Neural Computing and Applications (2023) 35:9517–9533
https://doi.org/10.1007/s00521-022-08169-2

ORIGINAL ARTICLE

State-of-the-art session key generation on priority-based adaptive neural machine (PANM) in telemedicine

Joydeep Dey[1]

Received: 31 May 2022 / Accepted: 6 December 2022 / Published online: 22 March 2023

Abstract
Telemedicine is one of the safest methods to provide healthcare facilities to the remote patients with the help of digitization. In this paper, state-of-the-art session key has been proposed based on the priority oriented neural machines followed by its validation. State-of-the-art technique can be mentioned as newer scientific method. Soft computing has been extensively used and modified here under the ANN domain. Telemedicine facilitates secure data communication between the patients and the doctors regarding their treatments. The best fitted hidden neuron can contribute only in the formation of the neural output. Minimum correlation was taken into consideration under this study. Hebbian learning rule was applied on both the patient's neural machine and the doctor's neural machine. Lesser iterations were needed in the patient's machine and the doctor's machine for the synchronization. Thus, the key generation time has been shortened here which were 4.011 ms, 4.324 ms, 5.338 ms, 5.691 ms, and 6.105 ms for 56 bits, 128 bits, 256 bits, 512 bits, and 1024 bits of state-of-the-art session keys, respectively. Statistically, different key sizes of the state-of-the-art session keys were tested and accepted. Derived value-based function had yielded successful outcomes too. Partial validations with different mathematical hardness had been imposed here too. Thus, the proposed technique is suitable for the session key generation and authentication in the telemedicine in order to preserve the patients' data privacy. This proposed method has been highly protective against numerous data attacks inside the public networks. Partial transmission of the state-of-the-art session key disables the intruders to decode the same bit patterns of the proposed set of keys.

Keywords Telemedicine · PANM · State-of-the-art session key · Partial validation

1 Introduction

There occurred abrupt changes in all spheres of life since the cameo of COVID-19. Due to COVID-19 pandemic limitations, medical organizations had shifted at online telecare health systems. This critical phase of novel corona virus had allowed us to opt for remote online services. Different E-health applications had tremendously supported the medical systems throughout the world. Patients can get their treatments benefits through such remote services. To reduce the redundant costs likes of traveling costs and others, and noscomial infections, a larger section of the populations had underwent the Telecare Health services in terms of their check-ups, regular follow-ups, and expert treatment views, etc. The Internet facilities have fueled the telecare health system amidst COVID-19 [1, 2]. Such online telecare health systems mainly deal with the patients' private medical reports and data. It includes E-prescriptions, clinical and pathological reports, CT and MRI scan images, ECG, NCV, etc. These data must be protected against the middle way attackers in the open channel. To deal with the data security and privacy, cryptographic engineering can be used to make such confidential data more secure.

Certainly, there are plenty of patients' data security related alarming issues in the telemedicine systems. The disclosures of the patients' data to the intruders can lead to several major hazards such as patient embarrassment, loss of reputation, legal consequences, loss of trust, financial loss. The patients may not be able to claim their legal treatment bills and appropriate legal steps. Once such

✉ Joydeep Dey
joydeepdey@mucwcburdwan.org

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

patients' confidential data are available to the intruders they can withstand the entire data or partial data. It can result to very poor quality of treatment in the telemedicine services, legal faults, and economic loss to the patients. Intentionally, the intruders will modify the patients' medical reports and hence wrong treatment of the patients can happen along with poor management of the system. Partial treatments can also occur in such data damage done by the intruders. Telecare health systems enable the non-invasive and non-critical patients to interact with their physicians from distant places [1, 2]. During the COVID-19 lockdown phase, telemedicine was the safest method adopted to treat the non-critical patients from the remote locations. Cryptographic scientists are continuously endeavoring to develop stronger system with stronger security features. In Diffe—Hellman key exchange protocol, there is an exchange of session key between the users for symmetric key cryptographic functions. There exist some problems likes of it lacks the authentication part of the users applied only on the symmetric key cryptography which can lead to many vulnerabilities inside the wireless networks [3]. Also this protocol is a bit more expensive. Eavesdroppers can guess the orientation of the session key. They can do it by feeding the fetched data into numerous parallel existing ANNs of different topological configurations.

This paper deals with implementation of Priority based Neural Machine (PANM) at the user levels of the Telemedicine to generate state-of-the-art session key. Artificial Neural Networks (ANNs) are inspired from neural processing of the human brain. ANN is a mathematical model to optimize various problems using the machine learning language. It is an adaptive model having the input, hidden and output neurons. Tree Parity Machine (TPM) is a type of ANN in which two TPMs establish a common session key after synchronization. The purpose of the TPM is to have synchronized their synaptic links through iterative simulations without exchanging the vectors. Hebbian learning rule has been stated at the following Eq. 1, which has been used here. Thus, the session key that needs not to be transported through the public medium. Although the architecture of both the TPMs must be equivalent. The learning rule of TPM has been mentioned below with respect to this proposed scheme [4]. The author had implemented adaptive TPM based on configuration as PANM in this paper Eq. (1)–Hebbian Rule.

$$w_i^+ = f\left(w_i + \sigma_i x_i \theta(\sigma_i \tau)\theta\left(\tau^A * \tau^B\right)\right) \tag{1}$$

In the above equation number 1, the term theta function 'θ' will provide + 1 when its inputs are all positive values, else 0 will be provided. And the function 'f' is a function which will bound the maximum or minimum boundary of the weight vectors [5].

$$f(w) = \begin{cases} \text{Signum}(w)*L & ;|w|L \\ w & ; \text{else} \end{cases} \tag{1.1}$$

The definition of Signum function has been provided in the next section.

1.1 Author's contributions

State-of-the-art session key synchronization is the main objective of this paper in the Telemedicine domain. In this paper, the best fitted hidden neuron of the proposed PANM can be selected by the proposed technique to have its efficacy in the telemedicine system. The inputs were kept tightly hidden from the external agents and the intruders. To reinforce data security on the patients' data, it has been proposed so. The correlation cannot be determined by the intruders during the patients' data transmission phase. Thus, the neural machines at the patient's end and the doctor's end are adaptive in configurations. All the hidden neurons do not participate in the contribution of the Tree Parity Machine's (TPM) output. So, the time complexity of the TPMs synchronization can be made lower. With the change in its weight system, the best fitted hidden neuron can be changed with the adaptive nature. Lesser iterations were found for proposed TPM synchronization when compared with existing TPM on the same data. In the later phase, an authentication protocol has also being added in the proposed algorithm. Only partial state-of-the-art session key bits were passed in the public medium in two way communication. Thus, the users' authenticity can be examined in the Telemedicine system.

1.2 The Composition

This paper has been composed as follows. Section 1 has the introduction segment. Section 2 contains the background knowledge. Section 3 presents the review of literature. Section 4 describes the present constraints in functioning of telemedicine. Section 5 contains the proposed solution. Section 6 gives the proposed research methodology in details. The experimental results were mentioned in Sect. 7 with detailed explanations. Section 8 has the conclusions, limitations, and future scope. Acknowledgement, Funding Statement, Ethical Statements, and References are added then.

