Multimedia Tools and Applications (2022) 81:17747–17778
https://doi.org/10.1007/s11042-022-12440-y

Neural perceptron & strict lossless secret sharing oriented cryptographic science: fostering patients' security in the "new normal" COVID-19 E-Health

Joydeep Dey[1] · Anirban Bhowmik[1] · Sunil Karforma[2]

Received: 17 April 2021 / Revised: 3 August 2021 / Accepted: 25 January 2022 /
Published online: 7 March 2022

Abstract
Patients' data security is an open challenge on any telemedicine system. The challenge has been extended enough in this unprecedented corona virus led pandemic. COVID-19 has brought abrupt adaptations in medical sciences. To reduce corona virus transmission, quarantine yourself and opting for online services is mostly apt even during "New Normal" second wave of COVID-19. The emergence of telemedicine is a significant contribution in the medical sciences. Relevant online security and challenges are the contemporary and relevant challenges in COVID-19 E-Health. The objective of this proposed technique is to reinforce the technical safeguards to the electronic health system against the tricksters. Perceptron based session key and modified logistic map based intermediate key were proposed. A strict lossless secret sharing has been proposed to protect patients' clinical reports and data. Participation of all the recipients is bare essential in regenerating the original report. Simple mathematical operations were carried out to develop the secret shares. Electing the head of the recipients has also been included here. Different secret shares were encapsulated with the proposed frame structure. The chaotic sequences in the ranges of $r = [0.41,0.53]$, $r = [0.61, 0.66]$, and $r = [0.91, 0.99]$ on the initial values $x = 3.64, 3.81$, and 3.88 respectively were noted under this technique test. An appropriate correlation between the proposed encryption and cryptographic time, and proposed decryption and cryptographic time were found. Such values were r_{ec}= 0.989929 and r_{dc}= 0.988828 respectively. Myriad mathematical tests likes of statistical randomization, brute force, graphical analysis, performance time, etc. were carried on the proposed technique. Their results have proved our efficacy in fostering the patients' data transmission in "New Normal" COVID-19 E-Health.

Keywords COVID-19 · Session key · Intermediate key · Logistic map · Lossless secret sharing

✉ Joydeep Dey
joydeepmcabu@gmail.com

[1] Department of Computer Science, M.U.C. Women's College, Burdwan, India

[2] Department of Computer Science, The University of Burdwan, Burdwan, India

1 Introduction

Medical care might be characterized as the demonstration of taking protection or important techniques to improve an individual's prosperity. This might be finished with a medical procedure, medication, or different adjustments in an individual's way of life. These administrations are ordinarily given by doctors through a medical care framework. At the point of COVID-19, when these are administered through Internet empowered hubs in the form of E-Health [1, 51]. Subsequently, patients experiencing non-obtrusive and non-emergency infections might be dealt with distantly. The requirements of social separation, lockdown limitations, night check-in-time, should be kept up by the mass individuals to endeavor against this destructive Corona virus disease. Co-morbid patients are at higher dangers of COVID-19 due to their severe degree of illness. However, through COVID-19 E-Health, such patients can be prudently treated from their protected far off areas at any ounces of time. Additionally, nascomial diseases can be made to invalid and void to such co-morbid remote patients [31, 43]. Because of this novel corona virus, hospitals have migrated towards a "New Normal" of life. Once again the second wave of COVID-19 is hitting different places of the world. In many countries, re-lockdown has been imposed to reduce its transmission effect. Clinics and hospitals have moved from actual meeting modes to virtual conference modes. Patients are urged more to practice the office of virtual counsels with their suitable doctors. Physicians, medical attendants, patients, medical care staffs, and so forth are then less presented to COVID-19 under the umbrella of E-Health. During this pandemic, the latest things in medical services industry are the digitization of medical services frameworks. Their work process has been relocated towards electronic patient records. An electronic record of a patient includes patient's clinical history like socio-economic health cards, patients' progress notes, issues and complications, digital prescriptions, past clinical and hospital history, vaccines (perhaps COVISHIELD, Covaxin [53], and so on), research oriented information and radiology reports and so forth. The volume of such clinical information has increased in enormous rate regarding intricacy, variety and flow directions basically during this hyper computerized E-Health of corona virus. Henceforth, information security support is the greatest hindrance observed. A COVID-19 E-Health is treated as great as it protects the patients' medical information during the public transmission. This paper has proposed a cryptographic system to risen the degrees of information security through neural key generation and secret sharing idea.

Amid COVID-19, E-Health has become a boon in the medical sciences. Apart from invasive and surgery, other formats of treatments are possible through such COVID-19 telemedicine [38, 48]. E-Health best serves the chronic disease management from quarantines likes of bronchial infection, diabetes, hypertension, arthritis, etc. Patients can be treated without getting further exposed to COVID-19. It can provide psychological boosts to the patients and their family in a safe manner without corona virus transmission. It releases the offline patients' pressure on the district hospitals to a large extent. Thus, larger percentage of patients are being locally treated without the chances of nascomial infections and save of time and costs. But the psychological impact of actual visiting the doctors is not possible through telemedicine. Corona virus infection control is highly achievable through telemedicine which is mandate now. However, data theft on digital transactions is an issue of critical challenge.

2 Background scenario

In the context of global pandemic, psychological downfall is the common complication apart from the physiological complications. There had been huge economic loss incurred in almost everyone's life. Patients are more psychologically sick in such critical era. Even patients can boost other patients through the digital health system. The different types of E-Health systems were improved by using developed mobile computing and Internet of Things (IoT) [18, 28]. The key feature of such system is that the patients can get their treatment from the health care providers directly from their homes. Patients can communicate with each other that have the same symptoms. They also may form a group for exchanging their illness-related information, treatment experience, diets, medicines and specialist doctor recommendation. Besides, patients may communicate to encourage each other to overcome the disease, regardless of the patients' locations and conditions. Sometimes, self-confidence and friendly environment are more effective than drugs in patients' conditions. Such can boost the confidence levels of the patients.

2.1 Role of IoT in electronic medical sciences

Internet of Things (IoT) can be defined as a set of networking technologies that consist of different appliances, devices and electronic gadgets to interact and communicate among themselves. At present different healthcare systems widely use the IoT devices for smooth functioning, monitoring and assessment of patient's conditions and records. PMD (Personal Medical Devices) are small electronic devices used for monitoring the medical condition of a patient. These Personal Medical Devices (PMDs) are of two types according to its location internal (i.e. inside the patient's body) or external (i.e. attached to the patients' body externally). PMDs use a wireless interface to perform communication with a base station that is further used to read status of the device, medical reports, and change parameters of the device, or update status on the device. Unfortunately, the most of these devices and applications are not secure for data or information communication. IoT may be prone to different types of unwanted attacks. The IoT devices are targeted by attackers and intruders. Different types of risks are incurred for such compromised patients. Every health care system should ensure the security of network in order to prevent the privacy of patient from unwanted malicious attacks. To strengthen the sensitive information and other types of security, a proactive, preventive approach and measures must be taken by every healthcare organization with attention to future security and privacy needs.

2.2 Relevance of security and privacy protection in E-health

Security is a most important issue in any healthcare system. The attackers aim is to steal the information, attack on devices to utilize patient's resources, or may shut down some applications that are monitoring the patient's condition. There are many types of attacks on medical devices that include eavesdropping and intruding, in which privacy of the patient is leaked and the integrity error in which the message is being altered. The IoT based health care system provides huge benefits in society but it is also prone to different types of unwanted attacks. These types of attacks mainly cause information leakage and loss of services in communication channel. The IoT consists of different types of devices and platforms with different credentials and each device and platforms need security according to their characteristics. In

IoT platform, lot of personal medical information is shared among various types of devices so the privacy of user is a vital part in health care system. Hence a secure cryptosystem is needed for the data or information protection.

The different types of IoT attacks are physical attack, network attack, software attack, and encryption attack. In our paper we have emphasized only on encryption attacks such as side channel attacks, cryptanalysis attacks, and man in the middle attacks. The different algorithms in our cryptosystem which are described above provide strong protection mechanism of different encryption attack [37]. The result section of our study proves the robustness of the proposed cryptosystem by using different data, graphs, comparisons etc.

This proposed algorithm works on application model. Here, different types of complex and strong mathematical functions were used and as a result the algorithms when running provides minimum side channel information so that attacker cannot guess the session key. Our scheme also provides confidentiality and integrity by checking authentication at the patient and doctor end.

2.3 Cryptographic science

Cryptographic science is a branch of science that deals with message protection, so that it becomes unreadable by the others, and can be shared in public communication. Different types of encryption and decryption algorithm are invented at regular basis with updated features. Here the plain text is converted into cipher text using an encryption algorithm so that intruders cannot read it, but authorized user i.e. correct recipient can only access it. The decryption algorithm works in the reverse order and converts the cipher text into plain text. Two broad categories of cryptography are: symmetric key cryptography and asymmetric key cryptography with respect to key [49]. To ensure data security any one of these two category algorithm will be used. This paper focuses on symmetric key cryptography. Some of existing symmetric key cryptography methods are IDEA, AES, DES, Triple DES, Blowfish, RC5, RC6, etc. [2, 50]. Symmetry key is the value that is used to combine with original data to generate cipher text. It is independent of the original data.

2.3.1 Online session key

Session key is a unique code that is used at the encryption and decryption process in a data communication session [36]. The compliance of such key usage is immense on any online cryptographic system. Once the data decoding are constrained by session key, then different cryptanalytic intruders' task becomes more complicated [24, 35]. Secure online transaction systems use One Time Password (OTP) based session key to foster their security features and services. Thus, such systems are better to resist against vulnerable data threats. In COVID-19 E-Health, the session key is very much needful to have online medical transaction by the patients and the doctors.

2.3.2 Secret sharing

Secret sharing is another type of cryptography. Here the entire message is dismantled into multiple pieces termed as shares. No share contains the complete information of the actual file. These shares would be transmitted to different number of receivers. In Shamir's Secret Sharing Scheme is based on (n, k) threshold. Here, n is the number of receivers and k is the number of threshold value [47]. In their scheme, a $(k - 1)$ degree polynomial is needed. The polynomial of order $(k - 1)$ is given in the following Eq. 1.

$$f(x) = (p_0 + p_1x_1 + p_2x_2 + p_3x_3 + \ldots + p_{k-1}x_{k-1})\%Num \tag{1}$$

Here, p_0 the secret message to be encrypted and Num is a prime number and all other coefficients were selected randomly from secret message.

