Cryptographic Engineering on COVID-19 Telemedicine: An Intelligent Transmission Through Recurrent Relation Based Session Key

JOYDEEP DEY (joydeepmcabu@gmail.com)
M.U.C. WOMEN'S COLLEGE
ANIRBAN BHOWMIK
Maharajadhiraj Uday Chand Women's College
ARINDAM SARKAR
Ramakrishna Mission Vidyamandira
SUNIL KARFORMA
The University of Burdwan
BAPPADITYA CHOWDHURY
Belle Vue Clinic

Research Article

Keywords: Cardiovascular Disease, COVID-19 Telemedicine, Secret Share Encapsulation, Statistical Tests, Cryptographic Time

Posted Date: March 23rd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-183712/v1

Version of Record: A version of this preprint was published at Wireless Personal Communications on September 9th, 2021. See the published version at https://doi.org/10.1007/s11277-021-09045-3.

Cryptographic Engineering on COVID-19 Telemedicine: An Intelligent Transmission Through Recurrent Relation Based Session Key

[1]Joydeep Dey, [2]Anirban Bhowmik, [3]Arindam Sarkar, [4]Sunil Karforma, [5]Bappaditya Chowdhury

[1]State Aided College Teacher & Head, Department of Computer Science, M.U.C Women's College, Burdwan, India

[2] State Aided College Teacher, Department of Computer Science, M.U.C Women's College, Burdwan, India

[3]Assistant Professor, Department of Computer Science & Electronics, R.K.M. Vidyamandira, Belur, India.

[4]Professor & Head , Department of Computer Science, The University of Burdwan, Burdwan

[5]Neuropsychiatrist, Belle Vue Hospital, Kolkata, India

Corresponding Author: [1]Joydeep Dey, Email Id: joydeepmcabu@gmail.com

Abstract: Constraints imposed due to the cameo of the novel coronavirus has abruptly changed the operative mode of medical sciences. Most of the hospitals have migrated towards the telemedicine mode of services of the non-invasive and non-emergency patients during the COVID-19 time. The advent of telemedicine services has remotely rendered health services to different types of patients from their quarantines. Here, the patients' medical data has to be transmitted to different physicians / doctors. Such data are to be secured with a view to restore its privacy clause. Cardio vascular diseases (CVDs) are a kind of cardiac disease related to blockage of arteries and veins. This paper presents an intelligent and secured transmission of cardiac reports of the patients through recurrence relation based session key. Such reports were made through the following confusion matrix operations. The beauty of this technique is that confusion matrices are transferred to specified number of cardiologists with further secret shares encapsulation. The case of robustness checking, transparency and cryptographic engineering has been tested under different inputs. Different types of result and its analysis proves the efficiency of the proposed technique. It will provide more security in medical data transmission, especially in the needy hours of COVID-19 pandemic.

Keywords: Cardiovascular Disease, COVID-19 Telemedicine, Secret Share Encapsulation, Statistical Tests, Cryptographic Time

1. **Organization:** This paper has been organized as follows. Section 1 highlights the overall organization module. The objectivity of the proposed technique has been mentioned in section 2. Introduction on COVID-19 pandemic, contemporary relevance of telemedicine and its security aspects, cardiovascular diseases and reports, session key generation, etc were briefly stated at section 3. Related works were focused in section 4. Contemporary challenges faced by the COVID-19 telemedicine systems are being briefly highlighted in the section 5. Section 6 contains the proposed redressal strategy in short. Prime relevant points of the proposed technique are hereby stated in section 7. The core cryptographic proposed engineering technique was illustrated in section 8. Section 9 will display the block diagram of the proposed encryption technique. Results obtained for this paper has been explained in section 10. Comparative statements are given in section 11 followed by conclusion in section 12. Future scope of works is stated in section 13. Acknowledgement, Ethical compliance statements, and references are given the last followed by the author's profiles.

2. **Objective**: The objective of this paper is to propose a secured cryptographic transmission mechanism. A recurrence relation based session key has been generated for the COVID-19 telemedicine encryption. The robustness of the session key fails the intruders to detect the cipher text. The proposed transmission of encapsulated secret shares is strong enough to keep the patients' data privacy. This may be used as an efficient way when designing COVID-19 telemedicine system for the non-invasive and non-emergency patients.

3. Introduction:

The novel coronavirus (COVID-19) was first identified in China in December, 2019 and then rapidly

spread to the other countries in Asia, and then Europe and America. More than a million people had been infected and or died due to this global coranavirus [1-2]. Mutation rate is very high for this virus, and hence treated as very deadly virus. There incurs a huge amount of risks involved for the patients, geriatric citizens, children, etc [3]. In most of the countries there occurred a long term lockdown period. Proliferation of the technology in the telemedicine services has provided a boon to all global patients especially when patients need to be treated from their remote quarantines. With the wide developments in the advanced medical domain, sustainability of secured data transmission is a cornerstone issue. Keeping the patients' confidentiality clause under consideration, the emergence of intelligent cryptographic engineering is a better solution approach.

During the COVID-19 pandemic, obligatory social distancing and the absence of physical consultations have made telemedicine the most secured technique between patients and doctors. There has been a rapid increase in interests of provision of telemedicine with the advent of coronavirus. COVID-19 telemedicine is overcoming any issues between the doctors and patients [4]. It empowers everybody, particularly suspected patients and susceptible peoples, to remain safe at home and consult with doctors through virtual platforms. Thus, it is immensely assisting with diminishing the spread of the infection to mass populaces and the medical staffs and workers. COVID-19 telemedicine systems are serving as an efficient mechanism to stop the coronavirus transmission and providing safer medical assistance to the remote patients [5-6].

Cryptography [7-9] is the branch of computer science to protect the data from the unauthorized retrieval. It transforms data into a non readable format for the eavesdroppers. Thus, a message is made secured from the intruders. Involving the same key used at the encryption and decryption processes, is termed as symmetric key cryptography [10]. This paper presents a secured transmission of cardiological diseases related information. Here a novel encryption process comprised of recurrence relation based session key, generation and encapsulation of secret shares, and final transmission to the known group of recipients of COVID-19 telemedicine.Patients' data security has been kept on the frontier issue here. A class of cardiac disease that involves the narrowing or blockage of the arteries or blood vessels is known as Cardiovascular Diseases (CVDs). There are different CVDs like Coronary Artery Diseases(CADs), cardiac strokes, heart failure, hypertensive heart disease, cardiomyopathy, arrhythmia, etc. Hypertension, smoking, diabetes, increased cholesterol levels, malnutrition, alcohol consumptions, etc are catalyzing towards the formation of CVDs. Electro Cardio Graph is a measurement process to record the electrical activities of the heart. It is a continuous process of polarization and depolarization of all four chambers of the heart muscle [11]. The integral components of ECG are P-wave, QRS complex and T-wave. P wave denotes the atrium activation through SA node, QRS depicts the ventricular activation and T-wave represents the recovery state to restart again, as shown in figure 1.

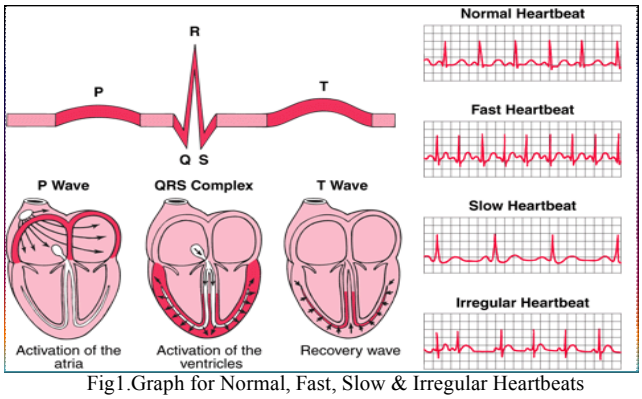


Fig1.Graph for Normal, Fast, Slow & Irregular Heartbeats

Hypertrophic cardiomyopathy [12] is a significant and frequent heart disease in rural areas of India. Lack of medical infrastructure persists in almost majority areas. Hypertrophic cardiomyopathy, dilated cardiomyopathy, restrictive cardiomyopathy, arrhythmogenic right-ventricular dysplasia, and are different types of cardiomiopathy. In hypertrophic cardiomyopathy the heart muscles enlarge and thicken. In dilated cardiomyopathy the ventricles enlarge and weaken. In restrictive cardiomyopathy the ventricle stiffens. The heredity, but the condition may also be acquired as a part of aging or high blood pressure. In other instances, the cause is unknown. The magnetic resonance images are given below.

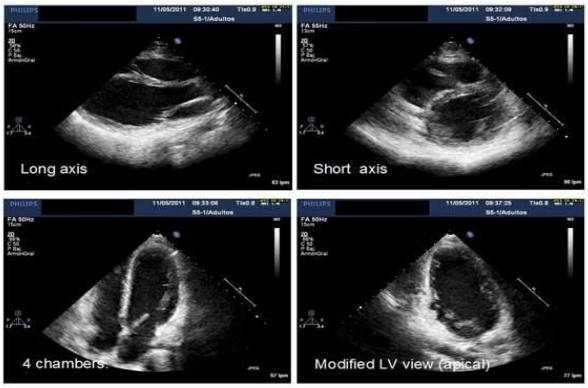


Fig 2. MRI of Heart

Secret sharing is a phenomenal part of cryptographic engineering [13]. To ensure security on the medical data, the proposed technique plays a pivotal role. There exists a lot of cryptography techniques such as DES, Triple DES, RC6, TWO FISH [7, 8] etc, each having their own pros and cons. This proposed technique works on secret sharing on cardiovascular disease related data using recurrence relation based session key.

4. Related Works

4.1 Cardiac Related Works

Patients can avail their medical facilities from a distant place through electronic health services. The use of Internet based technology has reduced the recurrent hospitals visits post cardiac surgery [14]. It provides constant monitoring of patients' health status and conditions from a remote place. Electronic telemedicine services are the emerging health care components when cardiac patients are facing difficulties during this COVID-19 crisis. Patients can manage and safeguard their health through online services [15]. The usage of Internet technology has offered to access and exchange medical data online anytime [16]. A device based integrated care component may be installed in patients suffering from myriad cardiovascular diseases. It may offer COPD patients a self-management approach. It may act as a measure before their treatments [17].

Hypertrophic Cardiomyopathy (HCM) [18] is related with thickening of the heart muscle, most commonly at the septum between the ventricles, below the aortic valve. This leads to thickening of the walls of the heart and abnormal aortic and mitral heart valve function, both of which may impede normal blood flow out of the heart. Hypertrophic cardiomyopathy (HCM) has no symptoms or only minor symptoms, and lives a normal life. Symptoms of HCM can occur at any age and may include chest pain, breathing shortness (dyspnea), fatigue, fainting (caused by irregular heart rhythms, abnormal responses of the blood vessels during exercise). Palpitations are caused due to abnormal heart rhythms (arrhythmias), such as atrial fibrillation or ventricular tachycardia.

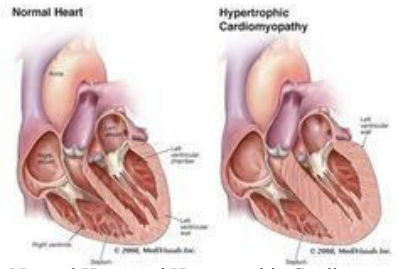


Fig 3. Normal Heart and Hypertrophic Cardiomyopathy

4.2 Cardiology Telemedicine in COVID-19

Patients having co-morbidity in terms of cardiac complications are more prone to the novel coronavirus. Such patients require special attention through digital healthcare support system. Neubeck L. et al. [19] had reviewed some articles regarding the digital healthcare support to the cardiovascular diseases (CVDs) patients. They have tried to bring the evidence of digital healthcare support in this contemporary quarantine times and COVID-19 isolations. Bryant M.S. et al. [20] had reviewed the articles in context of

the functioning of telehealth to the cardiopulmonary rehabilitation amid COVID-19 pandemic. Telehealth curtails the treatment time, cost, and physical travel for the patients. By using such services, geographical barriers are being diminished, else such patients would not be able to attend the hospitals physically due to various COVID-19 lockdown constraints. Peter R.J.G. et al. [21] had mentioned the importance of telemedicine on the cardiac rehabilitation patients in the period of coronavirus. Miller J.C. et al. [22] had surveyed the relevance of the smart devices used by the remote cardiac patients in this global pandemic crisis. Moreover, such patients were monitored through Remote Patient Monitoring (RPM) from their homes / quarantines from the heart perspectives. Chowdhury D. et al. [23] had provided a brief introduction of telehealth resource utilization in the view of pediatric cardiac unit. A rapid shift has been made in order to focus on the telehealth day to day services due to the COVID-19 social distancing and lockdown constraints.

