Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/taut20

A secured and optimized deep recurrent neural network (DRNN) scheme for remote health monitoring system with edge computing

D. Pavithra, R. Nidhya, S. Shanthi & P. Priya

AUTOMATIKA
2023, VOL. 64, NO. 3, 508–517
https://doi.org/10.1080/00051144.2023.2195218

REGULAR PAPER

OPEN ACCESS Check for updates

A secured and optimized deep recurrent neural network (DRNN) scheme for remote health monitoring system with edge computing

D. Pavithra[a], R. Nidhya[b], S. Shanthi[c] and P. Priya[d]

[a]Department of Information Technology, Dr. N. G. P. Institute of Technology, Coimbatore, India; [b]Department of Computer Science and Engineering, Madanapalle Institute of Technology & Science, Madanapalle, India; [c]Department of Computer Science and Engineering, Malla Reddy College of Engineering and Technology, Hyderabad, India; [d]Department of Computer Science and Engineering, M.Kumarasamy College of Engineering, Karur, India

ABSTRACT

Patients now want a contemporary, advanced healthcare system that is faster and more individualized and that can keep up with their changing needs. An edge computing environment, in conjunction with 5G speeds and contemporary computing techniques, is the solution for the latency and energy efficiency criteria to be satisfied for a real-time collection and analysis of health data. The feature of optimum computing approaches, including encryption, authentication, and classification that are employed on the devices deployed in an edge-computing architecture, has been ignored by previous healthcare systems, which have concentrated on novel fog architecture and sensor kinds. To avoid this problem in this paper, an Optimized Deep Recurrent Neural Network (O-DRNN) model is used with a multitier secured architecture. Initially, the data obtained from the patient are sent to the healthcare server in edge computing and the processed data are stored in the cloud using the Elliptic Curve Key Agreement Scheme (ECKAS) security model. The data is pre-processed and optimal features are selected using the Particle Swarm Optimization (PSO) algorithm. O-DRNN algorithm hyper-parameters are optimized using Bayesian optimization for better diagnosis. The proposed work offers superior outcomes in terms of accuracy and encryption latency while using computational cloud services.

ARTICLE HISTORY
Received 2 January 2023
Accepted 21 March 2023

KEYWORDS
Optimized deep recurrent neural network; enhanced elliptic curve cryptography; remote monitoring system; bilinear mapping; particle swarm optimization; edge computing security

1. Introduction

Health care is one of the fields that is tremendously developing in terms of technology as well as services. One of the prominent development in this healthcare field is remote patient monitoring and fast and early identification of diseases. Remote patient monitoring has gained more importance in the current scenario due to various reasons such as more elderly population, shortage of experts and fewer hospital facilities. Remote Patient Monitoring allows the doctors to monitor their patients remotely without any clinical support. Healthcare systems along with the support of remote monitoring aids in improving the quality of patient's life with reduced costs. Early illness diagnosis, the capacity to monitor patients constantly and remotely, lowering hospital stays and death rates, among other benefits of remote patient monitoring. While designing and implementing a remote monitoring system, many challenges are involved such as sensors which are used, the processing algorithms used for implementation, the choice of contact or contactless method, and secure data communication [1].

Healthcare wireless and mobile applications are becoming more and more prevalent as a result of economic development and technical advancement [2]. The monitoring of human health makes extensive use of internet of things devices. Because of the heterogeneity and excessive noise in streaming data [3], there are several obstacles to effective health data analysis and diagnosis. Strong support for addressing this issue is provided by the development of cloud computing and deep learning technologies. Nevertheless, using a deep learning model based on a cloud platform for real-time health monitoring still has certain issues. A lot of network resources will be used at first due to the continual transmission of health data. As a result of network transmission fluctuations, the return time of the cloud decision is also uncertain. Lastly, the cloud storage of users' health data will result in difficulties with personal privacy. In order to provide location-aware and delay-sensitive monitoring with intelligent and dependable control, data-intensive analysis in smart healthcare necessitates a novel computational paradigm [4].

CONTACT D. Pavithra ✉ pavimba07@gmail.com Department of Information Technology, Dr. N. G. P. Institute of Technology, Dr. N.G.P. Nagar, Kalapatti Main Rd, Coimbatore, Tamil Nadu, 641048, India

This article has been corrected with minor changes. These changes do not impact the academic content of the article.

