A novel Double Tier Cryptographic System (nDTCS) to Reinforce Patients' Privacy in Contemporary COVID-19 Telemedicine

ANIRBAN BHOWMIK
Maharajadhiraj Uday Chand Women's College
JOYDEEP DEY (joydeepmcabu@gmail.com)
Maharajadhiraj Uday Chand Women's College
SUNIL KARFORMA
The University of Burdwan

Research Article

Keywords: COVID-19, Logistic Map, Session Key, Secret Sharing, Linear Congruence

Posted Date: April 13th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-363039/v1

A novel Double Tier Cryptographic System (nDTCS) to Reinforce Patients' Privacy in Contemporary COVID-19 Telemedicine

[1]Anirban Bhowmik, [2]Joydeep Dey, [3]Sunil Karforma

[1]State Aided College Teacher, Department of Computer Science, M.U.C. Women's College, Burdwan
[2]Head & State Aided College Teacher, Department of Computer Science, M.U.C. Women's College, Burdwan
[3]Head & Professor, Department of Computer Science, The University of Burdwan, Burdwan

Abstract: In this modern COVID-19 telemedicine industry, privacy and security of patients' information is the most open challenge to keep it intact. Considering the current legal regulations, every hospital must impose a prominent security technique to maintain a secure electronic health records system. The realization of telemedicine is another notable advancement in the field of medical sciences. The healthcare services have increased its throughput with the help of Internet based computing. Recently, security flaws on patient's information have become a more significant challenge in electronic healthcare system. Electronics health record i.e. collection of health related patients' information are extremely sensitive in nature. So, it is very relevant to impose an advanced security techniques in such systems. Here, we have focused on security issues likes of technical safeguards. A novel Double Tier Cryptographic System (nDTCS) have been proposed here. We had proposed a modified logistic map and linear congruence based security model for the secured telemedicine transactions with an authentication technique. For encryption and decryption purpose, two keys have been used which were intermediate key, and session key. The modified logistic map and secret sharing were the backbone of the proposed technique. This new approach of key generation provides newness as well as extra robustness in our proposed technique. The chaotic sequences in the ranges of $r = [0.4,0.5], r = [0.6, 0.64]$, and $r = [0.9, 0.97]$ on the initial values $x = 3.65$, 3.84, and 3.90 respectively were noted under this technique test. 2^{64}, 2^{256}, 2^{1024}, 2^{4096}, 2^{16384}, and 2^{65536} were the possibilities of combined key space volumes. The different types of mathematical experiments like randomness test, brute force, histogram analysis and their obtained results have guided that it is very secured and efficient for patients' data transmission in health sectors.

Keywords: COVID-19, Logistic Map, Session Key, Secret Sharing, Linear Congruence.

1. Introduction

Health care may be defined as the act of taking preventative or necessary procedures to improve a person's well-being. This may be done with surgery, medicine, or other alterations in a person's lifestyle. These services are typically provided by hospitals and physicians through a health care system. When these services are provided through Internet enabled nodes, this comes under the telemedicine. Thus, patients suffering from non-invasive and non-critical diseases may be treated remotely. The constraints of social distancing, lockdown restrictions, night curfew, are supposed to be maintained by the mass people to strive against this deadly corona virus [1]. Co-morbid patients are at higher risks of COVID-19. But through COVID-19 telemedicines, such patients can be tactfully from their safe remote locations at any pint of time. Also, nascomial infections can be made to null and void to such co-morbid patients [2]. Due to this novel corona virus, hospitals and clinics have shifted from physical consultation modes to virtual consultation modes. Patients are encouraged more to exercise the facility of virtual consultations with their physicians. Doctor, nurses, patients, healthcare staffs, etc are then less exposed to COVID-19 under the umbrella of telemedicine [3]. In this perspective, the current trends in healthcare industry are the digitization of healthcare systems. Their workflow is migrated towards electronics patient records. An electronic record of a patient means electronic version of a patient's medical history like demographics, progress notes, problems, medications, vital signs, past medical history, immunizations (maybe COVID Shield, CoVaxin [4-5], etc), laboratory sample data and radiology reports etc. These medical data are maintained by the hospital provider over time. The volume of such clinical data has risen in huge rate in terms of complexity, diversity and timeliness mainly during hyper digital telehealth. Hence, data security reinforcement is the biggest obligatory here. A COVID-19 telemedicine is treated as good as it preserves the patients' data during the public network transmission. This paper has proposed a novel Double Tier Cryptographic System (nDTCS) to risen the levels of data security through mathematical linear congruence, modified logistics maps, and secret sharing.

This paper has been systematically organized as follows. Section 1 contains the introduction. Background knowledge has been embedded in the section 3. Prior works have been explained in the next section 3 in the form of literature survey. Section 4 has the objectives and novelties of the proposed technique. Section 5 has some open challenging issues. The proposed methodology is given in the next section 6. The results and discussion were elaborated at section 7. The efficacy of the proposed technique under the comparative studies has been kept in the section 8. Conclusion is mentioned in the section 9. The limitations and future scope of work has been stated in the section 10. Acknowledgement, Statements of Ethical Compliances, and References were mentioned at the end.

Security is a most important issue in any COVID -19 telemedicine. The tricksters aim is to steal the private data, and they attack on the nodes and transmission paths to utilize patient's information, or may shut down some applications that are controlled by the telemedicine servers. There are many types of attacks on telemedicine systems that include eavesdropping and intruding of data, forgery of clinical reports, falsification of insurance claims, etc. All in such attacks the privacy of the patient gets severely compromised and the integrity error affects the message / a report is being altered intentionally. The technology based telemedicine system provides huge benefits in the society but it is also very much prone to different types of unwanted attacks. These types of attacks mainly cause information leakage and loss of medical serviCOVID-19 telemedicine platform, a lot of personal medical information is shared among various types of devices so the privacy of user is a vital part [6-8] in such system. Hence a reinforced security cryptographic system is needed for the data or information protection amid this corona virus pandemic.

2. Background

This section deals with the background knowledge and mathematical concepts that were taken into consideration in this proposed technique.

2.1 **Need of Data Security Reinforcements in COVID-19 Telemedicine**

The entire world is facing the unforeseen corona pandemic since November, 2019. Greater challenges are faced by the health care personnel. Any COVID-19 telemedicine must consider patients' data security as the most prior issue [9]. It needs data secrecy from the outer world and protection, transparency, co-ordinations within the system entities. Data integrity and consistency must be ensured by theses online medical systems. Another aspect is its authentication checks from the fake falsification users. For this, digital signatures and encoding techniques must be utilized. Clinical data frameworks must be shielded adequately against any tricksters coming about the open organizations of the telemedicine [10]. Electronic medical records might be only available just to the treating physicians and dealing clinical staffs, guaranteeing the chance of a crisis access may be avoided. Any entrance beyond that requires the extraordinary assent from the patient regarding her / his electronic medical records. The clinical secret must be guaranteed here. The electronic medicine with a documentation of the patient's prescription requires the assent of the patient and should secure the privileges of the doctors. Specifically it needs to guarantee that the separate doctor's recommending conduct can't be put away or get known from an outsider. This is done in case of expert opinions needed from senior doctors or surgeons. COVID-19 telemedicine necessitates the software developers to incorporate higher levels of encryption / decryption and different shields into their connections with patients. Be that as it may, patients' devices / gadgets / nodes on the low computing power can operate smoothly. Cyber securities on the telemedicine depend strongly on the end-to-end application levels. As the tricksters and intruders consistently abuse the existing techniques to explore new weaknesses, so the software engineers are in a steady competition to stay aware of new modes of hacking. Patients' data protection is just pretty much as solid as its most vulnerable component in such systems [11]. Secured telemedicine applications should be supplemented by different measures of cryptographic engineering. Therefore, online health care suppliers ought to teach patients about network protection and the means they should take to improve the general wellbeing of their collaborations online by the following ways.

- By making patients aware and cautious related to the telemedicine security risks.
- By making them to understand the vulnerabilities of patients' medical data [12].
- By updating the online telemedicine apps and internal configurations at regular basis.
- By installing anti-virus software in their machines / nodes.
- By denying access to unnecessary resources and process in their system.
- By considering the risks incurred in social engineering and other middle way attacks.

1.4 Cryptography and Secret Keys

Cryptography deals with art of codifying messages, so that it become unreadable and can be shared secretly over public communication channels. It is study of developing and using different types of encryption and decryption

techniques. Here the plain text is converted into cipher text using an encryption algorithm so that hackers cannot read it, but authorized person can only access it. The decryption algorithm works in the reverse order and converts the cipher text into plain text. Cryptography is divided into two types such as symmetric key and asymmetric key cryptography with respect to key [13-15]. A COVID-19 telemedicine should be developed under the cryptographic science. This is the best way to resist the unwanted tricksters and hackers.

1.5 Chaotic System

Chaotic systems [16-17] are basically nonlinear in nature and exhibiting an apparently random behavior for certain ranges of values of system parameters. However, the solutions or trajectories of the system remain bounded within the phase space. This unstable state is strongly depending on the values of the parameters and on the way the system begins.