4.3 Classical Cryptographic Engineering

Symmetric key cryptography can carry huge amount on data on any online transactions. Some of the common such algorithms are stated below.

Data Encryption Standard (DES): It is widely used symmetric block encryption method that was developed by Lucifer Cipher of IBM [7]. It encrypts data at blocks length of 64 bits each. Then 64 bits of cipher text are generated. The Feistel block cipher [9] technique has been used in DES. Here, two different forms of inputs are given i.e. plaintext and secret key. Different mathematical rounds of operation are carried out here.

Advanced Encryption Standard (AES): The Advanced Encryption Standard (AES) [7, 8] is an encryption technique for secured electronic data communication that was established in the year of 2001 by the U.S. National Institute of Standards and Technology. It is based on the Rijndael cipher method. Three variations of this algorithm exist with different three key lengths. The key lengths are 128 bits, 192 bits and 256 bits. 10, 12, and 14 rounds of processing are done for 128, 192, and 256 bits key lengths. All rounds are accompanied by S-Box, shift rows, mix column and add round keys.

4.4 Session Key Generation

Chen C.L. et al. [24] had proposed session key for the wireless sensory network communications. A secret key should be shared between the participating nodes for encryption purpose. They had designed dynamic key in order to reduce the intruding. Meena U. et al. [25] had designed a secured key agreement mechanism for the wireless transmissions. They had tried to abolish the data security challenges. Thei technique involves fuzzy C means clustering and social spider optimization with low power consumption. Azarderskhsh R. et al. [26] had proposed a secured clustering technique based on deterministic pairing of public keys. Two nodes belonging to the same cluster will be able to establish a key pair without disseminating any further information to the remaining nodes. Their technique has shown terminal-to-terminal authentication, minimum memory space, and resistance to terminal attacks. Dwivedi R. et al. [27] had proposed a fingerprint basis biometric cryptographic mechanism for the secured data communication. They has used the person's biometric trait to have the session key. Key leakage has been reduced. Sarkar A. et al. [28] had proposed a nature-inspired salp swarm based session key generation of 256 bits length for the transmission in E-health. Biometric traits were also included in their scheme for better patient data security. Sarkar et al. [29] had proposed a dynamic key generation scheme which works under the metaheuristic cuckoo search algorithm.

4.5 Secret Sharing

Secret sharing technique is used to divide the data by into multiple shares. And the original can be reconstructed only through minimum number of shares. Shamir's secret sharing scheme is based on a polynomial function [30]. Blakey's Secret Sharing Scheme has been used to solve secret sharing problem by the geometrical concepts [31]. Beimel A. et al. [32] had used multi-linear secret sharing concept on field elements. Sharing is done on random field secret elements and fixed field elements. Their technique seems to be very powerful on linear configurations. Sarkar A. et al. [33] had proposed soft computing on neural networks for the intraoral information sharing in the electronic medical field. Bhowmik A. et al. [34] had proposed a symmetric key based secret sharing of information. Their novel cryptographic technique defends against the intruders. Csirmaz L. et al. [35] had investigated the secret online sharing methods. Sarkar A. et al.

[36] had used the gingival data transmission through secret sharing in the teledental domain. Their scheme has the resistance against the malicious attackers.

5. Contemporary Challenges in COVID-19 Telemedicine

Symmetric cryptographic algorithms are good enough to transmit huge volume of medical data in e-Health. Amid COVID-19 pandemic, an exponential deluge has been observed in the telemedicine domain. If any node of the telemedicine is being compromised, the secured key will be revealed to the intruders. Existing data transmission algorithms do not vary their session key with every transmission session.

- Extensive use of digital platform on COVID-19 telemedicine without proper security.
- Different session keys for every unique session.
- Robustness of the session key in terms of its fitness.
- Cipher text may be prone to myriad attacks.
- Public channel may be compromised.
- Sender and recipient are likely to be compromised.
- Patients' data privacy gets unprotected.
- Slower functioning of the COVID-19 telemedicine systems.

6. Proposed Redressal Strategy

Contemporary challenges that were stated in earlier section5 have been addressed in this paper. The proposed technique provides an encryption methodology for secured procurement of cardiovascular disease data during COVID-19 period. Session key has been proposed by the recurrence relation. Use of multiple sessions key can safeguard the patients' confidential data in a more secured way. Their robustness has been tested through statistical tests. The good thing is that intruders can intercept the partial shares but they cannot regenerate the original one. Moreover, each partial share has been encapsulated into a different shield termed as Head-Tail structure [37]. Secret cardio sharing information has been done in this proposed technique in order to combat the intruders. Thus, the compromization of a single node has been addressed against the intruders. The cryptographic time of the proposed technique is acceptable.

7. Prime Points of the Proposed Technique

Following are the prime points that can be found in this proposed methodology.

- Recurrence relation based session key generation.
- Myriad session keys were generated for discrete telemedicine sessions.
- Data encapsuled secret sharing enabled COVID-19 telemedicine.
- Generation of partial secret shares based on mask matrix and confusion matrix.
- COVID-19 telemedicine: Resistance against the intruders.
- Evaluation of time complexity of individual modules.
- Standard graphical analysis against intruding.
- Cryptographic time has been calculated.
- Comparison against the existing techniques.
- Patients' data analysis has been carried out.

8. Proposed Cryptographic Engineering Technique

Here, the cardiac reports of the patients were being converted into binary matrix by a built in function. A user- defined mask matrix has been generated for every transmission session. In this paper, a mask generation matrix has been proposed for the encrypting the cardiac data. The binary matrix would be successively bitwise XORed with the binary mask matrix to generate a confusion matrix needed at COVID-19 telemedicine. Furthermore, each row of the mask matrix is being ANDed with the confusion matrix, in order to generate secret shares. At the receiver end, at least k numbers of partial shares are mandatory to reconstruct the original cardiac report [38].

This technique has raised the level of performance in terms of medical data transmission. A better treatment opinion is easily available through this technique in case of more critical patients.

Proposed Algorithm 1: Secured Encryption of Cardiac Data

$Requirement(s)$: $Cardiac\ Report\ of\ a\ patient\ (CR.pdf\ )$
$Input(s)$: $No.of\ Doctors\ (n), Threshold\ (k)$
$Output(s)$: $No.of\ Partial\ Ciphered\ Shares\ (n)$
/ Session Key Generation*/*
SK[128]← Call Session Key Module( )
$/*\ User-defined\ masking\ generation\ */$
Set P = $n_{C_{k-1}}$ & Q = n
$For\ i\ =\ 1\ to\ P$
  $For\ j\ =\ 1\ to\ Q$
    $MaskedMatrix[P][Q] =\ Call\ MaskGeneration(n,k)$
  $End\ for$
$End\ for$
$/*\ Cardiac\ Reports\ to\ Binary\ Matrix\ Convert\ */$
$For\ i =\ 0\ to\ Row\_len$
  $For\ j =\ 0\ to\ Colm\_len$
    $Rep[i][j]\ =\ Call\ Convert\_to\_Bin(\ CR.pdf\ )$
  $End\ for$
$End\ for$
$/*\ Confusion\ Matrix\ Generation\ */$
  $Call\ Confusion\_Mat\_Gen$(MaskMat[n][$n_{C_{k-1}}$]), Rep[r][c])
$/*\ Partial\ secret\ shares\ by\ bitwise\ AND\ operation\ */$
$Set\ k = 1\ and\ m = 1$
$For\ i\ =\ 1\ to\ Q$
  $For\ j\ =\ 1\ to\ P$
    $SecretShares[i][j] = MaskedMatrix[i][j]$ ***AND*** $Rep[k][m]$
      $j \leftarrow\ j + 1$
      $k \leftarrow\ k + 1$
      $m \leftarrow\ m + 1$
    $End\ for$
  $i \leftarrow\ i\ +\ 1$
$End\ for$
$/*\ Encapsulation\ of\ Secret\ Shares\ */$
$For\ i =\ 0\ to\ n_{C_{k-1}}$
  $Encapsuled\ Share\ \leftarrow Call\ Head\ Tail\ Encapsule(\ Secret\ Share[i][\ ], SK[128])$
$End\ for$
$/*\ Final\ Transmission\ of\ Secret\ Shares\ */$
$For\ i =\ 0\ to\ n_{C_{k-1}}$
  $Ciphered\ Share \leftarrow AES(\ Encapsuled\ Share[i][\ ], SK[128])$
$End\ for$

8.1 Proposed User-Defined Mask Generation Method

The mask matrix [39-40] of the order n * $^{n}C_{k-1}$ has been called to generate the confusion matrices. Algorithm for said masking function is given below.

Proposed Algorithm 1.1: User − Defined Mask Generation

Input: $\boldsymbol{No.of\ Secret\ Shares\ (n)}$ & $\boldsymbol{Threshold\ (k)}$
$Output$: $MaskMatrix[n][nCk-1]$
$T =\ 2^n$, D=$^{n}C_k$, $k1 =\ k2 = i\ = 0$, $H = Half\ +\ 1, Mid1\ =\ Floor\_Of\ ((0 +\ (D-1)\ /2\ )$
do {
  $T\ \leftarrow\ T\ -\ 1$

$BIN[n] = Call\ ConvertBinary\ (i)$
$If\ (CountOne\ (BIN\ [n]\ ) = 3)\ then$
$INDICES\ [k1++] = T$
$End\ if$
$\}\ while(\ T \geq 1)$
$INDICES\ [D] \leftarrow \{\ INC\ SORT(INDICES\ [0, H]\}\ Merge\ \{\ INC\ SORT\ (INDICES\ [H + 1]\ , D - 1\ )\}$
$do\{$
$INDICES2\ [k2++] \leftarrow INDICES[i]$
$INDICES2\ [k2++] \leftarrow INDICES\ [j]$
$i \leftarrow i + 1$
$j \leftarrow j + 1$
$\}\ while\ (i <= Mid1\ \ \textbf{AND}\ \ H <= D - 1\ )\ then$
For R = 1 to ${}^{n}C_{k}$
$Mask[R][\ \ ] \leftarrow Convert\ to\ Decimal(INDICES[\ INDICES2[R]\ ])$
$End\ for$
$Mask\ [n][D] \leftarrow\ Convert\ to\ Transpose(Mask[D][n]\ )$

In the above algorithm, a mask matrix has been proposed. It comprised of n number of shares. The dimension of such matrix is given by n * ${}^{n}C_{k-1}$. In this COVID-19 telemedicine system, this matrix is used to generate the confusion matrix. Let n=5, and k=3, the mask matrix will look like as in the row-major format in the following figure 4.

1010101011	**1011110100**	**1100011110**	**0111001101**	**0101110011**

Fig 4. Row-major of Mask Matrix

For example consider a data (D) of ten bytes long be like $COMSCMUCWC$. The following table 1 will provide the OR operation performed on the mask matrix of figure 1 and data (D).

Tab 1. OR Operation on mask matrix

$Share\ 1$	1	0	1	0	1	0	1	0	1	1
$Data\ (D)$	C	O	M	S	C	M	U	C	W	C
$Share\ 2$	1	0	1	1	1	1	0	1	0	0
$Data\ (D)$	C	O	M	S	C	M	U	C	W	C
$Share\ 3$	1	1	0	0	0	1	1	1	1	0
$Data\ (D)$	C	O	M	S	C	M	U	C	W	C
$Share\ 4$	0	1	1	1	0	0	1	1	0	1
$Data\ (D)$	C	O	M	S	C	M	U	C	W	C
$Share\ 5$	0	1	0	1	1	1	0	0	1	1
$Data\ (D)$	C	O	M	S	C	M	U	C	W	C

The resultant individual shares will be of double length where first row is being attached first followed by OR operations of the above matrix, as given in the following figure 5.

C0M0C0U0WC	**C0MSC0C00**	**CO000MUCW0**	**0OMS00UC0C**	**0O0SCM00WC**

Fig 5. Result of OR operation as row - major

It is very much obvious that each share will contain some missing bytes and those may be retrieved by accumulation of threshold k number of shares.