2.4 Chaotic system

Chaotic methods have recently used more in the process of encryption. Chaos based frameworks [26, 39] are fundamentally nonlinear in nature and showing an obviously arbitrary conduct for specific scopes of estimations of system boundaries. There are certain numbers of proper reasons to deploy chaotic sequence in the cryptographic engineering. Such may be listed as: controlling parameter, initial condition sensitivity test, non-convergence property, etc. [16, 30, 55]. In any case, the arrangements or directions of the framework stay limited inside the stage space. This insecure state is unequivocally relying upon the estimations of the boundaries and in transit the framework starts.

2.4.1 Logistic map

The logistic map guide [2] is a notable one dimensional chaotic map proposed by R.M. May, addressing a romanticized natural model for portraying yearly variety in the number of inhabitants in a creepy crawly species. The numerical recipe is characterized as given in the following Eq. 2.

$$K(\mathrm{m}+1) = \propto*\{\mathrm{Km}*(1-\mathrm{Km})\}\ldots \tag{2}$$

Here, ∝∈[0,4] is the control boundary and y_0∈[0,1] is the underlying condition [56]. The strategic guide shows acceptable conduct and is often utilized in numerous applications for its tumultuous nature in explicit reach. The hopf bifurcation graph shows the dynamical properties of the strategic guide. The strategic guide shows chaotic nature for ∝∈[3.57, 4.0] and slight varieties of the underlying worth produce significant contrasts in the created arbitrary qualities. This grouping of qualities is non-intermittent in nature. This logistic map is based on chaos theory. Any chaotic function provides random numbers in a specific range. This random numbers can be used in any purposes such as key generation, weight vector generation in ANN etc. In this article we have used this map in key generation process.

2.5 Pell's equation

Pell's equation is a Diophantine equation of the form $a^2 - Kb^2 = \pm 1$, a,$b \in Z$, where K is a given natural non- square number [24]. It can be found in the following lemma number 1.

Lemma Number 1: For every non-square positive integer K, there are infinite positive integers *a and b*: such that $\left|a-\sqrt{K}\,b\right| < \frac{1}{b}$.

2.5.1 Lagrange's theorem

For every positive non-square integer K, the equation of the type $a^2 - Kb^2 = 1$ has a non-trivial solution. Here we have considered the integer solutions of Pell's equation. The two integers for a particular K provide a set of numbers for two or more number of K ' s, which is used for encryption generation in this proposed technique.

2.6 Neural perceptron

A neural perceptron can be viewed as a combination of logical statements to generate an output. Generally, it contains input layer, hidden layer, and output layer. The aim of such neural network is to classify the features from the input signals [3, 15]. A simple perceptron has been shown in the following Fig. 1.

3 Literature survey

This segment reviews the prior works on COVID-19 E-Health on the field of cryptographic science. Keesara S. et al. [34] had proposed to bring telehealth revolution because of COVID-19 in consistence with the patients' law and security rules. Bindra V. et al. [9] had recommended that pregnant ladies and females can be treated distantly through the telemedicine in COVID-19 period with restricted exposures. Such ladies are more prone to the COVID-19. Whaibeh E. et al. [54] had tended to the telemental wellbeing as a drawn out productive impact in post COVID-19 period as well. During this COVID crisis, mental entanglements have risen dramatically. Patients can be guided through online E-Health frameworks. Telemental wellbeing can be viewed as protected, advantageous, versatile, proficient, and supportable approach to treat such sick patients from their isolates. Zhou X. et al. [57] had expressed the

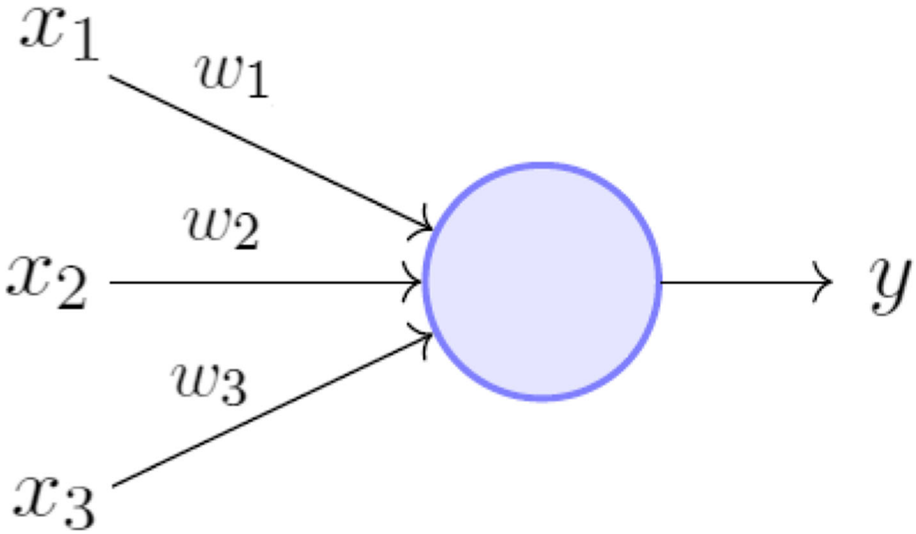


Fig. 1 Neural perceptron with 3 inputs

treatment plans for COVID-19 patients ought to be both regarding physiological and mental help for them. Both are similarly significant. Mental treatment may diminish their psychological weights. Be that as it may, in this basic circumstance, patients ought to be treated by the E-Health. It might incorporate email, virtual visit, video calls, calls, and so on. Jnr B.A. [11] had clarified the extreme changes that were made by the wellbeing frameworks to give medicines to the patients in the midst of COVID-19. Medical clinics have reacted well to embrace advanced wellbeing to serve the mankind. Virtual interviews, telemedicine, video call, and so forth are the inescapable parts of the E-Health systems. They have guided the average citizens how to utilize advanced wellbeing in this worldwide Corona virus emergency. Tanaka M.J. et al. [52] had clarified the requirements of telemedicine in the muscular fields. Its rise has been hurried with the beginning of COVID-19. Virtual muscular assessments have become a fundamental part. They have given the rules how such patients distantly be inspected through virtual checking. It improves the treatment methodology and decreases the patients' openness to the novel corona virus.

Smith A.C. et al. [48] had recalled the significance of telemedicine in the corona virus pandemic by reducing the contact contaminations. They had highlighted the key features needed to make telemedicine into mainstreamed services. It includes strategies to handle acute emergency situations apart from daily services. Making it into proactive mode will generate higher profits to the hospitals in the longer run. Borchert A. et al. [14] had evaluated the risks involved in urology patient consultation. They had evaluated the benefit of triage based consultations to the urologists during a specific COVID-19 time. Christianson J. et al. [17] have studied different obile telemedicine applications and observed that it is safe, reliable, efficient and scalable mode of treating the patients distantly. Such systems help the doctors and patients to reduce the transmission of novel corona virus. Bokolo Anthony Jnr. [11] had provided guidance on the use of telemedicine in this corona virus pandemic. With the emergence of COVID-19, hospitals have shifted more towards telemedicine with low cost treatments. Doctors are finding it as a suitable way to treat the patients in a safer way without any physical contacts. Gillman-Wells et al. [27] had explained the relevance of telemedicine in the context of COVID-19. Doctors have realized the only option to see the patients is through virtual consultations. They had discussed the advantages and next routes to the executed for the greater interests of the patients. Reyad O. et al. [42] had proposed a secured technique of transmission of COVID-19 CT chest images of patients inside real world of transmission. Safe pseudo-random generation codes were used by them in this regard. Statistically they had proved their efficacy of the proposed technique. Boneh D. et al. [12] had provided a comprehensive study on security issues in IoT networks in their work. Various security requirements such as authentication, integrity, confidentiality were discussed in this paper. This paper provides a comparison among different types of attacks, their behavior, and their threat level. These attacks are categorized into four level which are low-level, medium-level, high-level, and extremely high-level attacks and also suggested possible solutions to encounter these attacks. Joshi C. et al. [32] had surveyed various types of healthcare applications based on wireless medical sensor network (WMSN). IoT environment is suitable to implement these applications. Also, the different types of hybrid security techniques were discussed for handling the security issues of healthcare systems. Yen J. C. et al. [56] had proposed an idea on encryption method called BRIE based on chaotic logistic map. The bit recirculation of pixels is the basic principle of BRIE. It is controlled by a chaotic pseudo random binary sequence. The secret key of BRIE consists of two integers and an initial condition of the logistic map. Further, Yen J. C. et al. [56] had proposed an encryption method called CKBA

(Chaotic Key Based Algorithm) in which a binary sequence was generated using a chaotic system.]. Kinzel et al. [33] had proposed a protocol to exchange a cryptographic key between the sender and the receiver by learning rules, which was earlier proposed by Diffie and Hellman 1976. Each neural network was fed with same random vector, and they were trained to synchronize their weight vectors. Youssef Harmouch [29] proposed two chaotic pseudo-random number generators CPRNG for key stream. Two CPRNGs showed a good degree of randomization based on NIST statistical test suites, quasi-ideal entropy, good key stream distribution, and good sensitivity to initial conditions, indicating resistance to differential attacks.

3.1 Pros & cons of existing techniques and our proposed technique

In this sub-section, we have presented the advantages and disadvantages of the existing techniques. This has been mentioned in the following Table 1.

4 Critical issues

Amid COVID-19, patients' credentials are at higher risks. Due to the high spread of the novel corona disease, patients are not allowed to visit the hospitals physically. With lockdown constraints in different cities, co-morbid patients are also treated distantly. The following points will highlight the critical issues observed during COVID-19 E-Health [1].

1. COVID-19 E-Health is questionable whenever any data provided by the users is misinterpreted by the fraudsters [33].
2. Maintaining the privacy of the patients in the E-Health is the key for global acceptance by the medical professionals and patients. Such confidentiality guidelines must be accommodated.

