# Episode of COVID-19 Telepsychiatry Session Key Origination Upon Swarm-Based Metaheuristic and Neural Perceptron Blend

Joydeep Dey[1] · Arindam Sarkar[2] · Bappaditya Chowdhury[3] · Sunil Karforma[4]

## Abstract

Current pandemic has immensely disrupted the entire world in the field of medical science. The novel corona virus has not only brought physical sufferings but also huge psychiatric complications on the patients. Treating the psychiatric issues from remote locations can be best done through telepsychiatry. Patients can virtually consult with psychiatrists from their quarantines. However, during this COVID-19 era of excessive digital transactions, patients' data security mechanism is a challenging issue to prevent from intruding. Efficient cryptographic algorithms are used depending on the transmission key. This paper deals with the episode of transmission key origination with the help of salp swarm algorithm and neural perceptron. Threshold cryptography provides the generation of the partial shares of the E-prescriptions, which can be restructured on the threshold set of shares. The property of lossless theory has been implemented on the proposed set of telepsychiatry shares. A mask matrix has been proposed to diffuse the E-prescription shares into the specified group of users. The transmission key validation has been carried out in this paper based on myriad statistical tests. Chi Square test, $\chi^2 = 17.04$ has been observed under 5% level of significance. Thus, there exists no similarity between the bit patterns of the transmission key. A correlation coefficient between the average encryption and decryption time and the functional time has been estimated as 0.92076 and 0.72340, respectively. Also, it confirms the data resistance against the opponents in terms of different mathematical and statistical methods.

**Keywords** COVID-19 telepsychiatry · Secret sharing · Lossless theory · Histogram · Floating frequency

✉ Joydeep Dey
joydeepmcabu@gmail.com

Arindam Sarkar
arindam.vb@gmail.com

Bappaditya Chowdhury
drbappadityachowdhury@gmail.com

Sunil Karforma
sunilkarforma@yahoo.com

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

[2] Department of Computer Science & Electronics, Ramakrishna Mission Vidyamandira, Belur Math, Howrah, WB, India

[3] AMRI Hospital, Salt Lake, Kolkata, India

[4] Department of Computer Science, The University of Burdwan, Burdwan, WB, India

## Introduction

The outbreak of novel corona virus has led the entire world into pandemic crisis. There is a challenge to make every essential change in the public health science. Due to restrictions imposed by the government, people and patients have faced huge difficulties during this corona pandemic. On the onset of its very beginning, it had put huge impact on the psychological issues on the human society. The common people and healthcare support providers are on the verge of acute psychological problems faced in the light of COVID-19. Once a patient gets COVID suspected, she/he will be quarantined. It reduces the direct access to the family and society. Different forms of psychological implications likes of loneliness, anxiety, insomnia, stress, depression, etc. are common in such patients. Telepsychiatry has the provision that deals such remote patients with the help of Internet technologies. Telepsychiatry services are more feasible in treating the COVID patients, family members, doctors, nurse, healthcare staffs, etc. from their remote locations

[1–3]. It is a "New Normal" way to treat those mentally affected patients without the risk of COVID transmission. The objective of this paper is to have secured medical data transmission during the COVID-19 era, so that remote psychiatric patients can be treated easily. It aims to generate a metaheuristic and neural network-based secret key for the cryptographic purpose. A metaheuristic session key has been proposed that may be used in the telepsychiatry system in this post COVID era. There could be immense scope of this paper as patients are more treated from their quarantine locations. They are not allowed to visit the hospitals except emergency and invasive cases. Lockdown restrictions were imposed to reduce the corona virus transmission rates. Thus, from the theoretical perspectives, psychiatric patients can opt for telepsychiatric support in a more secured manner. Their private data could be preserved during the public mode of transmission.

Cryptography is the branch of science that protects the data from the external unauthorized agents and intruders. Enormous cryptographic tools are available in the market to deal with data security. Each one having some pros and cons within their algorithm. Symmetric key cryptography works on the same key by the users. Node compromisation may occur during single node failure. Another solution is to provide different secret shares of the psychiatric E-prescription to different users in the specified group on pre-defined conditions. A specified group of patients and psychiatrist of $n$ numbers, and $k$ is the minimum threshold value. Threshold-based secret sharing [4–6] cryptography can be used where the secret E-prescription is shared among n numbers of users having underlying condition that a group of $k$ or more secret shares are eligible to regenerate the E-prescription. It is false if it is less than $k$ [7].

A mathematical function share problem is a drawback of perfect secret sharing technique. Here the function computation is shared according to the secret sharing technique [8]. There are different such schemes likes of Shamir secret sharing on the polynomial interpolation, Blakley's secret sharing on the hyper plane geometry, Asmuth–Bloom secret sharing on Chinese remainder theorem, etc. In this paper, we have proposed a transmission key generation based on salp swarm algorithm and perceptron. Furthermore, COVID-19 telepsychiatry E-prescription's secret shares were encrypted by the proposed mask generation function. The robustness of the transmission key has been shown with respect to intriguing.

The motivation behind the proposal of session key through salp swarm and neural network was to remotely serve the psychiatric patients in this unprecedented corona era. Due to lockdown restrictions and quarantine protocols, most of the mental treatments have recommended through digital modes. Patients can easily avail the online telehealth services from their homes. It would certainly reduce the corona virus transmission in the society. The signification

contributions of this proposed technique can be said as follows. It presents a session key origination from metaheuristic salp swarm algorithm and neural perceptron. The key pool will serve as different session keys for different online transactions. This could be used in the secured session key in the telepsychiatry COVID-19 using the AES method. With the help of proposed secret sharing, the medical data could be broken into partial shares, and those shares would be diffused with the session key. The privacy of the patients is to be maintained in secret way is the main theme of this proposed technique. Several statistical experiments were carried out on the proposed technique to have its efficacy. During the COVID-19 times, the volume of digital medical transactions has immensely flooded the healthcare networks. Along with that the intruding attackers have also increased at high rates. There should be a resistant telepsychiatry COVID-19 system to deal with such intruders.

The overall structure of this paper has been arranged in this way. Introduction has been given in the Section "Introduction". Section "Literature Survey" contains the literature survey. It includes the related works on the Secret Sharing of data, Salp swarm algorithm, COVID-19 telepsychiatry, Session Key generation, and neural perceptrons. Section "Challenging Domain" displays the challenging issues related to the COVID-19 telepsychiatry. The proposed methodology has been explained in the Section "Proposed Methodology". The novelty of the proposed technique has been given in Section "Novelties of the Proposed Technique". Section "Proposed Flow Diagram" shows the flow diagram of the proposed technique. The result section has been given in Section "Result Sections". It includes different tests such as analysis on mask generation, histogram analysis, floating frequency analysis, entropy analysis, lossless theory on proposed secret shares, single flip effectiveness, significance of modular approach on secret shares, time complexity of the proposed sharing, functional time evaluation, and comparative statements. Conclusion and future work has been stated in Section "Conclusions and Future Scope of Works". Acknowledgement, research funding, compliance of ethical statements, and references were mentioned at the end.

## Literature Survey

In this section, we have surveyed different papers which were related to our proposed technique. Such were mentioned in the following sub-sections.

### Related to Secret Sharing

Shamir's Secret Sharing Scheme relies upon $(k, n)$ edge-based secret sharing procedure [9]. In this arrangement, a

$(k − 1)$ degree polynomial is bare essential. The polynomial limit of solicitation $(k − 1)$ is worked as follows in the Eq. 1.

$$f(x) = p_0 + p_1 x_1 + p_2 x_2 + \cdots + p_{k-1} x_{k-1} \text{MOD} N. \qquad (1)$$

Here, $p_0$ is the secret and $N$ is a number and all various coefficients are picked randomly from secret. All of the $n$ shares is a couple $(x_i, z_i)$ of numbers satisfying $f(x_i) = z_i$ and $x_i > 0, 1 \le i \le n$ and $0 < x_1 < x_2 < x_3 < \cdots < x_k \le (N − 1)$. Given any $k$ offers, the polynomials are exceptionally settled and in this manner the secret $p_0$ can be figured through Lagrange's expansion. The computational complexity was very high in their sharing scheme.