1.5.1 Logistic Map in Chaotic System

The logistic map [14] is a well-known one dimensional chaotic map proposed by R.M. May representing an idealized ecological model for describing yearly variation in the population of an insect species. The mathematical formula is defined as: $y_{n+1} = a * y_n(1 - y_n)$, where a∈[0,4] is the control parameter and $y_0 \in [0,1]$ is the initial condition [18]. The logistic map shows good behavior and is frequently used in many applications for its chaotic nature in specific range. The hopf bifurcation diagram shows the dynamical properties of the logistic map. The logistic map shows chaotic nature for a∈ $[\,3.57, 4\,]$ and slight variations of the initial value produce major differences in the generated random values. This sequence of values is non-periodic and non-conversing in nature.

1.6 Linear Congruence

Let f(x) $= a_0x^n + a_1x^{n-1} + \cdots + a_n (n \geq 1)$ be a polynomial with integer coefficient $a\, a_0, a_1, \ldots, a_n$ with $a_0 \not\equiv 0 (mod\ m)$. Then f(x)$\equiv 0 (mod\ m)$ is said to be a polynomial congruence $(mod\ m)$ of degree n. If there exists an integer x_0 such that$f(x_0) \equiv 0\ (mod\ m)$, then the solution of the congruence is x_0 [19].

Theorem 1*: If* $gcd\ (a, m) = 1$, *then the linear congruence* $ax \equiv b\ (mod\ m)$ *has a unique solution*[20].

Proof: Since $gcd\ (a, m) = 1$, there exist integers u, v such that $au + mv = 1$.

Therefore, $a\ (bu) + m\ (bv) = b$. This gives a$(bu) \equiv b\ (mod\ m)$. This shows that $x = bu$ is a solution of the congruence$ax \equiv b\ (mod\ m)$. Let x_1 and x_2 be solutions of the congruence$ax \equiv b\ (mod\ m)$. Then $ax_1 \equiv b\ (mod\ m)$ and$ax_2 \equiv b\ (mod\ m)$. It implies$ax_1 \equiv ax_2\ (mod\ m) \rightarrow x_1 \equiv x_2\ (mod\ m)$, since$gcd\ (a, m) = 1$. This proves that the congruence has a unique solution. The concept of the above theorem is used in generation of intermediate key in our proposed technique [21].

1.7 Liner and Non-liner functions

A linear function [22] has the form $y = f(x) = ax + b$. A linear function has one independent variable which is x and one dependent variable which is y. b is constant term or y intercept. The coefficient 'a' is the coefficient of the independent variable. It is also known as slope and it gives the rate of change of the dependent variable. A linear equation is used in our technique in intermediate key generation.

A simple non linear equation is of the form $x^2 + by^2 = c$. A non linear equation looks like a curve when graphed. Its slope value is variable. The degree of a non linear equation is at least 2 or other integer values. The input and output of a non linear system is not directly related. In this article a non linear function is used in encryption process. The aim of the use of non linear function is to create a non linearity in cipher text [23].

1.8 Pell's Equation

Pell's equation is a Diophantine equation of the form $x^2 - dy^2 = \pm 1,\ x, y \in Z$, where d is a given natural number which is not a square[16].

Lemma: For each non-square positive integer d, there are infinitely many positive integers $x\ and\ y$ such that $\left|x - \sqrt{d}\, y\right| < \frac{1}{y}$.

1.8.1 Lagrange's Theorem

For every positive integer d that is not a square, the equation $x^2 - dy^2 = 1$ has a nontrivial solution [17]. Here we have specially focused on the integer solutions of Pell's equation. The two integers for a particular d provide a set of numbers for two or more number of $d's$ which is used for key generation in this article.

3. Literature Survey

This section deals with the earlier works on COVID-19 telemedicines on the field of cryptographic science. Keesara S. et al. [24] had suggested to bring telehealth revolutions due to COVID-19 in compliance with the patients' law and security. Bindra V. et al. [25] had suggested that pregnant women and females can avail the telemedicine services in COVID-19 era with limited editions. Such women are greater risks of corona virus. Their exposure to physical visits can be curtailed by the triage implementation. Whaibeh E. et al. [26] had addressed the telemental health as a long term fruitful effect in post COVID-19 period too. During this corona virus emergency, mental complications has risen exponentially. Patients can be guided through online telemental systems. It would be best to resolve and counsel their issues and the corona contamination is also absent. Telemental health can be regarded as safe, convenient, scalable, efficient, and sustainable way to treat such mentally ill patients from their quarantines. Zhou X. et al. [27] had stated the treatment schemes for COVID-19 patients should be both in terms of physiological and psychological support for them. Both are equally important. Psychological treatment smay reduce their mental burdens. But in this critical situation, patients should be treated by the online telehealth. It may include email, chat, video calls, phone call, etc. Jnr B.A. [28] had explained the radical changes that were made by the health systems to provide treatments to the patients amid COVID-19. Hospitals have responded well to adopt digital health. Virtual consultations, telemedicine, video call, etc are its inevitable components. They have guided the common people how to use digital health in this global crisis. Tanaka MJ et al. [29] had explained the needs of telemedicine in the orthopedic fields. Its emergence has been hastened with the onset of COVID-19. Virtual orthopedic examinations have become an essential component. They have provided the guidelines how such patients remotely be examined through virtual monitoring. It enhances the treatment procedures and reduces the patients' exposure to the novel corona virus.

Yen J.C. et al. [30] 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. [31] also had proposed an encryption method called CKBA (Chaotic Key Based Algorithm) in which a binary sequence is generated using a chaotic system. Abdelaziz et al. [32], has shown the analysis of the security vulnerabilities and the risk factors detected in mobile medical apps. These apps can be categorized into remote monitoring, diagnostic support, treatment support, medical information, education and awareness, and communication and training for healthcare workers. Categories are done according to its risk factor standards. Eight security vulnerabilities and ten risks factors of mobile security project are detected and analyzed by the World Health Organization. Amin et al. [33] first proposed Medical Information System (TMIS) where novel authentication and key agreement protocol for accessing remote multi-medical server. Xiaoxue Liu et al. [34] proposed a heterogeneous cross-domain AKA protocol with symptoms-matching in TMIS. This protocol has been composed of four phases. These phases were registration phase, login phase, authentication and key agreement phase. Here two patients realize mutual authentication as well as session key establishment but the generation of session key and authentication process is very complex. In this regard the communicating parties have to face four phases.

4.Objectives and Novelties

The main objective is to enhance life quality for people or patients who need support of telemedicine by avoiding unnecessary healthcare costs and efforts, and to provide the proper medical support and treatment at the right time. Most importantly, the transmission of corona virus can be made reduced from such telemedicine services. From above stated introduction and literature review part, it is seen that different types of chaotic map is used for encryption decryption purposes. In this article we have developed a cryptosystem based on modified logistic map and linear congruence and this system acts against security breach in communication network. Here we had provided some better security algorithms that protect different attacks in the communication network of COVID-19 telemedicine system. We have focused on two basic things related to message communication which are authentication and encryption-decryption. For authentication we have used hash function and a key, named, intermediate key which is generated by using the two public keys of sender and receiver and the concept of linear congruence and Pell's method. For encryption-decryption, two keys (session key and intermediate key) were used one session key and other intermediate key. We have modified the logistic map of chaotic system. The modified version is given in the following equation 1.

$$x_{n+1} = r * x_n(1 - x_n^2)(1 - x_n) \quad \ldots (1)$$

Here, r ∈ [0 , 4.3] is the control parameter and $x_0 \in [0, 1.3]$ is the initial condition. This map is chaotic for r ∈ [3,4.3]. Our revised logistic map outperforms the existing maps. The details of experiments and results are given in the later result section. The session key has been proposed by using the modified logistic map. The modified logistic map is an important aspect of our proposed cryptosystem. To get the better non linearity in encryption we have used mathematical linear and non-linear functions.

The novel concept of secret sharing on the patients' data has been proposed here with low time complexity. There exists a multiple recipients (say n). So the proposed technique creates a mask matrix for generating different n number of shares. It is based on unit matrix and mathematical operation carried out on those data. Only simple bitwise functions were utilized. The detail descriptions have been mentioned in the later section.

A rigorous frame structure has been used for message transmission in COVID-19 telemedicine network. Different types of information are accumulated in this structure and this information is used for identity verification, key generation and encryption-decryption. Medical data protection against the tricksters is the chief contribution in this paper. It reflects the acceptance probability of revolutionary adaptations made in the advanced medical science due to COVID-19.

5. Open Challenging Issues

There are different types of challenges exists in any COVID-19 telemedicine system. Different types of attacks or malicious activity may degrade activity of the medical devices and disrupt the communication system of telemedicine. A common method of attack involves tampering or altering of the messages. 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. Digital platforms on different COVID-19 telemedicine were used without having patients' proper security. Same transmission or meeting key is used for every multiple sessions to reduce the session key complexity. But it has some limitations. Once it gets compromised then all session medical data will be theft by the tricksters and intruders. Robustness of the used session key in the light of its generalization is not seen in different proposed methods. Thus, the encrypted cipher text is highly prone to middle way attacks. If the public transmission paths get compromised, then any medical data travelling through that network will be stealed by the tricksters. Thus, the patient and the doctor are likely to be affected in all respect. Patients' medical data privacy will be hampered immensely. More to say that patients' treatments will be in danger if data communication is altered.