8.2 Proposed Session Key Generation based on Recurrence Relation

Recurrence relation is defined as a sequence of linear function of earlier terms. There are two types of recurrence relations: a) linear recurrence relation, and b) linear non homogeneous recurrence relation [41].

Linear recurrence relation is a homogenous recurrence relation of degree k with constant coefficients is of the form $b_n = c_1 b_{n-1} + c_2 b_{n-2} + \ldots + c_k b_{n-k}$, where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$. b_n is expressed in terms of the previous k terms of the sequence. Let $b_n = c_1 b_{n-1} + c_2 b_{n-1} + \ldots + c_k b_{n-k}$ be an assumed linear homogeneous recurrence. It has been assumed that the sequence term b_n satisfies the recurrence formula. Also the sequence term b'_n satisfies the given recurrence formula. So, $p_n = b_n + b'_n$ and $d_n = \propto b_n$ are also sequences that satisfy the recurrence, $\propto$ may be any constant value.

Linear non-homogeneous recurrence is a non-homogenous recurrence relation [10] with constant coefficients is a recurrence relation of the form $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k} + f(n)$, where $c_1, c_2, \ldots, c_k$ are real numbers, and $f(n)$ is a function depending only on n. The recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_{n-k} a_{n-k}$, is called the associated homogeneous recurrence relation. Here the concept of recurrence relation is used for random number generation that has been implemented for the session key generation in this paper. This novel idea of key generation is a unique concept in discrete mathematics [42-43].

This module describes the process of session key generation for the purpose of further encrypting the medical data. This key is used in confusion matrix generation. Here the concept of non-homogeneous recurrence relation is used for the said key generation module. At first session key is XORed with symmetric key and then divide into n number of shares using mask matrix and then each share of session key is transmitted to receiver end attached with each share of message.

Proposed Algorithm* 1.2: *Recurrence Relation based Session Key Generation

Input(s): - S$eed\ values, coefficient\ value\ and\ non\ homogeneous\ recurrence\ equation.$

Output(s): - S$ession\ Key\ of\ 128\ bits$

Assign $i, j, m, n, f, lr\ as\ numbers$ & $a[m], r[n], c[m] as\ array$

n: total random number, m: total no.of coefficient in non-homogeneous recurrence relation

For $i = 0\ to\ m$

$c[i] = get\_coeff\ ()$

$a[i] = get\_seedVal\ ()$

$End\ for$

$lr = get\_largestPrimeFact\ (a[2]\ xor\ c[3])$. /* $a[2]$ & c [3] are randomly chosen */

$a[0] = a[0]\ xor\ lr.$

For $i = 1\ to\ m$

$a[i] = (a[i] xor\ a[i-1])\ xor\ lr$

$End\ for$

For $i = 3\ to\ n$

$a[i] = get\_val\ (rec\_Funct\ (i))$

If $(a[i] < 0)$

$a[i] = a[i]$

$End\ if$

$r[i] = a[i]$

F = $((((a[i] xor\ c[1]) xor\ c[3]) xor\ c[5]) xor \ldots c[m])$

$a[i] = f$

$End\ for$

If $(n >= 3)$

$r[n] = get\_shuffle(r[n])$ // $r[n]$ is here session key.

$End\ if$

8.3 Proposed Confusion Matrix Generation

The proposed technique implies XOR operation of each rows of the masked matrix on the cardiac report binary matrix. Confusion matrices will be thus generated before transmission in this coronavirus pandemic time. The following algorithm will explain the concept of confusion matrix.

Proposed Algorithm* 1.3: *Confusion Matrix Creation

$Input$: $Masked\ Matrix$: $MaskMatrix[n][n_{C_{k-1}}])$, $Binary\ Cardiac\ Report(Rep[\,][\,])$, Session Key (SKey128])

$Output$: $'1'\ number\ of\ Confusion\ Matrix$

$Assign\ Row \leftarrow\ Call\ ReturnRow\ (Rep[r][c])$

$Assign\ Colm \leftarrow\ Call\ ReturnColumn\ (Rep[r][c])$

$For\ i = 0\ to\ (Row - 1)$

$For\ j = 0\ to\ Colm - 1$

$ConfusionMat[i][j] \leftarrow Call\ XORBitwise\ (Rep[i][j], MaskMatrix[n][\ \ ], SKey\ [128\ ])$
$Increment\ j$
$End\ for$
$Increment\ i$
$End\ for$

8.4 Proposed Encapsulation of Secret Shares

This sub-section deals with the encapsulation of the individual secret shares into a proposed shield structure of Head-Tail. An art of wrapping the secret shares into a different layered structured of single unit before the final departure of the shares in the wireless domain is done through this share encapsulation. Two different structures of head and tail are added at the front and rear of each share respectively. It is deliberately done to make the secret shares more protected against the task of intruding. The following figure 6 represents the block diagram of the said concept.

Fig 6. Encapsulation of Secret Shares into Proposed Head-Tail Structure

Algorithm 1.4: Encapsulation of Secret Shares into Head − Tail Structure
Input(s): Session Key: S_Key[128]
Output(s): Head-Tail Concatenation with Encrypted E-Data
Assign SKey1, SKey2.
SKey1$\leftarrow$ $S\_Key[0\ \ldots\ 63]$, $SKey2 \leftarrow S\_Key2\ [64\ \ldots\ 128]$
$C \leftarrow ToCharacter(\ S\_Key2[64 \ldots 127])$
$m = ASCII\ (C)$
$Header \leftarrow ((SKey1\ [\ ]\ XOR\ SKey2))\ <<\ (m\ MODE\ Strlen(SKey))$
$ColmnEl \leftarrow get\_2ndColmn\ (S\_Key[128])$
$Tailer \leftarrow Bitwise$ XOR-OPR$(ColmnEl,\ SKey2)$ // ColmnEl *is XORed with* $SKey2$ *bit by bit*

9. Block Diagram of the Proposed Methodology

In this section, the schematic block diagram of the proposed technique has been given below in figure 7. It represents the flow control of the proposed COVID-19 telemedicine system.

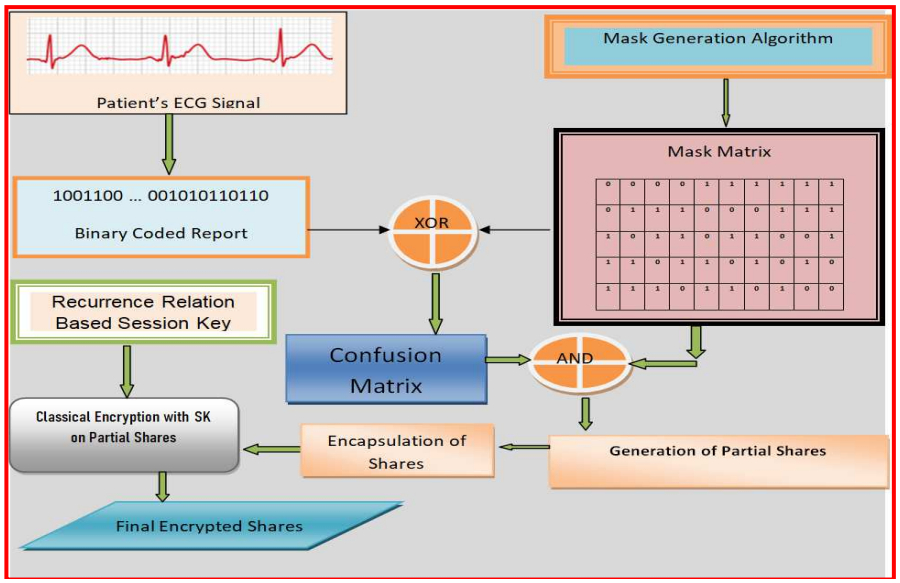


Fig 7. Block diagram of the proposed technique

10. Result Sections

The decimal precision was taken in accordance with the standards of IEEE 754 in this paper. The following configurations were taken into consideration for obtaining the results here.

Processor name: Intel Core (*i*9) – Xth generation, Processor Speed: 2.6 GHz, HDD: 1TB, RAM: 28GB, Operating System: Windows 10; 64 bits, Programming Language: Python 3.9.1.

In the following sections, the efficacy results have been presented with its implications. The objective of this section is to have favorable outcomes while designing the COVID-19 pandemic telemedicine security and privacy issues. Different set of tests were conducted on the proposed technique to substantiate its efficiency.

10.1 Case of Histogram Analysis

The clinical signal online database has been used in this study for different sets of tests to establish its efficiency and effectiveness [44]. Histogram analysis has been carried out at this proposed technique. How binary values of 1s and 0s of a cardiac report are spread, this has been studied. A graphical representation of frequency distribution inside the cardiac file has been shown in following figure 4. The distribution of data i.e. peaks; spreads and symmetricity is not relevant. The peaks bars represent the maximum occurrences and spreads represent the information variation. The results as per histogram obtained at the following figure 8 are neither skewed and nor well distributed.

Different cardiac reports were analyzed in this proposed technique with such extensions likes of .pdf, .txt, .doc, etc. This technique is valid in telemedicine systems that between threshold numbers of doctors, the original patients' cardiac file cannot be generated [45]. So the confusion matrices are more intelligent enough to make the intruders fool. Each confusion matrix is nothing but a double dimensional matrix of 1s and 0s. Only the valid doctors can open the file that is needed for patients' treatments. Thus, the proposed confusion matrix generation technique may be accomplished as a COVID-19 Telemedicine.

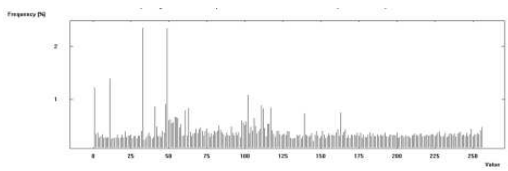


Fig 8.Histogram of ECG Report

The bar graphs observed in the above figure 8 are not appropriate in terms of patients' data security. However, the fruitfulness of the proposed technique in terms of histogram in given in the later sub-section 10.4.

10.2 Case of Autocorrelation Analysis

Analysis of autocorrelation of different types of source files was carried out in this paper. Autocorrelation of a plain file is an index of the similarity at various levels. Autocorrelation of source file without encrypting through proposed technique is given at the following figure 9.

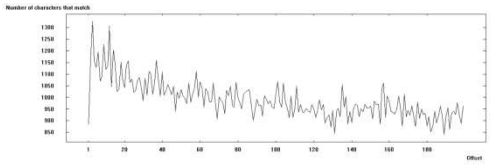


Fig 9. Autocorrelation of ECG Report

From the above figure, it can be said that there exists similarities in the characters inside the source file. Moreover, the utility of the proposed cryptographic technique is illustrated in the later sub-section 10.4.

10.3 Case of Floating Frequency Analysis

In this sub-section, the analysis of floating frequency of the source files was carried out. The local information content inside the file is shown here in graphs. It means how many varieties of sixty four characters are present in the source medical file. Figure 10 shows the floating frequencies of the same file without any proposed encryption.