2 Background Knowledge

In the crucial phase of COVID-19 pandemic, telemedicine support was the main stream of treatment procedures in case of non-emergency, non-invasive, and non-critical patients. The cameo of COVID-19 had rapidly accelerated the digital

healthcare transformations with better patients' management capacity. Telemedicine was the safest way to interact between the patients and the doctors. In case of chronic cardiac patients, the patients can remotely be monitored through IoT based telemedicine. Patients' cardiac related data can be made in live sensing mode, so that the cardiologists may monitor those cardiac signals. It may include ECG, Holter Monitoring, BP, etc. Psychiatric patients can be treated through telepsychiatry. General patients can get the treatment services by using this telemedicine. Virtual consultations with doctors will terminate the traveling hazards and can be fitted easily into the patients' daily schedule. Not only it reduces the time consumption but also the overall treatment costs of the patients. The registered medical practitioners can provide diverse treatment services through computerized mode of telemedicine. The telemedicine venture was almost initiated with emergency with the rise in corona virus positive patients. Through this venture, the patients can transmit their medical data in secure way. Different laboratory reports, prescriptions, etc. can be shared between the patients and the physicians in a more protected manner. It is matter of high confidentiality that the patients' data should not be available to the external intruding agents. It must be made secure during the phase of online transmission inside the open medium. To prevent the data security breaches of conduct, cryptographic science is the most suitable thing to protect the patients' private data [6, 7]. The most common techniques that could widely be used in the healthcare domain are data encryption and data decryption. Adaptive artificial neural networks can be arranged to get more stronger and efficient cryptographic functions. Encrypting the patients' data is the way to hide from external entities in any phase of its transmission cycle [8]. It could be from Key Distribution Centre, doctor's terminals, patient's terminals, management's terminals, etc. It protects the data sniffing of medical packets. Decryption is the inverse process of the encryption technique. In symmetric key encryption, it is strongly based on the same key at the doctor's terminal and patient's terminal and the key can be generated through mathematical algebraic theory [9, 10]. The similar key is the symmetric session key which needs to be highly robust in terms of true randomness. The problem in such case is the session key exchange between the nodes which is a challenging issue in this era. The probable solution to this problem in the healthcare domain is the neural cryptographic science. In neural cryptographic science, the common secret key can be formed at the both terminals without exchanging the key. The neural machines kept at the patient's terminal and the doctor's terminal can be made auto synchronized to form the unique secret key. It is extremely difficult to intervene the secret key in such neural cryptographic science by the intruders. The architecture of those neural networks is known to the intruders too. Tree Parity Machine (TPM) is also a special type of multilayer neural machine that can be placed at both the users of the telemedicine system. Such TPMs will be topologically equivalent in their functioning. Both the users can tune their TPMs to generate the similar weight vectors. They initialize random weight vectors and random inputs were fed into them. The input vectors are made secret from external agents for the security issues. Both the TPMs can generate their outputs and they share between themselves followed by weight adjustments. Such procedure can be repeated until both the TPMs get similar weight vectors. The following Figure 1 displays the basic Tree Parity Machine.

In Fig. 1, the TPM has three layers, namely input layer, hidden layer, and output layer. In the input layer (N) it has four neurons, and three hidden neurons (K) and one neuron is present in the output layer. The range of the weight vectors are [− L, + L]. N number of input neurons with input vector as $x_{ij} \in \{-1, 0, +1\}$, the weight vectors are generated in between $-L$ & $+L$. The output of the hidden unit can be calculated as the weighted sum with the input vectors. It is given in the following Eq. 2.

$$H_i = \sum_{i=1}^{N} (w_i * x_i) \tag{2}$$

The intermediate output of the ith hidden neuron (K) can be found through Eq. 3.

$$\sigma_i = Signum(H_i) \tag{3}$$

Signum is a very simple linear function which can return 1,0, or −1.

If $(Signum(t) > 0)$ then.
Return (+ 1).
Else if $(Signum(t) < 0)$ then.
Return (−1).
Else.
Return (0).
End if.

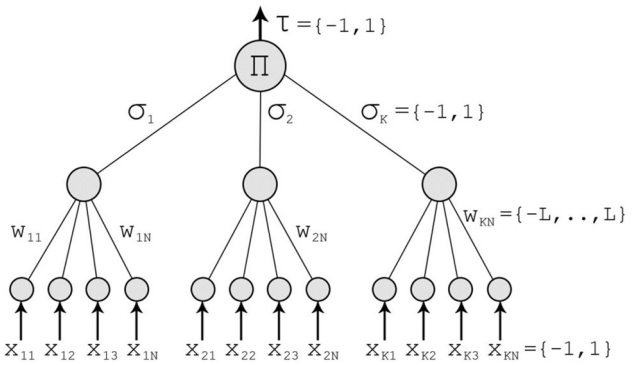

Fig. 1 Sample TPM Structure

The output of the TPM can be calculated as the product of the hidden neurons. It has been represented in the following Eq. 3.

$$\tau^{TPM} = \prod_{i=1}^{K} \sigma_i \tag{4}$$

The TPM of patient (P) and TPM of doctor (D) will receive get random weight vectors $w_i^{P/D}$. The input vectors are randomly fed into the TPMs. And the TPMs' output bits $\tau^{P/D}$ and $\tau^{D/P}$ were generated in every iteration. These outputs of both the TPMs will be shared between themselves. If they are unequal then $\tau^P \neq \tau^D$, the weights will not be adjusted. Else the learning rules for weight vector synchronization will be used in every iteration. Any one of the following three rules can be applied on the neural TPMs Hebbian Rule [4]–Eq. (5), Anti-Hebbian Rule [10]–Eq. (6), Random Walk [11]–Eq. (7).

$$w_i^+ = f\left(w_i + \sigma_i x_i \theta(\sigma_i \tau)\theta\left(\tau^P * \tau^D\right)\right) \tag{5}$$

$$w_i^+ = f\left(w_i - \sigma_i x_i \theta(\sigma_i \tau)\theta\left(\tau^P * \tau^D\right)\right) \tag{6}$$

$$w_i^+ = f\left(w_i + x_i \theta(\sigma_i \tau)\theta\left(\tau^P * \tau^D\right)\right) \tag{7}$$

In the above equation numbers 5–7, the term theta function 'θ' will provide + 1 when its inputs are all positive values, else 0 will be provided. And the function 'f' is a function which will bound the maximum or minimum boundary of the weight vectors [5].

3 Review of literature

Francke J.A. et al. [12] had surveyed a group of patients who took telehealth treatments during the COVID-19. It had provided healthcare services in the critical hours. Alonso S.G. et al. [13] had reviewed the benefits of telemedicine applications during the COVID-19 era to cure the patients from remote locations. It had helped to resist the transmission of corona virus. Telemedicine had served the mankind a lot. Ghosh A. et al. [14] had given suggestions for the diabetic patients during the national lockdown of COVID-19. They had given certain guidelines to be followed by the diabetic patients for their well-being. Abo-Zahhad M. et al. [15] had reviewed emergency telemedicine applications which can monitor the patients' health conditions. Hatcher-Martin J.M. et al. [16] had discussed the importance of telemedicine in the field of neurology. They had reviewed the pivotal role played by telemedicine to treat neurological problems except brain stroke. Norman S. [17] had explained the use of telemedicine supports in the field of psychiatric treatments. Psychiatric patients can be treated easily through digital media. Tresenriter M. et al. [18] had stated the fruitful implementation of telehealth on emergency medicine in the phase of corona virus pandemic. Plenty of patients were successfully treated through this approach. Bokolo A. et al. [19] had explored the adoption of virtual platform based online treatments for the outpatients in the period of COVID-19. Yang L. et al. [20] had stated that video consultations had accelerated the treatment process for the ambulatory neurological patients in COVID-19. Chauhan V. et al. [21] had leveraged telemedicine to optimize the corona virus transmission and patients' exposures. Due to prolonged lockdown and quarantine protocols, patients could be managed through telehealth services in case on non-invasiveness during the COVID-19 period. Jnr Bokolo A. [22] had used the telemedicine to treat the patients remotely in the hours of COVID-19 pandemic. Dey J. et al. [23] had proposed a wireless telehealth secure system through amino acids oriented harder encryption. Sarkar A. et al. [24] had designed a new secure transmission system on the intraoral data through electronic health. They had proposed a newer secret sharing method in groups. Rahman S. et al. [25] had viewed the impact of corona virus and telehealth on mental well-being in Bangladesh. Dash S. et al. [26] had discussed the telemedicine novelties during COVID-19 along with its challenges. It is recommended to address those challenges.