6. Proposed Methodology

In this article, we have built up a cryptographic framework dependent on COVID-19 telemedicine. This framework acts against various security conducts in correspondence network particularly where online clinical data exchanges which were overwhelmed massively in this COVID-19 circumstance. The proposed strategy has been sorted into six sub modules. They are as follows.

1. $Session\ Key\ Generation\ -\ SSKG(\ )$
2. $Intermediate\ Key\ Generation - INTMKG\ (\ )$
3. $Secret\ Share\ Generation - SECRETSHARES(\ )$
4. $Double\ Tier\ Patients'\ Data\ Encryption - ENCRYPT(\ )$
5. $Authentication\ Realization - AUTH\_CHK$
6. $Decryption\ by\ the\ receipient - DECRYPT\ (\ )$

This protocol is described below by a compact algorithm with modular effects in the following algorithm 1. For the double tier cryptographic system, two proposed set of keys were generated. Such are session key and intermediate key. The session key has been created by the linear congruence and revising the logistics map of chaos theory. A story secret sharing has been proposed on the patients' information with lower time complexity. To improve non linearity in the double tier of encryption, linear and non linear functions were consolidated in this strategy. A thorough authentication structure has been added before the message transmission of the partially encrypted shares inside the COVID-19 telemedicine networks. The idea of linear congruence and Pell's strategy were used to have more power in the validation stage of the proposed frames.

PROPOSED ALGORITHM NO.1 (nDTCS ( ))

Input: $-$ *Plaintext*
Output: $-$ *Encrypted files for n number of recipients*
Methods:
Step 1. *Call SSKG* ( ) // *session key generation using modified logistic map.*
Step 2. *Call INTMKG* ( ) // *intermediate key generation using linear congruence.*
Step 3. *Call SECRETSHARES* ( ) // *partial secret shares have been proposed.*
Step 4. *Call ENCRYPT* ( ) // *file encryption process for generate cipher text for secure transmission.*
Step 5. *Call AUTH_CHK* ( ) // *Authentication check.*
Step 6. *Call DECRYPT* ( ) //*decryption process for generate plain text.*

All these steps have been illustrated below in brief. Here public key of patient means the patient-id provided by the hospital or clinic.

6.1 Session Key Generation

Session key is a secret key for symmetric encryption which is used for a particular transaction or session and is valid for a small period of time. In our scheme modified logistic map is used to create the session key. At first the user chooses the numbers within the range of control parameter and initial values. The session key length is also by chosen by user.

PROPOSED ALGORITHM $-$ **1.1** (***SSKG*** ())
Input: *values within range of control parameter and initial values*
Output: *session key*
Methods:
Step 1: *Set* x, r, *as double and* n, i *as integer.*
Step 2: x & $r \leftarrow$ *get input within range from user.*
Step 3: $n \leftarrow$ *key length.*
Step 4: *For* $i = 0$ *to* $(n-1)$*step size* 1
Step 5: $x_n = r * x_n(1.0 - x_n^2)(1.0 - x_n)$ // *the values of* x_n *are the required session key.*
*Step*6: *End for*

This session key is used to generate cipher text from plain text and vice-versa. This established session key provides confidentiality for subsequent communication and for each session the session key will be new. This key is sent to the recipient end through a frame structure which is described later.

6.2. Intermediate Key Generation

In our scheme we have used the intermediate key for authentication checks between two patients and also for encryption process. Here intermediate key has been generated by using two public keys of two patients. So the intermediate key may vary for different pair of patients and also session. To generate intermediate key we have used the concept of linear congruence in number theory, three variables linear function and Pell's formula. The details algorithm is given below.

PROPOSED ALGORITHM $-$ **1.2** (***INTMKG*** ( ))
Input: *Two public keys of two patients and four constants.*
Output: *Intermediate key.*
Methods:
Step 1. *Set* $d, i, len, fval$ *as integer* (*as global variable*).
Step 2. *Set* imk [], ps[], pr[] *as integer array.*
Step 3. *Set* $fval \leftarrow$ *Call* ***Key_Defn***( )/* *the key_fn*( ) *is a module which provides a value in key generation.*/
Step 4. pr [] $\leftarrow$ *public key of receiver.*
Step 5. ps[] $\leftarrow$ *public key of sender.*
Step 6. $len \leftarrow$ *get_length* (*receiver's or sender's public key*).
Step 7. *For* $i = 0$ *to len*
Step 8. $ps[i] \leftarrow ps[i]$ *XOR d and* $pr[i] \leftarrow pr[i]$ *XOR d.* /* *d is a random value between the lowest ascii value of sender and highest ascii value of receiver.*
Step 9. *If* ($gcd(ps[i], fval) == 1$) *then*
Step 10. $imk[i] \leftarrow$ *call linear_congr* $(ps[i], pr[i], fval)$ {/* *linear congruence, the equation*

$ps[i]x \equiv pr[i]\ (mod\ fval)$ *provides unique solution* ($Theorem1$) *which is stored in* $imk[]$.
This is the required intermediate key.$*/\}$
Step 11. *else* $imk[i] \leftarrow$ *call* $linear\_congr\ (ps[i]+1, pr[i], fval)$
Step 12. *End if*
Step 13. *End for*
Step 14. *Stop*

PROPOSED SUB ALGORITHM $-$ **1.2.1** (***Key_Defn*** ( ))
Input: *Public keys of patient, and public key of doctor*
Output: *Intermediate Integer Value for Key Generation*
Methods:
Step 1. *Set* $n_1, n_2, n_3 \ n_4, d_1, d_2$ *as integer variables*
Step 2. $d_1 \leftarrow$ *Value chosen by user and* $d_2 \leftarrow$ *value chosen by user.*
Step 3. n_1 & $n_2 \leftarrow$ *randomChar (public key of sender) such that* $(n_1 \sim n_2) \geq d_1$. *If it is not possible to get such numbers* $n1$ *and* $n2$ *with said condition then we take* $n1$ *and* $n2$ *such that* $(n1 \sim n2)$ *nearest to* d_1.
Step 4. n_3 & $n_4 \leftarrow$ *randomChar (public key of receiver) such that* $(n_3 \sim n_4) \geq d_2$. *If it is not possible to get such numbers* n_1 *and* n_2 *with said condition then we take* n_1 *and* n_2 *such that* $(n1 \sim n2)$ *nearest to* d_2.
Step 5. *We get two numbers for each* $n1, n2, n3, n4$ *respectively using the Pell's equation* ($x^2 - ny^2 = 1$).
Thus we get 8 *numbers in total.*
Step 6. *The modulus operation is done on* 8 *numbers by average of* (d_1, d_2).
Step 7. *Variable number of times the shuffle operation is done on* 8 *numbers.*
Step 8. *First three or four numbers are used for constant terms in a three variable linear function* $f(x, y, z)$ *and again after shuffle operation remaining numbers are used for values of* x, y *and* z *in the function. This module returns the functional value which is used for key generation.*
Step 9. *End sub procedure.*

This intermediate key is transmitted to the recipient end through secured channel before encryption. In recipient end this key is used for authentication purpose and decryption purpose.

6.3 Secret Share Generation

The art of disguising data into multiple components in a new concept has been proposed in this paper. In fact, those multiple components are being treated as individual shares. In COVID-19 telemedicine, patients' data is being dismantled into different disguised components. We have got no restrictions on the number of recipients. Let it be n number of recipients receiving the different shares. The obligatory thing is that all the partial shares are mandatory to restructure the original patients' data. All the proposed shares will have plenty of missing binary bits. The algorithmic approach has been mentioned in the following algorithm.

An extra added feature on the proposed secret sharing can be stated as modular coupling. An intelligent methodology concerning shares is tied in with destroying the patients' data into more modest fractional encoded components. Its insider facts have the secrecy without entire data. The fundamental piece of this sort of proposed share generation is that each share has a type of highlights of software coupling. In the event of dismantling the COVID-19 patients' data into number of fragments, say $n_1, n_2, \ldots, n_n$. The concept seclusion is kept up at most. The greatest benefit of such a utilization of secluded idea concerning is that it offers the retransmission of only debased shares can be done. The negative mark of applying the procedure of seclusion on shares ages is that the time intricacies will increment both at the patient and doctor.

PROPOSED ALGORITHM $-$ **1.3** (***SECRETSHARES*** ( ))
Input: k *number of recipients* & *Patient's data.*
Output: *Secret Shares for* n number of recipients
Methods:
Step 1: From n number of total recipients we can choose any k number of recipients to send message; k<=n.

Step 2: A unit matrix of order kxk is taken.
Step 3: Random shuffling all the rows and columns of the unit matrix.
Step 4: Bitwise AND on row-wise data set.
Step 5: Bitwise ORing of Step 4 leads to secret shares.

