are many security and data privacy concerns threatening cloud computing services, especially through key sharing. So, there is an important need to improve security algorithms. An electrocardiogram (ECG) measures heart performance and detects arrhythmias. Nowadays, they are used for identification because they vary from one person to another. Therefore, securing an ECG signal is important. Homomorphic encryption (HE) is a security solution that processes encrypted data without decryption. HE supplies the same raw data results. In this paper, to enhance security and maintain data privacy while getting rid of sharing key restrictions, a new fully homomorphic encryption algorithm with an advanced encryption standard (FHEAES) is proposed to encode the ECG signals. This is accomplished by proposing the evaluation process to be appended to an AES algorithm as an additional security layer, which performs a variety of mathematical operations homomorphically on the encrypted data without decrypting it, instead of the original data. The evaluation process is proposed to be a linear polynomial function with variable values to enhance security. A Pan and Tompkins algorithm is used to process ECG signals. Then, the FHEAES algorithm was used for encoding the ECG signal. At last, ECG signals were classified for further diagnosis. According to the findings, FHEAES will take 1.078950 × 1033 years to break or hack. This is due to the using of the proposed three encryption keys to make it harder to break. Also, the FHEAES algorithm has 95.8% accuracy in classification and 100% accuracy in decryption (recovering the original signal). When compared to other algorithms, it is nearly 6 times and 3 times faster during encryption and decryption, respectively. This is because it is proposed to be based on computationally lightweight matrix operations, making it perfect to address the noise that arises from any FHE scheme. Thus, FHEAES provides superior security and privacy while computing and is solid against attacks.

Keywords: Fully homomorphic encryption (FHE), AES, Encryption, Decryption, Cryptosystem.

1. Introduction

Cloud computing is an effective technology that is used to store and share a massive amount of data and applications by the internet and on remote servers. For maintaining and processing data in diverse fields, cloud computing supplies resources available on-demand through lower effort in management [1]. Cloud computing is classified into three major classes with reference to service models: Infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Providing these services is insufficient if the cloud service provider cannot ensure 100% confidentiality and better security for the client's data. There are many information security issues and privacy concerns associated with cloud computing [2]. Therefore, there is a necessity to enhance security algorithms in data systems and processes.

Traditionally, encryption systems rely on key exchanges (private or public) among the peers to secure transmission when they are sharing an encrypted message. However, initially, there is a need to decrypt the stored data in the cloud to perform computations on it, which makes the data exposed to the service provider. Nevertheless, these systems with public cloud services lead to a breach of privacy. Furthermore, with existing encryption technologies; data analysis on the encrypted database in the cloud is considered a hard matter to obtain.

A brute-force attack can break any key with enough computational power. As a result, building a cryptography algorithm with a strong key is substantial for improving the interaction between present and modern technologies; and for providing additional levels of security.

The ECG is a wave form that measures the functioning of the heart. ECG signals are employed in numerous implementations including medical diagnosis, interpreting heart arrhythmia's types, illustration to researchers, while recently as an identification factor. Securing an ECG transmission is considered a promising method for further studies of arrhythmia detection in an attempt to aid the physician in assessing the cardiac status of patients. There are many security and privacy concerns while sharing medical information through public domain, especially for VIP people. Also, there is little attention to verify and assure the medical data; so that it was focused by hackers. Therefore, secure detailed information must be available.

Actually to address these concerns and by utilizing security enhancing techniques, the system's privacy and security characteristics will maintain the confidentiality and authenticity of the user's information. This can be achieved via utilizing Homomorphic Encryption to encrypt ECG signals. HE is a particular form of encryption scheme used in the public domain which permits a service provider to process encrypted data without the need to decrypt it first [3]. The major idea behind HE is to allow access to critical data only by authorized users, by allowing them performing arithmetical or logical operations directly on encrypted data. Similar to other cryptographies, an essential target is to preserve the confidentiality of client data not only at transmission and storage but also at processing time [4].

This study proposed a security solution that could be employed in a connected healthcare domain. Initially, the processing and analysis of an ECG signal are performed by using the Pan and Tompkins method in order to detect the QRS complex of the signal [5]. Subsequently, an ECG is encrypted via utilizing the proposed FHEAES algorithm, which adds an evaluation procedure as a linear polynomial function with the three suggested encryption keys: the AES key, the round number, and the heart rate (HR). The keys are suggested to be variable values with decimal places. These keys provide high security for ECG signals, ensure data confidentiality, and make the FHEAES algorithm resistant to brute-force attacks. According to security analysis, the required cipher breaking time is increased more than 100 million times compared to a standard AES technique. So the personal data is kept accurate and secret by FHEAES under this scheme, even if the data is stored or calculated on an untrustworthy server without fear of disclosure. The reason behind this is that encrypted data can only be decrypted by the intended recipient. Finally, the heart rate was determined and arrhythmia was identified. The classification accuracy for FHEAES is 95.8%. A correct decoding of the ciphertext is crucial to the success of homomorphic encryption. Therefore, after an evaluation, the ciphertexts' original format should be preserved. The decryption process of FHEAES is a perfect 100% (recovering the original signal without losing any data). FHEAES is about 6 times faster at encrypting and 3 times faster at decrypting than other methods because it uses simple matrix operations. This makes it perfect for a wide range of internet of things (IoT) applications.

The following is the structure of this paper: Section 2 presents a brief summary of related works. Section 3 displays the methodology of the suggested algorithm. Section 4 details the results of experiments in addition to security analysis of the proposed algorithm. Finally, in section 5, the key conclusions are provided.

2. Related work

Homomorphic encryption allows performing addition, multiplication, or other operations over encrypted data without decryption, rather than the original data. Rivest, Adleman, and Dertouzos introduced the HE idea for the first time in 1978 [6]. HE performs the following four basic functions: key generation, encryption, decryption, and evaluation. Homomorphic encryption schemes are classified based on the design of the evaluation function:

-Partially homomorphic encryption (PHE): Just one operation (either addition or multiplication) over encrypted data may be executed at once under such a scheme. Pailler and Goldwasser cryptographic algorithms use additive HE. RSA and Elgamal cryptographic algorithms are examples of multiplicative HE [7].

-Somewhat homomorphic encryption (SHE): More than one operation can be executed on encrypted data under such a scheme, with a limited number of addition and multiplication operations.

-Fully homomorphic encryption (FHE): Craig Gentry first proposed it in 2009 [8]. This scheme allows an unlimited number of additions, multiplications, and other arithmetic operations to be executed over encrypted data.

This section examines several encryption systems presented in the literature and discusses their pros and drawbacks, with a particular focus on techniques that allow calculations on encrypted data while maintaining privacy.