Lei X. et al. [27] had designed two-layer feed-forward artificial neural network model for neural cryptography purpose. Synchronization speeds were found to be better in their study with respect to other TPMs. Allam A. M. et al. [28] had described an authenticated session key exchange mechanism in the neural cryptography. Dey L. et al. [29] had developed a machine learning method to detect interactions between the human proteins and SARS-CoV-2 virus. Their technique had shown efficient and accurate results. Jeong S. et al. [30] had proposed vector-value based TPM for the key exchanges in the real life. Their protocol had shown higher degree of data security. Mislovaty R. et al. [31] had considered a combined neural synchronization model which can transmit secret keys in open medium. To transmit the session keys through the public medium was a big challenge. Rosen M. et al. [32] had reviewed various TPM synchronization methods, so that the discrete weights get synchronized equally after the iterations. The synchronization of discrete parity machines was done to have an ephemeral key-exchange mechanism in the public channel. Dolecki M. et al. [33] had stated the impact of tree parity machine's weight distribution on Neural Netwirk synchronization period. Ruttor A. et al. [34] had proposed synchronization of artificial neural networks in public medium for bidirectional weight vectors. They had designed attractive and repulsive forces to make the neural vectors unique in both ends. Neural cryptography has been designed to make the Brute-force attack non-

feasible. M. Volkmer et al. [35] had generated fast key generation by TPMs in the symmetric key cryptography. They had reduced the cost when compared to others. Santhanalakshmi S. et al. [36] had developed neural network synchronization with the genetic approach for the purpose of secure key generation protocol. Han Y. L. et al. [37] had designed an improved technique for neural key synchronization. Their objective was to evaluate the synchronization time needed in the artificial neural networks.

4 Present constraints in functioning

In web-based telemedicine frameworks, the serious issue is the safe conveyance of the secret key between the patients and the doctors inside the open medium. At the hour of trade of the secret key over open channel, gatecrashers can intercede that key by various possible phishing assaults. This specific issue must be tended to in this vital period of COVID-19 pandemic. Positively, there are huge loads of patients' information security related disturbing issues in the telemedicine frameworks. When such patients' secret information is free to the interlopers they can endure the whole information or halfway information. It can result to extremely low quality of treatment in the telemedicine administrations, lawful deficiencies, and monetary misfortunes, etc. to the various categories of patients. Deliberately, the gatecrashers will change the patients' clinical reports and henceforth remote treatments through telemedicine can occur alongside unfortunate administration of the framework. Halfway treatments can likewise happen in such information harm done by the gatecrashers. Different kinds of attacks or noxious activity could spoil activity of the clinical reports and information and upset the correspondence art of the telecare frameworks. An ordinary method for attack incorporates adjusting or changing of the messages or reports. The clinical data and information which are to be conveyed online is very touchy and fundamental for the patients' medicines. So any enemy assaults on such data or information will causes risk for the patients protection and security. Progressed stages on different COVID-19 telecare frameworks were used without having patients' suitable security. Same transmission or session key is used for each various gatherings to abridge the key generative costs. Through phishing attacks, the employees of the telehealth organization may click to unknown links and thus their credentials are automatically leaked to the intruders [38]. Thus, all the medical data are available to the intruders, and now the patient will bring charges against the telehealth organization for not providing proper data security to them [39]. Ransomware attacks were very much common in this COVID-19 pandemic.

Interlopers catching the clinical reports or medicines in the patients and the doctors and attempt to snatch all the data sending from double closures. Diffie-Hellman key trade procedure [40] experiences this kind of issues. Gatecrashers can reenact as the clients of the COVID-19 Telecare frameworks and all the while and attempt to re-establish the session key at the hour of trading key inside the public medium. At the point when it gets compromised then all clinical data of that session will be theft by the gatecrashers. Consequently, the cipher code text is outstandingly disposed to the center way attacks. In case the public transmission ways get compromised, any clinical data going through that association will be taken by the clowns. Subsequently, the patient and the expert are presumably going to be affected generally in all respect. It might prompt phony clinical cases too. Thus, an expedited secret key synchronization between the patient and the doctor should be designed intelligently. It is an urgent approach to design a secure key agreement system which may resist Brute force attacks and Man-In-The-Middle attacks. Patients' clinical data security will be hampered enormously. More to say that, patients' treatment strategies will be in danger as it was edited to accept data correspondence.

5 Proposed solution

The above-stated constraints in the earlier section were being addressed in this proposed solution approach. The biggest constraint in Telemedicine was the transfer of session key between the users. In this proposed method, we have tried to develop state-of-the-art session key with the help of Priority based Adaptive Neural Machine (PANM). Soft computing has been generously accessed to generate the state-of-the-art session key. Soft computing method used is artificial neural network. Soft computing can be regarded as one of the cutting-edge technologies of the present day. So the proposed key generation technique can be fitted as state-of-the-art session key generation. Only the best fitted neuron can be selected which will participate in the formation of the neural output. The correlation between the sum of weight vectors and the hidden neurons' output will be calculated. The most suited hidden neuron will contribute to the overall TPM output here. So after the synchronization process, both the patient TPM and the doctor TPM will have the same value as the proposed session key. In contrast, the normal TPM synchronization techniques take more time to auto synchronize

Fig. 2 Proposed flow diagram

their weight vectors. The weight vector has been synchronized after several iterations in latter cases. But the problem was noted in the verification of the identical bits inside the weights of the patient TPM and doctor TPM in existing models. When the entire vector is transferred through the open channel then it can be captured by the wrong intruders. This problem has also been addressed in this strategy. A novel session key validation has been proposed through partial validation. Half of the state-of-the-art session key will be shared to the destination TPM. Then it will be authenticated through the proposed mathematical functions. In the next way, the remaining of state-of-the-art session key will be authenticated. The Man-In-The-Middle attacks inside the Telemedicine can be ignored by this proposed strategy. Thus, the patients' privacy can be preserved in an efficient way.

6 Proposed research methodology

This paper deals to generate state-of-the-art session key in less time along with the session key validation procedure in the public channel of telemedicine. The term state-of-the-art reflects the modern scientific tools used in this methodology. The author had used soft computing to generate the state-of-the-art session key. Soft computing includes artificial neural networks and mathematical calculations done in this method here. Priority has been assigned to all the hidden neurons based on the correlation value. Correlation coefficient (r) was checked between sum of weights and hidden neuron outputs. The most acceptable correlation with closed to zero value could be selected. Thus, that neuron will directly contribute to the TPM output. The partial validation procedure has been proposed on the proposed state-of-the-art session keys. The authentication was done to resist different types of attacks inside the open medium. Intruders are staying silently for the phishing attacks. The proposed state-of-the-art session key generation method can be very much relevant in respect to the telemedicine systems in this pandemic era.

6.1 Proposed block diagram

In the following Fig. 2, the proposed block diagram has been shown.

In Fig. 2, the flow model can be understood. In telemedicine, both the patient neural machine and doctor neural machine will receive the same inputs and random weight vectors. Since the author had used adaptive neural machines, so the best sited neuron in the hidden layer will be active in the neural output formation. By

using Hebbian rule, best fitted neuron will be selected as described below [4]. After the complete synchronization, both the machines will have the same session key. Lastly, the author had given an authentication protocol on the proposed state-of-the-art session key.

6.2 Proposed research techniques

An adaptive neural machine has been used in this paper. Priority based Adaptive Neural Machines (PANM) were designed at the terminals' of telemedicine system. In existing TPMs, all the neurons of the hidden layer can participate to the formation of TPM output. But in this case, only the best suitable hidden neuron of TPM will be activated, and the corresponding neural output will be created. The best suitability of the hidden unit can be determined by the statistical correlation between the sum of weights and hidden output. Same input vector will be inserted into both the neural machines of the patient TPM and doctor TPM. It has been done to foster the patients' data privacy. This proposed technique also validates the state-of-the-art session key. Partial bits of the state-of-the-art session key are transmitted for validation in first step. And in the next step, the rest of the bits of session key are transmitted and then validated accordingly.