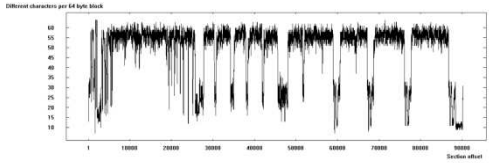


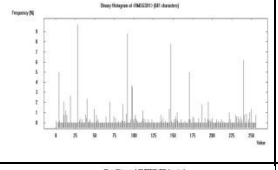
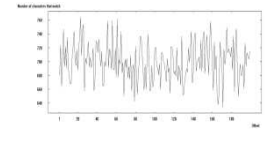
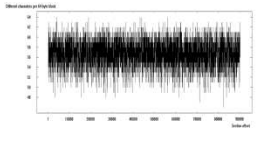
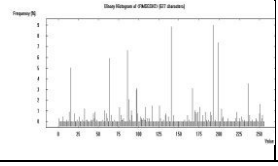
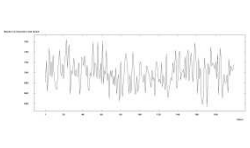
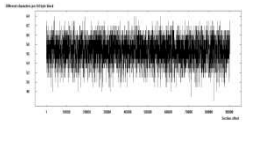
Fig 10. Floating Frequency of ECG Report

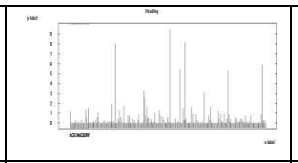
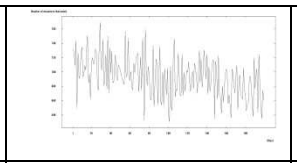
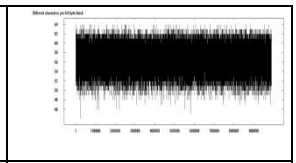
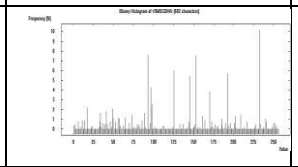
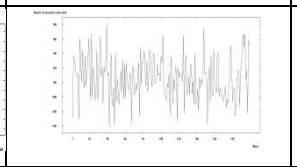
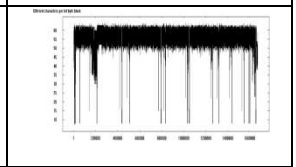
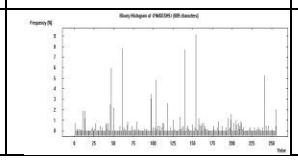
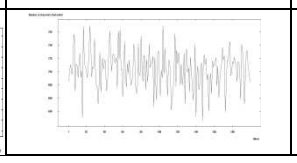
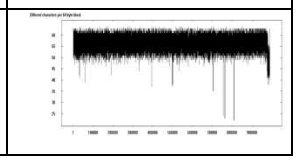
The robustness against the intruders of the proposed method is mentioned in the later sub-section 10.4.

10.4 Contrast in terms of Histogram, Autocorrelation, Floating Frequency

In the following table 2, there has been the histograms, autocorrelations, and floating frequencies of the same source file for n number of secret shares. These graphs were derived when encrypting the file with the proposed technique.

Tab 2. Histogram, Autocorrelation, Floating Frequency analysis of different proposed shares

Proposed Secret Share Number	**Histogram of Proposed Share post encryption**	**Autocorrelation of Proposed Share post encryption**	**Floating Frequency of Proposed Share post encryption**
TM$1			
TM$2			

TM$3			
TM$4			
TM$5			

The above stated histograms, autocorrelations, and floating frequencies of the secret shares developed by proposed methodology are showing equivalence distribution of the data of a shared cardiac source file. This proves the robustness of the proposed technique in this global pandemic. This cryptographic method on heterogeneous reports safeguards the different Man-in- the middle attacks [46-47]. Intruders will get no clues from the generated cipher texts inside the wireless networks.

10.5 Correlation Analysis

In this sub-section, the correlation [10, 17] between ASCII difference and total number of changed characters has been carried out on different sets of cardiac files. A secured cryptographic engineering technique should transform a text file (.pdf, .docx, .txt, .xls, etc) into a randomized encrypted file with low correlation. The formula for Pearson correlation coefficient [48] is given at the following equation 1.

$$r_c = \frac{\sum_{i=1}^{n}(x_i - x')*(y_i - y')}{\sqrt{\sum_{i=1}^{n}(x_i - x')^2 * (y_i - y')^2}} \quad \ldots (1)$$

Here, r_c means the coefficient of correlation, x_i, y_i are the values of x and y in the data file respectively, x', y' are the average of x and y data respectively. The rule of thumb which is used to draw the impact in this respect is given at the following table 3.

Tab 3. Impact of Correlation

Sl. No.	Range of Correlation	Impact of Correlation
1	-0.90 to -1.00 or +0.90 to +1.00	Very high negative or positive
2	-0.70 to -0.90 or +0.70 to +0.90	High negative or positive
3	-0.50 to -0.70 or +0.50 to +0.70	Medium negative or positive
4	-0.30 to -0.50 or +0.30 to +0.50	Low negative or positive
5	0.00 to -0.30 or 0.00 to +0.30	Very low negative or positive

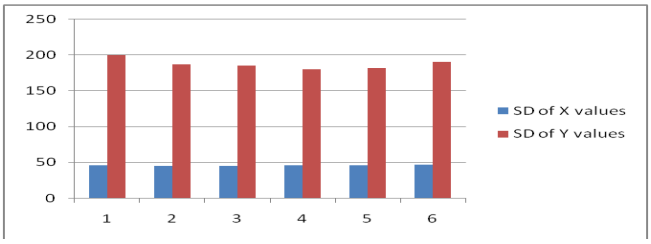
The above stated table contains the different ranges of the correlation coefficient values and its impact. The correlation values are given below at the table 4, when computed on different heterogeneous files. The significance of the session key may be drawn from the following table.

Tab 4. Data Analysis on correlation

Name of Input(s)	SD of X Values	SD of Y Values	Correlation Coefficient (r)	Coefficient of Determination (%)	Significance of Test Value	Standard error slope values
F1	45.89	200.05	-0.426	18.2	-1.33	1.394
F2	44.90	187.07	-0.420	18.2	-1.34	1.389
F3	44.90	185.07	-0.420	18.2	-1.34	1.389
F4	45.86	180.09	-0.422	19.0	-1.32	1.400
F5	45.56	181.76	-0.399	17.1	-1.35	1.402
F6	46.34	190.45	-0.398	18.1	-1.33	1.399

The above stated tables contains the headers as Name of Input(s), SD of X Values, SD of Y Values, Correlation Coefficient(r), Coefficient of determination, Significance of Test Value, and Standard error slope values. Here X and Y denote the number of changed characters and ASCII differences respectively. The Pearson correlation coefficient gives the strength and course of the straight connection between two factors. From the above table 2 it has been seen that the estimation of connection coefficient among X and Y is - 0.362 which is less than 0.0. This shows that there is a solid negative connection between the factors or the factors may have a nonlinear relationship. The relationship is negative in light of the fact that, as one variable expands different abatements [37]. In any case, from the disperse plot given in figure 11. There is nonlinear relationship exists between two factors (X, Y) from the above presented table.

Fig 11. Graph on correlation analysis



10.6 Chi-Square Context

The contrast between the noticed recurrence of characters and the genuine recurrence of characters is known as Chi-Square test. Individual Chi-Square computations were made on the different shares as generated by the proposed technique. The equation 2 shown below performs the said computation.

$$\chi^2 = \sum_{i=1}^{n} \frac{(OFC_i - AFC_i)^2}{AFC_i} \qquad \ldots \quad (2)$$

where, OFC_i and AFC_i means the existing occurrence and the contemplated occurrence of i^{th} character respectively in the share.

Tab 5. Chi-Square values on the proposed set of secret shares

Source File Number	Secret Share Number	Proposed Secret Share
F1	TM$1	292
	TM$2	139
	TM$3	647
	TM$4	140
	TM$5	65
F2	TM$1	206
	TM$2	102
	TM$3	552

	TM$4	273
	TM$5	94
F3	TM$1	512
	TM$2	216
	TM$3	855
	TM$4	206
	TM$5	81
F4	TM$1	380
	TM$2	212
	TM$3	686
	TM$4	243
	TM$5	65
F5	TM$1	321
	TM$2	178
	TM$3	811
	TM$4	197
	TM$5	60
F6	TM$1	347
	TM$2	205
	TM$3	565
	TM$4	339
	TM$5	58

The above stated table 13 is comprised of the following table headers as Source File Name, Secret Share Number, and Proposed Secret Share. It may be stated that the proposed technique of secret sharing based on recurrence relation for COVID-19 transmission provides good quality of cryptographic encryption in terms of Chi-Square values.

10.7 Statistical Strength of Session Keys

NIST Test Suite [49] is a statistics package comprised of fifteen tests. Its objective is to determine the randomness of recurrence relation session key proposed in this paper. Robustness of the session key is determined by these tests. Six different category source files were tested through seventy five set of session keys. Average values are being noted in the following tables 7- 12 as per our simulations done. The accompanying table 6 is the list table of the fifteen measurable statistical tests.

Tab 6: Indexing on NIST

Name of the NIST	Proposed Test Code
$Frequency$	TEST@01
$Frequency\ (Block-wise)$	TEST@02
Run	TEST@03
$Longest\ Run\ of\ Ones\ in\ Block$	TEST@04
$Binary\ Matrix\ Run$	TEST@05
$Discrete\ Fourier\ Transformation$	TEST@06
$Non\ overlapping\ Template\ Matching$	TEST@07
$Overlapping\ Template\ Matching$	TEST@08

Maurer's Universal Statistical	TEST@09
Linear Complexity	TEST@10
Serial	TEST@11
Approximate Entropy	TEST@12
Cumulative Sum	TEST@13
Random Excursion	TEST@14
Random Excursion Variant	TEST@15

Tab 7. Statistical tests on Source File Number 1

Proposed Test Code	Session Key with p-value >= 0.05	Percentage	Outcome (1: True,0:False)
TEST@01	909	90.9	1
TEST@02	857	85.7	1
TEST@03	871	87.1	1
TEST@04	802	80.2	1
TEST@05	914	91.4	1
TEST@06	793	79.3	1
TEST@07	959	0.9590	1
TEST@08	751	75.1	1
TEST@09	869	86.9	1
TEST@10	793	79.3	1
TEST@11	884	88.4	1
TEST@12	961	96.1	1
TEST@13	774	77.4	1
TEST@14	812	81.2	1
TEST@15	873	87.3	1

Tab 8. Statistical tests on Source File Number 2

Proposed Test Code	Session Key with p-value >= 0.05	Percentage	Outcome (1: True,0:False)
TEST@01	899	89.9	1
TEST@02	874	87.4	1
TEST@03	915	91.5	1

TEST@04	960	96.0	1
TEST@05	872	87.2	1
TEST@06	863	86.3	1
TEST@07	914	91.4	1
TEST@08	954	95.4	1
TEST@09	854	85.4	1
TEST@10	915	91.5	1
TEST@11	923	92.3	1
TEST@12	939	93.9	1
TEST@13	848	84.8	1
TEST@14	864	86.4	1
TEST@15	867	86.7	1

Tab 9. Statistical tests on Source File Number 3

Proposed Test Code	Session Key with p-value >= 0.05	Percentage	Outcome (1: True,0:False)
TEST@01	919	91.9	1
TEST@02	867	86.7	1
TEST@03	845	84.5	1
TEST@04	896	89.6	1
TEST@05	916	91.6	1
TEST@06	920	92.0	1
TEST@07	915	91.5	1
TEST@08	975	97.5	1
TEST@09	864	86.4	1
TEST@10	871	87.1	1
TEST@11	922	92.2	1
TEST@12	902	90.2	1
TEST@13	858	85.8	1
TEST@14	960	96.0	1
TEST@15	932	93.2	1

Tab 10. Statistical tests on Source File Number 4

Proposed Test Code	Session Key with p-value >= 0.05	Percentage	Outcome (1: True,0:False)
TEST@01	929	92.9	1
TEST@02	877	87.7	1
TEST@03	905	90.5	1
TEST@04	936	93.6	1
TEST@05	884	88.4	1
TEST@06	896	89.6	1
TEST@07	909	90.9	1
TEST@08	958	95.8	1
TEST@09	934	93.4	1
TEST@10	892	89.2	1
TEST@11	932	93.2	1
TEST@12	957	95.7	1
TEST@13	918	91.8	1
TEST@14	849	84.9	1
TEST@15	973	97.3	1

Tab 11. Statistical tests on Source File Number 5

Proposed Test Code	Session Key with p-value >= 0.05	Percentage	Outcome (1: True,0:False)
TEST@01	869	86.9	1
TEST@02	906	90.6	1
TEST@03	896	89.6	1
TEST@04	872	87.2	1
TEST@05	987	98.7	1
TEST@06	954	95.4	1
TEST@07	935	93.5	1
TEST@08	855	85.5	1
TEST@09	879	87.9	1
TEST@10	974	97.4	1
TEST@11	847	84.7	1
TEST@12	963	96.3	1

TEST@13	908	90.8	1
TEST@14	864	86.4	1
TEST@15	852	85.2	1

Tab 12. Statistical tests on Source File Number 6

Proposed Test Code	Session Key with p-value >= 0.05	Percentage	Outcome (1: True,0:False)
TEST@01	884	88.4	1
TEST@02	857	85.7	1
TEST@03	957	95.7	1
TEST@04	902	90.2	1
TEST@05	880	88.0	1
TEST@06	924	92.4	1
TEST@07	885	88.5	1
TEST@08	904	90.4	1
TEST@09	860	86.0	1
TEST@10	978	97.8	1
TEST@11	952	95.2	1
TEST@12	938	93.8	1
TEST@13	916	91.6	1
TEST@14	960	96.0	1
TEST@15	913	91.3	1

The above stated tables 7-12 contain the table headers as Test Code, Session Key with p-value >=0.05, Percentage and Outcome.