6.4 DOUBLE TIER ENCRYPTION

In this phase the intermediate key and session key took part in the encryption process. To provide nonlinearity in encryption process we have used circular left shift (CLS) operation in encryption process. A two variable non-linear function ($fn\_enc\ (session\ key, intermediate\ key)$) has been used where ASCII value of each character of session key and intermediate key and their difference is used to calculate functional value. The functional value is used as the number of times the circular left shift occurs. We have used a non linear function so the output of the function is not linear with input and this provides an extra non linearity in cipher text. This type of double encryption with session key and intermediate key provides extra robustness in our technique. In both cases XOR [19] operation is done with a CLS operation at end. An example is given below.

Example: Let $fn\_enc(x, y) = \frac{x^2}{y} + y^3$ be a non-linear function, where y= ASCII value of each character of session key, x= ASCII value of each character of intermediate key.
Now $m = fn\_enc(x, y)\%\ (ascii\ \_diff)$, where *ascii_diff*= the ASCII difference between each character of intermediate key and session key. The functional value m is used as the number of times the circular left shift occurs in each character of partial cipher text to generate final cipher text. The encryption algorithm is given below.

PROPOSED ALGORITHM- 1.4 (ENCRYPT ( ))

$Input: -\ Patient's\ Data(Pd), Intermediate\ Key(Ik), Session\ Key(Sk).$
$Output: -\ Encrypted\ file\ for\ n\ number\ of\ recipients$
$Method: -$
$Step\ 1.\ Set\ m\ as\ integer, plain\_file\ as\ plain\ text\ file\ and\ cipher\_file, cipher\_final\ as\ cipher\ text\ file.$
$Step\ 2.\ Set\ output_{file}\ as\ temporaryworking\ file.$
$Step\ 3.\ If\ (!\ eof\ )\ then$
$Step\ 4.\quad output\_file = bit\_XOROP\ (Pd, Sk)$
$Step\ 5.\quad cipher\_file = bit\_XOROP\ (output\_file, Ik)$
$Step\ 6.\quad m = fn\_enc\ (Sk, Ik)\quad /*\ one\ example\ is\ given\ above.*/$
$Step\ 7.\quad Cipher\_final = cipher\_file \lll m.\quad //\ circular\ left\ shift\ operation.$
$Step\ 8.\ End\ if$
$Step\ 9.\ End$

6.5 Authentication Realization

After finishing encryption process we have created a rigorous frame structure (transmission file) with four attributes such as Header, Cipher text, Tail_msg and Padding using the module AUTH_CHK ( ) [35]. MD-5 hash function has been used to generate hash value of intermediate key. The module provides a compact fame format which is ready for transmission to the receiver end.

PROPOSED ALGORITHM- 1.5 (AUTH_CHK ( ))

$Input: -\ Intermediate\ key, Session\ key, cipher\ text\ and\ d_1\ , d_2\ chosen\ by\ user.$
$Output: -\ transmission\ file\ (trans\_file).$
$Methods:$
$Step\ 1: For\ i = 0\ to\ n$
$Step\ 2.\ Set\ imk\ [\ ], ssk\ [\ ], Padding\ [\ ], Header\_msg\ [\ ], Tail\_msg[], enc\_val[]\ as\ integer\ array.$
$Step\ 3.\ Set\ trans\_file\ as\ a\ file.\qquad \{/*\ this\ file\ is\ transmitted\ to\ the\ receiver\ end\ */\}$
$Step\ 4.\quad imk\ [\ ] \leftarrow intermediate\ key\ and\ ssk[\ ] \leftarrow session\ key.$
$Step\ 5.\quad Padding\ [] \leftarrow hash\_ValOf(imk[]).$
$Step\ 6.\quad Header\_msg\ [\ ] \leftarrow hash\_ValOf\ (imk[\ ] \ll ((d_1 + d_2)/4))\ XOR\ ssk\ [\ ].$
$Step\ 7.\quad Tail\_msg[\ ] \leftarrow enc\_val[\ ]\ \{/*\ enc\_val[]\ contains\ encrypted\ value\ of\ d_1\ and\ d_2.*/\}$
$Step\ 8.\quad trans\_file \leftarrow Call\ concate\_text\ (Header\_msg\ [\ ], cipher\ text, Tail\_msg[], Padding[]).$
$Step\ 9.\ End\ for$
$Stop\ 10.\ Stop$

If the key size is 16 byte then total frame structure for transmission is given below which is created by the function AUTH_CHK ( ).

Fig 1: Proposed Frame Structure for authentication (Single Destination)

The Tail_msg part of transmission file contains encrypted value of two constants (d_1, d_2). This encryption is done by RSA technique. Padding field contains hash value of intermediate key. This padding field is used for authentication purpose. The session key is recovered from header part using CLS operation and the intermediate key.

6.6 Decryption Phase: -In decryption phase, at first receiver generates intermediate key by calling IMKG ( ) and then check authentication using hash value of intermediate key from padding field. After finishing authentication check, session key is generated from HEADER_MSG of transmission file and then decryption process is started using two keys. The entire decryption process is given below by a compact algorithm.

PROPOSED ALGORITHM- 1.6 (DECYRYPT ( ))

$Input$: $Intermediate\ key, cipher\ text.$
$Output$: $Plain\ text.$
Methods:
$Step1.\ Set\ a, n, i\ as\ integer\ and\ ssk\ [\ ], imk\ [\ ]\ as\ integer\ array.$
$Step2.\ Retrieve\ d_1\ and\ d_2 from\ TAIL\_MSG\ of\ transmission\ file\ or\ frame\ structure.$
$Step3.\ imk\ [\ ]\ \leftarrow\ intermediate\ key.$
$Step4.\ Call\ AUTHEN\_CHK\ (imk\ [\ ], trans\_file).$
$Step5.\ if\ (true)\ then$
$Step6.\ ssk\ [\ ]\ \leftarrow\ get\_SessionKey(\ Header\_msg\ of\ trans\_file, d_1, d_2)./*\ session\ key\ generation\ */$
$Step7.\ \ Decryption\ process\ is\ done\ with\ two\ keys\ which\ is\ reverse\ of\ encryption\ process.$
$Step8.\ else\ \ \ Print\ Authentication\ fails.$
$\quad end\ if$
$Step9.\ Stop.$

7. Result and Discussion

The above algorithms were implemented in latest version of Python in a high speed laptop of Core $i9$ (tenth generation or newer) processor, operating system of MS Windows $10x64$ bits, $16GB$ RAM and 2TB internal storage. In this section, simulations of the results on the proposed method have been presented in details. In our experiments, several sizes of different types files were used as source inputs.

A good cryptographic technique should be robust against different types of cryptanalytic, statistical and brute-force attacks. In this section, we have discussed different type's security analysis of like key space analysis, graphical analysis, etc. Different types of randomness analysis, sensitivity analysis, statistical analysis and functionality analysis on our proposed encryption scheme have been reflected in the following sub sections [16, 35].

7.1 Key Randomness Test

Randomness means all elements of the sequence are generated independently of each other, and the value of the next element in the sequence cannot be predicted, regardless of how many elements have already been produced. Random and pseudorandom numbers generated for cryptographic applications should be unpredictable (forward and backward). The outputs of a PRNG are deterministic functions of the seed; i.e., all true randomness is depended on seed generation. An RNG uses a nondeterministic source i.e., the entropy source. Here we have used RNG and modified logistic map for generating numbers with true randomness. These random numbers are used for generation of session key. To prove the randomness of our session key we have used serial test [36-38]. The following equation 2 is used for serial test.

$$X = \frac{4}{(n-1)}(n_{00}^2 + n_{01}^2 + n_{10}^2 + n_{11}^2) - \frac{2}{n}(n_0^2 + n_1^2) + 1 \quad \ldots (2)$$

This approximately follows a χ^2 distribution with 2 degrees of freedom if n ≥ 21. The table 1 is given below.

Table 1: Serial test results obtained on Session Key

Serial Number	Session Key Size (in bytes)	Result of proposed technique	Result of only PRNG()[39]	Result of only RNG()[40]
1	16	1.125	1.092	1.082
2	24	1.202	1.022	1.011
3	36	1.264	1.145	1.204
4	48	2.126	2.108	2.135
5	56	11.040	8.984	10.036
6	64	19.170	17.589	18.048

For a significance level of α = 0.05, the threshold values of X for serial test values were1.125, 1.202, 1.264, 2.126, 11.040, 19.170 respectively. Thus the sequence generated by the above algorithm passes serial test for the proposed session key.