Proposed Main Algorithm: *State-of-art Session Key Generation in PANM*

Input(s): Input Vector (x_i), No. of Hidden Neurons (K), Hidden Neural Output (σ_i), Key Size (KS)
Output(s): SASK: Required Session Key, and its validation.

1. While (KS)
2. Set m=0
3. For i = 1 to K
4. Evaluate $H_i = \sum_{i=1}^{K}(x_i * w_i)$
5. Hidden Unit(σ_i) = $Signum(H_i)$
6. End for
7. Priority Hidden Unit (K_{pr})= ***Call Priority Hidden Neuron***(x_i, K, σ_i)
8. Evaluate TPM outcome as $\tau_{TPM} = \sigma_{pr}$
9. SASK[++m]= τ_{TPM}
10. End while
11. Result=***Call State-of-art Session Key Validation(SASK[KS])***
12. If (Result=1) then
13. Ready SASK[KS] as State-of-art Session Key
14. Else
15. Invalid State-of-art Session Key

The above-mentioned algorithm authenticates the proposed state-of-the-art session key in a novel bidirectional way. It is two way validations. Both the patient TPM and doctor TPM will participate in its way to make sure regarding the authenticity of the session key. If any one way fails, then the entire authentication gets failed.

Proposed Algorithm: *Priority Hidden Neuron*

Input(s): Input Vector (x_{ij}), $Weight\ Vectors\ (W_{ij})$, Hidden Neural Output ($\sigma_i$)
Output(s): Best fitted hidden Neuron(K_{pr})
Method(s): The hidden unit having the correlation value closest to zero will be selected as the best fitted neuron. The correlation will be calculated between the sum of weights and hidden neural output. The maximum repeated hidden neural output will be the output of the entire TPM as it gets the priority based on lowest correlation.

1. For i = 1 to 10
2. SoW(i)= $\sum_{i=1}^{K} w_i$
3. Corr[i]= Correlation (SoW(i), σ_i)
4. For i = 1 to K
5. *Apply* ***Hebbian Rule***: $w_i^+ = f\ (\ w_i + \ \sigma_i x_i\ \Theta\ (\sigma_i\ \tau\ )\ \Theta\ (\tau^A * \tau^B\ )\ )$
6. End for
7. End for
8. Return ***Min_Correlation*** (Hidden Neural Unit) as best fitted neuron

Proposed Algorithm: State-of-art Session Key Validation

Requirement(s): Let the length of the weight vector be D length at both TPMs of the patient and doctor.
Input(s): Vector WA[D]and WB[D]of two TPM(Sv)and TPM(Dv).
Output(s): True or false in case of success or failure respectively for every iteration, true at the final iteration.
Method(s): Half of the patient TPM's weight vector has been rotated first. Then it will be transmitted to the doctor TPM. The doctor TPM will next validates the received vector to return the valid string. Source TPM performs bits extraction and final validation to achieve full synchronization.

/*Ciphering on rotated weight vector by patient TPM(Sv) */
1. CP[D/2]←Call **Cipher on Rotate(WA[D/2])**

/*Partial Transmission to doctor TPM(Dv)*/
2. Call Public Transmission(TPM(Sv),TPM(Dv),CP[D/2])

/* State-of-art Session Key Validation by doctor TPM(Dv)*/
3. Result1←Call **Partial Validation**(RCW[D/2], TPM(Dv)

/*Ciphering on rotated weight vector by doctor TPM(Sv) */
4. CD[D/2]←Call **Cipher on Rotate(WB[D/2])**

/*Partial Transmission to patient TPM(Sv)*/
5. Call Public Transmission(TPM(Dv),TPM(Sv),CD[D/2])

/* State-of-art Session Key Validation by doctor TPM(Dv)*/
6. Result2←Call **Partial Validation**(RCW[D/2], TPM(Sv)

/* Bidirectional Authentication Completion*/
7. If (Result1 = True AND Result2 = True) then
8. Authentication of State-of-art session key is success
9. Else
10. Authentication of State-of-art session key is failure
11. End if

Proposed Algorithm: Cipher on Rotate ($W\left[\frac{D}{2}\right]$)

Requirement(s): Let the session key be of length D
Input(s): Session Key by the Patient or Doctor TPM, W[D/2] as an array
Output(s): Half length cipher weight vector of patient TPM(Sv) or doctor TPM (Dv)
Method(s): First half of the bits extracted from session key of patient TPM(Sv) followed by a left shift with carry, and subsequent XOR operations in a specific pattern to generate the desired cipher text. In the second round last half of the bits extracted from session key of doctor TPM(Dv) followed by subsequent XOR operations in a specific pattern to generate the desired cipher text.

1. For i=0 to {(D/2) – 1}
   PCW[i]←**Call Concatenation**(W[i])
2. i= i+1
3. End for
4. $Temp\left[\frac{D}{2}-1\right] \leftarrow PCW[0]$
5. J=(D/2) – 2
6. For i= {(D/2) – 1 } to 1
7. Temp[j]←PCW [i]
8. i=i-1
9. j=j-1
10. End for
11. GC[0] = Temp[0]
12. For i= 1 to ((D/2)-1)
13. GC[i]← (GC[i] XoR Temp[i+1])
14. i=i+1
15. End for
16. Return GC[D]

Proposed Algorithm: *Partial Validation*

Requirement(s): Length of the session key, D and the received ciphered text vector, RCW[D/2]
Input(s): RCW[D/2]:Received Encrypted Session key & WB[P]: Session key of TPM(Dv)
Output(s): Intermediate session key of length P or False value to terminate algorithm
Method(s): Received session key has been decoded with inverse XOR operation and then remaining half bits were added. Now it will fully validate to make its authentication with own session key.

```
1.  Temp1[0] = RCW[0]
2.  For i=  1 to ((D/2)-1)
3.     Temp1[i ]← ( Temp1[i] XoR RCW[i-1] )
4.     i=i+1
5.   End for
6.  For i = {(D/2)+1} to (D-1)
7.     RCW[i] ← Call StringConcat( W[i])
8.     i=i+1
9.  End for
10. For i =  0 to ( D-1)    /* Bitwise XOR operation*/
11.    IRES[i]←Call BitwiseXOR( W[i], RCW[i])
12.    i=i+1
13. End for
14. If (  ! Call EqualCheck(IRES[D], 0 )  THEN
15.          Return False
16. Else
17.          Return True
18. End if
```

7 Experimental results

In this paper, Priority based Adaptive Neural Machine (PANM) has been proposed at the patient and the doctor. As we all know that the strength of the session key determines the scalability of any cryptographic engineering techniques. The configuration of the author's computing device is: Intel processor (i3), 8 GB RAM, 1 TB SSG, and Windows 10 (64 bits). High level language (C) was used in this paper to synchronize the PANM of the patient and the doctor in telemedicine. The reason behind selecting C in this paper was its flexibility and easy to develop the programs. Also C language provides a lot of variations in the data types. MS Office Excel (version 10) was also used to have different statistical calculations. Patients' data security was main the main focus in this newer method of neural machines synchronization. In this segment, we have performed numerous mathematical tests on the derived state-of-the-art session keys. The following tests were primarily carried out to prove the efficacy of the proposed technique.