Table 1 Advantages and disadvantages over existing techniques

Sl. No.	Paper Reference No.	Pros	Cons
1	27, 28, & 29	Good key exchange protocol.	Weak technique with respect to time complexity, and performance analysis.
2	30,31, & 32	Hard encryption protocol	The key generation protocol is weak
3	33,34,35, & 36	Strong authentication protocol	Secret sharing technique is complex. The technique is not suitable to defend chosen plain text attack, and occlusion attack.
4	37, & 38	Benefits of Telemedicine in COVID- era	The technique is not suitable to defend chosen plain text attack, brute force attack.
5	39	Good encryption scheme	Authentication part is not strong.
6	40, & 41	Review of security vulnerabilities	No new model, existing models were applied.
7	43, & 44	Good key exchange protocol on neural networks	Weak encryption protocol.
8	This Paper	Strong Cryptosystem with respect to key generation, encryption, and decryption.	In the next phase, we will incorporate a strong authentication protocol with this technique.

3. Training the technical support teams is another key aspect in fostering the COVID telemedicine.
4. For any successful COVID-19 E-Health, following parameters are bare essential. They are: Patients' security, Internet enabled machines, telemedicine Hub, software developments and maintenance [29].
5. E-Health services need extra digital transmission cost for medical transactions [25].

Telemedicine is the emergent technique to covert traditional health is to online health care in this deadly OVID-19 phase. There are different types of more challenges that could exist in COVID-19 E-Health system. Different types of attacks or malicious activity may degrade activity of the medical devices and disrupt the communication system of telemedicine. There are two types of attacks namely Active Attack and Passive Attack. An active attack attempts to alter system resources or affect their operation. A passive attack does not affect system resources but attempts to theft vital information from the system. An attack can be occurred by an insider or from outside of the E-Health organization. Based on the target of the attack, there are mainly three types of attacks are noted in COVID-19 E-Health.

a) Attacks against any medical devices related to COVID-19 samples,
b) Attacks against the communication between devices and users of E-Health, and
c) Attacks against all the users simultaneously.

A common method of attack involves tampering or altering of the messages is the common method of attack. The medical data and information which are transmitted through online environment is very sensitive and vital for treatment. So any changes on these data or information causes risk for the patients.

5 Objectives and novel contributions

The main objective is to foster the patients' privacy especially during the corona virus pandemic. Such proposed E-Health system will avoiding unnecessary allied costs and time, and provide proper health support and facilities from isolated centers. From the above stated section of critical issues, it has been vividly significant that the security fostering to the COVID-19 E-Health system is an immediate mandate. The patients' confidential data are under threat of intruding in the overwhelmed online medical transactions. In this article a new cryptographic system has been proposed with the following things as novel contributions.

Artificial neural network has been used to generate the session key. Based on modified logistic map, an intermediate key has been proposed. Our proposed modified logistic map can be found in the following Eq. 3.

$$x_{n+1} = R{*}x_n\left(1.02{-}x_n^2\right)\left(1.02{-}x_n\right)\ldots \tag{3}$$

Here, R is the control parameter with R∈[0.01, 4.31] and x_0 is the initial condition with $x_0 \in [0.01,\ 1.302]$. Chaotic graphs has been discussed in the later section. Strict lossless secret sharing has been proposed on the patients' data. The property of no data loss satisfied the proposed secret sharing. Electing the head among the multiple receivers has been done here too. An encryption along with share encapsulation has been done on all the secret shares.

6 Proposed flow diagram

The following Fig. 2 illustrates the flow of the proposed cryptographic technique in COVID-19 telemedicine.

In brief, the above stated diagram may be discussed as follows. In the first step of neural perceptron, the key length will be inputted and corresponding session key will be formed. Next step is the intermediate key generation. Here, a random number will act as input, and an intermediate key will be generated through modified logistic map. In the next phase of lossless secret sharing, the number of recipients will be taken as input field, and corresponding equivalent number of secret shares will be created through our proposed technique. The election of the polling head module will elect a recipient as head. Here, the arrival times of each recipient will be considered as its input. The next step is the encryption and decryption. Here, the session key, intermediate key, and the plain message are considered as inputs. The output is the cipher text of the plain text. The final step of the proposed model is the share encapsulation. The inputs are session key, intermediate key, and plain text for this phase and the output are structured encapsulated shares through our technique.

7 Proposed work

To cope up the security issues on the contemporary COVID-19, cryptographic science is the best plan to have more reliable data security in the light of patients' private medical data. In this article, a scientific cryptographic approach has been proposed by a hybrid combination of neural networks and secret sharing. It may work against myriad security codes during "New

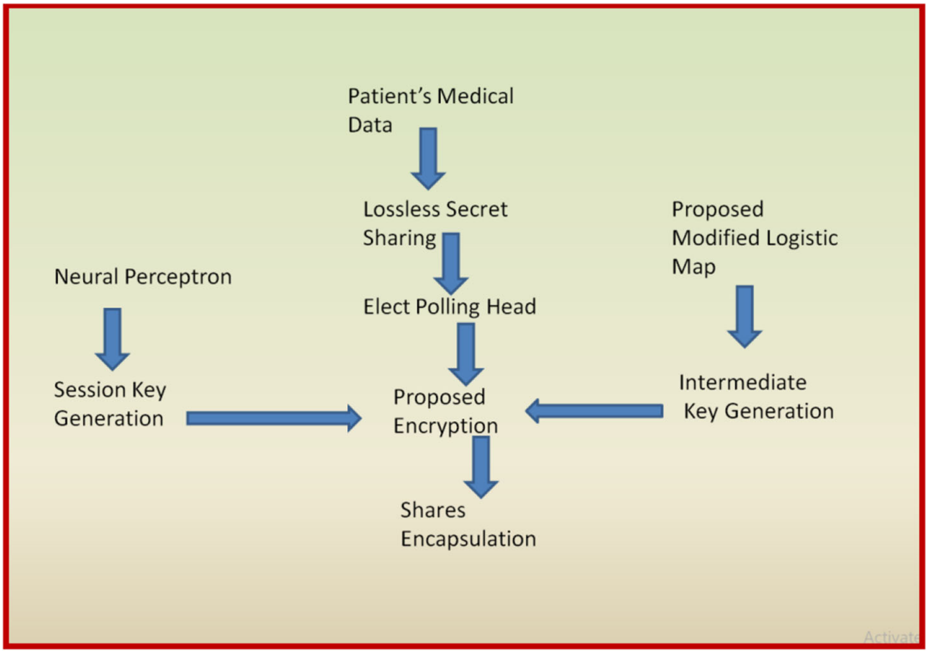


Fig. 2 Flow diagram of the proposed technique

Normal" online COVID-19 E-Health. This proposed technique has been dismantled into six sub-modules which are mentioned below.

1. *Neural Session Key Generation − PSKG*( ) // Perceptron Based
2. *Logistic Intermediate Key Generation – INTMKG* ( ) // Modified Logistic Map Based
3. *Strict Secret Share Generation – SECRETSHARES*( ) // Strictly Lossless Based
4. *Appointment of Head Recipients* - *Polling Head* ( ) // Electing Polling Head
5. *Patients*' *Info Encryption & Decryption – ENCRYPT & Decrypt*( ) // Encryption and Decryption Operations
6. *Share Encapsulation – ENCAPSULE*( ) // Encapsulation of Secret Shares

This protocol is described below by a compact algorithm with modular effects in the following algorithm 1. Two proposed set of keys were generated named as session key and intermediate key. First key has been derived by the neural perceptron and the later has been developed by modifying the chaotic map [4]. An impact of secret sharing has been proposed on the patients' data and that too having much less time complexity with respect to classical secret sharing schemes. Electing the head of the recipients has also been proposed here. Encapsulations of secret shares have been proposed on K number of recipients.

```
ALGORITHM NO. 1: Session key generation based on Neural Computing
Input(s): − Patient's Data (PT.PDF)
Output(s): − Encrypted & Encapsulated Shares (n)
Methods:
Step 1:   Call PSKG ( ) // Perceptron Session Key Generation
L = Input Key Length( )
LAST = Input Max Iteration ( )
For I = 0 to L
  /*Generation of Random Weight */
    Epocs ← 0
    While [Epocs != LAST]     /*Perceptron based first weight vector*/
          Set $X_i$← 1, $X_1$, $X_2$, … , $X_N$   /* Peceptron Input Vector */
      Weight[i] = Input Random(−1, +1 ) // Weight Initialization
          $HL1 \leftarrow Weight[Bias] + \sum_{i=1}^{N} Weight_i * X_i$   /* Hidden Output */
            If (HL <= Desired Value) Then /* Output Unit /
                  $Z_i \leftarrow 0$
            Else
                  $Z_i \leftarrow 1$
            End if
            If ($Z_i$ != Need )Then     /* Learning * /
                  $Weight_{Next} = Weight_{Prev} + \left\{\frac{1}{2} * X_i\right\}$
                  $Bias_{Next} = Bias_{Prev} + [\frac{1}{2} * Desired\ Value\ ]$
            Else
                  $Weight_{Next} = Weight_{Prev}$
                  $Bias_{Next} = Bias_{Prev}$
            End if
        Epocs ← Epocs + 1
      End while
```

Here weight vectors (*Weight$_{Next}$*) are required session key which is used in encryption decryption process.

```
Step 2:  Call INTMKG ( )          // Intermediate Key Generation on Modified Logistic Map
  δ ← Input Random ( ) MOD 3
  For  i = 0 to (Len(IK) − 1)
       $x_{n+1} = \delta * x_n(1.02 - x_n^2)(1.02 - x_n)$
  End for
```

