Post-COVID-19 Neural Cryptographic Onset of Homeopathy Psychiatry Medicine's Transmission in "New Normal Form"

[1,*]Joydeep Dey, [2]Salim Ahmad

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

[2] Consultant Homeopathic Doctor and Department of Nutrition,
Vidyasagar Uchcha Vidyalaya, Burdwan, India

**Corresponding Author Email: joydeepmcabu@gmail.com*

Abstract:

In telepsychiatric treatments, the medical data of various types of patients' data are to be communicated in a well-protected way between the patient and the psychiatrists. Homeopathy drugs play a significant role in treating such psychiatric patients. The objective of this manuscript is to develop a strong session key with the help of neural cryptography. Neural cryptography is the extensive usage of the artificial neural networks for the cryptographic functions. E-medicines were encrypted here by the classical methods and the proposed session keys of 128 bits long. The length has been selected to 128 bits in order to have less memory space needed. Alzheimer's disease, Dementia, Insomnia, Stress, OCD, Brain restlessness, Depression, etc are the most clinical mental complications observed in this post COVID-19 situations. This is the era of digital health to deal the remote patients who are non-invasive in nature. In this manuscript, a session key has been proposed by the Key Distribution Centre (KDC) with the aid of artificial neural networks. Strong session keys were derived of 128 bits length which in turn used for AES 128 encryption. To avoid the Man-In-The-Middle attacks, it has been designed that the server machine shall accumulate all the needful symptoms of the psychiatric patients.

Keywords: *Psychiatry, Homeopathy E-medicines, Neural Cryptography, Secure Transmission*

1. INTRODUCTION

Telepsychiatric systems have much bigger roles to play in the current society. It had played a crucial role in the COVID-19 period. Telepsychiatric means to provide mental treatments with the help of online modes [1]. Homeopathy treatments were of extreme fruitfulness in such mental health care domain. Easy access to the psychiatrists was done through this approach. Mental care was provided in the remote and underprivileged areas with the help of Internet supports. It decreases the medical costs and travelling costs. Automated examinations can be made possible through such ventures. In this COVID time, the majority of individuals are experiencing mental issues of some kind. The significant causes behind these psychological issues are tension, stress, unfortunate way of life, low eating regimens, hereditary qualities, hormonal imbalance, and so on. There exists such countless issues preferences of disappointment in working spot, cutoff times of works, pressure, stress, comprehensiveness, disappointment in projects, breakdown in positions, and so on. The effect of this COVID-19 is monstrous to such an extent that prompted quick flood in the telemedicine administrations. In the mental fields, larger parts of the patients are not able to visit the specialists because of a few elements. Timidity and mediocrity sensations of the mental patients are to be figured over here. This issue has been tended to in this proposed method. A transmission directed through internet based online interface for the homeopathic mental medications has been proposed here. Patients' clinical information security has been held under gotten plot utilizing information encryption. Smart devices are used to speed up the data processing in the scientific domain is the Internet of Things (IoT). The IoT network may consists of physical devices, sensors, RFIDs, routers, embedded software, etc for the purpose of data communication. Telehealth system based on IoT has emerged as an efficient tool to cure the patients in this COVID era [2]. It has mainly reduced the human efforts and interventions. Cryptography is the science to ensure data security from unwanted access [3-4]. The objective here is to treat the patients using web-portal E-health system. The proposed system works on the symmetric key cryptography. The same key is used at the time of encryption by the psychiatrists, and also at the time of decryption by the patients. The same secret key has been obtained through some of the authenticated key distribution centers (KDC). In symmetric cryptography, a secret key is must for the encryption as well as decryption purposes. So the generation of the session key is compulsory for cryptographic purposes here. In this paper, we have used artificial neural networks to generate the session keys. Before the transmission of the homeopathy psychiatric medicines, the secret key has been transferred to both the parties through protected channel. To counterfeit the Man-In-The-Middle attacks, the proposed approach of generating keys is a suitable technique in such E-Health systems. Online telehealth services are far better in this pandemic situation. Patients can take medicines, consult to their doctors, health check-ups, etc. most importantly, these services are taken from remote locations too. No chances of noscomial infections for the patients. Travelling cost and getting affected by the corona virus is being cancelled.