Blakey's Secret Sharing Scheme had utilized calculation to tackle mystery sharing issue [10]. The mystery message is a point in a $k$-dimensional space and $n$ shares are relative hyper planes that cross in this point. The set arrangement $y = (y_1, y_2, \ldots, y_k)$ to a condition $p_1 y_1 + p_2 y_2 + \cdots + p_k x_k = b$ structures a relative hyper plane. The mystery the convergence point is gotten by finding the convergence of any k of these planes. The time to obtain the convergence point in this technique was high.

Asmuth–Bloom's secret sharing scheme mystery sharing plan [11] shares a mystery among the individual gatherings utilizing measured number juggling and reproduction it by Chinese Remainder Theorem (CRT). The processing skills needed in this scheme was very large, and thus increasing the system complexity. Overall, the mystery sharing plans are viewed as an ideal mystery sharing plan since mixture of $(k − 1)$ shares does not uncover any data about the mystery.

Beimel et al. [12] had utilized multi-linear mystery sharing idea on field components. Sharing of data has been carried out on arbitrary field mystery components and fixed field components. Their strategy is by all accounts amazing on straight designs. However, the time complexity analysis with respect to previous works has been missed out there. Sarkar et al. [13] had proposed delicate figuring on neural organizations for the intraoral data partaking in the electronic clinical field. No privileged shares were added in their scheme of neural synchronization. Gupta et al. [14] had proposed neural cryptography for the secret sharing of data. They had synchronized both the parties to have a unique vector as secret key for transmission. The outputs of the neural networks at each synchronization step were shared between themselves through public channel. If those outputs were invasion, then it leads to vector compromisation. Dey et al. [15] had proposed a metaheuristic key for sharing the confidential medical data. Their tale of cryptographic procedure protects against the gatecrashers. But the time complexity of their technique was not computed on different datasets. Csirmaz et al. [16] had examined the mystery internet sharing strategies based on graph theory. Their performance was better in case of first fit graphs only.

Deshmukh et al. [17] had developed an $(n–n)$ secret sharing technique by the help of logic gates. It had raised the working complexity during the regeneration of images. Sarkar et al. [18] had utilized the gingival information transmission through mystery partaking in the teledental space. Their plan has the opposition against the vindictive aggressors. They had not shown on different intraoral images. Deshmukh et al. [19] had developed another secret sharing technique based on the binary tree operations and Boolean logics. However, they had not discussed the optimum time needed in binary tree operations.

## Related to Salp Swarm Algorithm

Salp swarm algorithm had been suggested by Mirjalili et al. [20]. It simulates the food searching behavior of the salps inside the deep oceans. Salps usually create a swarm which is commonly known as salp chain. Here, the leader is the salp present at the head of the chain and other salps are termed as followers. However, they could not identify the exact food searching patterns of the salps, as they reside inside the deep oceans. Sarkar et al. [21] had presented a biometric based session key generation technique by using the salp swarm protocol. They had considered only fingerprints of the patients to make dual layer of security. Other biometric traits could have also been included in their paper. Mirjalili et al. [20] had presented a bio-inspired optimizer for solving different engineering problems. They had not resolved and security problems over the cryptographic domain. Yaseen et al. [22] had developed a machine learning model based on salp swarm algorithm. However, the neural network simulations from the existing database were not observed in their method.

## Related to COVID-19 Telepschyiatry

Cui et al. have represented the challenges faced in the psychiatric treatments due to the novel corona virus [23]. But they had not opted for telepsychiatric approach in this COVID-19 era. Definitely, COVID-19 patients and suspects are more prone to psychological pressures in addition to their physical sufferings. They may experience fear of communicable disease spread and the contagion. Medical professionals are also of no exceptions. They get exposed directly while treating the COVID patients [24]. Mysers et al. [25] had stated that Boston and community hospitals in USA have molded themselves to embrace the telehealth facility. But the significance of migrating to telehealth was not sighted in their paper.

The COVID-19 patients may encounter depression, refusal, nervousness, gloom, sleep deprivation, and acute depression, which may bring down treatment adherence. A portion of these cases may even have expanded danger of

animosity and self-destruction. Suspected separated cases may experience the ill effects of nervousness because of vulnerability about their wellbeing status. Further, exacting isolate and compulsory contact following arrangement by wellbeing specialists could cause cultural dismissal, financial misfortune, segregation, and social stigmatization [26, 27]. Limited information on the corona virus and the staggering news may prompt nervousness and dread in the public society. The emergence of telepsychiatry has played a pivotal role in treating these psychiatric patients. However, the security approach must be included in such online systems.

### Related to Session Key Generation

Chen et al. [28] had designed session key for the wireless tactile organization systems. That secret key ought to be divided among the taking an interest hubs/terminals for the encryption/decryption reason. They had planned powerful key to diminish the encroaching. However, their technique suffers from the security issues of key management between the cluster and the sensor. Meena et al. [29] had planned a secured key arrangement mechanism for the remote transactions. They had attempted to abrogate the information security challenges. Their procedure includes fuzzy C protocols on clustering and social spider optimization with low force utilization. However, they had not solved any optimization technique based on their technique to prove their efficacy. Azarderskhsh et al. [30] had proposed a secured clustering strategy dependent on deterministic blending of public keys. Two terminals having a place with a similar cluster will actually want to build up a vital pair without scattering any additional data to the excess terminals. Their strategy has demonstrated terminal-to-terminal confirmation, least memory space, and protection from terminal assaults. But in case of WSNs located in different clusters were not able to pair up between themselves directly. This could be a real disadvantage of their proposed scheme. Dwivedi et al. [31] had proposed a finger mark premise biometric cryptographic system for the secured wireless information correspondence. They had utilized the human's biometric attribute to achieve the session key. Key spillage has been diminished in their strategy. Although there could be chances of middle attacks on the biometric keys. Kumar et al. [32] had proposed polynomial guiding non-interactive transmission key for dynamic number of users. The proposed polynomial is framed as a simple polynomial with $n$ number of users, and dynamicity exhibits in that. The data security of the key relies on different values of polynomial coefficients. They had combined the symmetric and asymmetric encryption which leads to extra computation heads. Bhowmik et al. [33] had proposed a symmetric key for encryption of the data. Their key length was fixed. Sarkar et al. [34] had proposed a unique key generation which works under the metaheuristic

cuckoo search calculation. Artificial intelligence could have been added to their scheme to reinforce the key security.

### Related to Perceptron

A perceptron is a variation of Artificial Neural Networks. Wang et al. [35] had developed a system to detect Alzheimer's disease from the MRI. They had classified their task into three components, such as: entropy of the wavelets, biogeography based optimization, and multilayer perceptrons. An accuracy around $92.40 \pm 0.83\%$ had been found by their classification technique. They had not stated their performance time of their proposed networks. Mallick et al. [36] had proposed an effective learning technique for the periodic perceptron on two real set of problems. Their technique has generated higher results with respect to simple multilayer perceptron. However, their technique had more structural complexities. Heidari et al. [37] have proposed a stochastic training on grasshopper optimization for different multilayer perceptrons. They had missed to derive a correlation coefficient between the noise and their network's performances. Sarkar et al. [38] had predictive model regarding the purchase willingness of the online customers. They have extracted features which were then fed to the support vector machines, random forest algorithm, and multilayer perceptron as inputs for the task of classifications. Their work had only survey localized servers. Struye et al. [39] had proposed to simulate the neocortex of the human brain towards data and time series predictions based on recurrent neural networks. Their technique has achieved higher degree of success. But their technique had consumed more time than the human brains. Tang et al. [40] had elaborated the use of multilayer perceptron models for synthetic-aperture radar image classification. Multiple hidden layers were made sure for the feed-forward training, and back-propagation of the neural network. Thus, the overall complexity and cost can be high in such artificial neural networks. Thomas et al. [41] had considered the issue of optimal multilayer perceptron structure. Variance sensitivity analysis was the key factor in their proposed technique. The computational time and precision of accuracy has been achieved better by their technique if compared to existing. However, with rise in neural architecture, it increases the topological costs in their proposed scheme.