The author, Tolga Soyata, in [9], tested the viability of their long-term health monitoring system for detecting patient health concerns. This is accomplished by fully homomorphic encryption for ECG data, which is based on Gentry's FHE and BGV techniques. The suggested technique, which is based on Gentry's FHE, demonstrates the requirement for a recryption process in order to avoid decryption errors. The recryption process is more time-consuming than the others. Results show that employing Gentry's FHE technique is unfeasible in terms of computation and storage. Messages and ciphertexts are specified over polynomial rings in the BGV system. The researchers, Hameed in [10], demonstrated the AES technique for encrypting ECG signals inside the e-healthcare system. According to the results of the study, the AES technique was computationally costly, especially when encrypting the complete ECG biological signal sample. As a result, data transfer latency for health information should be as quick and practical as possible and in real time, since it influences the life of a person in the healthcare system. Thus, the AES algorithm has to be improved to make it more appropriate for Internet of Things healthcare applications.

Vithya [11] employed the set partitioning in hierarchical trees (SPHIT) methodology. The RSA encryption algorithm is utilized to encrypt an ECG signal, which is then distributed for e-healthcare applications. The RSA algorithm permits executing only one operation on encrypted data: either addition or multiplication. So the RSA cryptosystem is not appropriate for large signals and in real-time. Instead of this, the FHE encryption algorithm has the ability to do simultaneous addition and multiplication, adding further security to the signal.

The authors, Jamal Madhloom in [12], presented a robust hybrid ECG encryption technique relying on DNA layers and AES to reduce encryption execution time and improve security for IoT health applications. The proposed technique proved that it can protect IoT signals using cloud computing. But the research is restricted to protecting medical information other than ECG signals, which may have different transmission needs and metrics. Although the DNA rules in the suggested method create and operate four keys, this might lead to an increase in the time of encryption, which makes it unsuitable for electronic IOT medical systems. Abeer Algarni [13] proposed a multi-layer cryptosystem for telemedicine applications to protect ECG signals. The headmost relies on random projection of the DWT coefficient of ECG signals, followed by a salting algorithm. The latter cryptosystem has 3 steps: fusion, substitution, and chaotic permutation. It combines raw ECG and speech signals when the ECG has lower activity. Then use the 2-D chaotic Baker map to obtain the permutation. Using a multi-layer cryptosystem improves security. In comparison to the chaotic logistic map, the suggested cryptosystems offer excellent security levels. Also, it is robust against attacks and has a preferable performance. But the drawback of this work is that it has no diagnosis feature. Furthermore, when the Structural Similarity Index (SSIM) is utilized, the system has a similarity ratio between the original and the encrypted signal.

Qin [14] suggested an algorithm for ECG processing to detect R-peak. This algorithm is accurate, efficient in time consumption, and adaptive. Moreover, it is superior to the Pan and Tompkins technique. Qin's method, on the other hand, can only acquire ECG signals. It is unable to connect to a database on the server side to obtain additional analysis. More importantly, signals were not protected.

Due to the rising of ageing and the incidence of mortality from cardiovascular heart diseases; Lin [15] came up with the idea of an ECG Monitoring System for people who have cardiovascular heart diseases. This system is improved for monitoring heart rate remotely, supplying electronic medical treatment, and improving person-to-person interaction. This system confirms the comfortable design of user interfaces. Also, it has robust performance that permits remote diagnosis and treatment by medical staff. However, the system lacks the capability to provide an internal diagnosis. And, furthermore, it is unable to guarantee the data authentication of patients. The other common secret key algorithm is suggested in [16], that uses a single key of 128 bits. It's achieved full diffusion after just one round. So a change in a single plaintext or key bit has an impact on about half of the ciphertext bits, which is distributed uniformly anywhere along the ciphertext. Since both the encryption and decryption processes for the LEA cipher are so identical, it is sufficient to just reverse the encryption procedure with the appropriate key to decode the ciphertext. Although the suggested algorithm attains a good performance, it doesn't keep privacy because it requires key exchange. Moreover, it cannot provide data confidentiality. Also, it has a limited security level due to the use of a single key. This algorithm is restricted to encrypting and classifying the signal because it has no preprocessing phase and is unable to establish a connection to a remote database for further analysis.

The proposed FHEAES has a broader scope than previous researches; it has lightweight properties for enhancing security, privacy, and arrhythmia detection.

3. Methodology

3.1 Data collection

The PhysioBank dataset is a huge, rapidly expanding repository of well-characterized digital recordings of physiological signals. ECG signals are acquired from the MIT-BIH Arrhythmia database [17, 18], which are employed for testing the proposed algorithm of this research. In total, 48 heartbeat recordings were contained in this database from diverse patients, with 30 minutes of each in rest condition. The signal length for each ECG record is 21600 samples, with 360 Hz as the sampling rate [19]. The minimum and maximum normal heart rates measured in the database were 24 bpm and 173 bpm, respectively. This database was the most important because it was utilized in many arrhythmia detection and classification researches [20]. Also, it was the most widely available set of standard test fabric for assessing.

3.2 The proposed methodology

This research is partitioned into: signal preprocessing, ECG encryption, and classification. The Pan and Tompkins technique was utilized for signal preprocessing and for detecting QRS complexes in the first part. The "QRS complex" is the combination of the three ECG graphical deflections: Q wave, R wave, and S wave. It is usually the most prominent area in the ECG. It represents the depolarization of both the heart's ventricles. In the second part, the proposed FHEAES algorithm was utilized to encrypt the signal, making it more secure and hard to penetrate by attackers. The result is classified into form of heart rate after decryption. Fig. 1 introduces the proposed methodology of the FHEAES algorithm.

3.2.1. The signal preprocessing

In real-time techniques, the Pan-Tompkins algorithm is commonly employed to identify QRS complexes according to its superior sensitivity and predictability [15]. The algorithm is divided into: preprocessing and decision stages. During the preprocessing stage, ECG signals are provided for use in the detecting procedure. Preprocessing eliminates the noise. Then it makes an ECG signal smooth and expands the QRS. The thresholds are utilized later in a decision stage to take signal peaks into account while ignoring noise peaks. The ECG signal's flow through the Pan and Tompkins method is as follows: The original ECG (x1) is gone over a band pass filter (Low Pass (x2) and High Pass (x3)) to detect the QRS and minimize noise. When the ECG signal exceeds the band pass filter (x3), the signal-to-noise ratio is raised. As a result, the detector's total sensitivity is enhanced. After that, the filtered signal goes through derivation (x4), squaring function (x5), and moving window integration (x6). Subsequently, at the decision stage, thresholds are used which are slightly above the noise peak levels. The signal peak represents the QRS complex; the noise peaks denote muscle noise and T waves. The thresholds were automatically modified to react to variations in QRS shape and heart rate. Once the QRS complex is identified, the R location is defined leading to the (RR) interval and calculating the heart rate. This algorithm uses a 200 Hz sample frequency rate. A digital band pass filter eliminates the wrong detections caused via noise and distortions in ECG signals. The Pan-Tompkins algorithm is designed to be an adaptive algorithm due to its ability to process the ECG signal at various sample rates with satisfactory results.