Serotonin is a hormone which is produced by the human brain. Its enough secretion results in better mood, and deficit results in depression. Psychiatric diseases are also contributed through inheritance. The pivotal thing of this manuscript is that psychiatric patients can avail their homeopathic treatments from their homes during the pandemic era. The transmission of E-medicines in a strong way is the main objective of this proposed technique. Homeopathy is based on the philosophy of curing the patients’ mental and physical health overall. Health is a matched frame of harmony dwelling with mental peace and physical fitness. Homeopathy medicines are selected based on patients’ existing conditions and then potency of the dose is selected. Following are the existing conditions which imparts in determining the homeopathy medicines. They are fear, anxiety, sleep, attitude, stress, dreams, OCD, sense of humor, reactions against common instances, etc. Some common medicines used in homeopathy treatments are listed as follows [5]. Calcarea Carbonica and Aconite can be prescribed for anxiety with palpitations, dry mouth, etc. Ignatia to be used for grief, loss, mood changer, etc. Kali phosphoricum is prescribed for over whelming the wishes that are unrealistics. Such psyciatric patients take too much stress on themselves. Lycopodium may be prescribed due to acute lack of self-confidence. Sepia is given to menopause females with mood swings.

The significant contributions in this paper are as follows. It has allowed Key Distribution Centre (KDC) to generate session keys with the help of neural cryptographic science. Neural cryptography has fast computing capacity when compared with other modes of algorithms. The proposed sets of keys were tested under various numerical tests to conclude the efficacy. No relationships were established between the generated keys which will defend the intruders.

The layout of this manuscript can be done as follows. Section 1 presents the introduction. The related works are being presented in the next section 2. Problem statements are illustrated in the section 3. Proposed frame of work may be mentioned in section 4. Section 5 has the conclusions. At the end, Acknowledgement, Funding, Ethical Statements, and References were presented.

2. RELATED WORKS

Rai S. C. et al. [6] have planned a system to identify the degrees of discouragement by the machine learning tools. Additionally utilizing ML, appropriate treatment is recommended. Be that as it may, they have not referenced with respect to the information transmission security issues. Jiménez-Serrano et al. [7] have fostered a portable E-wellbeing application to distinguish post pregnancy anxiety with the assistance of machine learning. Mdhaffar A. et al. [8] had proposed a method on Deep Learning for sadness identification utilizing smart phones. Their method had shown good outcomes. Mowery D. et al. [9] has displayed in their paper "Figuring out Depressive Symptoms and Psychosocial Stressors on Twitter". Naude F. D. et al. [10] had studied the efficacy of homeopathic simillimum in treating insomnia. Viksveen P. et al. [11] had run a randomized controlled trial on the depression treatments by the help of homeopathy medicines. Adler C. et al. [12] had also executed randomized study in connection with the depression treatments with homeopathy medicines. Grolleau A. et al. [13] had administered homeopathic drugs in treating the psychiatric symptoms of different patients. Davidson J.R. et al. [14] had suggested homeopathic treatments in curing the anxiety and depressions. Dey J. [15] had presented a pivotal new normal mechanism in the secure transmission of the psychiatric homeopathic drugs. In that paper, the psychiatric patients can be safely treated from their distant locations during COVID-19 period. Dey J. et al. [16] had presented secure homeopathic medicine transmission with the help of chaotic key generation. They had developed robust session keys which were tested through statistical results.

3. PROBLEM STATEMENTS

This section deals with those relevant problems present in the telepsychiatric domain. In the COVID-19 times, such problems had erupted in large numbers. The following are those problems that can be identified in this relevant domain.

- Fear of social popularization: In normal outdoor of psychiatric treatments, patients are very much anxious regarding their social effects. Society can know that she / he is a psychiatric patient. Hence they do not want to visit OPDs in general.
- Due to mental rigidness, non-participation and cooperation in the treatments: On account of various mental pressures, psychiatric patients do not want to participate in the treatment procedures. They are not comfortable with the physical consultation with psychiatrists.
- Data security in public network of telemental health: It is the biggest challenge in telemental systems to restore the patients' data privacy. Most of the psychiatric patients do hesitate to share their problems over online E-health platforms. Also the psychiatrists are not comfortable to treat the patients in unsecure platforms.
- Intruders' attacks on the medical sensitive data: Patients' data are very much sensitive. Intruders will remain active to steal those data. So it is very much important issue to have a very strong key generation and encryption methods
- Key compromization on Telemental health terminal(s): Session keys are likely to be compromised inside the telemental health domain. Any terminal can be hijacked by the intruders and they can get the session key of that period. It may be done through different malware and phising attacks.