## Challenging Domain

The novel corona virus had tremendously challenged the treatments in medical sciences [42–44]. The conventional ways to consult the physicians are extremely risky. Eventually, with the advanced telepsychiatry, the psychiatric patients may virtually consult the psychiatrists remotely

from their quarantines or homes. But the biggest challenge is to maintain the patients' data confidentiality in the field of COVID-19 telepsychiatry. The transmission of data between the patients and the psychiatrists are to be kept secret against the opponents. Opponents are capable to forge the medical data. Furthermore, they claim for fake and duplicate psychiatric insurance re-imbursements policies. Once any one of the users gets compromised, and then all sorts of private data can be made open to the intruders.

- COVID-19 telepsychiatry without appropriate patients' security [45, 46].
- Patients' data security gets leaked.
- Single keys for different sessions.
- Fitness of the session key.
- Opponents can access the private data in the middle.
- Public channel, nodes, hub, etc. may get compromised.
- Patients' data privacy gets unprotected.
- Poor security performance of the COVID-19 telepsychiatry.

## Our Remedies

The above-stated challenges have been addressed in this technique. Shaukat et al. [42] had shown different mental complications that were found on the healthcare staffs due to COVID-19 pressure. They need special mental care. But they have not mentioned on the telepsychiatry aspects that could be used to them remotely. Spoorty et al. [43] have also specified the mental problems faced by the medical support staffs. They have reviewed different types of psychiatric complications in this corona virus times. The idea of safe remote mental treatment was missing in their review. So we have tried to propose a secured cryptographic system on mental health. Cai et al. [44] had investigated the psychiatric

COVID-19 impacts on medical staffs between January 2020 and March 2020 in Hunan. They had also not suggested any online treatments procedures. In this manuscript, different session keys can be generated to have multiple transaction keys on telepsychiatry COVID-19. Ho et al. [46] had proposed different mental strategies to combat the novel corona virus. Their strategies could not be transmitted in online modes. There needs a tight security protocol to deal that. So, we have designed a salp swarm and perceptron based session key origination to transmit medical data. This could help the remote patients to avail virtual consultation with their psychiatrists.

## Proposed Methodology

This proposed technique may act as a solution to the problem domain specified in the above-stated Section "Challenging Domain" by involving the metaheuristic salp swarm algorithm and perceptron blend. Using the salp swarm algorithm and perceptron blend, a metaheuristic-based transmission key has been derived of 128 bits length [33].

A mask generation algorithm has also been proposed here. The objective of this proposed mask generation technique is to diffuse the E-prescription before transmitting to the telepsychiatry networks. In a system of $\{n, k\}$ users, $n$ denotes the number of shares, and $k$ represents the threshold values. Every share should contain some missing bits from the original data [47]. The mask matrix which has been created by the following technique would be used to generate the encrypted partial shares. A key pool would be formed as per the positions of the leader salps. Any key from that pool would be used to generate the proposed shares for the patients' E-prescriptions in COVID-19 telepsychiatry. The proposed algorithm is mentioned below.

---

***Algorithm No.*1**: ***Transmission Key Origination for COVID − 19 Telepsychiatry***
***Input(s)***: *Prescription (P1.txt), Salp Population (Sample)*
***Output(s)***: *Transmission Key based encrypted Partial Shares*
*// Binary Prescription Conversion*
*PR.pdf ← TOBINARY ( P1.txt )*
*Call Neural Weight Vector Generation(128)*
*Call Salp Key Pool Generation ( )*
*Mask_Mat[n][$^nC_{k-1}$] ← Call MaskGeneration( n,k)*
*CAll Secret Shares Generation*
*Call AES Encryption (Shares)*

---

## Neural Weight Vector Generation

$// \text{ Populace the initial salps}$
$\text{Set } N = 128$

$\text{For } I = 0 \text{ to } 127$
$/*\text{Generation of Random Weight }*/$

$\text{Assign Epochs} \leftarrow 0$
$\text{While } [Epochs != 128] \ /*/\text{Perceptron based weight vector}*/$
$\quad \text{Assign X1}_i \leftarrow 1, X_1, X_2, \ldots, X_N \quad /*\text{ Peceptron Input Vector } */$
$WT[i] = Random\ Numbers(-1, +1) \ /*\text{ Weight Initialization }*/$

$$HL1 \leftarrow WT[Bias] + \sum_{i=1}^{N} WT_i * X_i \quad /*\text{ Hidden Output }*/$$

$\quad \text{If } (HL <= Desired\ Value) \ Then \ /*\ Output\ Unit \ /$
$\quad\quad Z_i \leftarrow 0$
$\quad Else$
$\quad\quad Z_i \leftarrow 1$
$\quad End\ if$
$\quad If\ (Z_i != Desired\ Value) Then \quad /*\ Learning\ Rule *\ /$
$$WT_{Next} = WT_{Prev} + \left\{ \frac{1}{2} * X_i \right\}$$
$$Bias_{Next} = Bias_{Prev} + \left[ \frac{1}{2} * Desired\ Value \right]$$
$\quad Else$
$\quad\quad WT_{Next} = WT_{Prev}$
$\quad\quad Bias_{Next} = Bias_{Prev}$
$\quad End\ if$
$\quad Assign\ Epochs \leftarrow Epochs + 1$
$End\ while$

$SalpM[I] \leftarrow WT[128]$

$End\ for$

## Salp Key Pool Generation

$Set\ Counter = 0$
$\text{While ( EXIT CONDITION)}$

$\quad \text{For } I = 0 \text{ to ( Sample } - 1)$

$\quad \text{Set Counter = Counter } + 1$

$$P1 = \left[ \left\{ (2*e)^{\left\{ (-4*itrn) \middle/ (MAXITR) \right\}} \right\}^2 \right]$$
$\quad\quad //itrn\ is\ the\ current\ iteration\ and\ MAXITR\ is\ \ the\ limit\ of\ iteration$
$\quad P2 = RandomInteger\ [0,1]$
$\quad If\ (P2 > 0)\ Then$
$\quad\quad \text{SalpK[0][0...2]=AVG(Food}_n +[\{UPB_n - LWB_n\}* \ RandomInteger[0,1]+ \ LB_n] \ * \text{ RandomInteger}[0,1]$
$\quad Else$
$\quad\quad \text{SalpK [I][0...2]=AVG(Food}_n)-[\{UPB_n–LWB_n \}* \ RandomInteger[0,1] + LWB_n \ ] \ * \text{ RandomInteger}[0,1]$
$\quad End\ if$
$\quad\quad \text{SalpK [I][0 \ldots 2 ]= (SalpK[I][0 \ldots 2 ] - SalpK[I-1][0 \ldots 2 ] )/2}$
$\quad End\ for$
$End\ while$
$\text{Key Pool is ready as SKEY [ ][128]}$