The above algorithm provides the values for intermediate key generation. The logistic map is based on chaos theory. So using logistic map we have generated random numbers key formation. In above Step2 x_{n+1} provides the required intermediate key.

```
Step 3:  Call Secret Generation      // Proposed Strict Lossless Secret Sharing
K ← Input Users( )
For I = 0 to K − 1
   For J = 0 to J − 1
    If (I = J) then
      Mask[I][J] = 1
    Else
      Mask[I][J] = 0
    End if
  End for
End for
For t = 0 to 9
   a= Input Random( ) % (K-1)
   b= Input Random( ) % (K-1)
   Interchange( Mask[a][K], Mask[K][b])
End for
For i = 0 to K
  D1[ ] = Bitwise AND ( Mask[i][K] , PT.PDF)
  D2[K][ ] = D1
  D1 = NULL
End for

Step 4:  Call Polling Head ( )  // Electing Polling Head
   // Defined Below
Step 5:  Call Encryption ( )  // Encryption Operations
   // Defined Below
Step 6: Call Encapsulation ( )  // Encapsulation of Secret Shares
  // Defined Below
Step 7: End
```

```
$\boldsymbol{ALGORITHM\ \ NO.1.1}$: $\boldsymbol{Polling\ Head}$ ( )
$\boldsymbol{Input(s)}: -\ List\ of\ Recipients, Rec[K], List\ of\ Arrival\ time, Arr[K]$
$\boldsymbol{Output(s)}: -\ Head\ Recipient$
$\boldsymbol{Methods}$:
$Head\ =\ 0$
$For\ I\ =\ 1\ to\ K-1$
  $If\ (Arr[I]\ >\ Arr[Head])$
    $Head\ =\ I$
  $End\ if$
$End\ for$
$Return\ Head$
```

```
$\boldsymbol{ALGORITHM\ \ NO.1.2}$: $\boldsymbol{Encryption}$ & $Decryption(\ )$
$\boldsymbol{Input(s)}: -\ Session\ Key(SK), Intermediate\ Key(IK), plain\ text\ (PT.PDF)$
$\boldsymbol{Methods}$:
$For\ L\ =\ 0\ to\ Length(SK)$
    $x[L]\ \leftarrow\ ASCII\ (\ SK\ )$
$End\ for$
$For\ L\ =\ 0\ to\ Length(SK)$
    $y[L]\ \leftarrow\ ASCII\ (\ IK\ )$
$End\ for$
$f_{Encry}(x,y) = \frac{x^2}{y} + (y^3+1)$
$DIFF\ ASCII\ \leftarrow\ |\ ASCII\ difference\ of\ SK\ \&\ IK\ |$
$Temp\ File = \ BitwiseXOR\ (PT.PDF, SK)$
$Cipher\_file\ =\ BitwiseXOR(Temp\ File, IK)$
$Meu \leftarrow f_{Encry}(SK, IK)\%\ (DIFF\ ASCII)$
$Cipher\_final = \ Cipher\_file \ll Meu$
```

```
ALGORITHM NO. 1.3: Encapsulation( )
Input(s): − Values of r1 & r2 from Pell's Equation, Output of Algorithm 1.2 (CTEXT)
Output(s): − Encapsulated Shares (n)
Methods:
For I = 0 to K
  Result = $((r_1 + r_2)/4))$
  $\text{Pad}_{\text{I}}$[ ] ← DigestOf(IK)
  $\text{Header}_{\text{I}}$[ ] ← DigestOf (IK ≪ (Result BitwiseXOR SK ) )
  $\text{Tail}_{\text{I}}$[ ] ← GrayCode Encryption( r1)
  $\text{Tail}_{\text{II}}$[ ] ← GrayCode Encryption( r2)
  Tail[ ]← $\text{Tail}_{\text{I}}$[ ] ConcatFile $\text{Tail}_{\text{II}}$[ ]
    $Output_{file}$ ← ConcatFile(Header[ ], CTEXT, Tail[ ], Pad[ ])
End for
For I = 0 to K
  RSA( $\text{Tail}_{\text{I}}$[ ], Public Key(I))
  RSA( $\text{Tail}_{\text{II}}$[ ], Public Key(I))
End for
```

8 Result section

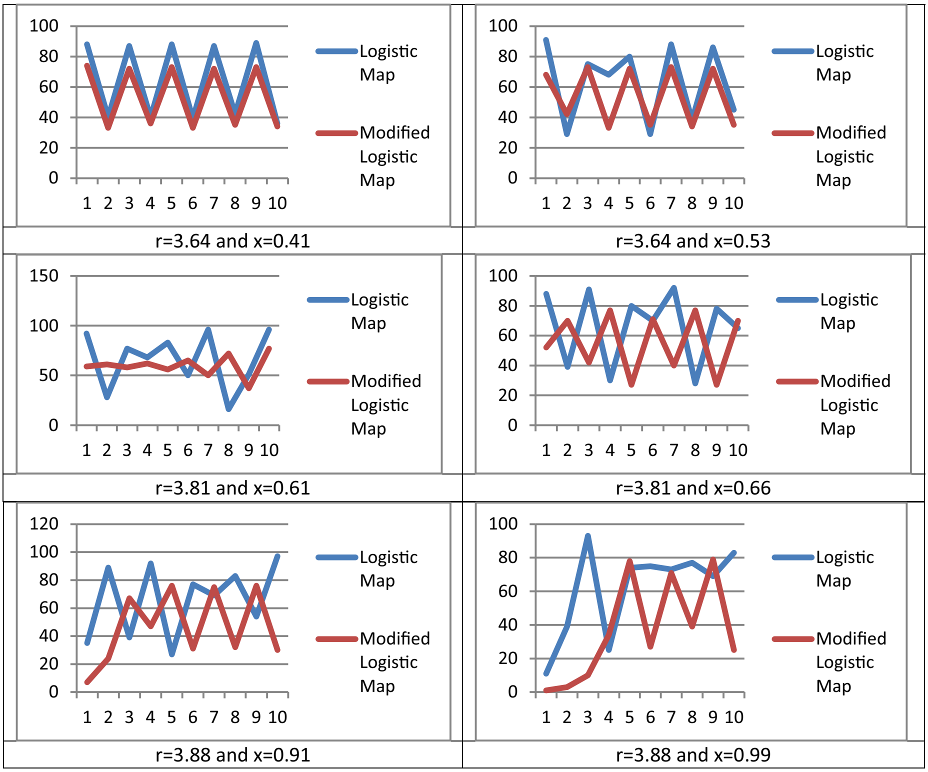
The above algorithms were implemented in latest version of Python in a PC of Intel Core i9 (tenth generation) processor, operating system of Microsoft Windows 10 × 64, 16GB RAM and 2 TB internal secondary storage. In the following sections, simulated results of the proposed cryptographic technique have been illustrated.

8.1 Efficacy of proposed modified logistic map

In the proposed cryptographic technique, we have successfully modified the logistic map to generate the intermediate key. Three chaotic observations were noted in the three set of data set. Firstly, $0.41 \leq x \leq 0.53$ with constant $r = 3.64$. Secondly, $0.61 \leq x \leq 0.66$ with constant $r = 3.81$. Thirdly, $0.91 \leq x \leq 0.99$ with constant $r = 3.88$. The following Fig. 3 indicates the efficacy of the proposed scheme by comparing between the logistic map and modified logistic map.

For a given initial condition, the future state can be predicted from a deterministic finite system. While in chaotic system, long term prediction of nature of trajectories cannot be judged with accuracy. For specific values of parameters, two trajectories, which are initially very close, diverge exponentially in a short time. Here initial information about the system is completely lost. Our proposed modified logistic map to generate the intermediate key can be seen in the above stated Eq. 3.

From the above Fig. 3 it is seen that our modified logistic map shows better chaotic nature than standard logistic map within the range. A small change in initial condition with fixed control parameter shows major difference in results as well as graphs. The following Table 2



r=3.64 and x=0.41

r=3.64 and x=0.53

r=3.81 and x=0.61

r=3.81 and x=0.66

r=3.88 and x=0.91

r=3.88 and x=0.99

Fig. 3 Efficacy in terms of proposed modification in logistic map

contains the sample set of intermediate keys (in hexadecimal) obtained through modified logistic map.

8.2 Neural session key generation

In this paper, we have simulated neural perceptron to generate the session key. Different architectural perceptron were designed for obtaining different session keys for multiple COVID-19 E-Health transactions [13]. It is also stated that the architecture of the perceptron

Table 2 List of generated intermediate keys

IK Key ID	Intermediate Key (IK)
IK$1	915cf
IK$2	d0076
IK$3	8796e
IK$4	3b511
IK$5	53a02
IK$6	b4681
IK$7	26f31
IK$8	0939d
IK$9	f8143
IK$10	ga8de

is made open to the public. The working principle of the perceptron can be found in the following Eq. 4.

$$hl = b + w_1 {*} x_1 + w_2 {*} x_2 + \ldots + w_n {*} x_n \ldots \tag{4}$$

$$\begin{gathered} If\ (hl \leq 0.5\ )\ then \\ y = 1 \\ Else \\ y = 0 \\ End\ if \end{gathered}$$

Since the input vectors are kept secret, so the exact pattern of the session key may not be decoded by the tricksters while using super computers. Different data set obtained can be found in the following Table 3 (in hexadecimal).

Table 3 List of generated session keys

SK key group	Perceptron architecture	SK ID	Session Key (SK)
SK#1	16–1-1	SK#1.1	64ae3
		SK#1.2	ed72b
		SK#1.3	75ab1
		SK#1.4	25,122
		SK#1.5	69,100
		SK#1.6	2fc9b
		SK#1.7	c97ef
		SK#1.8	452e2
		SK#1.9	eec4f
		SK#1.10	01369
SK#2	32–1-1	SK#2.1	da368
		SK#2.2	08e0a
		SK#2.3	06501
		SK#2.4	41c55
		SK#2.5	1743b
		SK#2.6	bf03c
		SK#2.7	0d521
		SK#2.8	b82d4
		SK#2.9	e9f94
		SK#2.10	212b4
SK#3	48–1-1	SK#3.1	a05df
		SK#3.2	a4940
		SK#3.3	3deff
		SK#3.4	1d1a8
		SK#3.5	601ba
		SK#3.6	f16ee
		SK#3.7	d52a3
		SK#3.8	68d72
		SK#3.9	40b94
		SK#3.10	733cf

8.3 Statistical robustness of proposed key sets

NIST Test Suite [5] is a measurements bundle involving fifteen statistical tests. Its goal is to decide the haphazardness of session key and intermediate key proposed in this paper. Robustness strength of these session key and intermediate key can be dictated by these fifteen tests. The keys which were mentioned in the Tables 2 and 3 were tested under NIST suite. The p values observed were categorically noted in the following tables. Only first ten tests noted in the Table 4 were considered under proposed technique.

In the following Table 5, the robustness of the intermediates keys were noted. All such keys as mentioned in the Table 2 have been fed into NIST suite. The noted p values and the output will be shown in the following Table 5.

The session keys that have been generated through the neural perceptron have been put into the statistical NIST package. The efficacy of those keys in the light of robustness can be summarized in the following Table 6.

The average p-values of the proposed intermediate keys, and three set of session key were plotted in the following Fig. 4. The Tables 4 and 5 contain the p values. Average was made and then plotted to have the desired efficacy of the proposed COVID-19 E-Health.