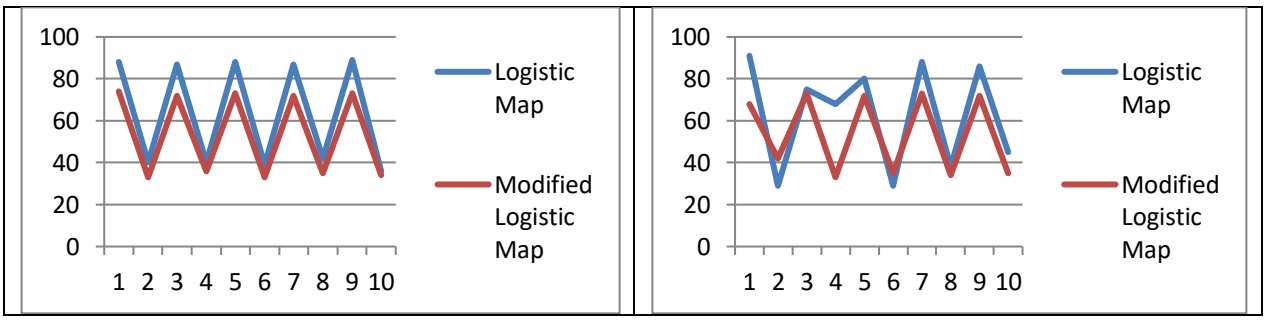
Table 2: Serial test results obtained on Intermediate Key

Serial Number	Intermediate Key Size (in bytes)	Result of Proposed technique	Result of only PRNG()[39]	Result of only RNG()[40]
1	16	1.037	1.012	1.067
2	24	0.912	0.954	0.901
3	36	1.184	1.048	1.269
4	48	2.113	2.009	2.085
5	56	10.520	10.412	10.016
6	64	14.181	14.004	13.258

Again considering the significance level of α = 0.05, the threshold values of X for serial test values were1.037, 0.912, 1.184, 2.113, 10.520, and 14.181. Thus the sequence generated by the above algorithm passes serial test for the intermediate key.

7.2 Comparison between Proposed Modified Logistic Map & Standard Logistic Map

In chaos theory, it has been noted that within a specific range (r) based on the fixed initial condition (x), chaotic characteristics would occur. This works has found chaotic sequence in the ranges of $r = [0.4,0.5], r = [0.6,0.64]$, and $r = [0.9,0.97]$ on their initial values $x = 3.65, 3.84$, and 3.90 respectively. The following figure 2 shows the sensitivity analysis on initial condition between logistic map and proposed modified logistic map.



r=3.65 and x=0.4	r=3.65 and x=0.5

Fig 2(a): Comparison at condition 1

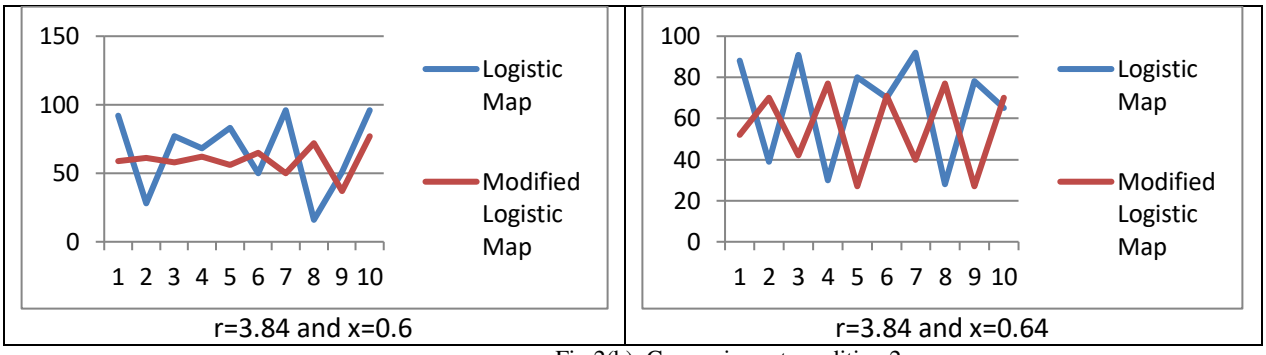


Fig 2(b): Comparison at condition 2

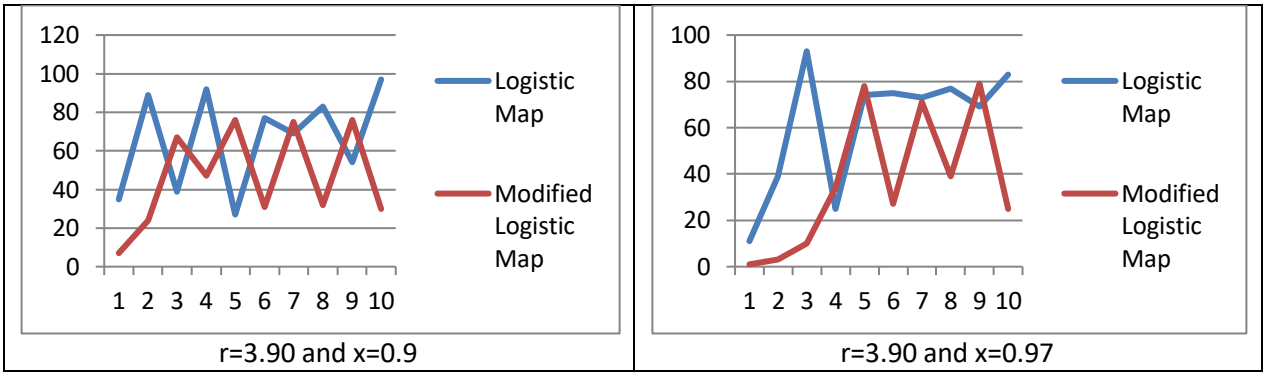


Fig 2(c): Comparison at condition 3

For a given initial state, the future state can be predicted from a deterministic system. But for chaotic systems, long term prediction of nature of trajectories is impossible. 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. From the above figure 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. This attribute has been considered in the proposed session key and intermediate key generation in COVID-19 telemedicine.

7.3. Graphical Analysis

Now-a-days different types of statistical attacks and statistical analysis are used by the intelligent intruders or hackers to analyze the cipher text for decryption. Therefore, an ideal cipher text should be robust against any statistical attacks. To prove the robustness of our proposed encryption scheme, we have performed statistical analysis by calculating the histogram, avalanche effect and randomness by calculating serial test.

7.3.1 Shares' Histogram Analysis

A text-histogram illustrates [37] [41- 42] how characters in a text are distributed by graphing the number of characters at each level. Here histogram analysis is done on the several encrypted as well as its original text files that have widely different content. We have shown the encrypted files of the original files (plain text) using the session and intermediate keys '$\boldsymbol{ecryption@12375}$' and '$\boldsymbol{muCWc182018AB81}$'. In this scheme, three number of COVID-19 telemedicine recipients were considered (n=3). Three secret shares generated by this technique were simultaneously compared with normal plain text as shown in the following figure 3.

***Session Key*:-'*encryption@12375*'**

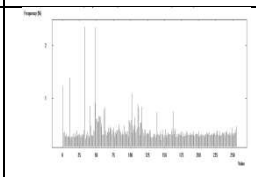
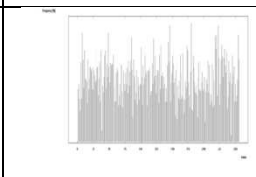
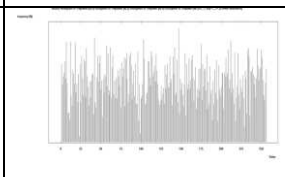
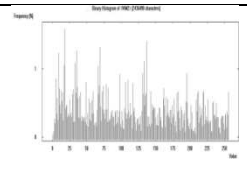
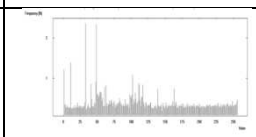
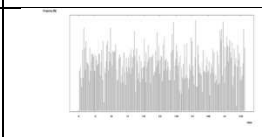
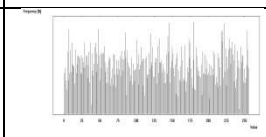
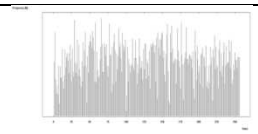
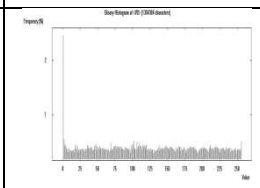
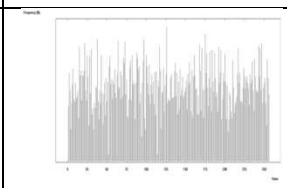
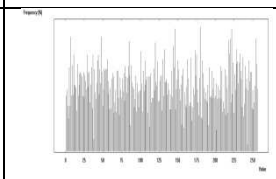
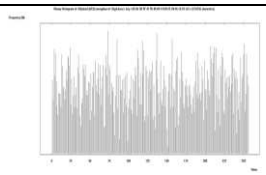
Intermediate Key:- 'muCWc182018AB81'				
FILE TYPE	PLAIN TEXT HISTOGRAM	HISTOGRAM OF CIPHER TEXT OF PROPOSED SECRET SHARE 1	HISTOGRAM OF CIPHER TEXT OF PROPOSED SECRET SHARE 2	HISTOGRAM OF CIPHER TEXT OF PROPOSED SECRET SHARE 3
TEXT(.txt)				
PDF (.pdf)				
WORD (.docx)				

Fig.3: Histogram Analysis

It is clear from the figure 3 that the histograms of the encrypted files are fairly uniform and significantly different from the respective histograms of the original files (plain text) and hence does not provide any clue to employ any statistical attack on the proposed encryption procedure.