4. PROPOSED FRAME OF WORK

In the proposed psychiatric online framework, there is a surge of very strong session key generation. If the psychiatric patient (P_ID) wants to consult through virtual mode with psychiatrist (D_ID) then P will request KDC for a session key. The KDC will generate a session key with the help of proposed neural cryptography and then sends it to both the patient and the psychiatrist. The neural network will multiply each inputs and weights and then generates the hidden output. Then this hidden output will be passed through the neural function to obtain the final neural output. This procedure will be repeated for 128 times so that 128 bits of session key can be found. The length of the session key has been selected as 128 bits to minimize the memory capacity on the computing device. These will be used in

AES 128 encryption. Through online interface, different patients' inputs (conditions) will be captured. Such may be age, sex, blood pressure, periodical status, mental status in terms of relationship or break-ups, marital status, etc. Thus, after analyzing those symptoms, the psychiatrist may provide homeopathic medicines though online electronic prescriptions. This may be done in a secure way by encryption of AES with proposed key. A key distribution centre may use a artificial neural network and its parameters were kept totally secret. Key received would be used for both encryption and decryption for the same session.

Proposed Algorithm: Neural Cryptographic Transmission of E-medicines

Input(s): Threshold of the ANN (Thetaa)

Output(s): Secret Key generation and AES transmission

```
/*Secret key of 128 bits generation */
N=Input( No. of Input Neurons?")
For J = 0 to 127
For I = 0 to N
     $T= ( X_I * W_I )$
End for
     HO= Call Hidden(T)
    ARR[J]= HO
   J=J+1
End for
Transfer of J[128] to the patient and doctor
/*Online Psychiatric Symptoms Collection by Server */
Server ← Patients' Symptoms (P_ID)
/*E-prescription by Doctor */
E-Medicine ← Analyzing by doctor(D_ID)
/*AES 128 BITS Encryption on E-Medicine */
Encry_file ←AES Encryption(J [128], E-Medicine )
```

```
/*AES 128 BITS Decryption on Encry_file */
Medicine ← AES Decryption ( J[128], Encry_file )
```

```
int Hidden( float Vector )
do begin
    Vector = | Vector |
    if ( Vector>= Thetaa)
    return (1)
    else
    return (0)
    end if
end
```

Treating the mentally challenged patients from the distant location in a secure manner was the main objective of this manuscript. The patients' medical data are very much important and must be preserved from different intruders.

5. RESULT SECTION

A secure session key generation mechanism has been proposed on the neural cryptography. High level programming language C was used to implement it. The other hardware requirements were 2.40 GHz processor (Intel), 8GB RAM, 1TB HDD, and Windows 10 Operating System.

The following table 1 contains some of its important proposed session keys of 128 bits in length.

Tab 1: 128 bits Proposed Session Keys

Session Key Id.	Proposed Session Key (in Hexadecimal)
#1	Xn2r5u8x/A?D(G-K
#2	&E)H@McQfTjWnZq4
#3	bPeShVmYq3t6w9z$

#4	G-KaPdSgVkYp3s6v
#5	%D*G-JaNdRgUkXp2
#6	w!z%C*F-J@NcRfUj
#7	3t6w9z$C&F)J@McQ
#8	kYp3s6v9y$B&E)H+
#9	RgUkXp2s5v8y/B?E
#10	@NcRfUjXn2r5u8x/

From the above presented table 1, obviously there has been no correspondence between any sets of session keys created in the proposed methodology. Hence, by scrambling the E-medicines by utilizing any of the proposed created key will be sufficiently able to camouflage the interlopers with AES 128 encryption [17-18].

In the following figures 1 to 20, histogram and autocorrelation of the E-prescriptions using AES 128 bits proposed keys were depicted inside the table 2.