10.8 Patients' Data Security Analysis

This sub-section explains the security of the medical data in this COVID-19. Recurrence relation based sesion key has been generated for the cryptographic engineering domain. The use of proposed confusion shares had redued the chances of stealing from different unknown malicious agents. Different types of attacks on the patients' confidential data against the proposed system have been briefly stated.

- Dos Attacks on Patients' Data: In this proposed strategy, the fractional mystery portions of the COVID-19 telemedicine was dispersed to all the partaking machines inside the gathering of known users. An indepndent hub has no advantage to remake the information without collaboration from the others. Consequently, the remaining task at hand of every hub has been diminished. Accordingly, the proposed method can effieciently withstand Dos assaults under such COVID-19 telemedicine.

- Mid-way Intervene Attacks on Patients' Data: Insightful transportation systems were conveyed in this proposed strategy of recurrence relation based session key in COVID-19. The sent information might be meddled by the outer intruders. The proposed COVID-19 telemedicine do opposes against the impedance

assaults. The session key that was generated here have been tried to detect under various statstistical properties [50]. But the results were failed to its strong efficiency.

- Replay Attacks on Patients' Data: This proposed method can oppose against the replay assault by the intruders. Since the cardiac reports was broken and scrambled into fractional offers, at that point it would not be conceivable to recover except if the edge shares are being summarized. That implies no single hub contains all the information. In the event of hub being compromized, the misfortune the information burglary has been checked here strongly.

- Man-in-the Middle (MITM) Attacks on Patients' Data: As a foe segment, gatecrashers are dynamic to take those patients' significant information inside the organization. To unscramble the information, gatecrashers need all the minimum number of offers to uncover the data. Yet, this would not be possible because of the quantity of partaking and threhols shares are kept covered up.

- Session Key Fitness: The session key has been generated through recurrence relation and ships off all the partaking hubs in a similar gathering of known users. Before that it has been checked by the NIST suite [49]. Thus, this proposed method guarantees genuine haphazardness in the session key.

10.9 Brute Force Attacks

Efficient management of key space makes the brute force attack [45] infeasible. In this attack, attacker tries to translate the cipher text into plain text using every possible key. On average, half of all possible keys are enough for achieving success. Algorithms are known to all in most networking system but brute-force attack will impossible if the algorithm uses large key space. Presently, the fastest super computer is Japan's Fugaku having speeded 415.53 $petaflops\ i.e.\ 415.53x10^{15}$ floating point operations per second. Let us consider each trial requires 2000 FLOPS to complete one check. So number of trials complete per second is: $207.77x10^{12}$. The quantity of seconds in a year is: $365 * 24 * 60 * 60 = 31{,}53{,}600\ sec$.

Now from the above stated key space the formula for breaking the session key is $2^{2C}/\ (207.77 * 10^{12} * 3153600) = Y$; Y denotes number of years. When C increases then Y increases i.e. $(C \infty Y)$. Thus for large key length it is very difficult to decode the session key. A cipher text with such a long key space is sufficient for reliable practical use in this corona virus era. It proves that a session key is good enough to overcome the brute force attack due huge computation time needed. More compatible security efforts are bare minimum requirements in any cryptographic system [51]. Hence it would be very efficient in developing the COVID-19 telemedicine where patients' confidentiality is an integral factor.

10.10 Differential Attacks

Intruders comprehensively endeavor to derive any sort of heuristics between the proposed cipher text and unique cardiac files. The set of seventy five session keys generated through proposed recurrence relation were tested under the differential attacks. A flip in the session key would incredibly change the entire composition of the cipher text. Thus, intruders are not in a good position for correct predictions. The following table 13 contains the randomized sampling done for this purpose. The length of recurrence relation session key is 128, which is further used as AES encryption in the COVID-19 telemedicine. The following table has been done on an arbitrary message of nominal size. There exists a frequency of keys extracted according to the flips occurred in the bits positions.

Tab 13. Flip in a bit results in number of bits changed in cipher text

Range of bit position (Class Interval)	Total No. of Keys (Frequency)	Affected No. of bits on cipher text
0-15	4	47
16-31	11	95
32-47	14	70
48-63	8	48
64-79	6	103
80-95	16	115
96-111	9	79

112-127	7	95

The above mentioned table 13 is composed by the following table headers as Range of bit position (Class Interval), Total No. of Keys (Frequency), and Affected No. of bits on cipher text. Graphical representation of the above stated table has been made at the following figure 12.

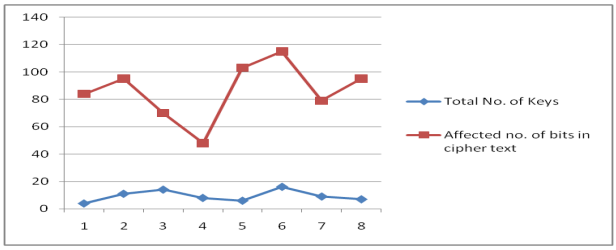


Fig 12. Graph for Flipping Effect on Keys

10.11 Analysis of Entropy

Entropy of a cardiovascular report file is the degree of distribution in terms of 256 ASCII characters. Generally in ordinary file, it doesn't contain all 256 characters at uniform distribution. The proposed encryption transforms the highly appeared characters to sparsely appeared characters at random. The following table 14 shows the entropy of the cardiovascular modules prior and post encryption. After encryption the entropy value is approaching the maximum limit of eight, which is acceptable.

Tab 14. Entropy Observations on Pre and Post-Encryption

Sl. No.	Type of Source File	Entropy Prior Encryption	Entropy Post Encryption on All Shares
1	PDF FILE	6.23	7.05
			7.11
			7.20
			7.06
			6.92
2	DOC FILE	5.44	7.16
			7.21
			6.92
			7.09
			7.36
3	TXT FILE	4.56	6.90
			7.00
			6.25
			6.84
			7.14
4	JPEG FILE	6.58	6.20
			7.11
			6.75
			7.34
			7.08
5	ZIP FILE	3.27	6.11
			7.19
			7.28
			6.56
			6.20
6	PNG	5.69	7.56
			7.20
			6.90

			7.36
			6.51

The entropy graph on different set of files based on the above table is shown in the following figure 13.

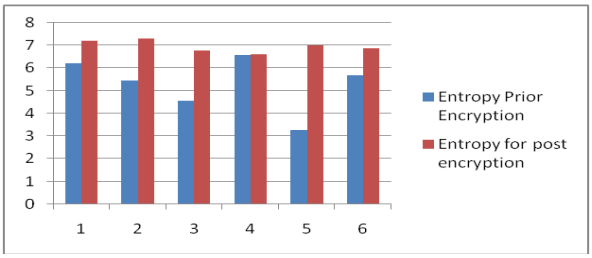


Fig 13. Graph of entropy value

The entropy post encryption has been computed as average values of all the shares. From the above mentioned figure it can be concluded that the proposed encryption has yielded much higher results if compared with pre-encryption.

10.12 Cryptographic Time

Using the proposed cryptographic technique on COVID-19 telemedicine, the transmission of the medical data, clinical reports, and prescriptions is possible to the physicians through online mode. The cryptographic time needed is another crucial index towards the effectiveness of the proposed technique [38]. It includes both the encryption time and decryption time. Six different source files were encrypted through proposed set of seventy five session keys one by one. The following table 15 contains the average cryptographic time for the said files.

Tab 15. Proposed Average Cryptographic Time

Sl. No.	File No.	Encryption Time (ms)	Decryption Time (ms)	Total Cryptographic Time (ms)	Average Cryptographic Time (ms)
1	F1	291.64	175.28	469.92	6.27
2	F2	217.25	157.20	374.45	5.00
3	F3	307.50	195.38	502.88	6.71
4	F4	196.31	165.07	361.38	4.81
5	F5	269.15	223.97	493.12	6.58
6	F6	348.32	311.84	660.16	8.80

The above stated table 21 contains the following table headers as Sl. No., File No., Encryption Time (ms), Decryption Time (ms), Total Cryptographic Time (ms), and Average Cryptographic Time (ms).

10.13 Time Complexity Evaluation of the Proposed Technique

The time complexity of any software is a vital aspect for its acceptance. In the sub-section, the time complexity of the proposed cryptographic method has been generated. This method has been divided into six modules, namely, Recurrence Session Key Generation, Mask-Generation, Binary File Conversion, Partial Encrypted Share Generation, Share Encapsulation, and Final AES Encryption. The individual time complexity of each module has been written in the following table 16. By summing up, the overall time complexity of the proposed method can be evaluated.

Tab 16. Modular Time Complexity Generation

Module No.	Proposed Module Name	Module's Time Complexity	Remarks (if any)
1	Recurrence Session Key Generation	$O(nlogn)$	n is the number of shares
2	Mask-Generation	$O\ (nlogn)$	n is the number of shares

3	Binary File Conversion	$O\ (r * c)$	r and c are the dimensions of the file
4	Partial Encrypted Share Generation	$O\ (nlogn)$	n is the number of shares
5	Share Encapsulation	$O\ (n)$	n is the number of shares
6	Final AES Encryption	$O\ (n)$	n is the number of shares

11. Comparative Statements

In this sub-section, two comparative tables were drawn. Firstly, where the proposed technique has been compared with the classical cryptographic algorithm likes of AES and 3DES [52]. The summary has been shown in the following table 17. Secondly, the proposed technique has been compared with the some of the existing related papers that were cited in section 4. The following table 2 contains the summarized values in that regard.

This section deals with a comparative tabular representation between the proposed methodology and existing encryption algorithms i.e. 3DES and AES [52]. It has been noted that the proposed method had provided efficacy results under the comparative study. The following table 17 contains the summarized comparison.

Tab 17. Comparative Study with classical cryptography

Sl. No.	Characteristics	3DES	AES	Proposed Here
1	Block Length	64	128	64
2	Key Length	168	128/192/256	128
3	Key Space Size	2^{168}	$2^{128}/2^{192}/2^{256}$	2^{128}
4	No. of Encryption Rounds	48	10	10
5	Cipher Type	Symmetric Block	Symmetric Block	Continuous Symmetric Block
6	Primitive Algorithm	Fiestel Network	Substitution Permutation Network	Encapsuled Confusion Secret Sharing
7	Flexibility	Low	High	High
8	Vulnerabilities	Prone to Brute Force Attacks	Prone to Side Channel Attacks	May resist against intruding better
9	Cryptographic Speed	Slow	Fast	Fast

In the following table 18, a comparative statement has been made against some of the related papers cited in above section 4. Thus, the efficiency of the proposed technique can be found at a glance when compared with the existing techniques.

Tab 18. Comparative Study with the related works at Section 4

Compari-son Criterion	COVID-19 Telecardiac	Session Key	Biometric Key	Fitness of Keys	Cryptograp-hic Time	Modular Time Complexity	Patients' Data Analysis	Standard Graphical Analysis	Brute-Force Attack	Comparative Statements
Neubeck L. et al. [19]	Yes	No	No	No	No	No	No	No	No	No
Bryant M.S. et al. [20]	Yes	No	No	No	No	No	No	No	No	No
Peters, R.J.G. [21]	Yes	No	No	No	No	No	No	No	No	No
Miller J.C. et al. [22]	Yes	No	No	No	No	No	No	No	No	No
Chen, CL. et al. [24]	No	Yes	No	No	No	No	No	No	No	No
Azarders	No	Yes	No	No	No	No	No	No	Yes	No

khsh R. et al. [26]										
Dwivedi, R et al. [27]	No	Yes	Yes	No	No	No	No	No	No	No
Beimel A. et al. [32]	No	No	No	No	No	No	No	No	No	No
Csirmaz L. et al. [35]	No	No	No	No	No	No	No	No	No	No
Proposed Here	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

12. Conclusion:

An intelligent cryptographic technique [53] on COVID-19 telemedicine has been proposed with higher efficiency. During the coronavirus pandemic, telemedicine has provided incredible services to the remote patients. In this paper, recurrence relation based session has been proposed for encryption. The robustness of the session keys has been checked under different sets of statistical tests. There will be partial encrypted shares produced for n number of physicians or cardiologists. Such partial shares are meaningless to the intruders as they cannot decode the actual information. The original cardiovascular report will be only generated if and only if threshold numbers of confusion matrices are connected together. Low computation overhead incurred at encryption and a decryption phase. In order to maintain the social distancing and lockdown constraints, telemedicine has brought vibes to the patients' treatment processes. In addition, such proposed system is capable enough to curtail the chain of coronavirus transmission. Patients' data are the most key points under severe security mechanism. The results obtained in this paper were acceptable in terms of fitness of session keys, standard graphical analysis, cryptographic time, data attacks, entropy, correlation, etc.