Table 1 Acronym of NIST

Serial number	Name of NIST	Used name here
1	Frequency test	TEST CODE:01
2	Frequency (Block-wise) test	TEST CODE:02
3	Run test	TEST CODE:03
4	Longest run of ones in block test	TEST CODE:04
5	Binary matrix run test	TEST CODE:05
6	Discrete fourier transformation test	TEST CODE:06
7	Non overlapping template matching test	TEST CODE:07
8	Overlapping template matching test	TEST CODE:08
9	Maurer's universal statistical test	TEST CODE:09
10	Linear complexity test	TEST CODE:10
11	Serial test	TEST CODE:11
12	Approximate entropy test	TEST CODE:12
13	Cumulative sum test	TEST CODE:13
14	Random excursiontest	TEST CODE:14
15	Random excursion variant test	TEST CODE:15

Table 2 NIST on proposed State-of-the-art Session Key Length 56bits

Assigned Id	*p*-value	Significant *p*-value	Result (Tr: passed or Fl:Failed)
TEST CODE:01	0.245	≤ 0.05	Tr
TEST CODE:02	0.316	≤ 0.05	Tr
TEST CODE:03	0.328	≤ 0.05	Tr
TEST CODE:04	0.267	≤ 0.05	Tr
TEST CODE:05	0.207	≤ 0.05	Tr
TEST CODE:06	0.319	≤ 0.05	Tr
TEST CODE:07	0.221	≤ 0.05	Tr
TEST CODE:08	0.147	≤ 0.05	Tr
TEST CODE:09	0.168	≤ 0.05	Tr
TEST CODE:10	0.352	≤ 0.05	Tr
TEST CODE:11	0.281	≤ 0.05	Tr
TEST CODE:12	0.207	≤ 0.05	Tr
TEST CODE:13	0.381	≤ 0.05	Tr
TEST CODE:14	0.271	≤ 0.05	Tr
TEST CODE:15	0.322	≤ 0.05	Tr

Table 3 NIST on proposed State-of-the-art Session Key Length 128 bits

Assigned Id	*p*-value	Significant *p*-value	Result (Tr: Passed or Fl:Failed)
TEST CODE:01	0.184	≤ 0.05	Tr
TEST CODE:02	0.309	≤ 0.05	Tr
TEST CODE:03	0.251	≤ 0.05	Tr
TEST CODE:04	0.355	≤ 0.05	Tr
TEST CODE:05	0.269	≤ 0.05	Tr
TEST CODE:06	0.203	≤ 0.05	Tr
TEST CODE:07	0.321	≤ 0.05	Tr
TEST CODE:08	0.148	≤ 0.05	Tr
TEST CODE:09	0.154	≤ 0.05	Tr
TEST CODE:10	0.217	≤ 0.05	Tr
TEST CODE:11	0.301	≤ 0.05	Tr
TEST CODE:12	0.291	≤ 0.05	Tr
TEST CODE:13	0.322	≤ 0.05	Tr
TEST CODE:14	0.234	≤ 0.05	Tr
TEST CODE:15	0.196	≤ 0.05	Tr

7.1 Statistical test

NIST Test Suite [41] is a measurements tool that involved fifteen (15) statistical tests. Its goal is to decide the randomness of the proposed session key. The indexing of these tests can be found in the following Table 1. Robustness attribute can be evaluated through those tests. The *p*-values observed were noted in the following table based on the size of the session key. The first ten tests were considered under proposed technique with better efficacy.

The proposed session keys that were generated through the TPMs kept at the both ends. The efficacy of those keys in the ray of robustness can be found in the following Tables 2, 3, 4, 5 and 6.

In the above-presented Tables 2, 3, 4, 5 and 6, the significant *p*-value is ≤ 0.05 under 5% significance levels. The obtained *p*-values were greater than 0.05 i.e., rejecting the null hypothesis, and the proposed session keys were totally random in nature.

7.2 Derived value based function

In this sub-section, the derived value which is based on a proposed function has been analyzed in details. It has been mentioned in the following Eq. 8.

Table 4 NIST on proposed State-of-the-art Session Key Length 256 bits

Assigned Id	*p*-value	Significant *p*-value	Result (Tr: passed or Fl:Failed)
TEST CODE:01	0.307	≤ 0.05	Tr
TEST CODE:02	0.254	≤ 0.05	Tr
TEST CODE:03	0.178	≤ 0.05	Tr
TEST CODE:04	0.233	≤ 0.05	Tr
TEST CODE:05	0.299	≤ 0.05	Tr
TEST CODE:06	0.344	≤ 0.05	Tr
TEST CODE:07	0.304	≤ 0.05	Tr
TEST CODE:08	0.276	≤ 0.05	Tr
TEST CODE:09	0.234	≤ 0.05	Tr
TEST CODE:10	0.360	≤ 0.05	Tr
TEST CODE:11	0.301	≤ 0.05	Tr
TEST CODE:12	0.269	≤ 0.05	Tr
TEST CODE:13	0.354	≤ 0.05	Tr
TEST CODE:14	0.160	≤ 0.05	Tr
TEST CODE:15	0.165	≤ 0.05	Tr

Table 5 NIST on proposed State-of-the-art Session Key Length 512 bits

Assigned Id	*p*-value	Significant *p*-value	Result (Tr: passed or Fl:Failed)
TEST CODE:01	0.331	≤ 0.05	Tr
TEST CODE:02	0.369	≤ 0.05	Tr
TEST CODE:03	0.204	≤ 0.05	Tr
TEST CODE:04	0.352	≤ 0.05	Tr
TEST CODE:05	0.290	≤ 0.05	Tr
TEST CODE:06	0.315	≤ 0.05	Tr
TEST CODE:07	0.309	≤ 0.05	Tr
TEST CODE:08	0.246	≤ 0.05	Tr
TEST CODE:09	0.264	≤ 0.05	Tr
TEST CODE:10	0.328	≤ 0.05	Tr
TEST CODE:11	0.221	≤ 0.05	Tr
TEST CODE:12	0.207	≤ 0.05	Tr
TEST CODE:13	0.344	≤ 0.05	Tr
TEST CODE:14	0.224	≤ 0.05	Tr
TEST CODE:15	0.208	≤ 0.05	Tr

$$\mathrm{DV}_{\mathrm{Len}}^{\mathrm{Key}} = f(\text{Mean of Randomness Test}) \tag{8}$$

In Eq. 1, $\mathrm{DV}_{\mathrm{Len}}^{\mathrm{Key}}$ denotes the required data value in terms of the proposed state-of-the-art session key. It has been presented in the following Table 7. The function 'f' is a user-defined function that determines the average *p*-values segregated with the session key lengths. This function adds all the obtained *p*-values and divides the result by fifteen to obtain the $\mathrm{DV}_{\mathrm{Len}}^{\mathrm{Key}}$. The same procedure has been carried out in the entire above individual Tables 2 to 6.

From the above-mentioned Table 7, it can be noted that the derived $\mathrm{DV}_{\mathrm{Len}}^{\mathrm{Key}}$ of all corresponding keys were acceptable in nature because all the values under the column heading $\mathrm{DV}_{\mathrm{Len}}^{\mathrm{Key}}$ in Table 7 are 0.75. The minimum value was supposed to be 0.05*15 = 0.75. Hence, the proposed function 'f' has achieved all the necessary values with respect to key sizes 56 bits, 128 bits, 256 bits, 512 bits, and 1024 bits.