Remote patient monitoring uses various types of sensors such as wearable sensors, and biosensors for collecting the health-related data about the patient and this data is first transferred to the hospital server and then data is transferred to the cloud storage from which the data could be accessed by the doctors and the medical team particularly the authorized members for providing their recommendations and assessments about the status of the patient. There is a need to analyse the data collected from the patient and to identify and detect the symptoms much earlier to avoid further complications. With the usage of wearable devices, the heart rate, temperature, blood pressure, blood glucose levels, and other variables are monitored. The hospital's end terminal, the hospital's data processing system, the data gathering system, and the communication network are all parts of the RMS. Data gathering through the use of various sensors or equipment with embedded sensors is known as data acquisition [5]. Data Processing is capable of processing the data with data receiving and transmission capability. Communication network is capable of connecting the data acquisition to the data processing system.

In the e-healthcare sector, many technologies are used such as machine learning, fog computing, cloud computing, Internet of Things are integrated to provide real-time solutions. Medical diagnosis along with artificial neural networks is one of the key research areas in the field of health care. A type of cloud computing termed "edge computing" uses data being gathered using an IoT network and by using various edge devices they are computed locally. Once the data processing is completed, for further storage and calculations, the data is moved to the cloud. Machine Learning, In several domains, including image recognition, deep learning techniques are frequently employed, in decision making, object recognition, and disease diagnosis. In the current scenario, the amount of data generated has become too large and the hidden patterns and abnormal patterns need to identify very efficiently. In the case of Remote monitoring system, the patient data should be analysed and an accurate result and diagnosis of the disease should be predicted. In order to predict the disease many algorithms are used such as K Nearest Neighbor, Convolutional neural network, Bayes Network, and Support vector machine. In this healthcare sector, the data is sensitive and need to be secured more efficiently starting from the Human body, Local Server, Communication network and then the Cloud Storage [6]. So Data needs to be highly secured and confidential. So in order to secure the data while reception and transmission many algorithms have been proposed by many researchers.

In this paper, Diabetes patients are considered for remote monitoring, as more individuals are developing diabetes every day and its consequences are having a significant negative impact on society. In this paper, an Optimized Deep Recurrent Neural Network (O-DRNN) model is to diagnose the disease and the processed data are stored in the cloud using the Elliptic Curve Key Agreement Scheme (ECKAS) security model. The data is pre-processed and optimal features are selected using the Particle Swarm Optimization (PSO) algorithm. O-DRNN algorithm hyperparameters are optimized using Bayesian optimization for better diagnosis which provides better results.

2. Literature survey

Leoni Sharmila.et al. [7] used liver data for performing classification and to carry out the comparative analysis. They used various machine learning algorithms such as decision trees, Fuzzy logic, and Fuzzy Neural network. According to the author Fuzzy neural networks performed better than other machine learning algorithms. Simplified Fuzzy ARTMAP is used by the author for improving the performance.

Shraddha Subhash Shirsath. et al. [8] employed the CNN-MDRP algorithm to predict illness using enormous amounts of hospital data, including both organized and unstructured data. Authors have used Naïve Bayes algorithm and CNNUDRP algorithm for disease prediction where CNNUDRP worked only for structured data. As compared to the CNNUDRP, supports CNN-MDRP both structured and unstructured data for reliably and efficiently predicting the disease.

Gudadhe et al. [9] combined used the concept of heart disease classification using multilayer perceptron (MLP) and support vector machine methods. An accuracy of 80.41% is achieved by the proposed classification system and found to yield better results. Kahramanli and Allahverdi et al. [10] suggested a hybrid neural network for categorizing the heart disease classification system that integrated fuzzy neural networks and artificial neural networks. The achieved accuracy of the suggested system is 87.4%. Using the use of many machine learning approaches such as Naive Bayes, decision trees, and ANN, Awang et al. [11] suggested a medical diagnosis system for predicting heart disease. Naive Bayes performed better when compared to ANN followed by a decision tree.

In [12], Wireless medical sensor networks have been proposed to be protected by a compact system. The proposed system mainly used the concepts such as symmetric cryptography, and hash operation. An anonymous authentication method for wireless body area networks was presented in the work of [13]. The ECC algorithm and identity-based authentication are used in their work. Providing safe data transmission between the cloud and MSNs is the primary objective of [14]. They have proposed a technique for capturing data confidentiality in WBANS. In [15] they proposed a friendly personal health information sharing and provided authorized users with access permission in cloud computing. The proposed work gave better results in avoiding various attacks and prevented malicious behaviour. In [16], the author proposed an MSN-cloud architecture to provide security and monitor the medical conditions for various medical services. In [17] author used symmetric cryptography in sensor/actuator modes for carrying out authentication, Key establishment schemes in MSNs.