3.2.2. ECG encryption

To prepare for ECG encryption, this phase will transform ECG signals into integer bits (by multiplying them by 106 using the MATLAB function). The AES is a symmetric block encryption which uses the same secret key for encrypting and decrypting. It's also called the Rijndael, symmetric, or secret key algorithm. It operates in multiple key sizes (128, 192, and 256 bits). AES is an excellent design area to research FHE approaches; because it enables both parallel and algebraic calculation capabilities. Also, it proved its efficiency across diverse platforms. Furthermore, AES is frequently employed and considered as a benchmark to protect the Computation Protocol Multi Party [21].

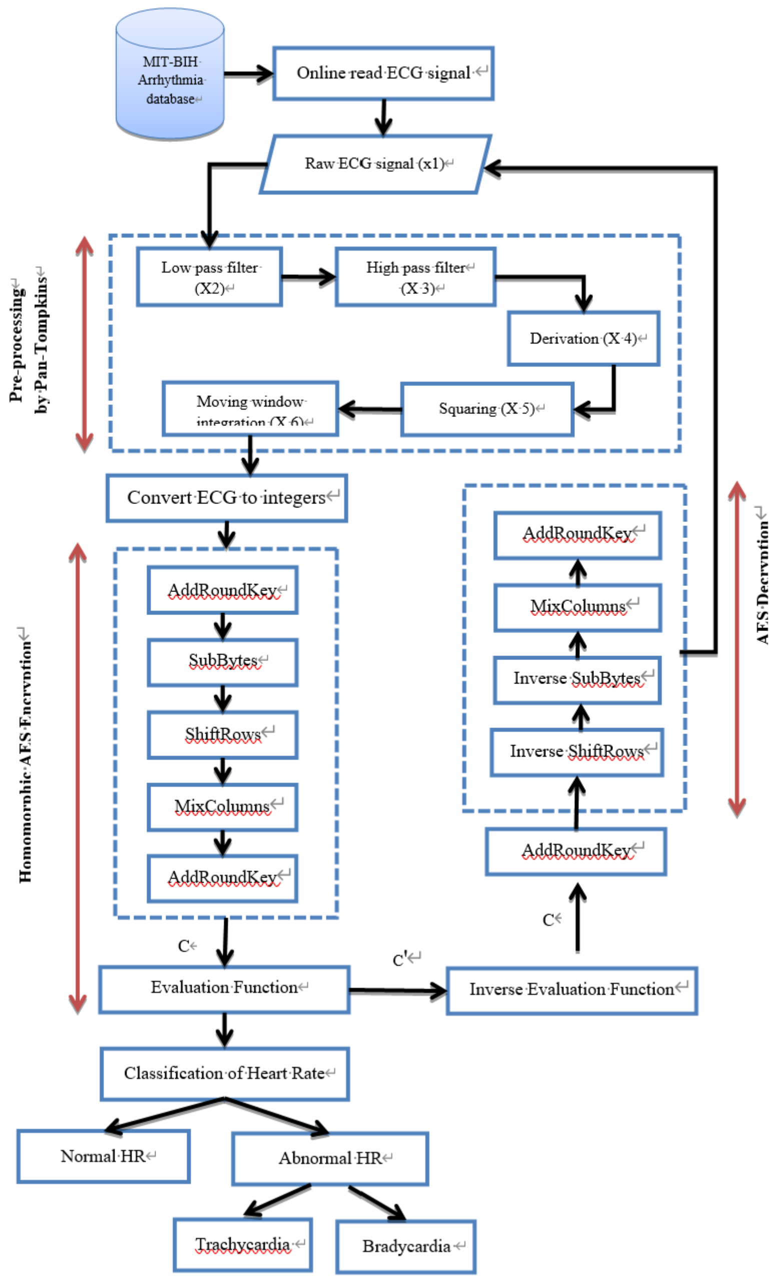


Figure. 1 The proposed FHEAES methodology

A new FHE scheme (FHEAES) based on AES is proposed, which permits to encrypt the ECG signal, making it more secure and resistant against attacks; this algorithm preserve the privacy by performing various computational operations on the encrypted data without decrypting it. As a result, the key exchange constraint that causes privacy breaches will be removed. During this scheme, even if the data is kept in an insecure location or the calculations are performed on an untrusted server, the data will remain private. This is due to the user being the only one who has the key to decrypt. Furthermore, FHEAES relied on computationally lightweight matrix operations with small key sizes of symmetric keys, making it ideal for a wide range of IOT applications and treating the noise that is deemed as a FHE scheme. Its security is derived from the difficulty of factoring a key, which is the fundamental of numerous public key based cryptosystems [22]. The FHEAES is proposed to be fully homomorphic encryption to cover the required operations (addition and multiplication) to compute the heart rate. The FHEAES is designed to be a realistic, feasible, and effective FHE. FHEAES proposed a 128 bit key length and is based on a 4 × 4 matrix of bytes. The essential idea is to convert an integrated ECG signal (x6) (incoming from preprocessing) into integer representation in 4 × 4 square matrix. The suggested algorithm consists of 4 processes in order to achieve the efficiency of the

FHE scheme:

- Key generation process:

A single key (secret key) is presented in the symmetric key system algorithm. It is necessary to maintain encryption keys safely so as to perform encryption successfully. Keys may be obtained even if the service provider in the cloud encrypts data. The encryption keys should be kept isolated from the rest of the system, and only the end user should have access to them. AES uses a 128 bit secret key (text); which is organized as a 4 × 4 byte integer matrix as follows in Eq. (1):

$$(\mathrm{k}) \leftarrow \mathrm{KeyGen}(\lambda) \tag{1}$$

where λ represents security variable, and k represents secret key.

- Encryption process:

The plaintext (M) is encrypted and converted to ciphertext (C) using the AES secret key as seen in Eq. (2). In the proposed algorithm, both the plaintext and ciphertext were organized in the format of 4 × 4 matrix. At the sender, the secret key was utilized to encrypt the plain ECG signals after window integrated output (x6) was converted to integers to create the ciphertext C by using 4 sequential operations in each round: the SubBytes, ShiftRows, Mix Columns, and AddRoundKey Operation. After that, the encrypted message C is sent to the appropriate receiver.

$$(\mathrm{C}) \leftarrow \mathrm{Enc}_{\mathrm{k}}(\mathrm{M}) \tag{2}$$

where M is the plain integrated ECG signal (x6), and C represents the ciphertex.