13. Future Scope of Work:

Artificial intelligence based automatic telemedicine unit may be further added into this proposed technique. Thus, the involvement of the human beings will be reduced with more time saving managements.

Acknowledgement

Authors do acknowledge the moral and congenial atmosphere support provided by Maharajadhiraj Uday Chand Women's College, B.C. Road, Burdwan, West Bengal, India.

Compliance with Ethical Standards: Not applicable.

Conflict of Interest: Joydeep Dey declares that he has no conflict of interest. Anirban Bhowmik declares that he has no conflict of interest. Arindam Sarkar declares that he has no conflict of interest. Sunil Karforma declares that he has no conflict of interest. Bappaditya Chowdhury declares that he has no conflict of interest.

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the

References:

1. Huang, L., Zhang, X., Zhang, X., Wei, Z., Zhang, L., Xu, J., et al. (2020). Rapid asymptomatic transmission of COVID-19 during the incubation period demonstrating strong infectivity in a cluster of youngsters aged 16-23 years outside Wuhan and characteristics of young patients with COVID-19: a prospective contact-tracing study. Journal of Infection, 80(6), e1–e13.
2. Rothe, C., Schunk, M., Sothmann, P., Bretzel, G., Froeschl, G., Wallrauch, C., et al. (2020). Transmission of 2019-nCoV infection from an asymptomatic contact in Germany. New England Journal of Medicine, 382(10), 970–971.
3. Jordan, R. E., Adab, P., & Cheng, K. K. (2020). Covid-19: risk factors for severe disease and death. BMJ,368, m1198.
4. Kadir, M. A. (2020). Role of telemedicine in healthcare during COVID-19 pandemic in developing

countries. Telehealth and Medicine Today.
5. dos Santos Puga, M. E., de Assis Reis, F. S., Milby, K. M., Pinto, A. C. P. N., Rocha-Filho, C. R., da Rocha, A. P., ... & Trevisani, G. F. M. (2020). Telehealth interventions in the context of the COVID-19 pandemic: Protocol for a scoping review.
6. Bokolo Anthony Jnr. Use of Telemedicine and Virtual Care for Remote Treatment in Response to COVID-19 Pandemic. J Med Syst 44, 132 (2020). https://doi.org/10.1007/s10916-020-01596-5.
7. Stallings William "cryptography and network security",Pearson India Education Service Pvt. Ltd., pp.111-155,2015.
8. Preeti Singh et al, "Symmetric Key Cryptography: Current Trends", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.12, pp. 410-415, 2014.
9. O. Billet, H. Gilbert, C. Ech-Chatbi, Cryptanalysis of a white box AES implementation, in H. Handschuh and A. Hasan, editors, SAC 2004. LNCS, vol. 3357 (Springer, Heidelberg, Germany, Waterloo, Ontario, Canada, Aug. 9–10, 2004), pp 227–240.
10. Kannan Y.R.A., Prasad S.A., Varalakshmi P. (2012) Cognitive Symmetric Key Cryptographic Algorithm. In: Meghanathan N., Chaki N., Nagamalai D. (eds) Advances in Computer Science and Information Technology. Computer Science and Engineering. CCSIT 2012. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 85. Springer, Berlin, Heidelberg.
11. Elliott PM, Anastasakis A, Borger MA et al (2014) 2014 ESC Guidelines on diagnosis and management of hypertrophic cardiomyopathy: The Task Force for the Diagnosis and Management of Hypertrophic Cardiomyopathy of the European Society of Cardiology (ESC). Eur Heart J 35:2733–2779.
12. Maron MS, Rowin EJ, Lin D et al (2012) Prevalence and clinical profile of myocardial crypts in hypertrophic cardiomyopathy. Circ Cardiovasc Imaging 5:441–447.
13. Prabir Kr. Naskar, Hari Narayan Khan, Ayan Chaudhuri, Atal Chaudhuri "Ultra Secured and Authentic Key Distribution Protocol using a Novel Secret Sharing Technique", International Journal of Computer Applications (0975 – 8887) Volume 19– No.7, April 2011.
14. Dong Kyun Park, Eun-Young Jung, rae woong park, young ho lee, hee jung hwang, in ah son, and min-hee hu, telecare system for cardiac surgery patients: implementation and effectiveness, Healthc Inform Res. 2011 Jun; 17(2): 93–100.
15. Lee KH, Kim HJ. Fuzzy trust evaluation model for virtual telecare team. J Soc Korea Ind Syst Eng. 2009;32:112–119.
16. Chaudhry SI, Phillips CO, Stewart SS, Riegel B, Mattera JA, Jerant AF, Krumholz HM. Telemonitoring for patients with chronic heart failure: a systematic review. J Card Fail. 2007;13:56–62.
17. Koff P, Jones RH, Cashman JM, Voelkel NF, Vandivier R. Proactive integrated care improves quality of life in patients with COPD. European Respiratory Journal. 2009; 33 (5) : 1031-8 .
18. Ashwal, A.J., Mugula, S.R., Samanth, J. et al. Role of deformation imaging in left ventricular non-compaction and hypertrophic cardiomyopathy: an Indian perspective. Egypt Heart J 72, 6 (2020).
19. Neubeck, L., Hansen, T., Jaarsma, T., Klompstra, L., & Gallagher, R. (2020). Delivering healthcare remotely to cardiovascular patients during COVID-19: A rapid review of the evidence. European Journal of Cardiovascular Nursing, 1474515120924530.
20. Bryant, M.S., Fedson, S.E. & Sharafkhaneh, A. (2020). Using Telehealth Cardiopulmonary Rehabilitation during the COVID-19 Pandemic. Journal of Medical Systems, 44.
21. Peters, R.J.G. Cardiac rehabilitation and telemedicine (and COVID-19). Neth Heart J 28, 441–442 (2020). https://doi.org/10.1007/s12471-020-01473-3.
22. Miller, J.C., Skoll, D. & Saxon, L.A. Home Monitoring of Cardiac Devices in the Era of COVID-19. Curr Cardiol Rep 23, 1 (2021). https://doi.org/10.1007/s11886-020-01431-w.
23. Chowdhury, D., Hope, K.D., Arthur, L.C. et al. Telehealth for Pediatric Cardiology Practitioners in the Time of COVID-19. Pediatr Cardiol 41, 1081–1091 (2020). https://doi.org/10.1007/s00246-020-02411-1.
24. Chen, CL., Li, CT. Dynamic Session-Key Generation for Wireless Sensor Networks. J Wireless Com Network 2008, 691571 (2008). https://doi.org/10.1155/2008/691571.
25. Meena, U., Sharma, A. Secure Key Agreement with Rekeying Using FLSO Routing Protocol in Wireless Sensor Network. Wireless Pers Commun 101, 1177–1199 (2018). https://doi.org/10.1007/s11277-018-5755-9.
26. Azarderskhsh, R., Reyhani-Masoleh, A. Secure Clustering and Symmetric Key Establishment in Heterogeneous Wireless Sensor Networks. J Wireless Com Network 2011, 893592 (2011). https://doi.org/10.1155/2011/893592.
27. Dwivedi, R., Dey, S., Sharma, M.A. et al. A fingerprint based crypto-biometric system for secure communication. J Ambient Intell Human Comput 11, 1495–1509 (2020). https://doi.org/10.1007/s12652-019-01437-5.
28. Sarkar A., Dey J., Karforma S. (2020) Secured Session Key-Based E-Health: Biometric Blended with Salp Swarm Protocol in Telecare Portals. In: Mandal J., Mukhopadhyay S. (eds) Proceedings of the Global AI Congress 2019. Advances in Intelligent Systems and Computing, vol 1112. Springer, Singapore. https://doi.org/10.1007/978-981-15-2188-1_56.
29. Sarkar A., Dey J., Bhowmik A., Ferdows S.S., A Dynamic Key Generation Scheme based on Metaheuristic Cuckoo Search, International Journal of Computer Sciences and Engineering, Vol.07, Issue.01, pp.184-187, 2019.
30. Shamir: "How to share a secret?",Comm ACM 22(11): 612-613, 1979.
31. G.R. Blakley, "Safeguarding cryptographic key", In Proceedings of AFIPS International Worhshop on Managing Requirements Knowledge, pp. 313, 1979.
32. Beimel A., Ben-Efraim A., Padró C., Tyomkin I. (2014) Multi-linear Secret-Sharing Schemes. In: Lindell Y. (eds) Theory of Cryptography. TCC 2014. Lecture Notes in Computer Science, vol 8349. Springer, Berlin, Heidelberg.

https://doi.org/10.1007/978-3-642-54242-8_17.
33. Sarkar A., Dey J., Chatterjee M., Bhowmik A., Karforma S. (2019). Neural Soft Computing based Secured Transmission of Intraoral Gingivitis Image in E-Health, Indonesian Journal of Electrical Engineering and Computer Science Vol -14(1), April,2019, pp 178-184.
34. Bhowmik A., Sarkar A., Karforma S., Dey J., A Symmetric Key based Secret Data Sharing Scheme, International Journal of Computer Sciences and Engineering, Vol.07, Issue.01, pp.188-192, 2019.
35. Csirmaz, L., Tardos, G. On-line secret sharing. Des. Codes Cryptogr. 63, 127–147 (2012). https://doi.org/10.1007/s10623-011-9540-y.
36. Sarkar A., Dey J., Bhowmik A., Mandal J.K., Karforma S. (2018), Energy Efficient Secured Sharing of Intraoral Gingival Information in Digital Way (EESS-IGI), In: Mandal J., Sinha D. (eds) Social Transformation – Digital Way. Communications in Computer and Information Science, vol 836. Springer, Singapore, ISSN: 1865-0929.
37. Bhowmik A., Karforma S., Dey J., Sarkar A.(2020), A Way of Safeguard using Concept of Recurrence Relation and Fuzzy logic against Security Breach in Wireless Communication, International Journal of Computer Science Engineering, Vol. 9 No. 4 Jul-Aug 2020, pp: 297-311.
38. Bhowmik A., Dey J., Sarkar A., Karforma S. (2019), Computational Intelligence based Lossless Regeneration (CILR) of Blocked Gingivitis Intraoral Image Transportation, IAES International Journal of Artificial Intelligence (IJ-AI), Vol 8(3), September,2019, pp:197-204.
39. Bhowmik A., Sarkar A., Karforma S., Dey J., A Symmetric Key based Secret Data Sharing Scheme, International Journal of Computer Sciences and Engineering, Vol.07, Issue.01, pp.188-192, 2019.
40. Dey J., Bhowmik A., Sarkar A., Karforma S. (2019), Privileged Authenticity in Reconstruction of Digital Encrypted Shares, IAES International Journal of Artificial Intelligence (IJ-AI), Vol 8(2), June,2019, pp:175-180.
41. S. A. Chaudhry et al. An improved and provably secure privacy preserving authentication protocol for SIP. Peer-to-Peer Networking and Applications. 2017; 10(1): 1-15.
42. J.G. Chakravorty, P.R. Ghosh, Advanced Higher Algebra, U.N. Dhur and Sons Private Ltd., 2018. ISBN 978-3- 80673-67-7. 22.
43. Hong Yaling. Research on computer network security analysis model [J]. Computer CD Software and Applica tions, 2013(z):1-152.
44. Physionet.org (2016). PhysioBank ATM. Available on: https://physionet.org/cgi-bin/atm/ATM. Accessed on December' 2020.
45. Sarkar A., Dey J., Bhowmik A., Mandal J.K., Karforma S., Computational Intelligence Based Neural Session Key Generation on E-Health System for Ischemic Heart Disease Information Sharing, In: Mandal J., Sinha D., Bandopadhyay J. (eds) Contemporary Advances in Innovative and Applicable Information Technology. Advances in Intelligent Systems and Computing, vol 812. Springer, Singapore.
46. DeyJ., Karforma S., Sarkar A., Bhowmik A., "Metaheuristic Guided Secured Transmission of E-Prescription of Dental Disease", International Journal of Computer Sciences and Engineering, Vol.07, Issue.01, pp.179-183, 2019.
47. Dey, J., Sarkar, A. & Karforma, S. Newer post-COVID perspective: Teledental encryption by de-multiplexed perceptrons. Int. j. inf. tecnol. (2021). https://doi.org/10.1007/s41870-020-00562-1.
48. Rodgers JL, Nicewander WA. Thirteen ways to look at the correlation coefficient. Am Stat. 1988;42:59–66.
49. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., and Vo, S.: A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST special publication 800–22, 2001.
50. Z. Wu and N. E. Huang, "A study of the characteristics of white noise using the empirical mode decomposition method," Proceedings of the Royal Society of London, Series A: Mathematical, Physical and Engineering Sciences, 2004, vol. 460(2046), pp. 1597-1611.
51. Sarkar, A., Dey, J. & Karforma, S. Musically Modified Substitution-Box for Clinical Signals Ciphering in Wireless Telecare Medical Communicating Systems. Wireless Pers Commun (2021). https://doi.org/10.1007/s11277-020-07894-y.
52. Patel, K. Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files. Int. j. inf. tecnol. 11, 813–819 (2019).
53. Bhowmik A., Karforma S., Dey J., Sarkar A. (2020), Fuzzy-Based Session Key as Restorative Power of Symmetric Key Encryption for Secured Wireless Communication. In: Kundu S., Acharya U., De C., Mukherjee S. (eds) Proceedings of the 2nd International Conference on Communication, Devices and Computing. Lecture Notes in Electrical Engineering, vol 602. Springer, Singapore.