Table 4 Index of NIST Suite

NIST Name	*Assigned Id*
Frequency	NIST#01
Frequency (Block−wise)	NIST#02
Run	NIST#03
Longest Run of Ones in Block	NIST#04
Binary Matrix Run	NIST#05
Discrete Fourier Transformation	NIST#06
Non overlapping Template Matching	NIST#07
Overlapping Template Matching	NIST#08
Maurer' s Universal Statistical	NIST#09
Linear Complexity	NIST#10

Table 5 Statistical robustness on intermediate key

IK Key ID	Assigned Id	p value	Standard p value	Output (T: Passed, F:Failed)
IK$1	NIST#01	0.240	0.250	T
IK$2	NIST#02	0.148	0.150	T
IK$3	NIST#03	0.168	0.165	T
IK$4	NIST#04	0.252	0.251	T
IK$5	NIST#05	0.160	0.155	T
IK$6	NIST#06	0.281	0.280	T
IK$7	NIST#07	0.247	0.245	T
IK$8	NIST#08	0.185	0.185	T
IK$9	NIST#09	0.164	0.165	T
IK$10	NIST#10	0.223	0.220	T

Table 6 Statistical robustness on intermediate key

SK Key Group	Assigned Id	p-value	Standard p value	Output (T: Passed, F:Failed)
SK#1	NIST#01	0.174	0.150	T
	NIST#02	0.250	0.250	T
	NIST#03	0.148	0.150	T
	NIST#04	0.207	0.200	T
	NIST#05	0.153	0.155	T
	NIST#06	0.241	0.240	T
	NIST#07	0.164	0.145	T
	NIST#08	0.236	0.235	T
	NIST#09	0.254	0.255	T
	NIST#10	0.125	0.120	T
SK#2	NIST#01	0.151	0.150	T
	NIST#02	0.232	0.230	T
	NIST#03	0.175	0.175	T
	NIST#04	0.214	0.201	T
	NIST#05	0.156	0.151	T
	NIST#06	0.237	0.230	T
	NIST#07	0.178	0.175	T
	NIST#08	0.221	0.220	T
	NIST#09	0.224	0.220	T
	NIST#10	0.139	0.140	T
SK#3	NIST#01	0.162	0.160	T
	NIST#02	0.247	0.245	T
	NIST#03	0.151	0.151	T
	NIST#04	0.212	0.210	T
	NIST#05	0.165	0.165	T
	NIST#06	0.229	0.220	T
	NIST#07	0.177	0.175	T
	NIST#08	0.247	0.246	T
	NIST#09	0.244	0.245	T
	NIST#10	0.120	0.120	T

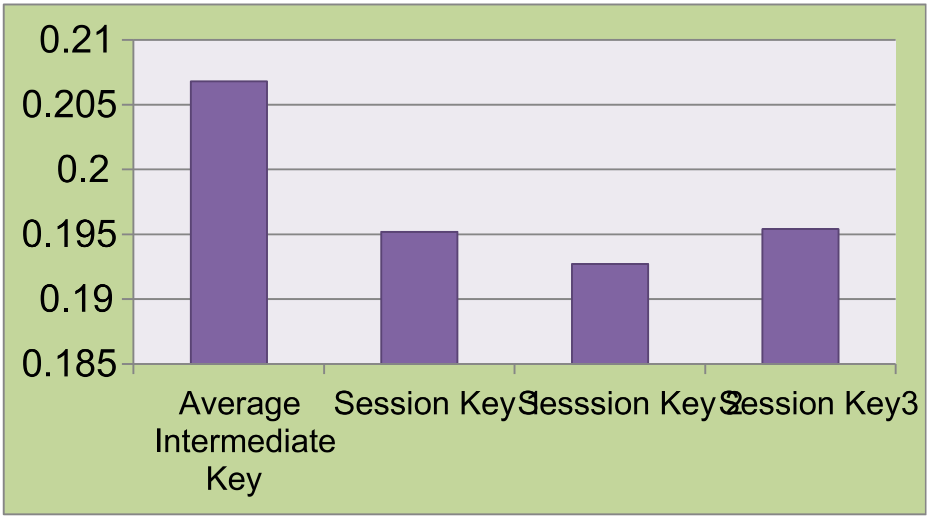


Fig. 4 Average –values on the proposed set of keys

8.4 Histogram analysis

In this sub section, histogram analysis has been carried out on the proposed COVID-19 cryptographic technique. Histogram indicates the frequency of different of characters present in the plain text. There has been a comparative graph between the pre-encryption and post-encryption of the plain text using our proposed technique. Furthermore, it was done on individual shares generated by the proposed technique. The post-encryption graphs resulted from individual shares were more variant than pre-encryption shares. Those could be found in the following Table 7. Tricksters will not be able to trace any linkage from the encrypted secret shares when compromised in the middle [22, 44]. In fact, the chances of malicious attacks on the patients' data are higher. In the following Table 7, histogram comparison has been made. The histograms were generated on the pre-encryption and post-encryption on the same shares.

From the above histograms, there could be significant changes on the shares during the ore-encryption and post-encryption phase. It strongly boosts the proposed methodology.

8.5 Floating frequency analysis

Floating frequency means the counting of similar types of characters available in the plain text. The proposed technique has been tested through the floating frequency analysis. In the following Table 8, comparison graphs have been plotted. The graphs obtained during post-encryption on the partial shares have better performance than the pre-encryption graphs.

Table 7 Histogram comparison on secret shares

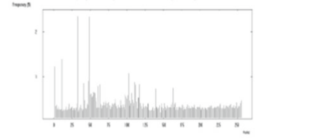
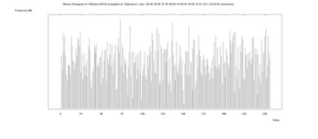
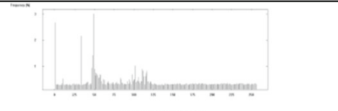
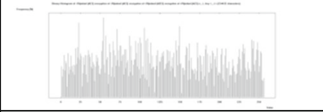
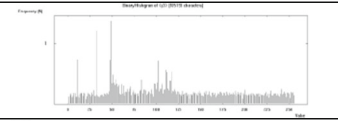
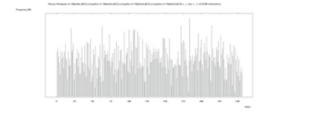
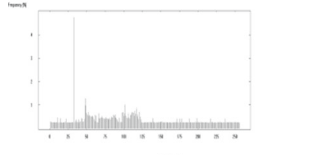
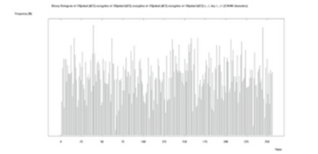
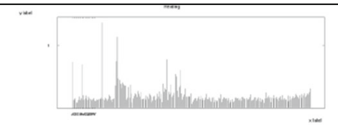
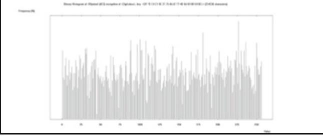
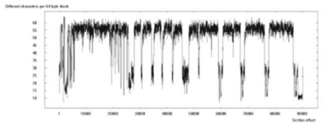
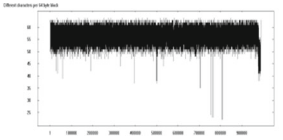
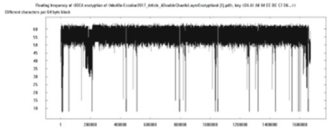
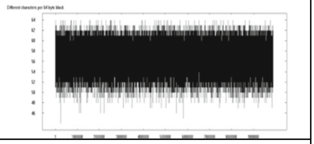
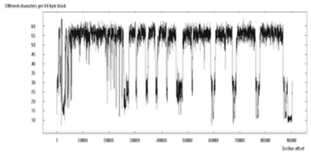
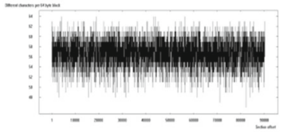
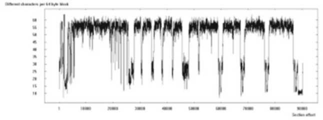
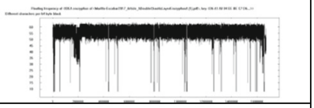
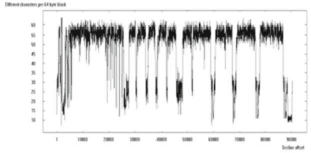
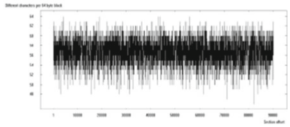
Partial Share ID	Histogram pre-encryption	Histogram post-encryption by our technique
PS$1		
PS$2		
PS$3		
PS$4		
PS$5		

Table 8 Floating frequency comparison on secret shares

Partial Share ID	Floating Frequency pre-encryption	Floating Frequency post-encryption by our technique
PS$1		
PS $2		
PS $3		
PS $4		
PS $5		

From the above floating frequencies, there could be huge changes on the offers during the pre-encryption and post-encryption stage. It emphatically supports the proposed philosophy of COVID-19 telemedicine.

8.6 Entropy analysis

Entropy is the act of randomness nature that is used for information hiding from the outsiders and intruders. Since a message can contain any character between 0 and 255. So the highest entropy is 8. Low entropy denotes lower security to the encryption system. In the following Table 9, entropy values were noted on different secret shares of the plain text. Let there will be n! Possible permutation types according to embedding dimension n. The relative frequency p (π_i) is determined for each π_i, for 1≤≤!, according to the following equation:

Table 9 Entropy comparison on secret shares

Partial Secret ID	Entropy of pre-encryption	Entropy post- encryption by our technique
PS $1	6.18	7.54
PS $2	6.19	7.76
PS $3	6.25	7.55
PS $4	6.36	7.21
PS $5	6.54	7.48

$$\mathrm{p}\ (\pi_i) = \frac{number\ of\ occurrences\ of\ type\ \pi_i}{N - n + 1}.$$

The permutation $H(n)$ is then calculated as follows:

$H\ (n) = -\sum_i^{n!} p(\pi_i) log\, p\ (\pi_i)$. Where $0 \leq H(n) \leq \log(n!)$. Here 0 indicates a series that is monotonically increasing or decreasing and log n! Indicates a completely random series. When experiment occur, H(n) is rescaled by dividing by log n!, thus normalizing H(n) to return values between 0 and 1 with 0 indicating highly regular data and 1 indicating maximal entropy. The efficacy of the proposed COVID-19 E-Health can be found in the following Table 9 in this regard.