- Evaluation process:

The evaluation process accepts ciphertexts (C) that come from the encryption process as input and produces new ciphertexts (C') as output, which will be called evaluated ciphertexts. An evaluation process is performed on the server side before decryption. The evaluation process is the basic process which was proposed to be added to an AES algorithm so as to achieve the principle of homomorphic encryption. It performs mathematical computations homomorphically on the ciphertext. Evaluation was also performed in a 4 × 4 matrix format. f is defined as the generic evaluation function used for computation (Eq. (3)). In the proposed algorithm, f is translated into a linear polynomial function that is used to create a new ciphertext due to its performance simplicity and ability to reinforce the security as shown in e Eq. (4). A linear polynomial uses constant real numbers with a degree of 1 polynomial [23]. The proposed evaluation function employs two parameters: Round Key (a), and Heart Rate (HR) as evaluation keys to perform the evaluated ciphertexts (C'). As shown in the following formula:

$$(\mathrm{C}') \leftarrow \mathrm{Eval}_{\mathrm{a,HR}}(\mathrm{f}, \mathrm{C}) \tag{3}$$

where f is defined as the generic evaluation function, and $\mathrm{C}'$is an evaluated ciphertext.

$$(\mathrm{C}') \ = \mathrm{aC} + \mathrm{HR} \tag{4}$$

where a represent the round key, and HR is the heart. The (HR), and (a) were proposed in the FHEAES algorithm to be variable numbers rather than constant numbers to strengthen the algorithm's security level by making it more difficult to hack or break. This is due to the fact that the variable number itself costs the hacker or third party. He should first determine whether the number is variable or not before applying it to the encryption equation. This necessitates extra efforts to break the encryption. Furthermore, the constant number indicates one solution probability, while the variable number provides more probabilities of the solution.

The HR is additionally proposed to be a value consisting of a number with four decimal places, which leads to an increase in the security level of the algorithm. This is due to the use of the threshold value with decimal places, in addition to calculating the HR according to Eq. (5):

$$\mathrm{HR}\ (\mathrm{bpm}) = \frac{\mathrm{Signal\ size}}{\mathrm{time\ (m)}} \tag{5}$$

where bpm = beats per minute.

The proposed FHEAES system is a symmetric cryptographic algorithm that permits both multiplicative and additive homomorphic features, i.e., indicating that it is a fully homomorphic encryption algorithm (as defined in Eq. (4)).

The most important aspect of homomorphic encryption is that the ciphertext are decoded correctly. Therefore, the ciphertexts' format should be maintained after an evaluation process. Furthermore, the ciphertext's size should remain consistent.

- Decryption process:

This process represents employing the secret key to decode the evaluated ciphertexts (C') using the symmetric algorithm AES to obtain the original plaintext (M) matrix as in Eq. (6). At first, the inverse of a linear polynomial function is performed; then, using AES decryption operations, each round consists of four operations that are performed in reverse order: AddRoundKey, Mix Columns, ShiftRows, and SubBytes. Each operation is performed in a reverse manner.

$$(\mathrm{M}) \leftarrow \mathrm{Dec}_{\mathrm{k}}(\mathrm{C}') \qquad (6)$$

3.2.3. Classification

Once the signal is encrypted, its value will be altered. The decryption output was classified as either normal or abnormal HR (tachycardia or bradycardia); which supports the medical expert in achieving the desired deduction. It also aids the analyst for further analysis and detection. Finally, the algorithm's performance is assessed using statistical analysis by computing the accuracy, encryption and decryption times, correlation coefficient, and mean square error (MSE).

4. Experimental results, discussions, and security analysis

Security is considered the major problem with any encryption technology. The robust cryptographic algorithm must be designed to resist most known attacks. A suggested FHEAES algorithm that was used in this study was entirely examined for its sufficient security. Furthermore, to assess the strength of the cipher against different forms of attacks, diverse security analysis approaches were utilized.

4.1 Simulation environment

A credible simulation tool, "MATLAB version R2018b" was used to simulate the suggested algorithm. Experiments are executed utilizing the Microsoft Windows operating system platform on a computer with the following specifications as shown in Table 1:

Table 1. Simulation machine specifications

Specification	Details
Model	HP ProBook 450
Windows edition	Windows 8.1 © 2013 Microsoft Corporation all rights reserved
CPU	Intel ® Core ™ i5-4200M CPU @ 2.5 GHz 2.5 GHz
Installed Memory RAM	8.0 GB
Generation	4th generation
System type	64- bit Operating System
Algorithm simulated using	MATLAB (R2018b)

4.2 Keyspace analysis

The resistance of the proposed FHEAES algorithm to brute-force attacks is measured via keyspace analysis. A brute-force attack is one in which an adversary tries to break the cryptosystem by searching for all potential keys in an exhaustive manner. When compared with other studies and according to the findings, it will take 1.078950 × 10^{33} years to break or hack the suggested algorithm. This number overtakes the efficient key size desired for protection versus brute-force attacks. The suggested approach, as shown in Table 2, provides superior protection against brute-force attacks. And the desired cipher breaking time is improved by more than 100 million times when compared to a traditional AES and [16] algorithm's breaking time. This superiority result can be attributed to the following factors: First, the proposed algorithm used three encryption keys: the AES key, the round number (a), and the Heart Rate (HR) instead of using a single key. Second, the (HR) and (a) were suggested in the FHEAES algorithm to be variable numbers rather than constant numbers, because the hacker needs to estimate if the number is variable or not. Also, the constant value implies one solution probability, while the variable number shows numerous solution probabilities. Third, the security level of FHEAES is improved by making the HR a four-decimal-place number according to the decimal

Table 2. Ciphertext breaking time

Algorithm	Keyspace key1× key2 × key3	Ciphertext Breaking Time (years)
AES	2^{128}	1.078950 × 10^{25}
[16]	2^{128}	1.078950 × 10^{25}
[12]	$2^{4} \times 2^{128} \times 3 \times 10$	5.179340 × 10^{27}
FHEAES	AES key× a ×HR $2^{128} \times 10 \times 10^{7}$	1.078950 × 10^{33}