Tab 2: Histogram & Autocorrelation of E-Prescription using proposed Session Keys

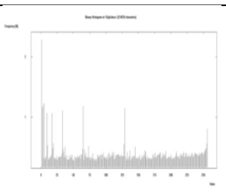
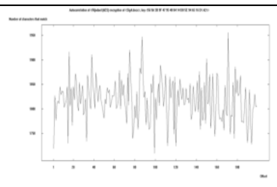
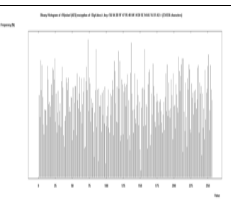
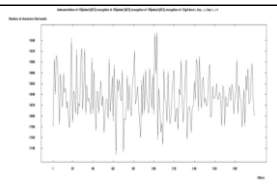
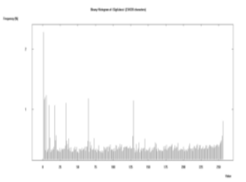
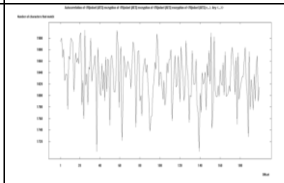
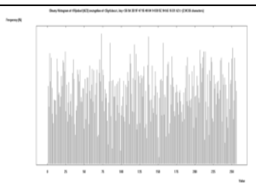
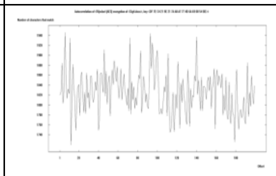
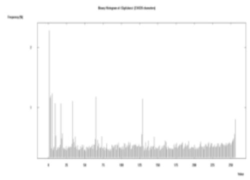
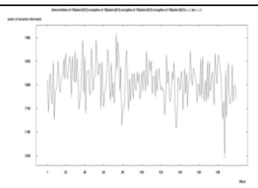
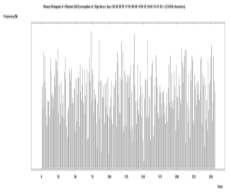
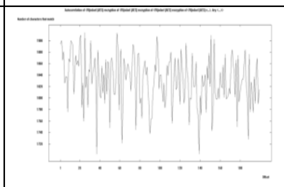
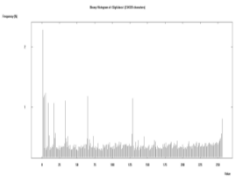
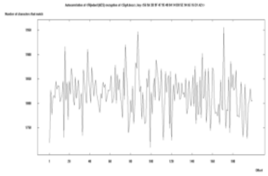
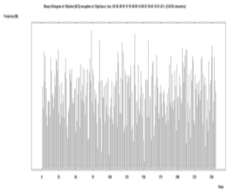
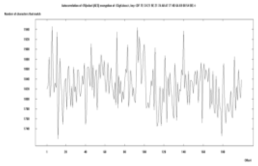
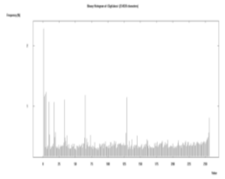
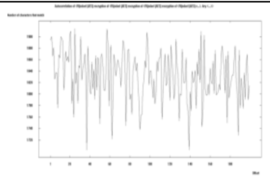
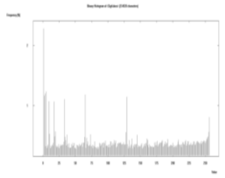
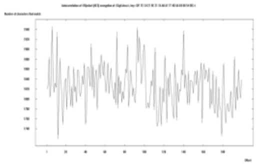
Session Key Id	**Graph of Histogram**	**Graph of Autocorrelation**
K **E** **y** **#1**	 Fig 1: Histogram of encrypted E-prescription post encryption	 Fig 2: Autocorrelation of encrypted E-prescription post encryption
K **E** **y** **#2**		 Fig 4: Autocorrelation of

	Fig 3: Histogram of encrypted E-prescription post encryption	encrypted E-prescription post encryption
K **E** **y** **#3**	 Fig 5: Histogram of encrypted E-prescription post encryption	 Fig 6: Autocorrelation of encrypted E-prescription post encryption
K **E** **y** **#4**	 Fig 7: Histogram of encrypted E-prescription post encryption	 Fig 8: Autocorrelation of encrypted E-prescription post encryption
K **E** **y** **#5**	 Fig 9: Histogram of encrypted E-prescription post encryption	 Fig 10: Autocorrelation of encrypted E-prescription post encryption
K **E** **y** **#6**	 Fig 11: Histogram of encrypted	 Fig 12: Autocorrelation of encrypted E-prescription post