7.4 Shares' Entropy Analysis

The measurement parameter of entropy indicates the randomness of the secret shares generated by the proposed nDTCS. It avoid further predictability factor. The proposed system may contains any character in the ASCII range less than 256. Each character is represented by eight bits in the cipher text. It can be evaluated through the following equation 3.

$$E_i = -\sum_0^{256} ln\ PR * log_2(PR) \quad \ldots(3)$$

Here, $E_i$means the entropy of the corresponding secret shares, PR means the equal probability distribution on the cipher text. The following table 3 displays the entropy values of the secret shares generated by the proposed technique.

Table 3: Entropy on proposed shares

FILE TYPE	PLAIN TEXT ENTROPY	ENTROPY OF CIPHER TEXT OF PROPOSED SECRET SHARE 1	ENTROPY OF CIPHER TEXT OF PROPOSED SECRET SHARE 2	ENTROPY OF CIPHER TEXT OF PROPOSED SECRET SHARE 3
TEXT(.txt)	5.63	7.45	7.48	7.41

PDF (.pdf)	6.38	7.05	6.96	7.18
WORD (.docx)	7.12	7.36	7.25	7.49

7.5 Session Key Sensitivity

An ideal encryption technique should be sensitive with respect to the secret key i.e. a single bit change in the secret key should produce a completely different cipher text. For testing the key sensitivity of the proposed encryption procedure, we have performed the encryption process in the files (.txt) with slight changes in the secret key. The avalanche effect is shown below only for changed session key and with fixed intermediate key. The following table 4 and graph (Fig. 4) shows the total scenario.

Table 4. Changes in the Session Key

Key	ASCII Difference	Total number of added characters	Total number of deleted characters	Total number of changed characters
encryption@12345	0	3526	3545	2540
e**c**cryption@12345	7	3716	3710	2362
encry**d**tion @12345	8	3860	3838	2271
encryption @1234**6**	107	3928	3876	2217
encryption **#**12345	29	3615	3610	2458
encryptin**n** @12345	80	4262	4245	1892
encryption @1234**z**	7	3795	3778	2314
encryption @12**4**45	118	3868	3845	2245
encryption @**0**2345	4	4105	4081	2049
Encryption @12345	65	4091	4088	2032

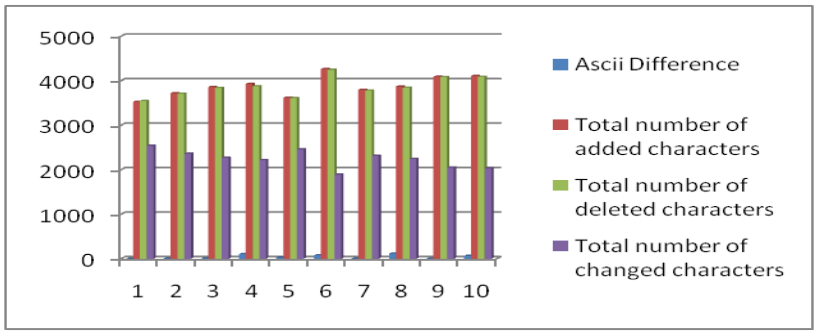


Fig. 4. Graph for the changes in the Session Key

We have shown the results of some attempts to decrypt an encrypted file with slightly different secret keys than the one used for the encryption of the original file. The above table 4 shows the added characters, deleted characters and changed characters with slight change (one byte) in session key and the above graph (Fig.5) also shows the increasing and decreasing performance among added characters, deleted characters and changed characters for one byte change in key. It is clear that the decryption with a slightly different key fails completely and hence the proposed encryption procedure is highly key sensitive.

7.6 Key Space Volume Security

The total number combination of key search space is greater than 2^{100} as proposed by Alvarez G. et al. [43]. Ismail S.M. et al. [44] had proposed a crypto system with 2^{192} number of combinations. On the other hand, this paper has proposed two keys i.e. session key and intermediate key of same length. Due the dynamicity of the key length, let us suppose it to be length L. The volume of the proposed key search space may be calculated with the following equation 4.

$$2^L * 2^L = K \qquad \ldots (4)$$

Here, L denotes the session key length and intermediate key length, K is the number of possible keys. The following table 5 will show the efficacy of the proposed technique in terms of key space security on COVID-19 telemedicine.

Table 5. Key Search Possibilities

Key length (L)	No. of Possible Keys(K)	Observation
8	2^{64}	Low Security
16	2^{256}	Good Security
32	2^{1024}	Moderate Security
64	2^{4096}	Moderate Security
128	2^{16384}	Higher Security
256	2^{65536}	Extremely High Security

7.7 Significance of Authentication

The identity proof is done by Authentication mechanisms [45-48]. The authentication process ensures the originality of document that is the document is coming from right person or not. In secure system mainly in medical Internet domain, the user must identify himself / herself, and then the system will authenticate the identity before using the system because without proper authentication medical data transmission may occur severe damage in patient party. The authentication process can be professionally seen as: 1) SMS based authentication 2) Intermediate key based authentication 3) Public key authentication. The intermediate key based authentication and public key based authenticity are used in our proposed system, the user shares a single session key with an algorithm named, RSA which provides public key authentication. The hash value of amalgamation of two keys i.e., 1st part of intermediate key and 2nd part of session key is concatenated with the plain text. In recipient's side, the receiver gets session key using RSA technique and generates intermediate key using above stated algorithm and after checking the hash value using Algorithm-4 of our scheme, the sender decides whether the message has come from right person or not.

7.8 Different Medical Data Attacks

7.8 .1 Replay Attacks

Replay attack [34] [49] is one type of network attack in which an attacker detects a data transmission and it has delayed or repeated fraudulently. As a result attacker can gain access to a network, gain vital information from other or complete a duplicate transaction. An attacker may launch a replay attack to delay or even stop the response to any request message. To defend against replay attack in this article the concept of session key is used and in every session the session key is fresh. Thus when attacker retransmit or has delayed to send message then the previous key may not work.

7.8.2 Data Tampering Attacks

An attacker tampers [50 - 51] other users' information or data using tampering attack. An attacker may launch a tampering attack to a smart system if it intends to change data illegally. In our proposed methodology, we have introduced a rigorous frame structure with multiple attributes. Among the multiple attributes the cipher text is one so it is hard to detect the range of cipher text. Thus the attacker cannot launch tampering attack easily.

The above comparative analysis shows strength of our plan. The proposed convention gives greater usefulness like solid client verification, common confirmation between the two patients, it sets up a safe session key for the client i.e., patients and these are the central prerequisites for remote medical care applications. It is worth notification that our proposed convention gives imperative security highlights. The accompanying table gives the relevance of our approach contrasted with other existing methods.

7.8.3 Classical Attacks

Based on the cryptanalytic attacks, there could be little bit of information available to the cryptanalysis. There are four types of such attacks on the proposed COVID-19 telemedicine.

Cipher text: Tricksters can get only the cipher text. The plain text is made unavailable to them.
Known plain text: Only a specific plain text and cipher text is available to the tricksters. Rest to the session will be decoded by them.
Chosen plain text: Here the encryption algorithm and plain text is made accessible to the tricksters. From there, they generate their own cipher text. Hence the session key would be decoded by them.
Chosen cipher text: Decryption technique is known to the tricksters. They can detect the plain text on the reverse processing.

7.9 Evaluation of Modular Time Complexity

The overall time complexity of any telemedicine is dependent on all the modules. That means the phenomenon of coupling exists in this sub section. It is always desirable to have low time complexity. Modular time complexity of nDTCS has been shown in the following table 6. This method has been divided into six modules, Session Key Generation, Intermediate Key Generation, Secret Share Generation, Double Tier Encryption, Authentication Realization, and Decryption.

Table 6. Modular Time Complexity Generation

This Work Modules	Time Complexity Observed	Comment(s)
Session Key Generation	$O(k)$	k is the length of the session key.
Intermediate Key Generation	$O(k)$	k is the length of the session key.
Secret Share Generation	$O\ (n)$	n is the number of recipients.
First Tier Encryption	$O\ (k^2)$	k is the length of two keys.
Double Tier Encryption	$O\ (n * k^2)$	n is added for secret sharing.
Authentication Realization	$O\ (n)$	n is the number of secret shares.
Decryption	$O\ (n)$	n is the number of recipients.

8. Efficacy under Comparative Studies

A comparison table was made to prove the efficacy of the proposed nDTCS on COVID-19 telemedicine. In the first table this work has been compared with the classical algorithm likes of IDEA, AES and 3DES [52-53]. The following table 7 contains its outcome.