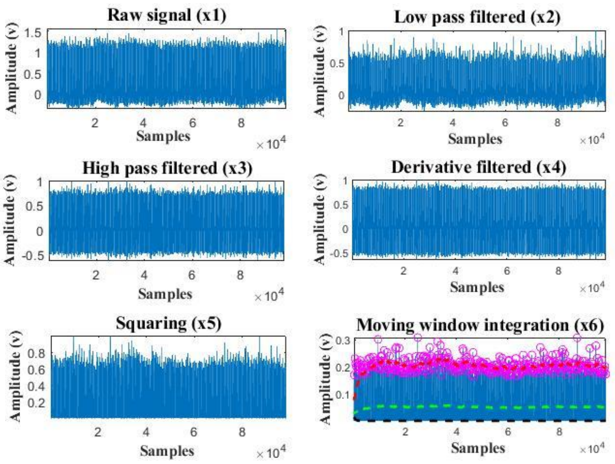


Figure. 2 Pan and Tompkins stages for ECG

Table 3. Results after FHEAES algorithm compared with MIT-BIH data

ECG Record	MIT-BIH HR \ bpm	FHEAES HR\ bpm	Classification	
100	70-89	75.5337	Normal	✓
101	55-79	62.1084	Normal	✓
102	72-78	72.842	Normal	✓
103	62-92	69.2198	Normal	✓
104	69-82	79.1226	Normal	✓
105	78-102	87.962	Normal	✓
106	49-87	64.3349	Normal	✓
107	68-82	71.8118	Normal	✓
108	44-78	94.9405	Normal	✓
109	77-101	94.7411	Normal	✓
111	64-82	70.549	Normal	✓
112	74-91	84.3731	Normal	✓
113	48-87	59.6493	Bradycardia	✓
114	51-82	62.5736	Normal	✓
115	50-84	64.8998	Normal	✓
116	74-86	79.5878	Normal	✓
117	48-66	51.0093	Bradycardia	✓
118	54-91	75.8992	Normal	✓
119	61-84	66.0296	Normal	✓
121	55-83	61.9755	Normal	✓
122	67-97	82.3127	Normal	✓
123	41-65	50.3447	Bradycardia	✓
124	47-64	52.9035	Bradycardia	✓
200	69-111	84.7059	Normal	✓
201	31-61	63.4044	Normal	✓
202	49-69	70.7484	Normal	✓
203	63-173	100.656	Tachycardia	✓
205	80-99	88.5269	Normal	✓
207	57-90	78.8567	Normal	✓
208	91-134	95.8377	Normal	✓
209	82-116	99.8918	Normal	✓
210	63-158	87.1644	Normal	×
212	63-108	91.3183	Normal	✓
213	101-113	106.372	Tachycardia	✓
214	49-92	75.002	Normal	✓
215	81-124	111.722	Tachycardia	✓
217	69-103	73.141	Normal	×
219	38-75	71.4463	Normal	✓
220	58-74	68.0567	Normal	✓
221	47-110	80.053	Normal	✓
222	49-84	82.6118	Normal	✓
223	75-94	86.4334	Normal	✓
228	54-80	74.005	Normal	✓
230	63-99	74.9687	Normal	✓
231	49-69	52.2056	Normal	✓
232	24-28	59.5164	Bradycardia	✓
233	98-110	101.819	Tachycardia	✓
234	84-99	91.3515	Normal	✓

threshold value. All of these factors make the algorithm more difficult to hack or break, as described in section 3.2.2 (Evaluation process).

4.3 FHEAES accuracy

The ECG signals are obtained and read online from the MIT-BIH database to detect arrhythmia. Then the Pan and Tompkins method is applied for ECG preprocessing. During the preprocessing step, low and high pass filters are utilized in order to reduce the noise. Then QRS complexes were then identified from the rest of the ECG waves using differentiation. The sample was then squared to enlarge the whole data, making it positive and to emphasizing the signal's elevated frequencies. Following that, the final step of preprocessing, the moving window integration processed the squared signal and found the average with 30 samples length. Fig. 2 shows the preprocessing steps. The black line represents noise, the green line represents the adaptive threshold, the red line represents the signal level, and the red circles represent the QRS adaptive threshold.

Fig. 3 shows the ECG record 101 as an input from the database and then the encrypted ECG signal by the FHEAES algorithm after the preprocessing.

When decrypting the signal, the result was either a normal heartbeat (if 60<=HR<=100). Else, it is an abnormal heartbeat format. Abnormal heartbeat means one of two arrhythmia's kinds: bradycardia (HR< 60 bpm) and tachycardia (HR > 100 bpm). The MIT-BIH database's arrhythmia was utilized to select all of the 48 ECG records as entries and to verify the proposed algorithm validity. Table 3 shows a summary of the outcomes collected. After decrypting the ECG signal, 46 of the 48 recordings yielded the classification result itself. Therefore, the FHEAES algorithm has a 95.8% accuracy of classification. Thus, it exceeds [24], which has 90% classification accuracy. On the other hand, FHEAES has 100% accuracy in decryption (recovering the original signal).

From these findings, the FHEAES overcomes the drawbacks in [15], which are that the system is incapable of offering an internal diagnosis. Additionally, it cannot ensure the authenticity of user data. while the FHEAES perform internal diagnosis with high accuracy (by using the Pan and Tompkins algorithm) on the encrypted data and maintain the data's privacy due to the use of the proposed FHE, which makes the user the only one who has the secret key and can decrypt the encrypted data. The FHEAES can connect online,