## Mask Generation Algorithm

$Input(s)$: $n$: No. of Participants in Telepsychiatry System, and $k$: Threshold Users
$Output(s) -$ $Mask\_Mat[n][10]$: Mask Matrix for Encryption
Set $P = C_k^n$, $NO1 = 3, k1 = 0, k2 = 0, Middle = floor[\{0 + (P-1)\}/2], i = 2^n$
$While (i >= 1)$
  $Bin[n] \leftarrow ToBinary(i)$
       $For\ j = 0\ to\ 9$
         $C = 0$
        $If\ (Bin[j] = 1)\ then$
          $C = C + 1$
        $End\ if$
       $End\ for$
        $If\ (C = 3)\ Then$
         $Index[k1 + +] \leftarrow i$
        $End\ if$
        $i = i - 1$
      $End\ while$
     $For\ i = 0\ to\ Middle$
        $For\ j = i + 1\ to\ Middle$
        $If\ (Index[i] < Index[j])\ then$
         $Swap\ (Index[i], Index[j])$
        $End\ if$
     $End\ for$
     $For\ i = Middle + 1\ to\ P - 1$
        $For\ j = i + 1\ to\ P - 1$
        $If\ (Index[i] < Index[j])\ then$
          $Swap\ (Index[i], Index[j])$
        $End\ if$
     $End\ for$
     $Set\ i = 0\ and\ j = Middle + 1$
     $While\ (i <= Middle\ \&\&\ j <= P - 1)$
       $Temp[k2 + +] \leftarrow Index[i]$
       $Temp[k2 + +] \leftarrow Index[j]$
       $i = i + 1, j = j + 1$
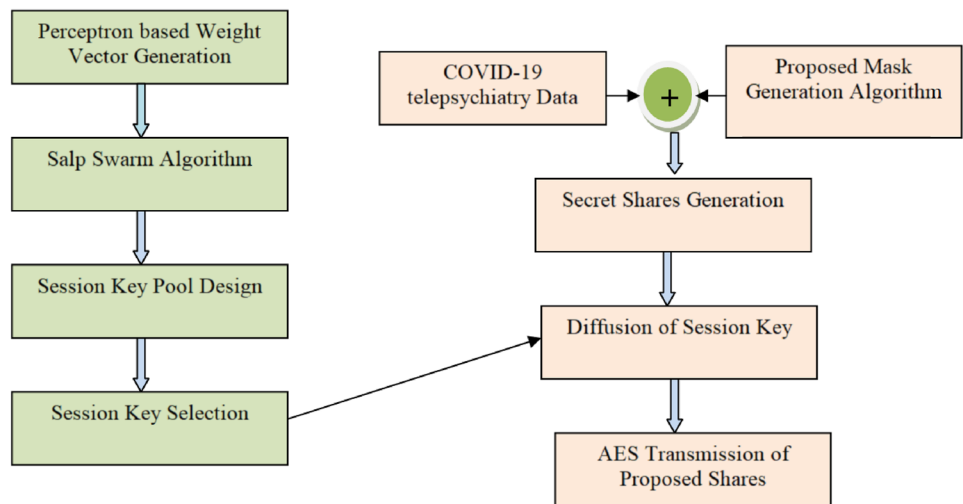$End\ while$
$For\ Z = 0\ to\ P - 1$
     $Mask\_Mat[Z][] \leftarrow ToBinary\ (Index[Temp[Z]])$
$End\ for$
     $Mask\_Mat[n][P] \leftarrow Mask\_Mat[P][n]]^T$

**Fig. 1** Flow diagram of our proposed technique



## Secret Share Generation

$$For\ I = 0\ to\ n$$
$$\quad CRYTOGRAM[I][\ ] \leftarrow XOROP\ (\ PR.pdf, Mask\_Mat[I][10])$$
$$End\ for$$
$$For\ I = 0\ to\ n$$
$$\quad CRYFINAL[I][\ ] \leftarrow XOROP\ (\ CRYPTOGRAM[I][\ ], SKEY[128])$$
$$End\ for$$

**1.5 AES Encryption (Shares)**
*Transmit n cryptograms to n psychiatrists of defined group through AES*
*// AES transmission of proposed shares of cryptogram*
$$For\ I = 0\ to\ n$$
$$\quad Cipher[I][\ ] \leftarrow AES\ (\ CRYFINAL[I][\ ], SKEY[\ ][128])$$
$$End\ for$$

## Novelties of the Proposed Technique

This paper presents a transmission key origination upon salp swarm and neural network. Psychiatric patients can avail online treatments in a safe way through this technique. Following are the novelties that were observed in this technique.

- Transmission key origination on the salp swarm and perceptron blend.
- Key pool of session keys was generated for different telepsychiatry COVID-19 transactions.
- Diffusion of session key into the source information.
- Production of partial secret shares on the proposed mask matrix.
- COVID-19 telepsychiatry: Protection against the opponents.

- Modular secret shares' time complexity.
- Standard graphs resistances against the opponents.
- Measurements of performance time.

**Table 1** Binary mask matrix

| Share ID-$1 | Share ID-$2 | Share ID-$3 | Share ID-$4 | Share ID-$5 |
|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 1 | 0 |
| 0 | 1 | 1 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 |

**Table 2** Snapshot of secret share

| Share ID-$1 | Share ID-$2 | Share ID-$3 | Share ID-$4 | Share ID-$5 |
|---|---|---|---|---|
| 0 | 0 | P | P | P |
| 0 | R | 0 | r | R |
| 0 | A | A | 0 | A |
| 0 | G | G | G | 0 |
| U | 0 | 0 | U | U |
| E | 0 | e | 0 | E |
| 1 | 0 | 1 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 |
| 2 | 2 | 0 | 4 | 0 |
| 4 | 4 | 4 | 0 | 0 |

**Table 3** Snapshot of compressed secret shares

| Share ID-$1 | Share ID-$2 | Share ID-$3 | Share ID-$4 | Share ID-$5 |
|---|---|---|---|---|
| U | R | P | P | P |
| E | A | A | r | R |
| 1 | G | G | G | A |
| 0 | 0 | E | U | U |
| 2 | 2 | 1 | 1 | E |
| 4 | 4 | 4 | 2 | 0 |

- Comparison statements in tabular forms.
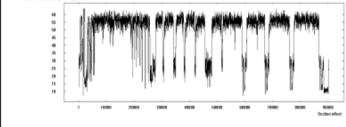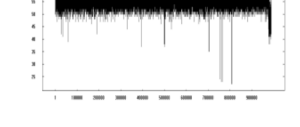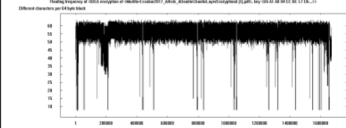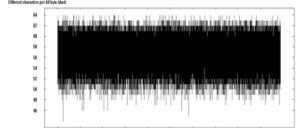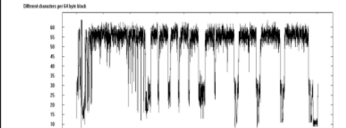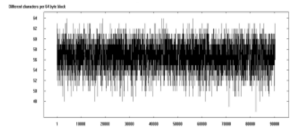
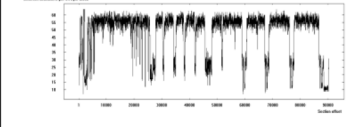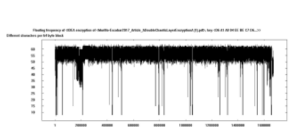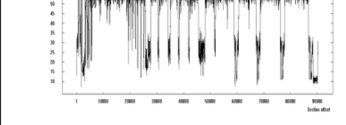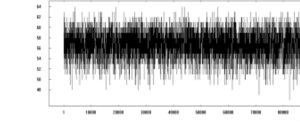The above-stated novelties were confronted in the above-stated algorithm in Seciton "Proposed Methodology". No research papers were found to work on telepsychiatry COVID-19 transmission key.

## Proposed Flow Diagram

The entire world is battling against the novel corona virus. This paper deals with a safe wave of COVID-19 telepsychiatry. In this section, we have presented the flow diagram of the proposed technique in the following Fig. 1.