Table 7. Comparative Study with classical cryptography

Sl. No.	Attributes	IDEA	3DES	AES	This Work
1	Block Length	16	64	128	Dynamic (L)
2	Key Length	128	168	128/192/256	Dynamic (L)
3	Key Space Size	2^{128}	2^{168}	$2^{128}/2^{192}/2^{256}$	2^{2L}
4	Data Transmission Volume	Medium	Medium	High	High
5	Cipher Type	Symmetric Block	Symmetric Block	Symmetric Block	Secret Sharing
6	Primitive Algorithm	Fiestel Cipher	Fiestel Network	Substitution Permutation Network	Chaotic Keys Generation, XOR Encryption, Authentication of Shares, & Decryption
7	User Flexibility	Average	Average	High	High
8	Vulnerabilities		Prone to Brute Force Attacks	Prone to Side Channel Attacks	Less prone to attacks
9	Time Complexity	Average	High	Low	Low

9.Conclusion

There are various sorts of difficulties in medical services framework at present COVID-19 time. The utilization of technology in medical services framework show fascinating new turns of events. They can upgrade and improve medical care capacities, help preventive consideration and encourage collective medical services. An essential methodology is vital for medical services framework which stands significant viewpoints like security and security insurance during this pandemic. In this paper, we have built up a novel Double Tier Cryptographic System (nDTCS) where an encryption procedure is introduced which is dependent on two keys. To give the more non linearity in text we have utilized round about left move activity with a non straight capacity in the encryption method. Our method additionally gives the verifications which improve the strength just as magnificent encryption strategy. Distinctive test results demonstrate the possibility and effectiveness of the proposed technique. Our technique has observed chaotic sequence in the ranges of $r = [0.4,0.5], r = [0.6, 0.64]$, and $r = [0.9, 0.97]$ on the initial values $x = 3.65$, 3.84, and 3.90 respectively. Relative investigation among proposed strategy and standard procedures, comprehensive key pursuit examination, grave

examination shows the agreeableness of our method. To the most amazing aspect our insight our proposed strategy is the least complex one having insignificant computational overhead during encryption, decryption [54]. The relevance of patients' data privacy has attributed towards the revolutions in the COVID-19 telemedicine.

10.Limitations of the technique with Future Scope of Work

This paper deals with novel Double Tier Cryptographic System (nDTCS) with dual key generation. These keys are: session key and intermediate key, generated through linear congruence and chaos theory. First one is used for COVID-19 telemedicine cryptographic function, and the second one has been utilized for the authentication realization of secret shares and second round of encryption. The limitation of this technique is that both such keys are of the equal length. Another limitation is the implementation of unit matrix in the proposed secret share generation scheme. Elementary operation were carried out on it for randomized shuffling.

In future, this work can be extended to machine learning based training and outcomes. So that its modules can automatically be simulated through advanced machine learning techniques.

Acknowledgement

Authors do acknowledge the moral and congenial atmosphere support provided by Maharajadhiraj Uday Chand Women's College, B.C. Road, Uttar Fatak, Burdwan, West Bengal 713104, India.

Compliance with Ethical Standards: Not applicable.

Conflict of Interest: There is no conflict of interest.

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

References

1. 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.

2. Jordan, R. E., Adab, P., & Cheng, K. K. (2020). Covid-19: risk factors for severe disease and death. BMJ,368, m1198.

3. Kadir, M. A. (2020). Role of telemedicine in healthcare during COVID-19 pandemic in developing countries. Telehealth and Medicine Today.

4. Thiagarajan K. Covid-19: India is at centre of global vaccine manufacturing, but opacity threatens public trust BMJ 2021; 372 :n196 doi:10.1136/bmj.n196.

5. Covid-19: Indian health officials defend approval of vaccine. BMJ2021;372:n52.pmid:33414156.

6. A. Das and C. E. Veni Madhavan, Public-key Cryptography: Theory and Practice, Pearson Education, in press.

7. D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, in Kilian, J. (ed.) *CRYPTO2001*. LNCS, vol. 2139, (Springer, Heidelberg, 2001), pp. 213–229

8. W. Stallings, Cryptography and Network Security: Principles and Practice, third edition, Prentice Hall, 2003.

9. Bokolo, A.J. Application of telemedicine and eHealth technology for clinical services in response to COVID-19 pandemic. Health Technol. 11, 359–366 (2021). https://doi.org/10.1007/s12553-020-00516-4.

10. Bokolo AJ. Exploring the adoption of telemedicine and virtual software for care of outpatients during and after COVID-19 pandemic. Ir J Med Sci (1971-). 2020:1- https://doi.org/10.1007/s11845-020-02299-z.

11. Kapoor A, Guha S, Das MK, Goswami KC, Yadav R. Digital healthcare: The only solution for better healthcare during COVID-19 pandemic?. Indian Heart J. 2020.

12. Kotian RP, Faujdar D, Kotian SP, D'souza B. Knowledge and understanding among medical imaging professionals in India during the rapid rise of the covid-19 pandemic. Health and Technology, 2020:1-6.

13. D. Stinson, Cryptography: Theory and Practice, third edition, Chapman & Hall/CRC, 2006.

14. A. Agrawal, S. Gorbunov, V. Vaikuntanathan, H. Wee, Functional encryption: New perspectives and lower bounds, in R. Canetti, J.A. Garay, (eds.) *CRYPTO 2013, Part II*. LNCS, vol. 8043. (Springer, Heidelberg, 2013), pp. 500–518.

15. Kumar, V. (2015). Ontology Based Public Healthcare System in Internet of Things (IoT). *Procedia Computer Science*, *50*, 99–102. doi:10.1016/j.procs.2015.04.067.

16. Ghansela S. , Network Security: Attacks, Tools and Techniques, IJARCSSE Volume 3, Issue 6, June 2013.

17. Olivier, F., Carlos, G., & Florent, N. (2015). New Security Architecture for IoT Network.*Procedia Computer Science*, *52*, 1028–1033. doi:10.1016/j.procs.2015.05.099

18. J.C. Yen, J.I. Guo, A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000, pp. 49–52.

19. Chaudhry, S.A., Naqvi, H., Sher, M. et al. An improved and provably secure privacy preserving authentication protocol for SIP. Peer-to-Peer Netw. Appl. 10, 1–15 (2017). https://doi.org/10.1007/s12083-015-0400-9.

20. A. Kak, “Lecture Notes on Computer and Network Security”, 2015, Purdue University [Online] Available: https://engineering.purdue.edu/kak/compsec/Lectures.html.

21. Zaidan B, Zaidan A, Al-Frajat A, Jalab H. On the differences between hiding information and cryptography techniques: An overview Journal of Applied Sciences. 2010; 10:1650–5.

22. Maia, P., Batista, T., Cavalcante, E., Baffa, A., Delicato, F. C., Pires, P. F., & Zomaya,A. (2014). A web platform for interconnecting body sensors and improving health care. *Procedia Computer Science*, *40*, 135–142. doi:10.1016/j.procs.2014.10.041.

23. C. Joshi, and U.K. Singh, “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) Volume 5, Issue 1, January 2015, pp 742-747.

24. Keesara S, Jonas A, Schulman K. Covid-19 and health care’s digital revolution. N Engl J Med. 2020.

25. Bindra, V. 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 (2020). https://doi.org/10.1007/s13224-020-01346-0

26. Whaibeh E, Mahmoud H, Naal H. Telemental Health in the Context of a Pandemic: the COVID-19 Experience. Curr Treat Options Psychiatry. 2020:1.

27. Zhou X, Snoswell CL, Harding LE, Bambling M, Edirippulige S, Bai X, Smith AC. The role of telehealth in reducing the mental health burden from COVID-19. Telemedicine and e-Health. 2020;26(4):377–9.

28. Jnr BA. Use of Telemedicine and Virtual Care for Remote Treatment in Response to COVID-19 Pandemic. Journal of Medical System. 2020;44:132. https://doi.org/10.1007/s10916-020-01596-5.

29. Tanaka MJ, Oh LS, Martin SD, Berkson EM. Telemedicine in the era of COVID-19: the virtual orthopaedic examination. J Bone Joint Surg Am. 2020. https://doi.org/10.2106/JBJS.20.00609.

30. J.C. Yen, J.I. Guo, A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000, pp 49–52.

31. J.C. Yen, J.I. Guo, A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000, pp. 49–52.

32. Al Ameen, Moshaddique & Liu, Jingwei & Kwak, Kyung. (2012). Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. Journal of medical systems. 36. 93-101. 10.1007/s10916-010-9449-4.

33. Al Ameen, Moshaddique & Liu, Jingwei & Kwak, Kyung. (2012). Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. Journal of medical systems. 36. 93-101. 10.1007/s10916-010-9449-4.

34. L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,” IEEE Transactions on industrial informatics, vol.10, no. 4, pp. 2233–2243, 2014.

35. Bhowmik A., Dey J., Sarkar A., Karforma S., 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.

36. J.G. Chakravorty, P.R. Ghosh, Advanced Higher Algebra, U.N. Dhur and Sons Private Ltd., 2018. ISBN 978-3-80673-67-7.

37. Hong Yaling. Research on computer network security analysis model [J]. Computer CD Software and Applications, 2013(z):1-152.

38. Joydeep Dey, Dr. Sunil Karforma, Dr. Arindam Sarkar, Anirban Bhowmik, "Metaheuristics Guided Secured Transmission of E-Prescription of Dental Disease", International Journal of Computer Sciences and Engineering, Vol.07, Issue.01, pp.179-183, 2019.

39. W. Stallings, Cryptography and Network Security: Principles and Practice, third edition, Prentice Hall, 2003.

40. A. Kak, "Lecture Notes on Computer and Network Security", 2015, Purdue University [Online] Available: https://engineering.purdue.edu/kak/compsec/Lectures.html.