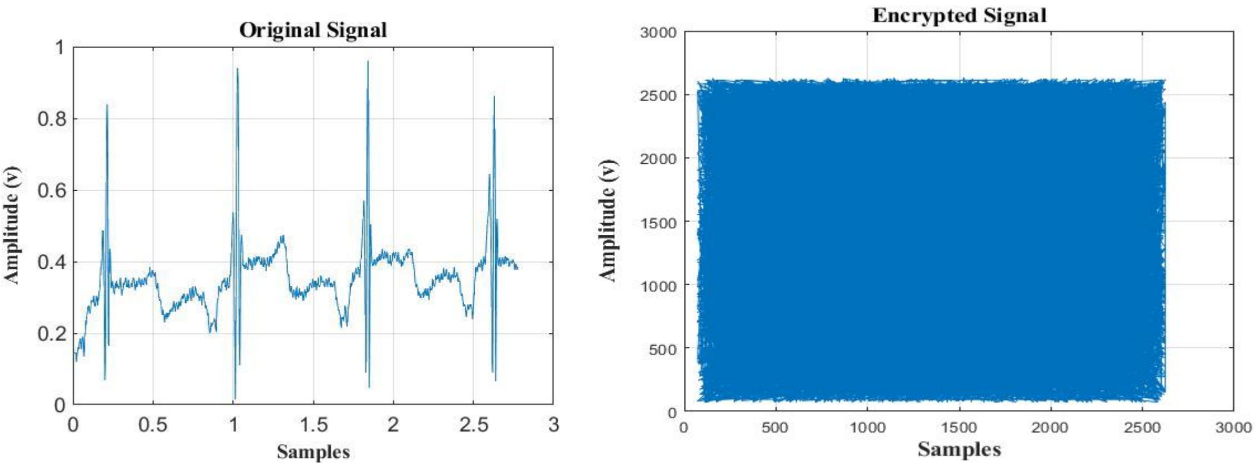


Figure. 3 The original and an encrypted ECG signals

Table. 4 Results of correlation coefficients of encrypted signals

Record No.	Correlation coeffecient	Record No.	Correlation coeffecient
100	-0.00362876	201	0.00940342
101	0.00539184	202	0.040104
102	0.0588394	203	0.0311167
103	0.0503466	205	0.0313714
104	0.0255472	207	0.00766766
105	0.0178331	208	0.0426498
107	-0.00379756	209	0.0241796
106	-0.00701422	210	0.046601
108	0.0133843	212	0.00481913
109	0.0116842	213	0.0340444
111	0.0159103	214	-0.0116054
112	0.0431796	215	-0.0115384
113	-0.00426961	217	0.0244614
114	0.0428497	219	-0.00105882
115	-0.0115384	220	0.0404914
116	0.0468573	221	-0.0358539
117	0.0109009	222	-0.00149086
118	0.0535848	223	0.0236081
119	0.0485984	228	-0.00663639
121	0.032939	230	0.0697645
122	0.0410916	231	0.0239827
123	0.0476107	232	-0.00308713
124	0.0234183	233	0.0233893
200	0.0570175	234	0.0197911

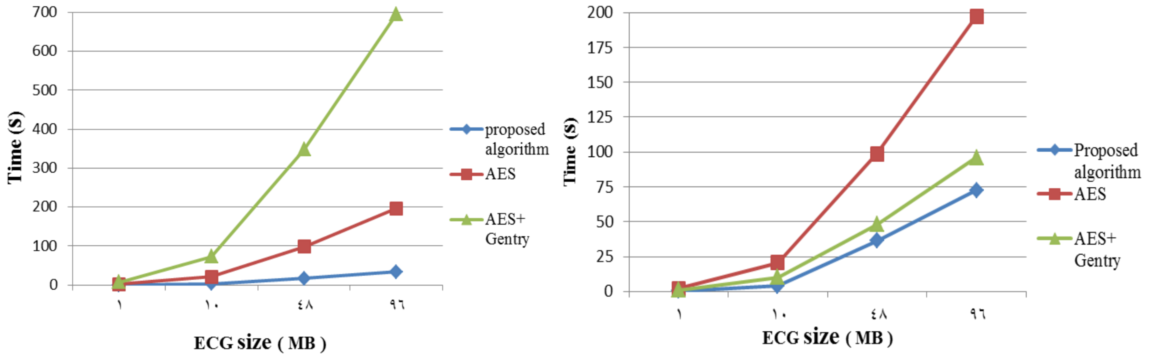
process, and secure any signal from the database. Contrary to [14], which is unable to connect to a database and can process the acquired signals, it also cannot protect the signals.

4.4 Correlation analysis

The correlation coefficient analysis of the raw and encrypted ECG signals was utilized as another metric to assess the statistical attack's resistance. To evaluate the FHEAES's efficiency, the correlation coefficient of both the plain and encrypted ECG signals was investigated by following the next steps: All pairs of columns and rows from the original and encrypted ECG signals were chosen. After that, each pair's linear correlation coefficient was computed according to [25, 26] as shown in Table 4. For encrypted signals, the correlation coefficients are extremely small and near zero. So, the proposed algorithm is resistant to statistical attacks. The reason behind this is the use of the three keys, which are suggested to have variable values with decimal places.

4.5 Analysis of encryption and decryption execution time

The algorithms' encryption and decryption throughput may be computed by utilizing their encryption and decryption execution times. The time taken within the FHEAES algorithm to encrypt and decode incoming ECG signals is considered one of the performance metrics. In this study, the experiment was repeated five times for all of the 48 ECG signal records to ensure that the results were not biased. Then the average is taken. The suggested FHEAES is compared to AES [10] and FHE (Gentry) [9] in this section. Fig. 4 demonstrates the encryption and decryption execution times for different file sizes of 1 MB, 10 MB, 48 MB, and 96 MB, respectively. 96 MB represents the signal length of 1000. In [9], the use of Gentry's FHE method is impractical due to its high computational and storage requirements. And also, a re-encryption procedure must be used to prevent decryption failures. The recryption process takes a significantly long time. According to [10], encrypting a whole ECG signal using the AES algorithm proved particularly computationally costly. Instead of this, the proposed FHEAES suggest using an evaluation process, which is better than a recryption process



(a) (b)

Figure. 4 Execution time analysis (a) Encryption time comparison (b) Decryption time comparison

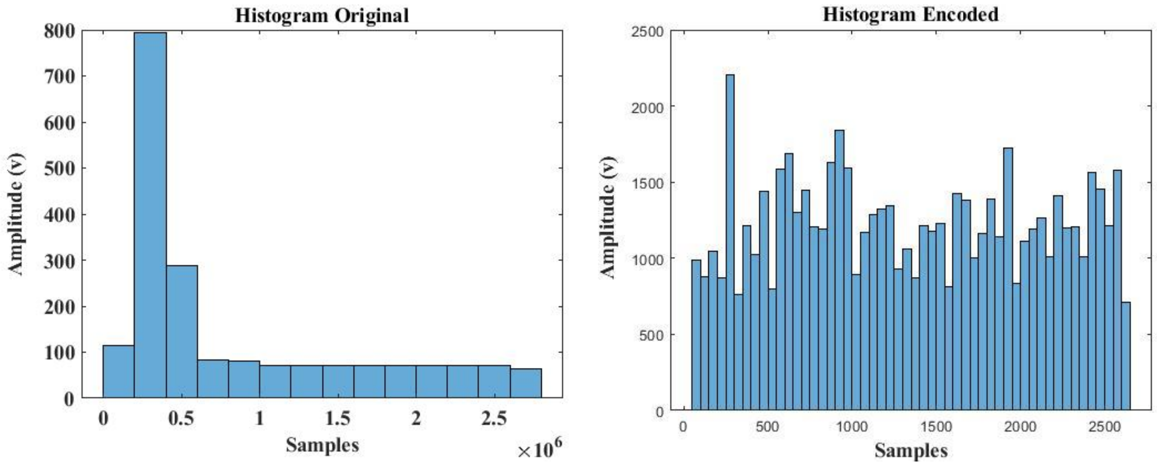


Figure. 5 Histogram of the original and the encrypted ECG of record 101

and takes a short time because it is based on computationally un-costly matrix operations. The suggested FHEAES algorithm is proven to take less time to encrypt and decode data than other algorithms. So, it is a very lightweight algorithm and suitable for many IOT applications.

4.6 Histogram analysis

The histogram is employed as a metric to assess statistical attack resistance. Different ECG signals were subjected to the suggested method. The histogram of the encrypted ECG signal is uniformly distributed and remarkably different from the original signal. Also, it is statistically indistinguishable from the original signal, as shown in Fig. 5. This is attributed to the use of the three proposed keys and the linear polynomial function, which provide robustness and complicate statistical analysis assaults on encrypted data. While [13] presents a similarity ratio between the original and the encrypted signal.