The above-mentioned Fig. 1 represents the working flow of the proposed model. It has a mix of metaheuristic salp and neural perceptron. A new secret sharing has been proposed to generate the partial shares of the data. It has been done to make the intruders confused regarding the patients' data. No secret share would have complete information. With the help of artificial neural perceptron and salp swarm algorithm, the key pool would be obtained. This key pool would actively be used as session key for various telepsychiatry online sessions. Furthermore, with the help of proposed session key,

**Table 4** Histogram comparison on shares

| Secret Share ID | Histogram of E-prescription without our technique | Histogram post encryption by our technique |
|---|---|---|
| $1 |  |  |
| $2 |  |  |
| $3 |  |  |
| $4 |  |  |
| $5 |  |  |

**Table 5** Floating frequency comparison on shares

| Secret Share ID | Floating Frequency of E-prescription without our technique | Floating Frequency post encryption by our technique |
|---|---|---|
| $1 |  |  |
| $2 |  |  |
| $3 |  |  |
| $4 |  |  |
| $5 |  |  |

the partial shares would be encrypted with AES technique. The proposed model will be fruitful for the psychiatric patients who could get the online psychiatric treatments in a secured manner.

# Result Sections

This paper deals with the COVID-19 telepsychiatry session key origination based on salp swarm and perceptron learning. Here, the decimal point has been considered in as per the standards of IEEE 754. The following hardware and

**Table 6** Entropy comparison on proposed secret shares

| Secret share ID | Entropy of E-prescription without our technique | Entropy post encryption by our technique |
|---|---|---|
| $1 | 6.20 | 7.42 |
| $2 | 6.17 | 7.82 |
| $3 | 6.03 | 7.49 |
| $4 | 6.47 | 7.39 |
| $5 | 6.65 | 7.57 |

software requirements met to achieve the results mentioned later.

Processor name: Intel Core ($i$9) – Generation-10th, Speed of the processor: 2.6 GHz, Secondary Storage Capacity: 1 TB, Primary Memory Capacity: 16 GB, Operating System: Windows 10 (Original) Sixty Four bits, Soft Skills: Python 3.9.1.

In the following sub-sections, the results have been mentioned along with its explanations. This section presents the outputs obtained after several sets of parametric tests on the proposed technique. Privacy issues related to the COVID-19 pandemic were prioritized the most here. Different types of mathematical tests were carried on the proposed COVID-19 telepsychiatry transmission key.

## Analysis on Mask Generation

Using the proposed mask generation technique, the following Table 1 has been filled with the binary mask matrix. Taking each row at a time, and performing XOR operation on the COVID-19 telepsychiatry E-prescription, $n$ number of different share were generted before the proposed round of shares encryption.

A snapshot which contains a set of five share masks corresponding to three threshold values given in the above Table 1.If we assume the following secret message (*M*) as "PrAGUe1024", then the corresponding secret masks can be shown in the following Table 2.

Then to curtail the conventional network traffic congestion especially during the COVID-19 digital health and to increase the network throughput, the above-stated secret shares were compressed by removing all zero data. It can be shown in the following Table 3.

## Histogram and Floating Frequency Analysis

In this section, histogram analysis has been briefly shown in the following Table 4. Histogram denotes the frequency of different of characters present in the file. It has been observed that post encryption resulted from individual shares are more robust than without encryption form. Intruders will not be able to trace any sort of information from the partial shares, if compromised [48].

Floating frequency is the count of group of characters present in the source file. The proposed technique has been analyzed in terms of floating frequency. From the following Table 5, it can be noted that graphs obtained post encryption on the partial shares were better than the earlier graphs.

## Entropy Analysis

It refers to the act of randomness structures which is used for the data hiding purpose from the opponents. Low entropy value means more vulnerable cryptosystem is. In the following Table 6, entropy has been computed on different shares of the E-prescription, and the results are on average good.

The above-mentioned Table 6 contains the Secret Share ID, Entropy of E-prescription without our technique and Entropy post encryption by our technique. An E-prescription of COVID-19 telepsychiatry was considered under the study.

Our proposed technique had generated better entropy values. A small negative $-0.1498$ correlation value has been observed from the above table [49]. Thus, the entropy of E-prescriptions i.e. without and with our technique moves in opposite direction. Opponents will not be able to trace any information from the proposed shares.

## Lossless Theory on Proposed Secret Shares

The novelty of the proposed mask generation technique is lossless theory in terms of the information security in this global unprecedented COVID-19. When a message is divided into t number of secret partial shares, then the x numbers of threshold shares are bare minimally joined together to restructure the actual data matter. However, good lossless theory flavor of this method is that no data matter
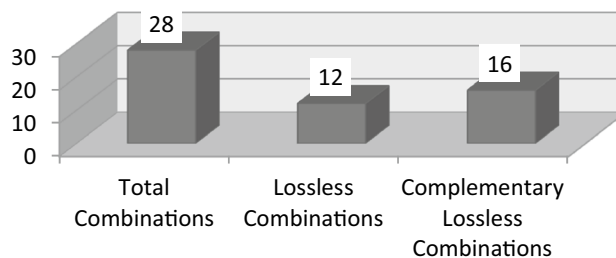


**Fig. 2** Lossless and Complementary Lossless combinations

**Table 7** Single bit flipping on the session key

| Class interval of bit positions | Frequency of keys | Expected frequency of keys | Changes in cipher text (Bit level) |
|---|---|---|---|
| 0–15 | 7 | 12.5 | 471 |
| 16–31 | 13 | 12.5 | 950 |
| 32–47 | 15 | 12.5 | 704 |
| 48–63 | 8 | 12.5 | 848 |
| 64–79 | 6 | 12.5 | 307 |
| 80–95 | 20 | 12.5 | 915 |
| 96–111 | 13 | 12.5 | 749 |
| 112–127 | 18 | 12.5 | 597 |

has been lost while transmission [47]. It is briefly explained using the following Eqs. 2 and 3, respectively.

Condition for Lossless Theory:

$$M = M_1 U M_2 U \ldots U M_t. \tag{2}$$

Condition for Complement Lossless Theory:

$$M \neq M_1 U M_2 U \ldots U M_{t-1}. \tag{3}$$

Let us consider a message M and consider the number of secret shares be t be five, and threshold shares x be three. Then the generated secret shares have been named as $M_1$, $M_2$, $M_3$, $M_4$ and $M_5$. The following twelve possible combinations guarantee the lossless theory on COVID-19 telepsychiatry.

*Case 1*:

$$M = M_1 U M_2 U M_3 U M_4 U M_5.$$

*Case 2*:

$$M = M_1 U M_2 U M_3 U M_5.$$

*Case 3*:

$$M = M_1 U M_2 U M_3 U M_4.$$

*Case 4*:

$$M = M_1 U M_2 U M_3.$$

*Case 5:*

$$M = M_1 U M_2 U M_4.$$

*Case 6:*

$$M = M_1 U M_2 U M_5.$$

*Case 7:*

$$M = M_1 U M_3 U M_4.$$

*Case 8:*

$$M = M_1 U M_3 U M_5.$$

*Case 9:*

$$M = M_2 U M_3 U M_4.$$

*Case 10:*

$$M = M_2 U M_3 U M_5.$$

*Case 11:*

$$M = M_3 U M_4 U M_5.$$

*Case 12:*

$$M = M_1 U M_4 U M_5.$$

From the above-stated cases, it may be concluded that the total number of combinations are 28. Out of which, the total number of lossless combinations is 12. So the complementary lossless combinations are 16. The following Fig. 2 shows the same.