The above stated Table 8 contains the Partial Share ID, Entropy pre-encryption, and Entropy post -encryption by our technique. This analysis shows the efficiency of our scheme in e-health sector.

8.7 Case of proposed mask generation

The proposed technique deals with a novel secret sharing method. In the group sharing of m number of users, any t number of recipients can be taken for secret sharing. Obviously, the value of t should be always less or equals to m. A snapshot which contains a set of ten recipients and only five recipients have been selected as recipients [7]. Thus, the threshold value is five. As per our proposed scheme of mask generation, a unit matrix of the order $5x5$ was selected and shuffled at threshold iterations, which can be found in the following Fig. 5.

From the above Fig. 5, considering each column at a time, the proposed shares can be derived. This is listed in the following Table 10.

We have assumed a plain text of arbitrary length as MSG = “*A*7*BC*1*DE*3*FH*2*G*”, session key, SK = “*BC*4*GE*8*RD*”, and intermediate key, IK= “*BF*67*$gAeS*”. Then, after doing bitwise XOR operation between the message, MSG and the session key, SK, the following cipher text has been found.

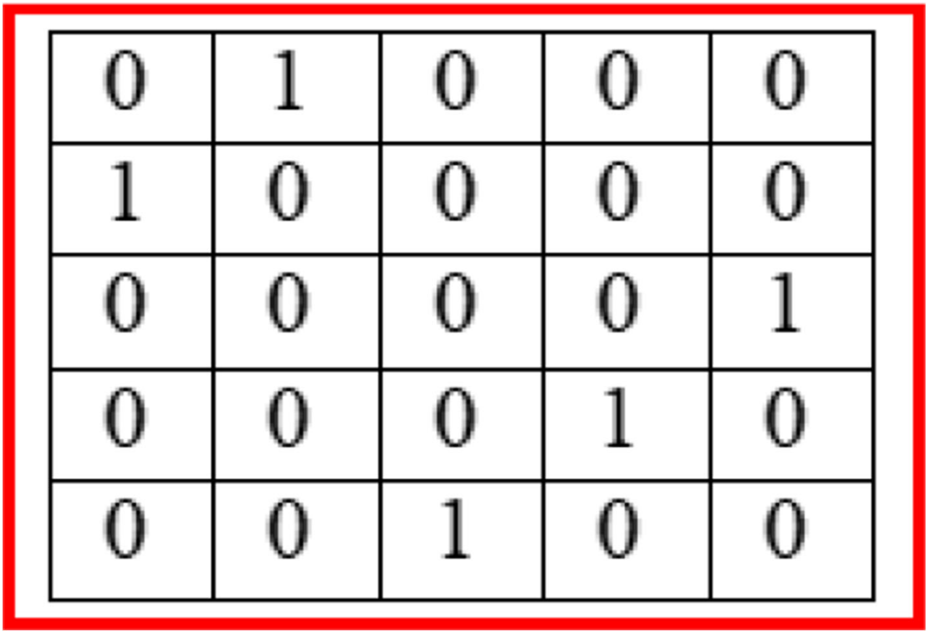
Cipher text, CT = “*dF*239*R*1*CS*5*qb*”

Using the proposed scheme of share generation, the following shares were derived which can be found in the following Fig. 6.

This proves as the novelty of the proposed cryptographic scheme for COVID-19.

8.8 Strict lossless on proposed sharing

The novelty of the proposed cryptographic technique is that it ensures strict lossless mask generation. During the global unprecedented COVID-19 uncertainty era, E-Health plays an

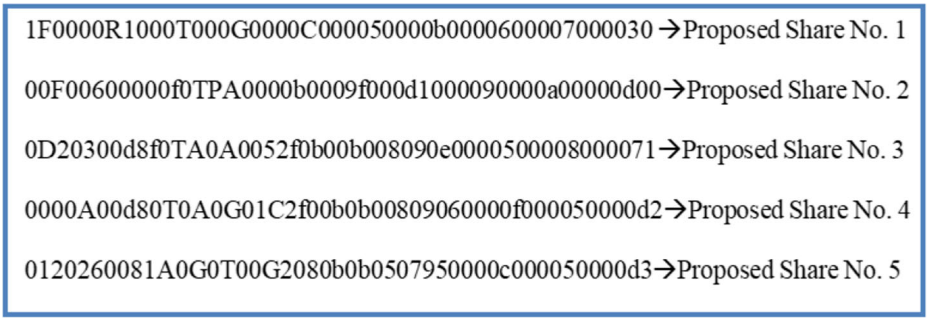


0	1	0	0	0
1	0	0	0	0
0	0	0	0	1
0	0	0	1	0
0	0	1	0	0

Fig. 5 Snapshots of after shuffling t times

Table 10 t number of proposed shares

Partial Share ID	Column 1	Column 2	Column 3	Column 4	Column 5
PS$1	0	1	0	0	0
PS$2	1	0	0	0	0
PS$3	0	0	0	0	1
PS$4	0	0	0	1	0
PS$5	0	0	1	0	0



1F0000R1000T000G0000C000050000b0000600007000030 →Proposed Share No. 1

00F00600000f0TPA0000b0009f000d1000090000a00000d00→Proposed Share No. 2

0D20300d8f0TA0A0052f0b00b008090e0000500008000071→Proposed Share No. 3

0000A00d80T0A0G01C2f00b0b00809060000f000050000d2→Proposed Share No. 4

0120260081A0G0T00G2080b0b0507950000c000050000d3→Proposed Share No. 5

Fig. 6 Proposed shares using session key

inevitable role in treating the patients. When a patient’s data is broken into t number of secret shares then t numbers of threshold shares are mandatory to reform the patient’s data. In addition there could be more users who are not being appointed as recipients to act in the group sharing. In our proposed sharing technique, no data loss has been observed during medical transactions [21]. Strict lossless may be found in the following eqs. 5 and 6 respectively.

Strict Lossless Sharing:

$$MSG = MSG_1\ U\ MSG_2\ U \ldots U\ MSG_{t-1} \ldots \tag{5}$$

it is the condition of strict lossless.

Lossy Sharing:

$$MSG = \ \ MSG_1\ U\ \ MSG_2\ \ U \ldots U\ \ MSG_{t-1} \ldots \tag{6}$$

On varying the number of recipients in the COVID-19 E-Health, the following Table 11 will depict the possible combinations of shares and strict lossless combination value to regenerate the patient's private reports.

From the above Fig. 4, it is quite true that all partial shares will be mandatory in the process of regeneration of data. Since all the shares are necessary to regenerate the text and whole the unit matrix takes part in share generation so from the eq. 5, it is clear that at the time decryption no information will loss that is lossless combination.

8.9 Attacks analysis

8.9.1 Brute force attacks on key set

The brute force attack can be handled efficiently by tricking the proposed key space. The tricksters will perform operation to decode session key on the cipher text by using latest super computers. Cryptographic algorithms are made available to the public. In this technique too, the codes are open to all. The latest super computer is Japan's Fugaku with performance speed of 415.53 *petaflops i. e.* $415.53x10^{15}$ floating point operations. Each trial requires one thousand floating operations to complete a single round. The number of trials thus can be completed is: $415.53x10^{12}$ per second. The amount of available seconds in a year is 31,53,600 *sec*. In the following Table 12, different session key lengths were consider under the proposed technique, and their corresponding time needed has been calculated under Brute-Force attack using the following eq. 7.

Table 11 Comparison in terms of strict lossless shares combinations

No. of recipients	Total share permutations	Strict lossless combination
2	2	1
3	6	1
4	24	1
5	120	1

Table 12 Time required for Brute-force attacks

Sl. No.	Length(Session Key)	Length(Intermediate Key)	Time Required to Decode(yrs)
1	20	20	$6.17*10^{325}$
2	30	30	$1.07*10^{332}$
3	48	48	$4.45*10^{342}$
4	80	80	$1.35*10^{362}$
5	128	128	$6.51*10^{390}$

$$T(L, K) = 2^{L+K}/\left(415.53*10^{12}*3153600\right)\dots \tag{7}$$

Here, T (L, K) is the time needed in Brute-Force, L and K represent the length of the session key and intermediate Key respectively. Upon various lengths of the proposed key, the following Table 12 will show the time needed to decipher the original patients' data.

8.9.2 Chosen plain text attack

Cryptographic algorithms are public and the secret key is hidden, this key is used for encryption. Intruders present silently on the network, will test several set of keys to decrypt the cipher text. In the TMCS, attackers try to decrypt the ECG signal components based on some heuristic keys. Length of the key size is proportionate to the complexity to resist against the chosen plain signal attacks. It is a tool to break image encryption under chaotic sequence [6]. The proposed bio-key and harmony search based encryption algorithm is robust to such chosen plain signal attack. It proves the resistant by the proposed technique against the chosen plain signal attack in the Telecare Medical Communication System.

8.9.3 Occlusion attack

Clinical transmission of the signals is obvious to compromise with certain percent of bits. The tolerance level of clinical signal has been estimated here against the occlusion attack [40]. Bits lost with greater than 5% is not suited in this context. Randomly, 210, 360, and 490 elements were selected. The Mean Squared Error (MSE) of recovered signal elements is mentioned in the following Table 13.

8.10 Cryptographic duration

With the proposed cryptographic scheme on COVID-19 E-Health, the transmission of patients' related clinical reports, documents and prescriptions can be made online to the

Table 13 Observations of noise attacks

Sl. No.	No. of Elements=210 Noise%=0	No. of Elements=360 Noise%=3	No. of Elements=490 Noise%=5
1	0.0	0.0	0.0
2	113.78	126.77	132.85
3	262.32	311.22	298.58

respective physicians in quick time. The cryptographic duration is a measuring index towards the efficiency of the proposed scheme. Time needed to encrypt the data at the patients' terminal and time required to decrypt by the doctors are both to be summed to get the cryptographic time [46]. The following Table 14 displays the average cryptographic duration on the proposed set of session keys.