41. Anirban Bhowmik, Dr. Arindam Sarkar, Dr. Sunil Karforma, Joydeep Dey, "A Symmetric Key based Secret Data Sharing Scheme", International Journal of Computer Sciences and Engineering, ISSN 2347-2693, Impact Factor Value, Vol.07, Issue.01, pp.188-192, 2019.

42. 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.

43. Alvarez, G.; Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurc. Chaos 16(8), 2129–2151 (2006).

44. Ismail, S.M., et al.: Generalized double-humped logistic map-based medical image encryption. J. Adv. Res. 10, 85–98 (2018).

45. Arindam Sarkar, Joydeep Dey, Anirban Bhowmik, Dr. J.K. Mandal, Dr.Sunil Karforma, "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, DOI: https://doi.org/10.1007/978-981-13-1540-4_3.

46. N.K. Pareek, Vinod Patidar, K.K. Sud, Cryptography using multiple one dimensional chaotic maps, Commun. Nonlinear Sci. Numer. Simul. 10 (7) (2005) 715–723.

47. J.C. Yen, J.I. Guo, A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000, pp. 49–52.

48. Joydeep Dey, Sunil Karforma, Arindam Sarkar, Anirban Bhowmik (2019). "*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.

49. J. E. Shockley, Introduction to Number Theory, Holt, Rinehart and Winston, New York, 1967.

50. L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santanna, "Internet of things in healthcare: Interoperatibility and security issues," in Communications (ICC), IEEE International Conference on. IEEE, 2012, pp. 6121–6125.

51. 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.

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. Kumari, M., Gupta, S. & Sardana, P. A Survey of Image Encryption Algorithms. 3D Res 8, 37 (2017). https://doi.org/10.1007/s13319-017-0148-5.

54. 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

Proposed Frame Structure for authentication (Single Destination)

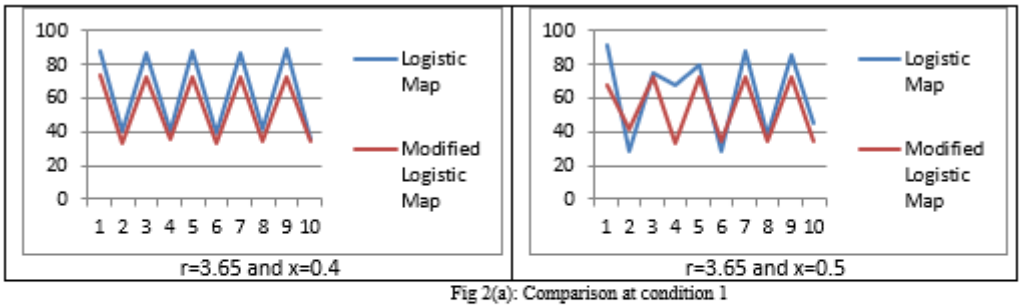


Fig 2(a): Comparison at condition 1

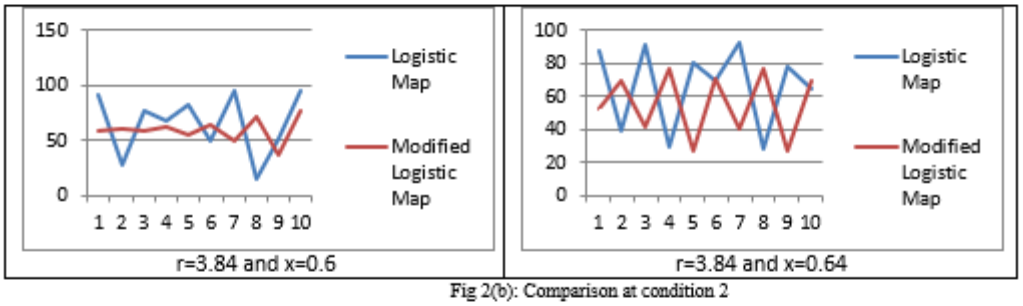


Fig 2(b): Comparison at condition 2

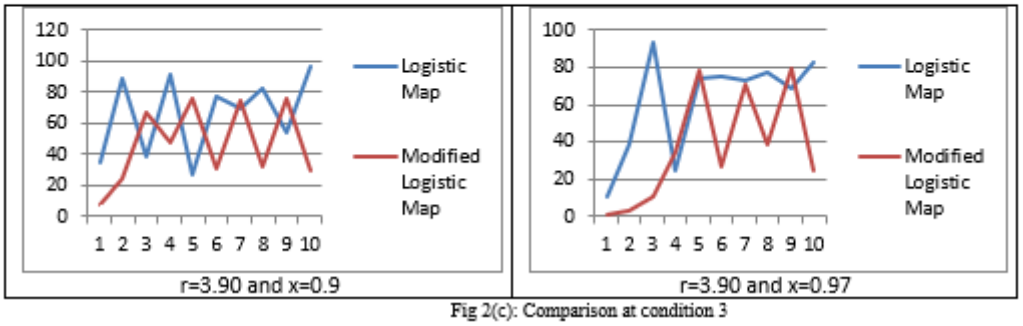


Fig 2(c): Comparison at condition 3

Figure 2

(a): Comparison at condition 1. (b): Comparison at condition 2. (c): Comparison at condition 3.

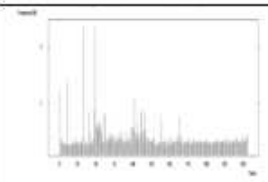
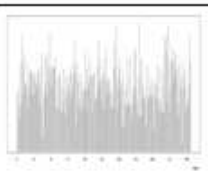
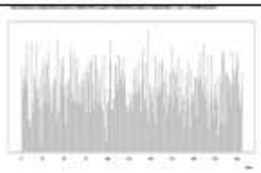
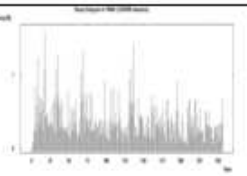
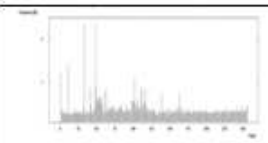
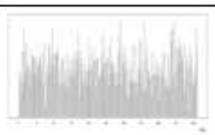
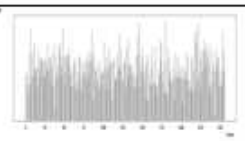
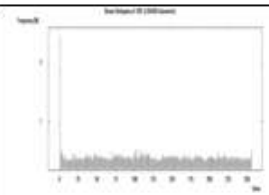
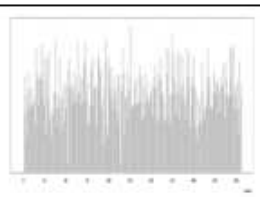
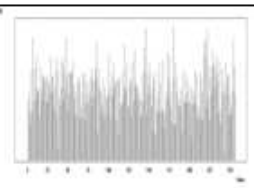
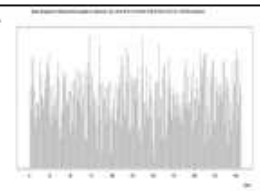
Session Key:-'encryption@12375' *Intermediate Key:- 'muCWc182018AB81'*				
FILE TYPE	PLAIN TEXT HISTOGRAM	HISTOGRAM OF CIPHER TEXT OF PROPOSED SECRET SHARE 1	HISTOGRAM OF CIPHER TEXT OF PROPOSED SECRET SHARE 2	HISTOGRAM OF CIPHER TEXT OF PROPOSED SECRET SHARE 3
TEXT(.txt)				
PDF (.pdf)				
WORD (.docx)				

Figure 3

Histogram Analysis

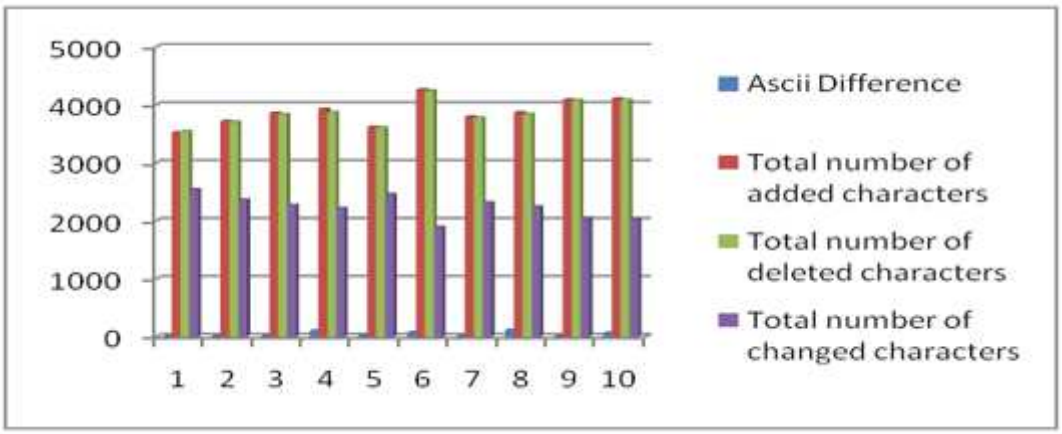


Figure 4

Graph for the changes in the Session Key