## Single Flip Effectiveness

Opponents have used advanced simulations to detect the transmission key in the telemedicine sectors. The key pool of one hundred transmission keys was considered for testing the flip effect. A flip in the single bit on all the session keys has been done. Subsequently, a plain message is encrypted before and after the flip operation. The position of the flip that took place has been randomly selected by the random function. The following Table 7 shows the frequency of the keys and its corresponding changes in the cipher text.

The above-mentioned Table 7 contains Class Interval of Bit Positions, Frequency of Keys, Expected Frequency of Keys, and Changes in cipher text (Bit level). Let us assume the following hypothesis based on the above Table 7.

**Null Hypothesis ($H_0$)** : Flipping bit position selection is dependent on the bit position.

**Alternative Hypothesis ($H_1$)** : Flipping bit position selection is not dependent on the bit position.

Using the Chi Square test [50], we have obtained $\chi^2 = 17.046$ (under 5% level of significance). Therefore, null hypothesis ($H_0$) will not be accepted. Thus, no autocorrelation is associated with the bits position in the COVID-19 telepsychiatry. This validates the data of our study.

## Significance of Modular Approach on Secret Shares

Secluded methodology as for shares generation in COVID-19 telepsychiatry has been tied in with destroying mystery message into more modest and incomplete encoded insider facts, with no mystery contains total information about the E-prescription of telepsychiatry. The pith part of this sort of partial secret shares generation is that each of it offers a type of highlights of attachment just as coupling. The ability of presence of strong cohesion property in each secret share is that they are treated as a free substance while the cycle of encryption is finished in COVID-19 telepsychiatry. Just the fractional encoded partial shares are available in the offers to make it stowed away from the unapproved access like interlopers, tricky programmers, hackers, and so on. The great part is that it builds the absolute framework practicality factor because of the way that legitimate changes done inside a specific space influence the less number of different modules.

In the event that a message M might be broken into fractional secret shares likes of $M_1, M_2, M_3, \ldots M_n$. At that point the idea of measured quality is kept up for the patients' security. The greatest favorable position of such use of secluded idea regarding such proposed telepsychiatry shares generation is that in the event that any share is being debased during transmission over the COVID-19 telemedicine network, at that point that specific share can be recovered and resent. The misfortune or mutilation to the secret telepsychiatry shares may occur in the organization because of different reasons like commotion, impulse, reversal of bits, and so forth.

## Time Complexity of the Proposed Secret Sharing

The strategy of applying the strategy of coupling on the proposed set of secret shares of telepsychiatry offers that the time complexity will raise both at the patient's end just as

**Table 8** Time complexity display

| Sl. no | Mode of transmission | No. of users | Time complexity |
|---|---|---|---|
| 1 | Plain text or data file | 2 | $O(2Tm)$ |
| 2 | COVID-19 telepsychiatry Secret Sharing | U | $O(U)$ (Proposed) |

**Table 9** Average functional time

| Sl. No | Name of COVID-19 psychiatric E-prescription | Average encryption time (ms) | Average decryption time (ms) | Functional time (ms) |
|---|---|---|---|---|
| 1 | File 1 | 3675 | 1790 | 5465 |
| 2 | File 2 | 2896 | 1802 | 4698 |
| 3 | File 3 | 2145 | 1697 | 3842 |
| 4 | File 4 | 1587 | 1572 | 3159 |
| 5 | File 5 | 2982 | 2714 | 5696 |

**Table 10** Comparative study with classical technique

| Functional characters | 3DES | Our Technique |
|---|---|---|
| Block length | 64 | 64 |
| Key length | 168 | 128 |
| Key space size | $2^{168}$ | $2^{128}$ |
| Rounds present | 48 | 10 |
| Cipher text | Symmetric block | Continuous symmetric block |
| Algorithm implementation | Fiestel network | Salp swarm, perceptron, and partial secret sharing |
| Degree of flexibility | Medium | High |
| Attacks on data | Prone to brute force attacks | May resist against intruding better |
| Functional time | Slow | Medium |

psychiatrist's end with the raise of users in the telepsychiatry system. The time complexity might be determined as $O(U)$, where $U$ signifies the quantity of users arranged for share transmission in the system. This time unpredictability factor will increment with the increment in the quantity of shares. Along these lines, here the time multifaceted nature is straightforwardly corresponding to the quantity of shares generation on COVID-19 telepsychiatry. Another interesting striking element is the coupling highlight. It implies the level of interdependency between the encrypted shares. During the reassembly of the threshold number of shares, coupling boundary exists together. The coupling boundary can be registered as $O(T)$, where $T$ denotes the threshold number of shares. Potentially, in that event $(T-1)$ number of partial shares or not exactly $(T-1)$ number of shares are consolidated together during the reproduction stage with failure result. At the end of the day, least T number of shares is barely needed to recover the COVID-19 telepsychiatry E-prescription.

When compared with the plain text transmission of the COVID-19 telepsychiatry E-prescription, then using the following Table 8, it can be said that higher time complexity is incurred in the proposed system.

The above-stated Table 8 contains Sl. No., Mode of Transmission, No. of Users, and Time Complexity. Here *Tm* is the time needed in plain text transmission, and U is the number of users in the proposed COVID-19 telepsychiatry system. The time complexity of the proposed system of shares is $O(U)$.

## Functional Time Evaluation

Different psychiatric E-prescriptions of COVID-19 were taken into consideration under testing phase. Using the same session key generated through salp swarm algorithm and perceptron blend, the encryption and decryption of secret shares were done. The following Table 9 contains the average amount of functional time on all the shares of individual E-prescriptions.

A correlation value was determined between the average encryption time and the functional time, and the average decryption time and the functional time. Both values were 0.92076, and 0.72340, respectively [49]. Thus, the functional time of the proposed COVID-19 telepsychiatry is fully dependent to the encryption and decryption time.

## Comparative Tabulations

In this sub-section, different comparative tabulations were done. At first Table 10, the proposed technique has been briefly compared with 3DES classical technique [51]. The table contains the summarized comparisons in this regard.

In the above-stated Table 10, our proposed technique has been compared with 3DES classical algorithm. The key length was 128 bits and 168 bits for 3DES. The number of rounds involved was reduced to ten in this work to minimize the complexity. Here, salp swarm, perceptron, and secret sharing were the principle components involved, whereas Fiestel network was present in 3DES. The degree of user

**Table 11** Comparative tabulation with literature survey papers

| Earlier works | Year of publication | Telepsychiatry on COVID-19 | Transmission key | Biometric key | Functional time | Histogram analysis | Floating frequency analysis | Entropy analysis | Lossless theory | Tabular comparison |
|---|---|---|---|---|---|---|---|---|---|---|
| Cui et al. [23] | 2020 | Yes | No | No | No | No | No | No | No | No |
| Xiang et al. [24] | 2020 | Yes | No | No | No | No | No | No | No | No |
| Myers et al. [25] | 2020 | Yes | No | No | No | No | No | No | No | No |
| Chen C.L. et al. [28] | 2008 | No | Yes | No | No | No | No | No | No | No |
| Azarderskhsh et al. [30] | 2011 | No | Yes | No | No | No | No | No | No | No |
| Dwivedi et al. [31] | 2020 | No | Yes | Yes | No | No | No | No | No | No |
| Mirjalili et al. [20] | 2017 | No | Yes | No | Yes | No | No | No | No | No |
| This Paper | Yet to be published | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes |

flexibility was found to be higher in our technique against 3DES. The operational time was average in this proposed method, when compared with 3DES. 3DES technique has the limitation to be attacked by the Brute-Force attacks, whereas the proposed technique may resist such attacks in the middle.

The following Table 11 has been designed to make a comparison between the proposed technique and some of the literature survey publications. The proposed technique's efficiency may be observed from that table.