Figures

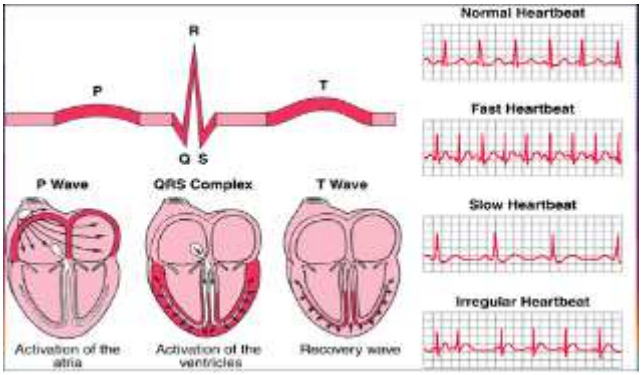


Figure 1

Graph for Normal, Fast, Slow & Irregular Heartbeats

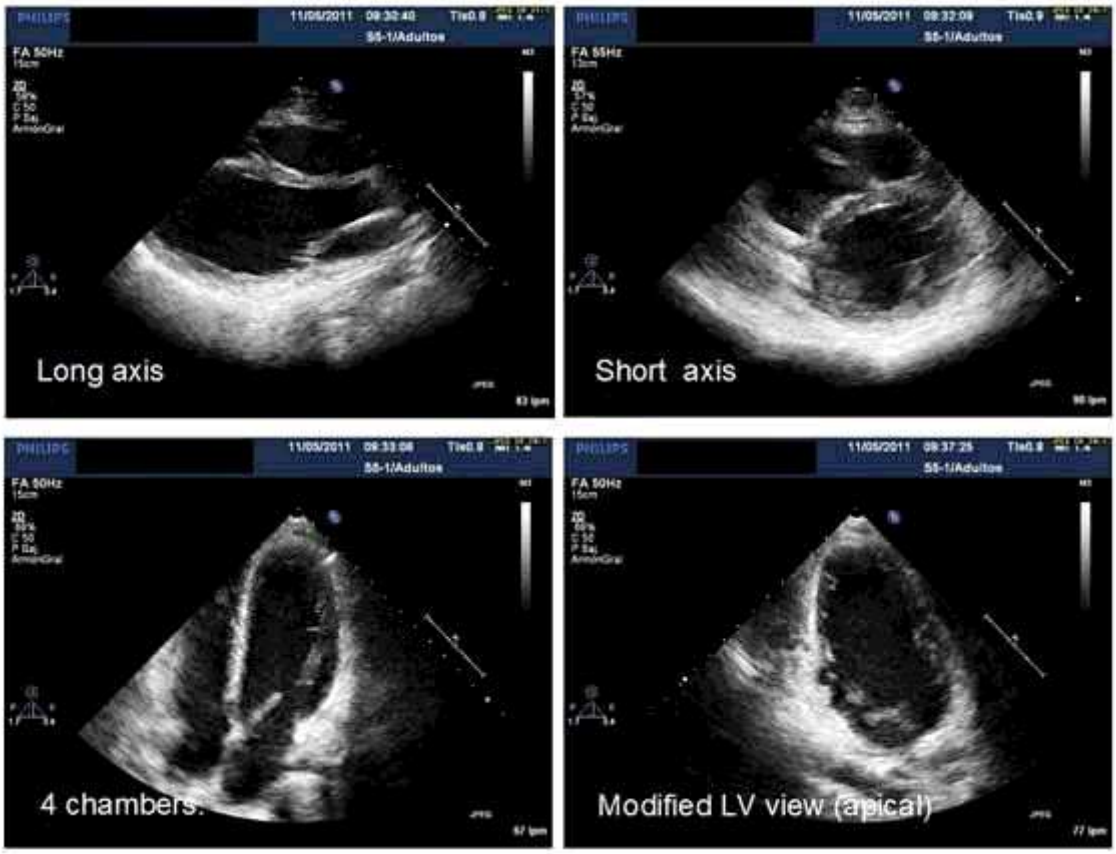


Figure 2

MRI of Heart

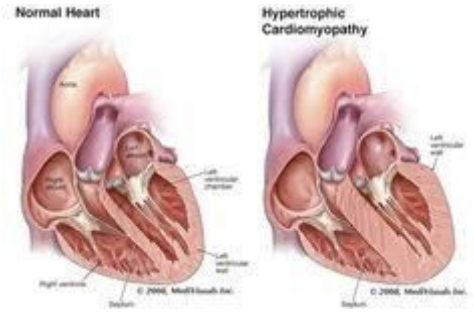


Figure 3

Normal Heart and Hypertrophic Cardiomyopathy

1010101011	1011110100	1100011110	0111001101	0101110011

Figure 4

Row-major of Mask Matrix

C0M0C0U0WC	C0MSC0C00	CO000MUCW0	0OMS00UC0C	0O0SCM00WC

Figure 5

Result of OR operation as row - major

Figure 6

Encapsulation of Secret Shares into Proposed Head-Tail Structure