7.3 State-of-the-art key generation example

For example, the author had considered a TPM with input neurons N = 3 and hidden neurons K = 2. The same input vector and a random weight vector had been fed into both the neural machines earlier. In this following example, an arbitrary length of state-of-the-art session key has been

Table 6 NIST on proposed State-of-the-art Session Key Length 1024 bits

Assigned Id	*p*-value	Significant *p*-value	Result (Tr: passed or Fl:Failed)
TEST CODE:01	0.165	≤ 0.05	Tr
TEST CODE:02	0.346	≤ 0.05	Tr
TEST CODE:03	0.210	≤ 0.05	Tr
TEST CODE:04	0.349	≤ 0.05	Tr
TEST CODE:05	0.295	≤ 0.05	Tr
TEST CODE:06	0.270	≤ 0.05	Tr
TEST CODE:07	0.301	≤ 0.05	Tr
TEST CODE:08	0.155	≤ 0.05	Tr
TEST CODE:09	0.304	≤ 0.05	Tr
TEST CODE:10	0.248	≤ 0.05	Tr
TEST CODE:11	0.251	≤ 0.05	Tr
TEST CODE:12	0.347	≤ 0.05	Tr
TEST CODE:13	0.218	≤ 0.05	Tr
TEST CODE:14	0.204	≤ 0.05	Tr
TEST CODE:15	0.364	≤ 0.05	Tr

Table 7 DV on Proposed Keys

Length of session key (in bits)	DV
56	4.032
128	3.755
256	4.038
512	4.212
1024	4.027

developed here for illustration. To increase the complexities, the topological configurations can be modified in both the patient TPM and the doctor TPM. The internal configurations of the TPMs, the inputs and the weights are all kept secret to the intruders. Thus, the exact bit pattern cannot be found by the intruders so easily.

In the last column of Table 8, the first bit of the needed state-of-the-art session key has been generated here. Thus, if the length of session key is 16 bits for example, then altogether 160 iterations (10*16 = 160) were needed. To curtail the length of the paper, only first ten iterations were shown above.

From the above-stated Table 9, the correlation values between the sum of weight vectors and the output of the hidden neural units were derived. Such values are as follows; Corr(Sow1(ij), HNU1) = 0.884985 and Corr(Sow2(ij), HNU2) = 0.15772. The minimum value i.e., 0.15772 has been prioritized to get involved in contributing to the output of the overall TPM. The maximum repeated value in the last column of Table 9 was '0', so '0' is the first bit of the required state-of-the-art session key. In Tables 8 and 9, the author had presented an exemplary of how the proposed state-of-the-art session key (first bit only) has been generated. The rest of the bits can be generated in the same fashion.

7.4 State-of-the-art key generation time

An integral factor of any telemedicine system depends on the amount of time needed in secret key generation. In this paper, we have proposed an adaptive artificial neural network which works only on the best suited neuron at the hidden layer. Neural synchronization was achieved by the patient TPM and doctor TPM of the users. The proposed synchronization has been made between the patient TPM and doctor TPM upto the key length bits needed. This is a dynamic approach which has no rigidity to generate various session key lengths. In the following Table 10, it has been made a comparison that same key length were derived using the proposed adaptive machines and normal TPMs [42]. The proposed technique has shown better performance over all the key lengths that were considered.

Through the above-mentioned Table 8, it has been observed that the proposed way of session key generation had taken lesser time when compared with the existing TPMs. Moreover, the efficacy can be proved with respect to all the key lengths which were considered under study.

Table 8 Tabular form of exemplary session key generation of data bits

Iteration number	X11	X12	X13	W11	W12	W13	∑xij*wij	HNU1	Corr(SoWij, HNU1)	X21	X22	X23	W21	W22	W23	∑xij*wij	HNU2	Corr(SoWij, HNU2)	Output (TPM)	Session key bit
1.1	1	0	−1	0.1	0	0.2	−0.1	−1	0.884985	0	−1	−1	−1.5	0.5	−1.5	1	1	0.15772	0	0
1.2	1	0	−1	1	0	1	0	0	0.884985	0	−1	−1	−1	−1	−1	−1	−1	0.15772	0	0
1.3	1	0	−1	1	0	1	1	1	0.884985	0	−1	−1	−1	0	0	0	0	0.15772	0	0
1.4	1	0	−1	1	0	1	1	1	0.884985	0	−1	−1	−1	0	0	0	0	0.15772	0	0
1.5	1	0	−1	1	0	1	1	1	0.884985	0	−1	−1	−1	0	0	0	0	0.15772	0	0
1.6	1	0	−1	1	0	1	1	1	0.884985	0	−1	−1	−1	0	0	0	0	0.15772	0	0
1.7	1	0	−1	1	0	1	1	1	0.884985	0	−1	−1	−1	0	0	0	0	0.15772	0	0
1.8	1	0	−1	1	0	1	1	1	0.884985	0	−1	−1	−1	0	0	0	0	0.15772	0	0
1.9	1	0	−1	1	0	1	1	1	0.884985	0	−1	−1	−1	0	0	0	0	0.15772	0	0
1.10	1	0	−1	1	0	1	1	1	0.884985	0	−1	−1	−1	0	0	0	0	0.15772	0	0

7.5 State-of-the-art session key attacks analysis

To analyze the proposed state-of-the-art session keys' attacks in the field of Telemedicine was a very sensitive work that has been carried out in this paper. It is very much relevant to analyze the attacks on the session key [43]. The combinations of the internal PANMs were changed in accordance with the priority of the hidden neuron and the amount of time to decode the key was calculated on theoretical approach. The length of the proposed key has been approximated to the nearest boundary value of the range. The minimum modular distance closed to the boundary data were taken into consideration in this section. The following Table 11 will display such approximation.

From the above-stated sixteen simulations, it can be easily found that the time needed to decode the proposed state-of-the-art session keys were nearly not possible by the intruders. The patients' data privacy concerns can be achieved in telemedicine through the proposed key generation methodology.

7.5.1 Brute-force attacks

Brute-Force attacks are needful to be carried out on any secret keys to verify its strength [41*42]. Contemporary supercomputers have high computational capacity of around 442.3 peta FLOPS i.e., 442.3 * 10^{15} floating point operations per second. One thousand FLOPS trials are required to complete one checking of any arbitrary message by such supercomputing machines. The total number of seconds in a calendar year may be 3,153,600 s in any non-leap years. Let us assume that intruders will deploy such high speed supercomputing machines in Telemedicine network to decode the state-of-the-art session keys and let S be the size of the proposed keys. The estimated time needed in Brute-Force attacks may be calculated from the following Eq. 9.

$$\text{Time (Brute} - \text{Force)} = 2^{S}/442.3 * 10^{12} * 3153600 \quad (9)$$

In the following Table 12, the author had presented the estimated time which is required in deciphering the state-of-the-art session key by the Brute-Force attacks [44, 45].

7.6 One bit input mutation

Intruders have used advanced neural machines to detect the state-of-the-art session key in the telemedicine [46]. In this sub-section, the author had mutated a single input vector. A flip in the input bit on different keys had been

Table 9 Sample calculation of Correlation Values

Iteration	Sow1(ij)	HNU1	Sow2(ij)	HNU2
1.1	0.3	−1	−2.5	1
1.2	2	0	−3	−1
1.3	2	1	−1	0
1.4	2	1	−1	0
1.5	2	1	−1	0
1.6	2	1	−1	0
1.7	2	1	−1	0
1.8	2	1	−1	0
1.9	2	1	−1	0
1.10	2	1	−1	0

done. With that effect cumulative key bits will also get altered. The following Fig. 3 will display the same.

From the above-mentioned Fig. 3, the author had observed that significant numbers of bits were changed on cumulative basis in the proposed state-of-the-art session keys of various lengths.