In the above-mentioned Table 11, a brief comparison was made with other papers. Cui et al. [23], Xiang et al. [24], Myers et al. [25], and our technique has only dealt with COVID-19 telepsychiatry. No other papers in the above table had worked on COVID-19 mental issues. Chen et al. [28], Azarderskhsh et al. [30], Dwivedi et al. [31], Mirjalili et al. [20], Yaseen et al. [22], and this paper have processes with transmission key generation. We have generated session key based on salp swarm and neural networks. No other papers have done in that approach. Yaseen et al. [22] and this method have calculated the functional time of the encryption system. We have presented the lossless secret sharing of data. Others have not illustrated this issue. Entropy, histogram analysis, and floating frequency were only discussed in this proposed methodology. At last, we have presented a tabular comparative study which indicates the quality of works performed on the proposed technique. Thus, we can prove the efficacy of the proposed COVID-19 telepsychiatry.

It has been noted that cryptographic science is the essential entity while crafting the data security. For that more robust session key is more crucial factor [52]. During the corona pandemic, the increased rate digital health transactions have been phenomenal [53, 54]. To keep a check on the patients' data security, different cryptographic techniques were proposed [55, 56]. This paper aims the same on the COVID-19 telepsychiatry.

## Validation Statements

In this sub-section, it contains the validation statements of the proposed technique. It can be illustrated in multiple ways to have its efficacy. The average encryption time, average decryption time, and functional time on different E-Prescriptions were found to be low. A correlation coefficient between the average encryption and decryption time and the functional time has been noted as 0.92076 and 0.72340, respectively. Entropy, histograms, and floating character frequency of all the proposed shares have yielded satisfactory outputs. The time complexity of the proposed secret sharing has been calculated as $O(U)$, with $U$ means the total number of patients and psychiatrists of the system. For Chi-square test, $\chi^2 = 17.046$ (under 5% level of significance) has been observed which means no similar patterns in the session key orientation. Moreover, lossless data sharing was observed in

this proposed technique as threshold number of shares was required to generate the original data.

## Conclusions and Future Scope Of Works

The recent spike in the COVID cases has urged the role of telepsychiatry into more proactive play. Patients' data security is the prime concern in this proposed technique. Salp swarm and perceptron oriented transmission key has been generated in this proposed technique with enriched key robustness. This key has been used an encryption key in the pre-defined users group. The E-prescription of the COVID-19 telepsychiatry would be splitted into multiple shares by the proposed mask matrix. This proposed method has provided efficacy results in terms of entropy, histogram, floating frequency, functional time. The lossless theory has been ensured on the set of proposed shares. For Chi-square testing, $\chi^2 = 17.046$ (under 5% level of significance) has been found. Thus, there exists no similarity between the bit patterns of the transmission key. Patients' data can be preserved in telepsychiatry systems in the face of COVID-19. The performance of the proposed COVID-19 has been measured in terms of correlation coefficients as 0.92076 and 0.72340. The complexity of the proposed shares was $O(U)$ ; $U$ denoting the number of patients and psychiatrists.

The future scope of works can be stated as follows. Artificial intelligence based automatic telemedicine unit may be further added into this proposed technique. Thus, the involvement of the human beings will be reduced with more time saving managements.

## Declarations

**Compliance with ethical standards**  Not applicable.

**Conflict of interest**  No conflict of interest is applicable here.

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

## References

1. Rajkumar RP. COVID 19–19 and mental health: a review of the existing literature. Asian J Psychiatr. 2020;52:102066.
2. Monnier J, Knapp RG, Frueh BC. Recent advances in telepsychiatry: an updated review. Psychiatr Serv. 2003;54:1604–9.
3. Hilty DM, Ferrer DC, Parish MB, Johnston B, Callahan EJ, Yellowlees PM. The effectiveness of telemental health: a 2013 review. Telemed J E Health. 2013;19:444–54.
4. Desmedt Y. "ome recent research aspects of threshold cryptography. In: Proc of ISW'97 1st International Information Security Workshop vol.1196 of LNCS paper 158–173 Springer-Verlag 1997.
5. Shivani S, Rajitha B, Agarwal S. XOR based continuous-tone multi secret sharing for store-and-forward telemedicine. Multimed Tools Appl. 2017;76:3851–70. https://doi.org/10.1007/s11042-016-4012-z.
6. Chen C-C, Wu W-J. A secure Boolean-based multi-secret image sharing scheme. J Syst Softw. 2014;92:107–14.
7. Feng JB, Wu HC, Tsai CS, Chang YF, Chu YP. Visual secret sharing for multiple secrets. Pattern Recogn. 2008;41:3572–81.
8. De Santis A, Desmedt Y, Frankel Y, Yung Y. How to share a function securely. In Proceedings of the twenty-sixth annual ACM symposium on Theory of Computing (STOC '94). Association for Computing Machinery, New York, NY, USA, 1994. 522–533. https://doi.org/10.1145/195058.195405.
9. Shamir A. How to share a secret? Comm ACM. 1979;22(11):612–3.
10. Blakley GR. Safeguarding cryptographic keys. In: Proceedings of AFIPS International Workshop on managing requirements knowledge. pp. 313. https://doi.org/10.1109/AFIPS.1979.98.
11. Asmuth C, Bloom J. A modular to key safeguarding. IEEE Trans Inf Theory. 1983;29(2):208–10.
12. Beimel A, Ben-Efraim A, Padró C, Tyomkin I. Multi-linear secret-sharing schemes. In: Lindell Y, editor. Theory of cryptography. TCC 2014. Lecture notes in computer science, vol. 8349. Berlin: Springer; 2014. https://doi.org/10.1007/978-3-642-54242-8_17.
13. Sarkar A, Dey J, Chatterjee M, Bhowmik A, Karforma S. Neural soft computing based secured transmission of intraoral gingivitis image in E-health. Indones J Electric Eng Comput Sci. 2019;14(1):178–84.
14. Gupta M, Gupta M, Deshmukh M. Single secret image sharing scheme using neural cryptography. Multimed Tools Appl. 2020;79:12183–204. https://doi.org/10.1007/s11042-019-08454-8.
15. Dey J, Karforma S, Sarkar A, Bhowmik A. Metaheuristic guided secured transmission of e-prescription of dental disease. Int J Comput Sci Eng. 2019;07(01):179–83.
16. Csirmaz L, Tardos G. On-line secret sharing. Des Codes Cryptogr. 2012;63:127–47. https://doi.org/10.1007/s10623-011-9540-y.
17. Deshmukh N, Nain N, Ahmed M. An (n, n)-Multi Secret Image Sharing Scheme Using Boolean XOR and Modular Arithmetic. In: 2016 IEEE 30th International Conference on advanced information networking and applications (AINA), Crans-Montana, 2016; pp. 690–697, https://doi.org/10.1109/AINA.2016.56.
18. Sarkar A, Dey J, Bhowmik A, Mandal JK, Karforma S. Energy efficient secured sharing of intraoral gingival information in digital way (EESS-IGI). In: Mandal J, Sinha D, editors. Social transformation—digital way. Communications in computer and information science, vol. 836. Singapore: Springer; 2018. (**ISSN: 1865-0929**).
19. Deshmukh M, Nain N, Ahmed M. Secret sharing scheme based on binary trees and Boolean operation. Knowl Inf Syst. 2019;60:1377–96. https://doi.org/10.1007/s10115-018-1268-9.
20. Mirjalili S, Gandomi AH, Mirjalili SZ, Saremi S, Faris H, Mirjalili SM. Salp Swarm Algorithm: a bio-inspired optimizer for engineering design problems. Adv Eng Softw. 2017;114:163–91.
21. Sarkar A, Dey J, Karforma S. Secured session key-based E-health: biometric blended with Salp swarm protocol in Telecare portals. In: Mandal J, Mukhopadhyay S, editors. Proceedings of the Global AI Congress 2019. Advances in intelligent systems and computing, vol. 1112. Singapore: Springer; 2020.
22. Yaseen ZM, Faris H, Al-Ansari N. Hybridized extreme learning machine model with salp swarm algorithm: a novel

predictive model for hydrological application. Complexity. 2020;8206245:14.