4.7 Mean square error (MSE)

Many numerical analyses (quantitative measures), such as MSE, were used to determine the differences between raw and decrypted ECG signals in order to assess the suggested algorithm's encryption strength. The MSE statistical metric is quite simple and widespread in distortion measurement. The result is better when the MSE is minimal. According to the result of this research, the value of MSE is equal to zero for all tested signals, which means that the proposed algorithm is perfect [27] and the integrity of the decoded ciphertext was kept by using the FHEAES algorithm. And, once the evaluation is complete, the ciphertexts remain in the same format without losing any data. This means that the use of computationally lightweight matrix operations allows the algorithm to handle the noise that arises from the FHE scheme. So, there isn’t any difference between raw and decrypted ECG signals, as shown in Fig. 6.

Experiments and statistical findings show that the suggested approach is resistant to traditional statistical attacks. The remarkable sensitivity of the three distinct keys is responsible for these findings, in addition to the high level of randomness of the evaluation function. Moreover, this research might be the start of a new age for the development and

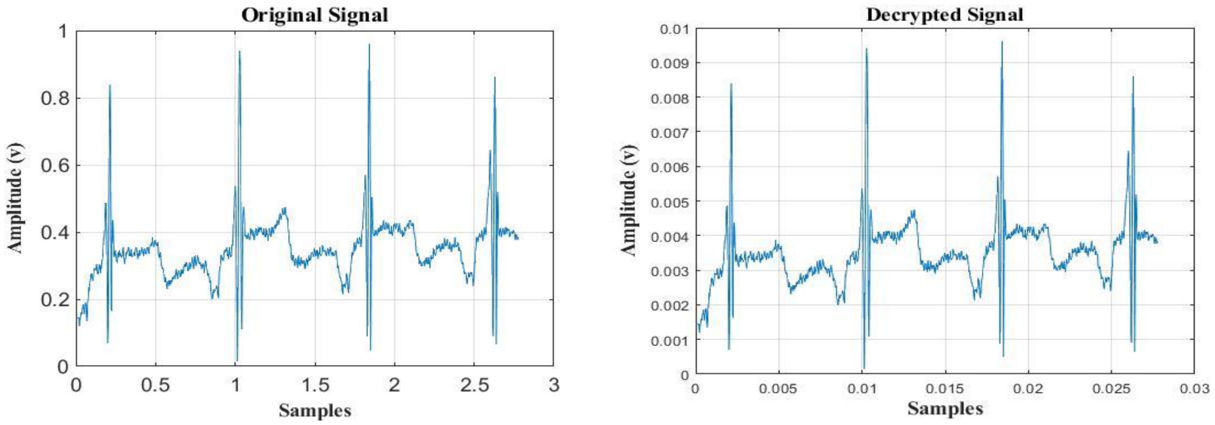


Figure. 6 Original and decrypted ECG of record 101

implementation of cryptographic algorithms in medical IOT based healthcare applications. The suggested algorithm may be implemented in other fields by changing the variable platform architectures.

5. Conclusion

The major purpose of signal security is to protect ECG signals from being tampered with, disrupted, changed, or destroyed, and furthermore, unauthorized access. In this paper, the FHEAES, a cryptography algorithm using the FHE algorithm with the AES algorithm, is presented. In the Internet of Things, particularly in medical e-health systems, increasing the keys offers several benefits. In this context, the complexity of mathematical operations will increase, which requires additional resources and needs a long processing time to complete. FHEAES employs three keys: AES key, round number, and HR, which increase encryption efficiency. Therefore, according to the findings, FHEAES will take 1.078950 × 1033 years to break or hack. This means that the required time to break the ciphertext is obviously increased more than 100 million times in comparison with the original AES algorithm. So, it enables the transfer of the ECG signals via unsecure network channels. Encryption and decryption operations are improved by combining the concepts of AES and FHE. The performance of the proposed cryptosystem was assessed using various ECG signals obtained from the MIT-BIH database. The HR was calculated and classified as normal or abnormal, which aids in the diagnosis of arrhythmias such as bradycardia and tachycardia. In comparison to an original database result, the suggested FHEAES technique has a 95.8% accuracy rate with the used of the Pan and Tompkins algorithm. FHEAES is considered a successful homomorphic encryption because it achieves the correct decoding of the ciphertext. Therefore, after an evaluation, the ciphertexts' original format was preserved. The FHEAES has 100% accuracy in the decryption process (recovering the original signal without losing any data). According to the findings, FHEAES outperforms several algorithms in time efficiency. Because of the use of computationally lightweight matrix operations, FHEAES is approximately 6 times faster in encryption and 3 times faster in decryption. FHEAES can be used in medical devices like body slices that measure heart rate. This is due to its ability to always measure heart rate and send it encrypted as long as it is connected to the internet. Therefore, FHEAES is suitable for IOT healthcare applications.

Generally, the combination of encryption algorithms is a wealthy field of research. The FHEAES concept can be applied to secure other medical signals, such as EEG signals. Also, by using parallel processing for FHEAES, the speed of encryption and decryption would be improved.

Conflicts of interest

The authors declare that they have no conflicts of interest to report regarding the present study.

Author contributions

Conceptualization, AAA, MMM, and SKG; methodology, AAA and SKG; software, AAA; validation, SKG, and MMM; formal analysis, AAA, MMM, and SKG; investigation, MMM, and SKG; resources, AAA; data curation, AAA; writing—original draft preparation, AAA; writing—review and editing, MMM and SKG; visualization, AAA; supervision, MMM and SKG; project administration, AAA, MMM and SKG; funding acquisition, AAA.

References

[1] V. Biksham and D. Vasumathi, "Homomorphic

Encryption Techniques for securing Data in Cloud Computing: A Survey", *International Journal of Computer Applications*, Vol. 160, No. 6, pp. 1-6, 2017. DOI: 10.5120/ijca2017913063.

[2] N. N. Mohamed, Y. M. Yussoff, M. A. Saleh, and H. Hashim, "Hybrid cryptographic approach for Internet of things applications: A review", *Journal of Information and Communication Technology (JICT)*, Vol. 19, No. 3, pp. 279-319, 2020. doi: 10.32890/jict2020.19.3.1.

[3] M. M. Potey, C. A. Dhote, and D. H. Sharma, "Homomorphic Encryption for Security of Cloud Data", In: *Proc. of International Conf. on Communication, Computing and Virtualization (ICCCV) 2016*, Procedia Computer Science, Vol. 79, Mumbai, Maharashtra, India, pp. 175-181, 2016, doi: 10.1016/j.procs.2016.03.023.