7.7 Brief security analysis on state-of-the-art session key

In any Telemedicine Software, the information transmission security should be sufficiently able to oppose the gatecrashers. In this paper, the author had designed state-of-the-art session key on the domain of Telemedicine. State-of-the-art means newer and scientific methods

Table 10 State-of-the-art session key generation time comparison

Sl. No	Session key size (in bits)	Existing TPM key generation time (in ms)	Proposed PANM Key generation time (in ms)	Modular deviation (in ms)
1	56	4.214	4.011	0.203
2	128	4.562	4.324	0.238
3	256	5.565	5.338	0.227
4	512	5.782	5.691	0.091
5	1024	6.244	6.105	0.139

Table 11 State-of-the-art Session Key Approximation

Serial number	Number of Input neurons(N)	Number of hidden neurons(K)	Range of session key(L)	Size of approxi-mated key	Possible session key permutations ($P = 2^K$)	Attack complexity on proposed session key	Time to decode the key (years)
1	10	13	[128,144]	128	2^{128}	2^{172}	$1.51*10^{31}$
2	10	14	[128,144]	144	2^{144}	2^{195}	$1.28 * 10^{38}$
3	11	12	[128,144]	128	2^{128}	2^{172}	$1.54*10^{31}$
4	11	13	[128,144]	144	2^{144}	2^{195}	$1.29* 10^{38}$
5	14	11	[144–160]	160	2^{160}	2^{219}	$2.09 * 10^{45}$
6	13	11	[144–160]	144	2^{144}	2^{195}	$1.32 * 10^{38}$
7	11	14	[144–160]	160	2^{160}	2^{219}	$2.08 * 10^{45}$
8	11	13	[144–160]	144	2^{144}	2^{195}	$1.27 * 10^{38}$
9	16	10	[160,176]	160	2^{160}	2^{219}	$2.11 * 10^{45}$
10	17	10	[160,176]	176	2^{176}	2^{244}	$7.25 * 10^{52}$
11	16	11	[160,176]	176	3^{176}	2^{244}	$7.25 * 10^{52}$
12	14	12	[160,176]	160	2^{160}	2^{219}	$2.07 * 10^{45}$
13	13	14	[176,192]	176	2^{176}	2^{244}	$7.25 * 10^{52}$
14	15	12	[176,192]	176	2^{176}	2^{244}	$7.25 * 10^{52}$
15	16	12	[176,192]	192	3^{192}	2^{269}	$2.39* 10^{60}$
16	19	10	[176,192]	192	3^{192}	2^{269}	$2.39* 10^{60}$

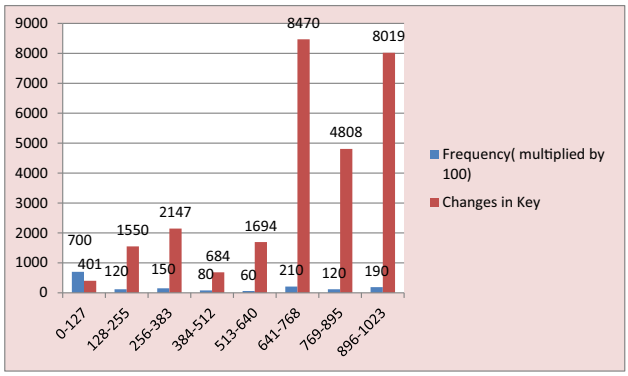

Fig. 3 Mutation Effect on State-of-the-art Session Key

Table 12 Time to decode the state-of-the-art- Session Key

Length of session key (in bits)	Time to decode (in years)
56	$5.16*10^{5}$
128	$2.43*10^{18}$
256	$1.31*10^{40}$
512	$9.61*10^{132}$
1024	$1.28*10^{287}$

which are very much contemporary in this situation. In this segment, a brief analysis has been made to review the effectiveness of the proposed system against the intruding.

Patients' Information Integrity: In case the patients' information bundles are gotten by encryption strategies with the secret keys. The adversaries cannot have the choice to examine or take data yet at the transmission time. It can add some bogus data or any dangerous malware data in the telemedicine treatment methodology. Strong session key can ensure that the data has not been changed during transmission period by the intruders.

Patients' Data confidentiality: Patients' data confidentiality has been placed at the top rank of the contemporary issues in the Telemedicine Software. We have designed state-of-the-art session key based on Priority based Adaptive Neural Machine (PANM) and such were tested under of statistical tests, derived value based function, Brute-Force attacks.

Session Key Confidential Exchange: In the greater part of the telemedicine cases, the session key is overall freely disseminated to the patient and physician in a public medium. There exists a greatest possibility catching those keys by the rivals. So there should be a gotten instrument for its dissemination. In this technique, we have successfully addressed this issue through session key partial exchange and validation.

Adaptation in Neural Machines: A neural machine has been proposed adaptation ability in this paper. Hidden neurons were assigned priority and the best fitted neuron has been selected to generate the neural output. It has been proposed to prevent the intruding in Telemedicine.

Fast Functionality: In this technique, we have designed state-of-the-art session key with fast key generation period on different key lengths. This means the time needed to generate the keys will be fast when compared to other similar methods.

Table 13 Comparative study with earlier methods

Sl. No	Comparative attributes	Essentiality of such attributes	Ref. No. 12	Ref. No. 14	Ref. No. 16	Ref. No. 27	Ref. No. 28	Ref. No. 31	Proposed technique here
1	Telemedicine	Contemporarily it is much of relevance	Yes	Yes	Yes	No	No	No	Yes
2	Patients' live data sensing	It is important to check the patients' data	No	No	No	No	No	No	No
3	Data encryption or secret key generation	Cryptographic applications can have an encryption method with secret key	No	No	No	Yes	Yes	Yes	Yes
4	Analysis on secret Key space	Time needed to detect the secret key	No	No	No	No	Yes	No	Yes
5	Secret key generation time	Determines the secret key generation time	No	Yes	No	No	No	No	Yes
6	Statistical NIST	Randomness checking in the secret keys	No	No	No	No	No	No	Yes
7	Genetic mutation attacks	Input vectors were mutated to know its effects	No	No	No	No	No	No	Yes
8	Adaptive TPMs	Priority was set inside the TPMs	No	No	No	No	No	No	Yes

7.8 Comparative study

In this sub-section, the author had compared between the proposed method and earlier works on the similar domain. The following Table 13 shows the comparative study in brief.

8 Conclusions, limitations, and future scope

As we all know that patients' data privacy is the biggest threat in the telemedicine. To resist the data breaching, strong cryptographic applications are being developed at rapid pace. This paper has dealt with the state-of-the-art session key generation with the help of adaptive neural machines in telemedicine. Soft computing on ANN was extensively implemented here as it fits with the term state-of-the-art key generation method. Here, the best fitted hidden neuron has been selected to contribute in the neural output. For that minimum correlation was considered under this approach. The notable thing can be found is that by the use of high speed supercomputers are not enough to detect the entire sequence of key by the external intruders inside the network. Lesser iterations were needed in the patient TPM and the doctor TPM synchronization. Thus the key generation time has been shortened here. Statistically, different key lengths of the session keys were tested and accepted. Derived value-based function had yielded successful outcomes too. Partial validations on the session keys had been verified also. Thus, the proposed technique is very good for the novel key generation and authentication in the telemedicine system to preserve data privacy.

One of the main limitations of this technique is that equivalent adaptive neural machines are to be fixed at the patient's end and the doctor's end.

The proposed methodology can be implemented in distributed computing which will increase the transaction rates in telemedicine.

Acknowledgements The author do acknowledges the moral and congenial atmosphere support provided by Maharajadhiraj Uday Chand Women's College, Burdwan, India -713104.

Funding Not applicable.

Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interests There is no conflict of interests in this manuscript.

Ethics approval and consent to participate Not applicable.

Consent for publication Not applicable.