	E-prescription post encryption	encryption
K **E** **y** **#7**	 Fig 13: Histogram of encrypted E-prescription post encryption	 Fig 14: Autocorrelation of encrypted E-prescription post encryption
K **E** **y** **#8**	 Fig 15: Histogram of encrypted E-prescription post encryption	 Fig 16: Autocorrelation of encrypted E-prescription post
K **E** **y** **#9**	 Fig 17: Histogram of encrypted E-prescription post encryption	 Fig 18: Autocorrelation of encrypted E-prescription post encryption
K **E** **y** **#10**	 Fig 19: Histogram of encrypted E-prescription post encryption	 Fig 20: Autocorrelation of encrypted E-prescription post encryption

Double Bits Mutation on Proposed Session Keys

Intruders exhaustively try their best to derive any relationship between the cipher text and original E-prescription by varying two bits on the proposed session keys [19]. Randomly two bits were taken into consideration by using a simple random function with the range 128. The corresponding changed observations were noted on the number of bits inside the cipher text by AES. The following table 3 displays those changes with respect to the proposed technique.

Tab 3: Two Bits Mutation

Proposed Key ID	Flipped bits positions	Difference of flipped positions	No. of changed bits
#1	(45,9)	36	2465
#2	(118,57)	61	3658
#3	(3,17)	14	4508
#4	(95,84)	11	7591
#5	(125,88)	37	2567
#6	(87,31)	56	4061
#7	(48,69)	21	1966
#8	(100,8)	92	3546
#9	(51,95)	44	1228
#10	(121,52)	69	3823

A negative correlation, r = -0.23465 has been observed between the differences in the position of the mutated bits and number of changed bits inside the cipher text. Since, the value of r is very much nearing to zero, hence it can be said that there exists no linkage inside the proposed session keys and the cipher text.

Brute – Force Attacks

Neural cryptographic key geneation has been proposed to encrypt the homeopathic prescriptions at the web servers. Intruders are always very intelligent and decode the session key. In this proposed technique, 128 bits long session key has been proposed by the help of neural networks. The present supercomputers operate at 442.3 peta Flops per second. It has been analysed in this paper that if intruders use such supercomputers then also the proposed set of keys will not be decoded. It will take plenty of years to decipher it. Hence, from the intrudding point of views, it is exactly next to impossible to decode the proposed session keys.

Security Analysis on the Session Key

In any Telemedicine Software, the data transmission security ought to be adequately ready to go against the interlopers. In this paper, we have planned session key generation on the space of homeopathic psychiatry. In this portion, a short examination has been made to survey the viability of the proposed framework against the barging inside the public networks.

- Psychiatric Patients' Information Integrity: On the off chance that the patients' data packets are gotten by encryption methodologies with the session keys. The enemies can't have the decision to inspect or take information yet at the transmission time [20].

- Patients' Data Secrecy: Patients' information secrecy has been put at the high level of the contemporary issues in the telemental health. We have planned session key in view of electronic prescriptions and such were tried under of factual tests for its testing.

- Session Key Exchange: In most of the telemedicine cases, the session key is by and large openly scattered to the patient and doctor in a public medium. There exists a biggest chance getting those keys by the opponents. So there ought to be a gotten instrument for its spread. In this strategy, we have effectively resolved this issue through KDC based session keys.

5. CONCLUSIONS

According to the calculations shown in the earlier result section, the proposed technique may be treated as an integral part on any telemental health portals. Thus, through homeopathic medicines, the psychiatric patients can be treated in a better and secure way. Artificial neural netwok has been explored inside the KDC to generate the session keys. In nutshell, the societal development may be reached through this proposed methodology.

ACKNOWLEDGEMENT

The authors acknowledge the moral and congenial atmosphere support provided by Maharajadhiraj Uday Chand Women’s College, Burdwan, India.

FUNDING

Not applicable.

ETHICS APPROVAL AND CONSENT TO PARTICIPATE

Not applicable.

CONSENT FOR PUBLICATION

Not applicable.

COMPETING INTERESTS

There is no conflict of interests in this manuscript.

REFERENCES

1. Dey J., Chowdhury B., Sarkar A., Karforma S., ***"Secured Telepsychiatry for Geriatric Patients (TGP) in the Face of COVID-19 IInd Wave*** ", Journal of Mathematical Sciences & Computational Mathematics, ISSN 2688-8300(Print)ISSN 2644-3368 (Online) Volume: 02 Issue: 04 | July -2021, pp: 564-571. DOI: doi.org/10.15864/jmscm.2409

2. Sarkar A., Dey J., Chatterjee M., Bhowmik A., Karforma S., Neural soft computing based secured transmission of intraoral gingivitis image in e-health care, Indonesian Journal of Electrical Engineering and Computer Science, 14(1): 178-184, April 2019.

3. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

4. Bhowmik A., Sarkar A., Karforma S., Dey J., A Symmetric Key based Secret Data Sharing Scheme, International Journal of Computer Sciences and Engineering, Vol.07, Issue.01, pp.188-192, 2019.

5. Viksveen P., et al., Homeopathy in the treatment of depression: a systematic review European Journal of Integrative Medicine Volume 22, September 2018, Pages 22-36.

6. Rai S. C., et al., Mood Mechanic, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-2S, December 2019.

7. Jiménez-Serrano, S., Tortajada, S., García-Gómez, J.M.: A mobile health application to predict postpartum depression based on machine learning. Telemed. J. E-Health: Off. J. Am. Telemed. Assoc. 21(7), 567–574 (2015).

8. Mdhaffar A. et al. (2019) DL4DED: Deep Learning for Depressive Episode Detection on Mobile Devices. In: Pagán J., Mokhtari M., Aloulou H., Abdulrazak B., Cabrera M. (eds) How AI Impacts Urban Living and Public Health. ICOST 2019. Lecture Notes in Computer Science, vol 11862. Springer, Cham.

9. Mowery D., Smith H., Cheney T., Stoddard G., Coppersmith G., Bryan C., & Conway M., "Understanding Depressive Symptoms and Psychosocial Stressors on Twitter: A Corpus-Based Study," Journal of Medical Internet Research, 19(2) (2017).

10. Naude FD, Couchman SM, Maharaj A (2010) Chronic primary insomnia: Efficacy of homeopathic

simillimum. Homeopathy. 99: 63-68.

11. 9. Viksveen P, Relton C (2014) Depression treated by homeopaths: A study protocol for a pragmatic cohort multiple randomized controlled trial. Homeopathy. 103: 147-152.

12. 10. Adler C, Kruger S, Teut M, Ludtke R, Schutzler L,et al. (2013) Homeopathy for depression: a randomized, partially double-blind, placebo-controlled, four-armed study (DEP-HOM). Plos one. 8:e74537.

13. 11. Grolleau A, Begaud B, Verdoux H (2013) Characteristics associated with use of homeopathic drugs for psychiatric symptoms in the general population. Homeopathy 102: 254-261.

14. 12. Davidson JR, Morrison RM, Shore J, Davidson RT, Bedayn G (2012) Homeopathic treatment of depression and anxiety. Altern theHealth Med3: 46-49.

15. 13. Dey, J. "*Pivotal "New Normal" Telemedicine: secured psychiatric homeopathy medicine transmission in Post-COVID***"**. Int. j. inf. tecnol. 13, 951-957(2021). https://doi.org/10.1007/s41870-021-00675-1.

16. 14. Dey J., Sarkar A., Karforma S., *"Internet of Things e-health revolution: secured transmission of homeopathic e-medicines through chaotic key formation*", Editor(s): Siddhartha Bhattacharyya, Paramartha Dutta, Debabrata Samanta, Anirban Mukherjee, Indrajit Pan, Recent Trends in Computational Intelligence Enabled Research,Academic Press,2021,Pages 317-337,ISBN 9780128228449, doi.org/10.1016/B978-0-12-822844-9.00001-3.

17. Roldán Lombardía, S., Balli, F. & Banik, S. Six shades lighter: a bit-serial implementation of the AES family. J Cryptogr Eng 11, 417–439 (2021). https://doi.org/10.1007/s13389-021-00265-8.

18. Arab, A., Rostami, M.J. & Ghavami, B. An image encryption method based on chaos system and AES algorithm. J Supercomput 75, 6663–6682 (2019). https://doi.org/10.1007/s11227-019-02878-7.

19. Dey, J., Bhowmik, A. & Karforma, S. Neural perceptron & strict lossless secret sharing oriented cryptographic science: fostering patients' security in the "new normal"COVID-19 E-Health. Multimed Tools Appl (2022). https://doi.org/10.1007/s11042-022-12440-y.

20. Dey, J., Bhowmik, A., Sarkar, A. et al. Cryptographic Engineering on COVID-19 Telemedicine: An Intelligent Transmission through Recurrent Relation Based Session Key. Wireless Pers Commun (2021). https://doi.org/10.1007/s11277-021-09045-3.