23. Cui LB, Wang XH, Wang HN. Challenges facing coronavirus disease 2019: Psychiatric services for patients with mental disorders. Psychiatry Clin Neurosci. 2020. https://doi.org/10.1111/pcn.13003 (**Epub ahead of print**).

24. Xiang Y-T, Yang Y, Li W, Zhang L, Zhang Q, Cheung T, et al. Timely mental health care for the 2019 novel coronavirus outbreak is urgently needed. Lancet Psychiatry. 2020. (**in press**).

25. Myers US, Birks A, Grubaugh AL, Axon RN. Flattening the curve by getting ahead of it: how the VA healthcare system is leveraging Telehealth to provide continued access to care for rural veterans. J Rural Health. 2020. https://doi.org/10.1111/jrh.12449 (**Epub ahead of print**).

26. Shigemura J, Ursano RJ, Morganstein JC, Kurosawa M, Benedek DM. Public responses to the novel 2019 coronavirus (2019-nCoV) in Japan: mental health consequences and target populations. Psychiatry Clin Neurosci. 2020. (**in press**).

27. Brooks SK, Webster RK, Smith LE, Woodland L, Wessely S, Greenberg N, et al. The psychological impact of quarantine and how to reduce it: rapid review of the evidence. Lancet (London, England). 2020. (**in press**).

28. Chen CL, Li CT. Dynamic session-key generation for wireless sensor networks. J Wirel Commun Netw. 2008;2008: 691571. https://doi.org/10.1155/2008/691571.

29. Meena U, Sharma A. Secure key agreement with rekeying using FLSO routing protocol in wireless sensor network. Wirel Pers Commun. 2018;101:1177–99. https://doi.org/10.1007/s11277-018-5755-9.

30. Azarderskhsh R, Reyhani-Masoleh A. Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks. J Wirel Com Netw. 2011. https://doi.org/10.1155/2011/893592.

31. Dwivedi R, Dey S, Sharma MA, et al. A fingerprint based crypto-biometric system for secure communication. J Ambient Intell Human Comput. 2020;11:1495–509. https://doi.org/10.1007/s12652-019-01437-5.

32. Kumar V, Kumar R, Pandey SK. Polynomial based non-interactive session key computation protocol for secure communication in dynamic groups. Int J Inf Technol. 2020;12:283–8. https://doi.org/10.1007/s41870-018-0140-1.

33. Bhowmik A, Sarkar A, Karforma S, Dey J. A symmetric key based secret data sharing scheme. Int J Comput Sci Eng. 2019;07(01):188–92.

34. Sarkar A, Dey J, Bhowmik A, Ferdows SS. A dynamic key generation scheme based on metaheuristic cuckoo search. Int J Comput Sci Eng. 2019;07(01):184–7.

35. Wang SH, Zhang Y, Li YJ, Jia WJ, Liu FY, Yang MM, Zhang YD. Single slice based detection for Alzheimer's disease via wavelet entropy and multilayer perceptron trained by biogeography-based optimization. Multimed Tools Appl. 2018;77(9):10393–417.

36. Mallick C, Bhoi SK, Panda SK, et al. An efficient learning algorithm for periodic perceptron to test XOR function and parity problem. SN Appl Sci. 2020;2:160. https://doi.org/10.1007/s42452-020-1952-8.

37. Heidari AA, Faris H, Aljarah I, et al. An efficient hybrid multilayer perceptron neural network with grasshopper optimization. Soft Comput. 2019;23:7941–58. https://doi.org/10.1007/s00500-018-3424-2.

38. Sakar CO, Polat SO, Katircioglu M, Kastro Y. Real-time prediction of online shoppers' purchasing intention using multilayer perceptron and LSTM recurrent neural networks. Neural Comput Appl. 2019;31:6893–908.

39. Struye J, Latré S. Hierarchical temporal memory and recurrent neural networks for time series prediction: an empirical validation and reduction to multilayer perceptrons. Neurocomputing. 2019. https://doi.org/10.1016/j.neucom.2018.09.098.

40. Tang X, Zhang L, Ding X. SAR image despeckling with a multilayer perceptron neural network. Int J Dig Earth. 2019;12(3):354–74.

41. Thomas P, Suhner MC. A new multilayer perceptron pruning algorithm for classification and regression applications. Neural Process Lett. 2015;42:437–58. https://doi.org/10.1007/s11063-014-9366-5.

42. Shaukat N, Ali DM, Razzak J. Physical and mental health impacts of COVID-19 on healthcare workers: a scoping review. Int J Emerg Med. 2020;13:40. https://doi.org/10.1186/s12245-020-00299-5.

43. Spoorthy MS, Pratapa SK, Mahant S. Mental health problems faced by healthcare workers due to the COVID-19 pandemic—a review. Asian J Psychiatry. 2020;51:102119.

44. Cai H, Tu B, Ma J, Chen L, Fu L, Jiang Y, Zhuang Q. Psychological impact and coping strategies of frontline medical staff in Hunan between January and March 2020 during the outbreak of coronavirus disease 2019 (COVID19) in Hubei, China. Med Sci Monit. 2020;2020:26.

45. Chan AOM, Huak CY. Psychological impact of the 2003 severe acute respiratory syndrome outbreak on health care workers in a medium size regional general hospital in Singapore. Occup Med Oxf Engl. 2004;54:190–6.

46. Ho CS, Chee CY, Ho RC. Mental health strategies to combat the psychological impact of COVID-19 beyond paranoia and panic. Ann Acad Med Singap. 2020;49:1–3.

47. Bhowmik A, Dey J, Sarkar A, Karforma S. Computational intelligence based lossless regeneration (CILR) of blocked gingivitis intraoral image transportation. IAES Int J Artif Intell (IJ-AI). 2019;8(3):197–204.

48. Dey J, Bhowmik A, Sarkar A, Karforma S. Privileged authenticity in reconstruction of digital encrypted shares. IAES Int J Artif Intell (IJ-AI). 2019;8(2):175–80.

49. Hauke J, Kossowski T. Comparison of values of Pearson's and Spearman's correlation coefficients on the same sets of data. Quest Geograph. 2011;30(2):87–93. https://doi.org/10.2478/v10117-011-0021-1.

50. Pearson K. On the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling. Philos Mag Ser. 1900;50:157–75.

51. Patel K. Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files. Int J Inf Technol. 2019;11:813–9.

52. Sarkar A, Dey J, Karforma S. Musically modified substitution-box for clinical signals ciphering in wireless telecare medical communicating systems. Wirel Pers Commun. 2021. https://doi.org/10.1007/s11277-020-07894-y.

53. Alexopoulos AR, Hudson JG, Otenigbagbe O. The use of digital applications and COVID-19. Community Ment Health J. 2020;56:1202–3. https://doi.org/10.1007/s10597-020-00689-2.

54. Owusu PN. Digital technology applications for contact tracing: the new promise for COVID-19 and beyond? Glob Health Res Policy. 2020;5:36. https://doi.org/10.1186/s41256-020-00164-1.

55. Dey J, Chowdhury B, Sarkar A, Karforma S. Patients' data security in telemedicine consultation in a "New Normal" post COVID-19 perspective. J Math Sci Comput Math. 2021;02(03):422–5. https://doi.org/10.15864/jmscm.2308 (**ISSN 2688-8300(Print) ISSN 2644-3368 (Online)**).

56. Dey J, Sarkar A, Karforma S. Newer post-COVID perspective: Teledental encryption by de-multiplexed perceptrons. Int J Inf Technol. 2021. https://doi.org/10.1007/s41870-020-00562-1.