References

1. Maatuk AM, Elberkawi EK, Aljawarneh S et al (2021) The COVID-19 pandemic and E-learning: challenges and opportunities from the perspective of students and instructors. J Comput High Educ. https://doi.org/10.1007/s12528-021-09274-2
2. Almaiah MA, Al-Khasawneh A, Althunibat A (2020) Exploring the critical challenges and factors influencing the Elearning system usage during COVID-19 pandemic. Educ Inf Technol 25:5261–5280. https://doi.org/10.1007/s10639-020-10219-y
3. Mislovaty R, Perchenok Y, Kanter I, Kinzel W (2002) Secure key-exchange protocol with an absence of injective functions. Phys Rev E 66:066102
4. Song S, Miller KD, Abbott LF (2000) Competitive Hebbian learning through spike-timing-dependent synaptic plasticity. Nat Neurosci 3:919–926
5. Jeong S, Park C, Hong D, Seo C, Jho N (2021) Neural cryptography based on generalized tree parity machine for real-life systems. Secur Commun Netw. https://doi.org/10.1155/2021/6680782
6. Hellman M (1978) An overview of public key cryptography. IEEE Commun Soc Mag 16(6):24–32
7. Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126
8. Anoop MS (2008) Security needs in embedded systems. *IACR Cryptology ePrint Archive* 198
9. Choi Y et al (2014) Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors 14(6):10081–10106
10. Carlson A (1990) Anti-Hebbian learning in a non-linear neural network. Biol Cybern 64:171–176
11. Yang XS (2010) Nature-inspired Metaheuristic Algorithms Luniver Press.
12. Francke JA, Groden P, Ferrer C et al (2022) Remote enrollment into a telehealth-delivering patient portal: Barriers faced in an urban population during the COVID-19 pandemic. Health Technol 12:227–238. https://doi.org/10.1007/s12553-021-00614-x
13. Alonso SG, Marques G, Barrachina I et al (2021) Telemedicine and e-Health research solutions in literature for combatting COVID-19: a systematic review. Health Technol 11:257–266. https://doi.org/10.1007/s12553-021-00529-7
14. Ghosh A, Gupta R, Misra A (2020) Telemedicine for diabetes care in India during COVID19 pandemic and national lockdown period: Guidelines for physicians. Diabetes Metab Syndr: Clin Res Rev 14:273–276. https://doi.org/10.1016/j.dsx.2020.04.001
15. Abo-Zahhad M, Ahmed SM, Elnahas O (2014) A wireless emergency telemedicine system for patients monitoring and diagnosis. Int J Telemed App. https://doi.org/10.1155/2014/380787
16. Hatcher-Martin JM, Adams JL, Anderson ER et al (2020) Telemedicine in Neurology. Neurology 94(1):30–38
17. Norman S (2006) The use of telemedicine in psychiatry. J Psychiatr Mental Health Nursing 13(6):771–777
18. Tresenriter M, Holdaway J, Killeen J et al (2021) The implementation of an emergency medicine telehealth system during a pandemic. J Emergency Med 60(4):548–553
19. Bokolo A (2021) Exploring the adoption of telemedicine and virtual software for care of outpatients during and after COVID-19 pandemic. Ir J Med Sci 190:1–10. https://doi.org/10.1007/s11845-020-02299-z

20. Yang L, Brown-Johnson CG, Miller-Kuhlmann R et al (2020) Accelerated launch of video visits in ambulatory neurology during COVID-19. Neurology 95(7):305–311
21. Chauhan V, Galwankar S, Arquilla B et al (2020) Novel coronavirus (COVID-19): leveraging telemedicine to optimize care while minimizing exposures and viral transmission. J Emerg Trauma Shock 13(1):20
22. Jnr Bokolo A (2020) Use of telemedicine and virtual care for remote treatment in response to COVID-19 pandemic. J Med Syst 44:132
23. Dey J, Mukherjee S (2021) Wireless COVID-19 telehealth: leukocytes encryption guided by amino acid matrix. Wireless Pers Commun 120:1769–1789. https://doi.org/10.1007/s11277-021-08534-9
24. Sarkar A, Dey J, Chatterjee M, Bhowmik A, Karforma S (2019) Neural soft computing based secured transmission of intraoral gingivitis image in E-health. Indonesian J Electr Eng Comput Sci 14(1):178–184
25. Rahman S, Amit S, Kafy A (2022) Impact of COVID-19 and telehealth on mental health in Bangladesh: a propensity score matching approach. Spat Inf Res. https://doi.org/10.1007/s41324-022-00434-9
26. Dash S, Aarthy R, Mohan V (2021) Telemedicine during COVID-19 in India—a new policy and its challenges. J Public Health Pol 42:501–509. https://doi.org/10.1057/s41271-021-00287-w
27. Lei X, Liao X, Chen F, Huang T (2013) Two-layer tree-connected feed-forward neural network model for neural cryptography. Phys Rev E 87(3):032811
28. Allam AM, Abbas HM, El-Kharashi MW (2013) Authenticated key exchange protocol using neural cryptography with secret boundaries. In: The 2013 International Joint Conference on Neural Networks (IJCNN) Aug 4 (pp. 1-8). IEEE.
29. Dey L, Chakraborty S, Mukhopadhyay A (2020) Machine learning techniques for sequence-based prediction of viral–host interactions between SARS-CoV-2 and human proteins. Biomed J 43(5):438–450
30. Jeong S, Park C, Hong D, Seo C, Jho N (2021) Neural cryptography based on generalized tree parity machine for real-life systems. Secur Commun Netw. https://doi.org/10.1155/2021/6680782
31. Mislovaty R, Perchenok Y, Kanter I, Kinzel W (2002) Secure key-exchange protocol with an absence of injective functions. Phys Rev E 66(6):066102
32. Rosen-Zvi M, Klein E, Kanter I, Kinzel W (2002) Mutual learning in a tree parity machine and its application to cryptography. Phys Rev E 66(6):066135
33. Dolecki M, Kozera R (2015) The Impact of the TPM Weights Distribution on Network Synchronization Time. Computer Information Systems and Industrial Management, pp.451–460.
34. Ruttor A, Kinzel W, Kanter I (2007) Dynamics of neural cryptography. Phys Rev E 75(5):056104
35. Volkmer M, Wallner S (2005) Tree parity machine rekeying architectures. IEEE Trans Comput 54(4):421–427
36. Santhanalakshmi S, Sudarshan T, Patra GK Neural synchronization by mutual learning using genetic approach for secure key generation. In: *Proceedings of the International Conference on Security in Computer Networks and Distributed Systems*, 422–431, Thiruvanathapuram, India, March 2014.
37. Han YL, Li Y, Li Z, Zhu SS (2020) An improved method to evaluate the synchronization in neural key exchange protocol. Secur Commun Netw. https://doi.org/10.1155/2020/8869688
38. Jalali MS et al (2020) Why employees (still) click on phishing links: investigation in hospitals. J Med Internet Res 22(1):e16775
39. Bassan S (2020) Data privacy considerations for telehealth consumers amind COVID-19. J Law Biosci 7(1).
40. Kahate A (2006) Cryptography and Network Security, 2003. Tata McGraw-Hill publishing Company Limited, Eighth reprint
41. Rukhin A, Soto J, Nechvatal J, Smid M, Barker E, Leigh S, Levenson M, Vangel M, Banks D, Heckert A, Dray J, Vo S (2001) A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST special publication 800–22.
42. Martínez Padilla J, Meyer-Baese U, Foo S (2018) Security evaluation of Tree Parity Re-keying Machine implementations utilizing side-channel emissions. EURASIP J on Info Secur 2018:3. https://doi.org/10.1186/s13635-018-0073-z
43. Wu B, Chen J, Wu J, Cardei M (2007) A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. In: Xiao, Y., Shen, X.S., Du, DZ. (eds) Wireless Network Security. Signals and Communication Technology. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-33112-6_5.
44. Hofstede R, Jonker M, Sperotto A et al (2017) Flow-based web application brute-force attack and compromise detection. J Netw Syst Manage 25:735–758. https://doi.org/10.1007/s10922-017-9421-4
45. Vykopal J (2013) Flow-based brute-force attack detection in large and high-speed networks. Ph.D. thesis, Masaryk University, Brno, Czech Republic.
46. Rui Z, et al. (2020). PassEye: Sniffing Your Password from HTTP Sessions by Deep Neural Network. In: Cyber Security. CNCERT 2020. Communications in Computer and Information Science, vol 1299. Springer, Singapore. https://doi.org/10.1007/978-981-33-4922-3_1.