[4] N. N. Kucherov, M. A. Deryabin, and M. G. Babenko, “Homomorphic Encryption Methods Review”, In: *Proc. of IEEE Conf. of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, Moscow, Russia, pp. 370-373, 2020, doi: 10.1109/EIConRus49466.2020.9039110.

[5] M. U. Shaikh, S. A. Ahmad, and W. A. W. Adnan, "Investigation of data encryption algorithm for secured transmission of electrocardiograph (ECG) signal", In: *Proc. of 2018 IEEE EMBS Conf. on Biomedical Engineering and Sciences*, Sarawak, Malaysia, pp. 274-278, 2019, doi: 10.1109/IECBES.2018.8626640.

[6] R. L. Rivest, L. Adleman, and M. L. Dertouzo, "On data banks and privacy homomorphisms", *Foundations of Secure Computation*, pp. 169-180, Academic Press, New York, 1978.

[7] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A Survey on Homomorphic Encryption Schemes: Theory and Implementation", *ACM Computing Surveys*, Vol. 51, No. 79, pp. 1–35, 2018, doi: 10.1145/3214303.

[8] A. Viand, P. Jattke, and A. Hithnawi, "SoK: Fully Homomorphic Encryption Compilers", In: *Proc. of 2021 IEEE Symposium Conf. on Security and Privacy (SP)*, IEEE Computer Society, pp. 1092-1108, 2021, doi: 10.1109/SP40001.2021.00068.

[9] Ö. Kocaba¸s and T. Soyata, “Medical data analytics in the cloud using homomorphic encryption”, *Handbook of Research on Cloud Infrastructures for Big Data Analytics*, pp. 471–488, IGI Global, 2014, doi:10.4018/978-1-4666-8756-1.ch038.

[10] M. E. Hameed, M. M. Ibrahim, N. A. Manap, and M. L. Attiah, “Comparative study of several operation modes of AES algorithm for encryption ECG biomedical signal”, *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 9, No. 6, pp. 4850–4859, 2019, doi: 10.11591/ijece.v9i6.pp4850-4859.

[11] R. Premkumar and K. P. Vithya, “Secured ECG Distribution using Compression and RSA Algorithm for Telemedicine Application", *International Journal of Recent Technology and Engineering (IJRTE),* Vol. 3, No. 2, pp. 46–48, 2014.

[12] J. K. Madhloom, M. K. A. Ghani, and M. R. Baharon, "Ecg encryption enhancement technique with multiple layers of AES and DNA computing", *Intelligent Automation & Soft Computing*, Vol. 28, No. 2, pp. 493–512, 2021, doi:10.32604/iasc.2021.015129.

[13] Algarni, A. D. Soliman, N. F. Abdallah, H. A. et al. "Encryption of ECG signals for telemedicine applications", *Multimedia Tools & Applications*, Vol. 80, issue 7, pp. 10679-10703, 2021, doi: 10.1007/s11042-020-09369-5.

[14] Q. Qin, J. Li, Y. Yue, and C. Liu, "An adaptive and time-efficient ECG R-peak detection algorithm", *Journal of Healthcare Engineering*, Vol. 2017, pp. 1-14, 2017. doi:10.1155/2017/5980541.

[15] B. S. Lin, A. M. Wong, and K. C. Tseng, "Community-based ECG monitoring system for patients with cardiovascular diseases", *Journal of Medical Systems*, Vol. 40, No. 4, pp.1-12, 2016. doi:10.1007/s10916-016-0442-4.

[16] H. M. E. Hennawy, A. E. Omar, and S. M. Kholaif, “Design of LEA: Link encryption algorithm new proposed stream cipher algorithm”, In: *Proc. of 31st National Radio Science Conf. (NRSC)*, pp. 82–91, 2014, doi: 10.1016/j.asej.2014.08.001.

[17] Z. F. M. Apandi, R. Ikeura, and S. Hayakawa, "Arrhythmia Detection Using MIT-BIH Dataset: A Review", In: *Proc. of 2018 International Conf. on Computational Approach in Smart Systems Design and Applications (ICASSDA)*, Kuching, Malaysia, pp. 1-5, 2018, doi: 10.1109/ICASSDA.2018.8477620.

[18] " MIT-BIH Arrhythmia Database ", https://archive.physionet.org/physiobank/database/mitdb/ (accessed 4/10/2022).

[19] M. A. Z. Fariha, R. Ikeura, S. Hayakawa, and S. Tsutsumi, "Analysis of Pan-Tompkins

Algorithm Performance with Noisy ECG Signals", *Journal of Physics: Conference Series*, Vol. 1532, Issue 1, 2020. Doi: doi:10.1088/1742-6596/1532/1/012022.

[20] E. J. S. Luz, W. R. Schwartz, G. C. Chávez, and D. Menotti, "ECG-based heartbeat classification for arrhythmia detection: A survey", *Computer Methods and Programs in Biomedicine*, Vol. 127, pp. 144-164, 2016, doi: 10.1016/j.cmpb.2015.12.008.

[21] Z. Brakerski and V. Vaikuntanathan, "Efficient Fully Homomorphic Encryption from (Standard) LWE", *SIAM Journal on Computing*, Vol. 43, pp. 831–871, 2014, doi: 10.1137/120868669.

[22] R. Rizk and Y. Alkady, "Two-phase hybrid cryptography algorithm for wireless sensor Network", *Journal of Electrical Systems and Information Technology*, Vol. 2, pp. 296-313, 2015, doi: 10.1016/j.jesit.2015.11.005.

[23] "Polynomial Function", https://byjus.com/maths/polynomial-functions/ (accessed 4/10/2022).

[24] M. U. Shaikh, W. A. W. Adnan, and S. A. Ahmad, "Secured Electrocardiograph (ECG) Signal Using Partially Homomorphic Encryption Technique-RSA Algorithm", *Pertanika Journal of Science & Technology*, Vol. 28, pp. 231–242, 2020, doi: 10.47836/pjst.28.s2.18.

[25] M. Li, M. Xu, J. Luo, and H. Fan, "Cryptanalysis of an Image Encryption Using 2D Henon-Sine Map and DNA Approach", *IEEE Access*, Vol. 7, pp. 63336-63345, 2019. doi: 10.1109/ACCESS.2019.29164.

[26] A. Mousa, O. S. Faragallah, S. E. Rabaie, and E. M. Nigm, "Security Analysis of Reverse Encryption Algorithm for Databases", *International Journal of Computer Applications*, Vol. 66, No. 14, pp. 19–27, 2013, doi:10.5120/11153-6255.

[27] "Mean Square Error & R2 Score Clearly Explained", https://www.bmc.com/blogs/mean-squared-error-r2-and-variance-in-regression-analysis/ (accessed 4/10/2022).