The above cited Table 14 will have the following table headers as SK Key Group, No. of Session Keys, Proposed Encryption Time (in ms), Average Encryption Time (in ms), Proposed Decryption Time (in ms), Average Decryption Time(in ms), Proposed Cryptographic Time (in ms), and Average Cryptographic Time (in ms). There has been observed an appropriate correlation between the proposed encryption and cryptographic time, and proposed decryption and cryptographic time. These two evaluated values are r_{ec}= 0.989929 and r_{dc}= 0.988828 respectively. These values closed to 1.0 denote the standard measures in this regard.

8.11 Complexity of the proposed system modules

Lower range time complexity is always desirable in any E-Health system. Amid corona virus, excessive digitization of medical records have been adopted by all the hospitals. Such E-Health system will acquire lower time complexity in its internal architecture to have its global acceptance. In the following Table 15, the internal modules' complexity has been stated.

Table 14 Proposed cryptographic duration

SK Key Group	No. of Session Keys	Proposed Encryption Time (in ms)	Average Encryption Time (in ms)	Proposed Decryption Time (in ms)	Average Decryption Time(in ms)	Proposed Cryptographic Time (in ms)	Average Cryptographic Time (in ms)
SK#1	10	401.58	40.16	346.74	34.68	748.32	74.83
SK#2	10	357.81	35.79	263.27	26.32	621.08	62.1
SK#3	10	241.24	24.12	189.42	18.95	430.66	43.1

Table 15 Complexity of internal modules

ID of the Internal Module	Name of the Internal Module	Internal Module's Time Complexity	Notes (optional)
IM@1	Session Key Generation	$O(n*w)$	W is the weight vector, n is the number of recipients.
IM@2	Intermediate Key Generation	$O\ (logm)$	m is the size of the key.
IM@3	Secret Sharing	$O\ (n*n)$	n is the number of recipients.
IM@4	Polling Head	$O\ (n+m)$	n is the number of recipients.
IM@5	Encryption	$O\ (xylog(x*y))$	x, y are the key set arrays.
IM@6	Encapsulation	$O\ (n)$	n is the number of recipients.

8.12 Comparative study

This section deals with the comparison statements over existing techniques. It has been mentioned in the following three sub-sections.

8.12.1 Discussion on attribute based performance analysis

In this present section, comparative statement was made to prove our efficacy. The proposed cryptographic method has been compared with existing techniques [8, 45] based different types of attributes. The following Table 16 will show the comparisons with respect to different testing parameters.

From the above presented Table 16, the performance of the proposed technique can be accepted when compared against the classical techniques. This proves our efficacy.

8.12.2 Comparison between existing secret sharing technique and proposed technique

Here we have discussed about the measurement of our proposed secret sharing technique with respect to other existing techniques [6, 40]. We have compared with respect to different attributes in the following Table 17.

Table 16 Attribute based comparison among techniques

Testing key parameters	AES	DES	Blowfish	3DES	This work
Block Length	128	64	64	64	Flexible on Length
Key Length	128/192/256	56	32–448	56/112/168	Flexible on Length
Cipher text	Symmetric Encryption	Symmetric Encryption	Symmetric Encryption	Symmetric Encryption	New Secret Sharing
Degree of Flexibility	High	Medium	Low	Medium	High
Performance Time	Better	Good	Good	Better	Better

Table 17 Comparison between existing secret sharing techniques and proposed technique

Secret sharing scheme	Perfect/Non-perfect	Single/Multi-Secret	Threshold/Non-threshold	Type	Proactive
Shamir [47]	Perfect	Single	Threshold	Polynomial based	No
Benaloh [49, 50]	Perfect	Single	Non-threshold	Circuit based	No
Pedersen [49, 50]	Perfect	Single	Threshold	Polynomial based	Yes
Herzberg [49, 50]	Perfect	Single	Threshold	Polynomial based	No
Blakley [10, 49]	Non-perfect	Single	Threshold	Vector space based	No
Asmuth-Bloom [41, 50]	Non-Perfect	Single	Threshold	CRT based	No
Bai (ramp) [50]	Non-Perfect	Multi-Secret	Threshold	Matrix Projection based	Partial
Franklin(ramp) [49, 50]	Non-Perfect	Multi-Secret	Threshold	Polynomial Based	No
Iftene [49, 50]	Non-Perfect	Single	Non-Threshold	CRT based	No
This Technique	Perfect	Multi-Secret	Non-Threshold	Unit Matrix based	No

Table 18 Comparison with respect to application model

Parameters for Comparison	Sinkhole Attack		Worm Attack		Side-Channel Attack	
	Network Layer	This Work	Application Layer	This Work	Application Layer	This Work
Active or Passive Attacks on Patients' Data	Active attacks means the misleading information which results in online medical packet dropping [50].	May resist Active attacks.	It may edit the medical report files [50].	May resist Active attacks.	Passive attack denotes the session key by using the side-channel by the intruders [2].	May resist Passive attacks.
Level of damage done on Medical Data	Higher degree of chances. Data flowing from compromised node to the attacker.	May be achieved.	Higher degree of chances. As it can delete files, mail documents from the server [50].	May be achieved.	Higher degree of chances. Intruder may retrieve the secret key [19].	May be achieved.
Prevention of Medical Data	May be achieved if node authentication is done [50].	Future Scope of work.	By avoiding suspicious web-sites, files, and documents [26].	May be achieved.	Using the preventive precautions [12].	May be achieved.
Guided Attacks on Medical data	Routing attack is possible here [39].	May resist routing attack.	Malicious Codes attack may happen here.	May resist against the malicious codes.	Side Channel Information attack is feasible here [49].	May resist different side-channel attacks.

8.12.3 Application model oriented comparison

In this sub-section, we have made a comparative table based on the application model. The following Table 18 shows the comparative analyses related to data attacks to the system. It also proves the efficiency of our proposed scheme with respect to different layers of application model. We had compared three types of attacks with the parameters such as damage level on patients' medical data, existing proposal and detection schemes, and their corresponding vulnerability in E-Health. Any type of vulnerable attack may can reverse the patients' data, drop the medical transaction packets, and decode the clinical reports and retrieval of the session key. The following Table 18 will display the efficacy of our proposed system with respect to different types of attacks.

9 Conclusion

There are various sorts of difficulties in medical services framework at present time. Hospitals have shown adaptabilities to upgrade and improve medical care capacities through digitization in this pandemic. It can help preventive consideration and encourage collective medical services to serve the patients from distant locations. It is a "New Normal" way to treat the non-invasive patients in larger perspectives, when second wave of corona virus is affecting us a lot. An essential methodology is the patients' data security and confidentiality through online transmission [6, 20, 23, 40]. In this paper, a cryptographic system was proposed to foster the essential patients' security where an encryption procedure is on the neural session key. Neural perceptron has been used to generate such session keys. Distinctive test results and its analysis, comparative studies demonstrate the efficacy and effectiveness of the proposed technique. Thus our proposed scheme is valid for secure telecommunication of COVID-19 E-Health. Strict lossless secret sharing of data has been incorporated here intelligently. Relative investigations among proposed secret shares and standard procedures, comprehensive key robustness, graphical charts show the agreeableness of our proposed method. On comparing at the application model, this proposed technique addresses the vital issues on the security frisks. To the most amazing aspect our insight our proposed strategy is the least complex one having insignificant computational overhead during encryption and decryption phase. It has been observed an appropriate correlation between the proposed encryption and cryptographic time, and proposed decryption and cryptographic time. These two evaluated values were r_{ec} = 0.989929 and r_{dc}= 0.988828 respectively. The computed average cryptographic time on three different session key groups have been calculated as 74.83, 62.1, and 43.1 ms respectively. To have more standards, the chaotic sequences in the ranges of r = [0.41,0.53], r = [0.61, 0.66], and r = [0.91, 0.99] on the initial values x = 3.64, 3.81, and 3.88 respectively were found and intermediate keys were derived here. Moreover, the internal modules' time complexity has been measured and found to be significantly lower.

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

Declarations

Ethics approval This article does not contain any studies with human participants or animals performed by any of the authors.

Conflict of interest There is no conflict of interest.

References

1. Agarwal N, Jain P, Pathak R, Gupta R (2020) Telemedicine in India: a tool for transforming health care in the era of COVID-19 pandemic. J Educ Health Promot 9:190. https://doi.org/10.4103/jehp.jehp_472_20
2. Agrawal A, Gorbunov S, Vaikuntanathan V, Wee H (2013) Functional encryption: new perspectives and lower bounds. In: Canetti R, Garay JA (eds) CRYPTO 2013, Part II. LNCS, vol. 8043. Springer, Heidelberg, pp 500–518
3. Aitkin M, Foxall R (2003) Statistical modelling of artificial neural networks using the multi-layer perceptron. Stat Comput 13:227–239
4. Baker J, Stanley A (2018) Telemedicine technology: a review of services, equipment, and other aspects. Curr Allergy Asthma Rep 18:60
5. Bhowmik A, Karforma S (2021) Linear feedback shift register and integer theory: a state-of-art approach in security issues over e-commerce. Electron Commer Res. https://doi.org/10.1007/s10660-021-09477-w
6. 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) 8(3):197–204
7. 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. Int J Comput Sci Eng 9(4): 297–311
8. Bhowmik A, Karforma S, Dey J (2021) Recurrence relation and DNA sequence: A state-of-art technique for secret sharing. International Journal of Reconfigurable and Embedded Systems (IJRES) 10(1):65–76
9. Bindra V (2020) Telemedicine for Women's health during COVID-19 pandemic in India: a short commentary and important practice points for obstetricians and Gynaecologists. J Obstet Gynecol India 70:279–282. https://doi.org/10.1007/s13224-020-01346-0
10. Blundo C, De Santis A, Stinson DR et al (1995) Graph decompositions and secret sharing schemes. J Cryptol 8:39–64. https://doi.org/10.1007/BF00204801
11. Bokolo A Jnr (2020) Use of telemedicine and virtual care for remote treatment in response to COVID-19 pandemic. J Med Syst 44:132. https://doi.org/10.1007/s10916-020-01596-5
12. Boneh D, Franklin M (2001) Identity-based encryption from the Weil pairing. In: Kilian J (ed) CRYPTO2001. LNCS, vol. 2139. Springer, Heidelberg, pp 213–229
13. Boodley CA (2006) Primary care telehealth practice. J Am Acad Nurse Pract 18:343–345
14. Borchert A, Baumgarten L, Dalela D, Jamil M, Budzyn J, Kovacevic N, Yaguchi G, Palma-Zamora I, Perkins S, Bazzi M, Wong P, Sood A, Peabody J, Rogers CG, Dabaja A, Atiemo H (2020) Managing urology consultations during COVID-19 pandemic: application of a structured care pathway. Urology. 141: 7–11. https://doi.org/10.1016/j.urology.2020.04.059
15. Burduk A, Stefaniak P (2012) Application of a Perceptron Artificial Neural Network for Building the Stability of a Mining Process. In: Yin H, Costa JAF, Barreto G (eds) Intelligent Data Engineering and Automated Learning - IDEAL 2012. IDEAL 2012. Lecture notes in computer science, vol 7435. Springer, Berlin, Heidelberg
16. Chen J-X, Zhu Z-L, Fu C, Yu H (2013) An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism. Opt Express 21(23):27873–27890
17. Christianson J, Christianson E. White paper: using telehealth in the emergency department to minimize risk to health care providers and conserve resources during the COVID-19 response. 2020.
18. Claypool B (2020) Telemedicine and COVID-19: 6 tips to ace your first visit. Ment Heal Wkly 30(17):5–6
19. Das A, Veni Madhavan CE (in press) Public-key cryptography: theory and practice. Pearson Education
20. Dey J (2021) Telecardiological COVID-19 (2nd) Wave: Metaheuristic-Key Guides Protected Encryption of Heterogeneous Cardiac Reports. Journal of Mathematical Sciences & Computational Mathematics, (accepted) 02(04):511–523. https://doi.org/10.15864/jmscm.2405
21. Dey J, Karforma S, Sarkar A, Bhowmik A (2019) Metaheuristic guided secured transmission of E-prescription of dental disease. Int J Comput Sci Eng 07(01):179–183