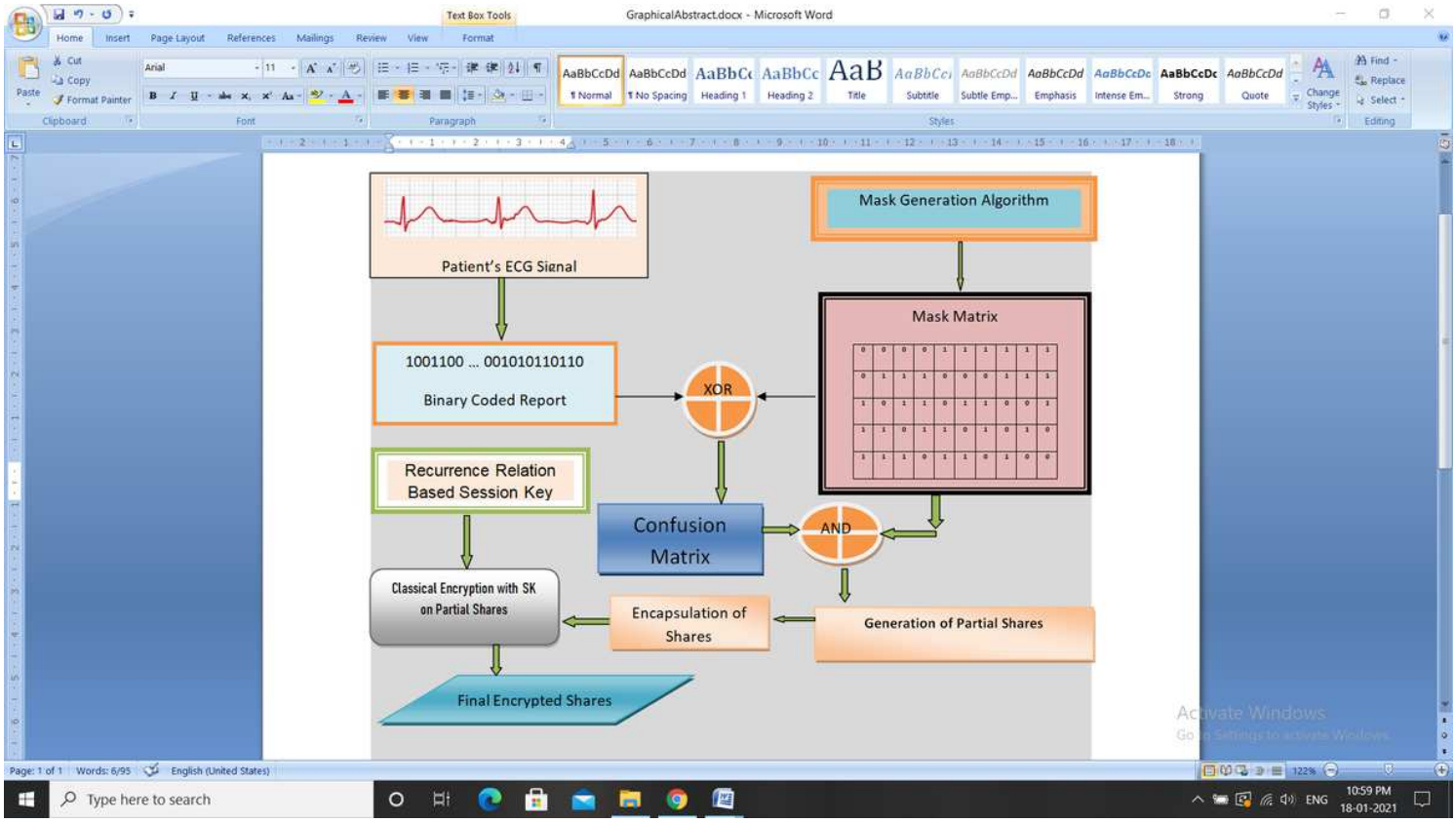


Figure 7

Block diagram of the proposed technique

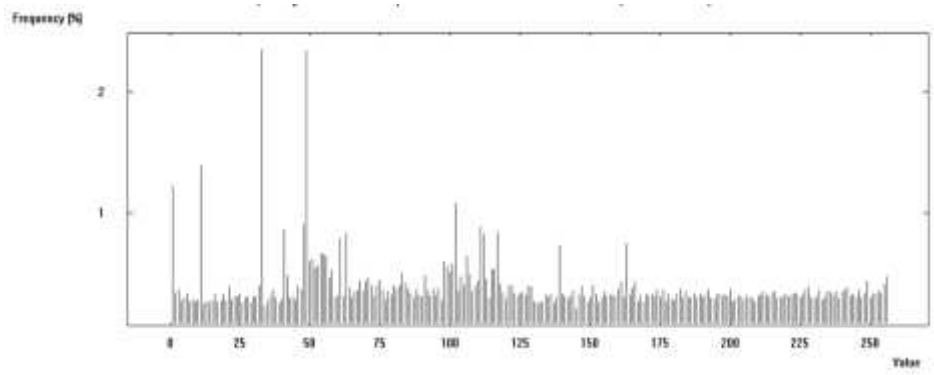


Figure 8

Histogram of ECG Report

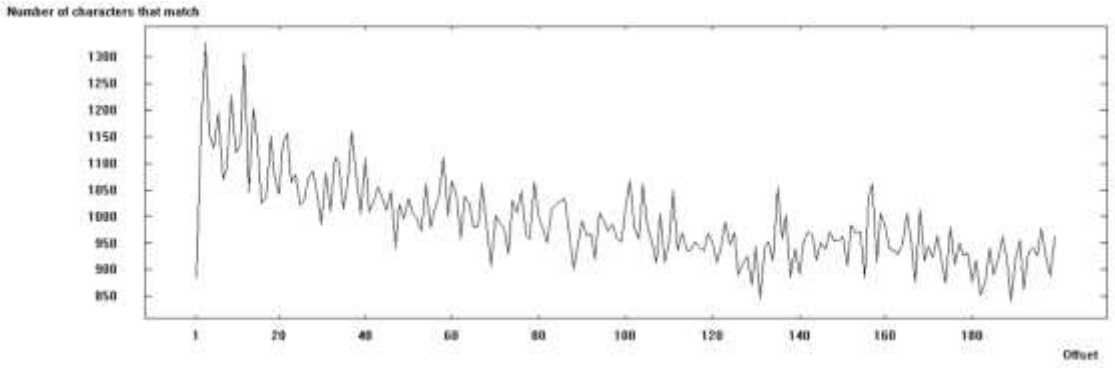


Figure 9

Autocorrelation of ECG Report

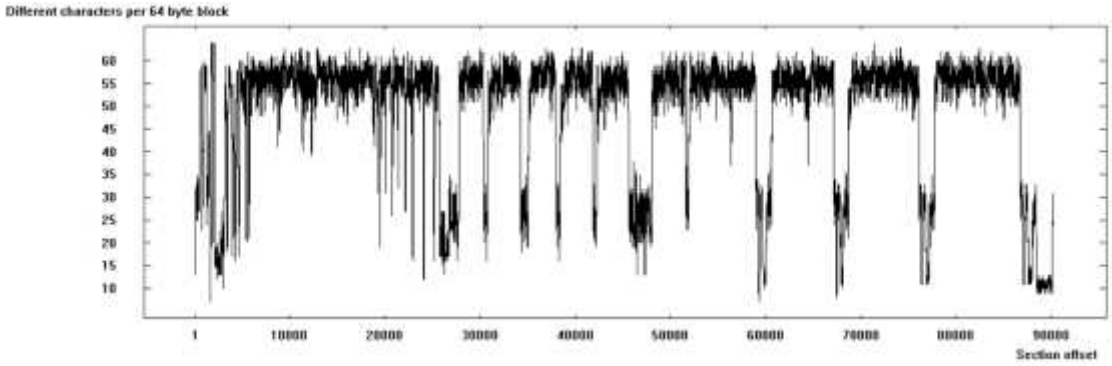


Figure 10

Floating Frequency of ECG Report

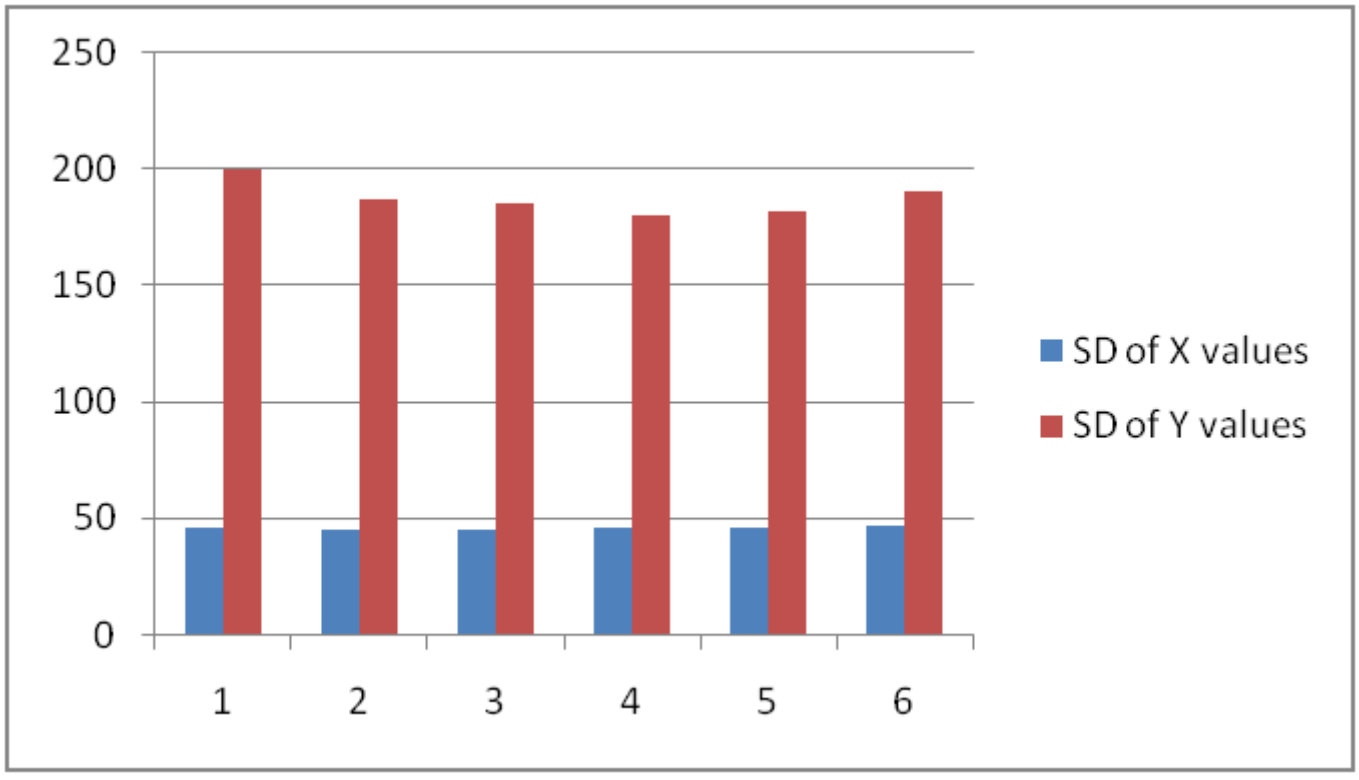


Figure 11

Graph on correlation analysis

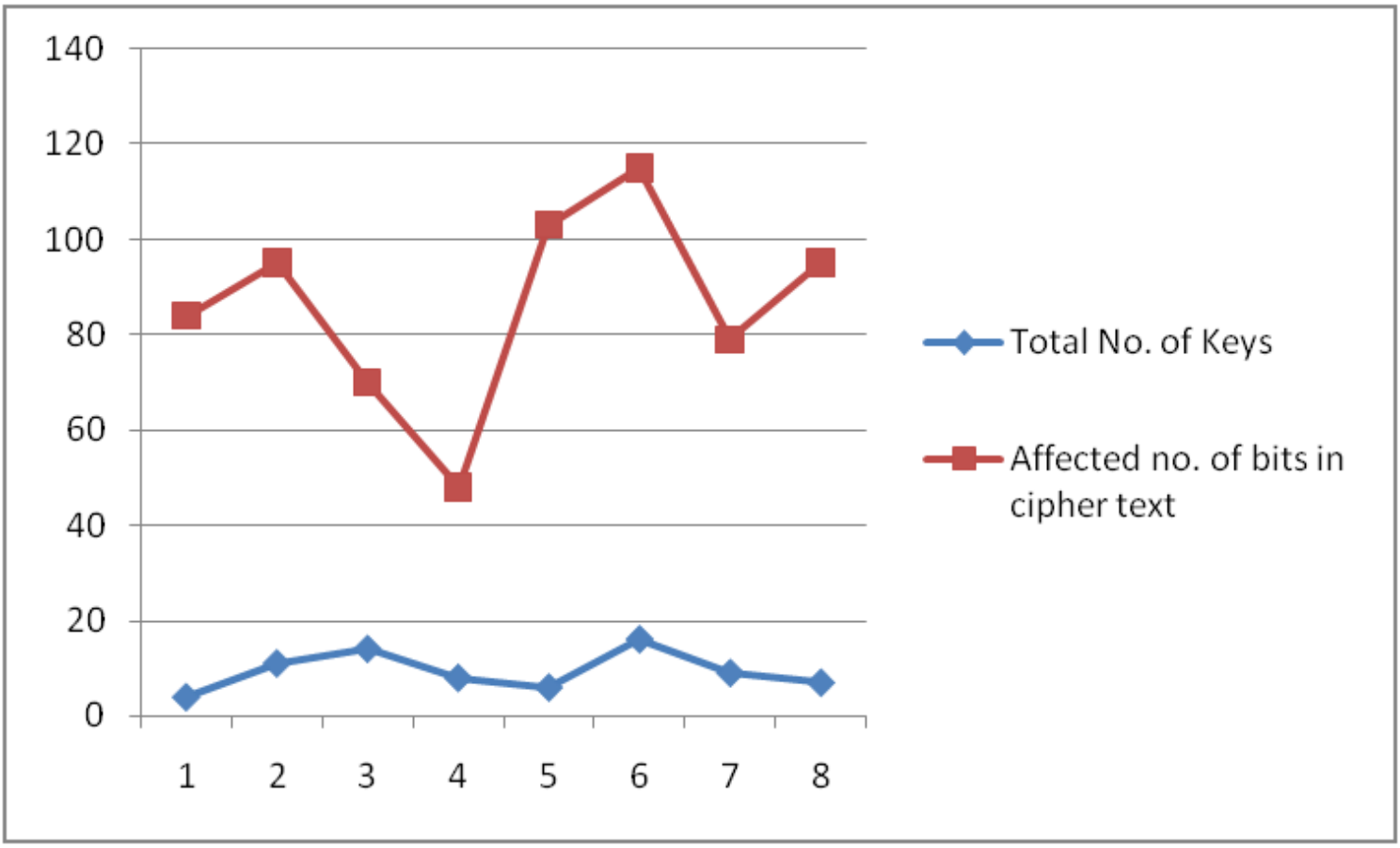


Figure 12

Graph for Flipping Effect on Keys

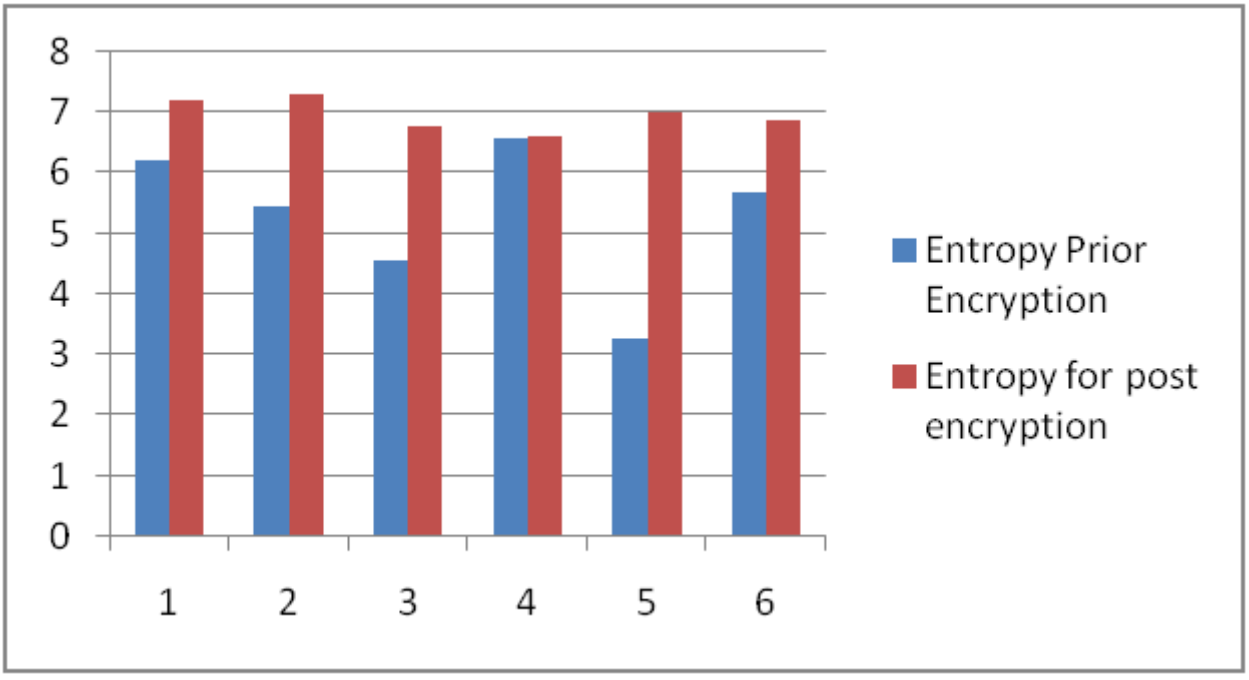


Figure 13

Graph of entropy value