22. Dey J, Sarkar A, Karforma S (2021) Newer post-COVID perspective: Teledental encryption by de-multiplexed perceptrons. Int J Inf Technol 13:593–601. https://doi.org/10.1007/s41870-020-00562-1
23. Dey J, Chowdhury B, Sarkar A, Karforma S (2021) Secured Telepsychiatry for Geriatric Patients (TGP) in the Face of COVID-19 IInd Wave. Journal of Mathematical Sciences & Computational Mathematics 02(04): 564–571. https://doi.org/10.15864/jmscm.2409
24. Dwivedi R, Dey S, Sharma MA, Goel A (2020) A fingerprint based crypto-biometric system for secure communication. J Ambient Intell Humaniz Comput 11:1495–1509. https://doi.org/10.1007/s12652-019-01437-5
25. Flodgren G, Rachas A, Farmer AJ, Inzitari M, Shepperd S (2015) Interactive telemedicine: effects on professional practice and health care outcomes. Cochrane Database Syst Rev 2015:CD002098
26. Ghansela S (2013) Network Security: Attacks, Tools and Techniques. IJARCSSE 3(6)
27. Gillman-Wells CC, Sankar TK, Vadodaria S (2021) COVID-19 reducing the risks: telemedicine is the new norm for surgical consultations and communications. Aesthet Plast Surg 45:343–348. https://doi.org/10.1007/s00266-020-01907-8
28. Greiwe J (2020) Telemedicine in a post-COVID world: how eConsults can be used to augment an allergy practice. J Allergy Clin Immunol in Practice
29. Harmouch Y A chaotic key stream generation for stream cipher. In: LOPAL '18: Proceedings of the International Conference on Learning and Optimization Algorithms: Theory and Applications May 2018 Article No.: 14, pp 1–6. https://doi.org/10.1145/3230905.3230942
30. Huang X, Ye G (2014) An efficient self-adaptive model for chaotic image encryption algorithm. Commun Nonlinear Sci Numer Simul 19(12):4094–4104
31. Jordan RE, Adab P, Cheng KK (2020) Covid-19: risk factors for severe disease and death. BMJ 368:m1198
32. Joshi C, Singh UK (2015) A review on taxonomies of attacks and vulnerability in computer and network system. International Journal of Advanced Research in Computer Science and Software Engineering (IJRCSSE) 5(1):742–747
33. Kanter I, Kinzel W, Kanter E (2002) Secure exchange of information by synchronization of neural networks. EPL (Europhysics Letters) 57(1):141
34. Keesara S, Jonas A, Schulman K (2020) Covid-19 and health care's digital revolution. N Engl J Med 382: e82
35. Khan HN, Chaudhuri A, Kar S, Roy P, Chaudhuri A (2015) Robust symmetric cryptography using plain-text variant session key. Int J Electron Secur Dig Forensics 7(1):30–40
36. Khan HN, Chaudhuri A, Das A, Chaudhuri A (2020) An ultra robust session key based image cryptography. Microsyst Technol 26:2193–2201. https://doi.org/10.1007/s00542-019-04518-9
37. Kumar V (2015) Ontology based public healthcare system in internet of things (IoT). Proc Comput Sci 50: 99–102. https://doi.org/10.1016/j.procs.2015.04.067
38. Kumar P, Huda F, Basu S (2020) Telemedicine in the COVID-19 era: the new normal. Eur Surg 52:300–301. https://doi.org/10.1007/s10353-020-00666-9
39. Olivier F, Carlos G, Florent N (2015) New security architecture for IoT network. Proc Comput Sci 52: 1028–1033. https://doi.org/10.1016/j.procs.2015.05.099
40. Patel K (2019) Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files. Int J Inf Technol 11:813–819
41. Quisquater M, Preneel B, Vandewalle J (2002) On the security of the threshold scheme based on the Chinese remainder theorem. In: Naccache D, Paillier P (eds) Public Key Cryptography. PKC 2002. Lecture notes in computer science, vol 2274. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45664-3_14
42. Reyad O, Karar ME (2021) Secure CT-image encryption for COVID-19 infections using HBBS-based multiple key-streams. Arab J Sci Eng 46:3581–3593. https://doi.org/10.1007/s13369-020-05196-w
43. Rothe C, Schunk M, Sothmann P, Bretzel G, Froeschl G, Wallrauch C, Zimmer T, Thiel V, Janke C, Guggemos W, Seilmaier M, Drosten C, Vollmar P, Zwirglmaier K, Zange S, Wölfel R, Hoelscher M (2020) Transmission of 2019-nCoV infection from an asymptomatic contact in Germany. N Engl J Med 382(10): 970–971
44. Rukhin A, Soto J, Nechvatal J, Smid M, Barker E, Leigh S, Levenson M, Vangel M, Banks D, Heckert A, Dray J, Vo S (2001) A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST special publication, pp 800–822
45. 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
46. Sarkar A, Dey J, Karforma S (2021) Musically modified substitution-box for clinical signals ciphering in wireless telecare medical communicating systems. Wirel Pers Commun 117:727–745
47. Shamir A (1979) How to share a secret? Commun ACM 22(11):612–613

48. Smith AC, Thomas E, Snoswell CL, Haydon H, Mehrotra A, Clemensen J, Caffery LJ (2020) Telehealth for global emergencies: implications for coronavirus disease 2019 (COVID-19). J Telemed Telecare 26(5):309–313. https://doi.org/10.1177/1357633X20916567
49. Stallings W (2003) Cryptography and network security: principles and practice, third edition. Prentice Hall
50. Stinson D (2006) Cryptography: theory and practice, third edition. Chapman & Hall/CRC
51. Tanaka MJ, Oh LS, Martin SD, Berkson EM (2020) Telemedicine in the era of COVID-19: the virtual Orthopaedic examination. J Bone Joint Surg American Volume
52. Tanaka MJ, Oh LS, Martin SD, Berkson EM (2020) Telemedicine in the era of COVID-19: the virtual orthopaedic examination. J Bone Joint Surg Am 102:e57. https://doi.org/10.2106/JBJS.20.00609
53. Thiagarajan K (2021) Covid-19: India is at Centre of global vaccine manufacturing, but opacity threatens public trust. BMJ 372:n196. https://doi.org/10.1136/bmj.n196
54. Whaibeh E, Mahmoud H, Naal H (2020) Telemental health in the context of a pandemic: the COVID-19 experience. Curr Treat Options Psychiatry 1:198–202
55. Ye G, Huang X, Zhang LY, Wang Z (2017) A self-cited pixel summation based image encryption algorithm. Chinese Physics B 26(1):010501
56. Yen JC, Guo JI (2000) A new chaotic key based design for image encryption and decryption. Proceedings of the IEEE International Symposium Circuits and Systems 4:49–52
57. Zhou X, Snoswell CL, Harding LE, Bambling M, Edirippulige S, Bai X, Smith AC (2020) The role of telehealth in reducing the mental health burden from COVID-19. Telemedicine and e-Health 26(4):377–379

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Joydeep Dey pursed Bachelor of Computer Application (Honours) from Cyber Research & Training Institute, Burdwan, India in 2007 and M.C.A. from the University of Burdwan in 2011 and he had secured First Class First (GOLD MEDALIST). He is working as State Aided College Teacher & Head in Department of Computer Science at M.U.C. Women's College, Burdwan since 2011. He has published 05 SCI indexed Springer journal paper, 10 SCOPUS Indexed journals, 04 Edited Book Chapters, 04 Book-Chapters (SPRINGER; SCOPUS INDEXED),03 International Conferences journals (UGC journals), and 45 others publications (International/National/State/Regional Level). His main research interest includes Cryptography and Computational Intelligence in Telehealth. He has more than 10.0 and 0.5 years of teaching experience at UG and PG level respectively.

Anirban Bhowmik has completed Bachelor of Science (Mathematics Honours) from Bolpur College, Bolpur, West Bengal, India and Master of Computer Application (M.C.A.) from the University of Burdwan in 2008. He is working as State Aided College Teacher in Department of Computer Science, M.U.C. Women's College Burdwan West Bengal, India since September 2018. He has published 01 SSCI journal, 02 Edited Book Chapters, 05 conference papers, 28 journal papers at reputed international journals, which are available online. His main research work focuses on Cryptography, Mathematical Modeling, and Soft Computing. He has 14 years of teaching experience at UG level.

Sunil Karforma has completed his Bachelors in Computer Science & Engineering, and his Masters in Computer Science & Engineering, from Jadavpur University. He received his Ph.D. in Computer Science, and is presently Professor & Head of the Dept. of Computer Science at the University of Burdwan, India. His research interests include Network Security, E-Commerce, and Telehealth. He has published 200 papers in both national as well as international reputed journals and conferences.