Fuzzy rules and deep neural networks are used to create an expert system that can diagnose heart disease with an overall accuracy of 96.5% [18]. CardioHelp is a technique that employs CNN for early heart failure prediction using a temporal model, integrating CNN with deep learning algorithms. With an accuracy rate of 97%, our technology exceeds other state-of-the-art techniques [19]. Sequential forward selection (SFS) is used as the feature selection method and a random forest is used for classification in an IoT-based hybrid system for the prediction of cardiovascular illness. When compared to other heuristic model recommender systems, this system's recommendation of physical activity and dietary plans to patients based on their age and gender has a 98% accuracy rate [20]. Kernel random forest [21], an ensemble classifier-based model that can handle medical data from various sensors, achieves 98% accuracy on a dataset for heart disease. A wearable sensor that detects a patient's blood pressure and ECG is coupled to a novel IoT framework based on deep convolution neural networks. This approach performs better with 98.2% accuracy when compared to logistic regression and existing deep-learning neural networks [22]. Based on the ensemble deep learning model Logit boost as well as the feature fusion approach, a smart system was described that predicts the risk of heart disease using data collected by wearable sensors and patient medical history. When automatically advising diets based on the health state, the system has a diagnosis accuracy of 98.5% for heart disease. Deep neural networks and the Linear SVC algorithm's integrated feature selection technique are used to create a model for heart disease prediction. When compared to the heart disease dataset, this system obtains 98.56% accuracy, 99.35% recall, 97.84% precision, and 98.3% F-measure, respectively [23].

The aforementioned state-of-the-art works pertaining to heart disease risk diagnosis harnessing the heart disease dataset predominantly avail statistical and machine learning algorithms and methods. The classification accuracy shown by the existing methods has the possibility of further enhancement when deep learning approaches are emphasized. Moreover, utilizing recurrent neural network algorithms has the potential to offer better outcomes. The ensuing sections elaborate on the proposed recurrent neural network model for accurate heart disease risk prediction.

3. Proposed model

In our proposed work, the remote data are collected from the patient is encrypted and sent to the healthcare server in edge computing. In this server, the optimized DRNN model is executed for detecting the presence and the level of diabetes. The model's data is processed, then delivered to a cloud server after being encrypted. The encrypted data can be viewed by healthcare professionals with proper authentication for further analysis. The secured data can be viewed by the patient and healthcare professionals through their login details. The process of the proposed model is depicted in Figure 1.

3.1. Data collection

Generally, the remote data are acquired using sensors that are transmitted through interconnected devices to the server. The sensors placed in the body of the patient provide data like temperature, pulse rate, blood pressure, cholesterol rate, glucose level, ECG, heart rate, etc,. The data collected are transferred to edge computing for analysing the health condition of the patient. Here the diabetes data is taken from the UCI repository with 520 instances, which is pre-processed and analysed by the proposed model at edge computing.

3.2. Preprocessing

Gathered data are pre-processed for better classification results. In this process, min–max scalar and standard scalar are applied after removing the missing values. The min–max scalar maintains the data between the values 0 and 1. The purpose of the standard scalar is to make the mean 0 and the variance to be 1. The formula used for min–max scalar and standard scalar is given in Equations (1) and (2) respectively

$$\mathrm{Y_s} = \frac{(\mathrm{Y} - \min(\mathrm{Y}))}{(\max(\mathrm{Y}) - \min(\mathrm{Y}))} \tag{1}$$

$$\mathrm{X}_s = \frac{(X - A)}{n} \tag{2}$$

where A is mean and n is standard deviation.

3.3. Feature selection using particle swarm optimization

After pre-processing, a feasible subset of data is obtained by performing feature selection using PSO. This process helps in providing better classification and processing time [24]. PSO algorithm is one of the swarm intelligence algorithms that is used for scientific and engineering applications. The main advantage of PSO is that it does not have any mutation and overlapping in the searching process. The PSO algorithm is meant for its global search technique [25].

Actual feature set x is the number of attributes in the diabetes dataset (17 attributes), which will be greater

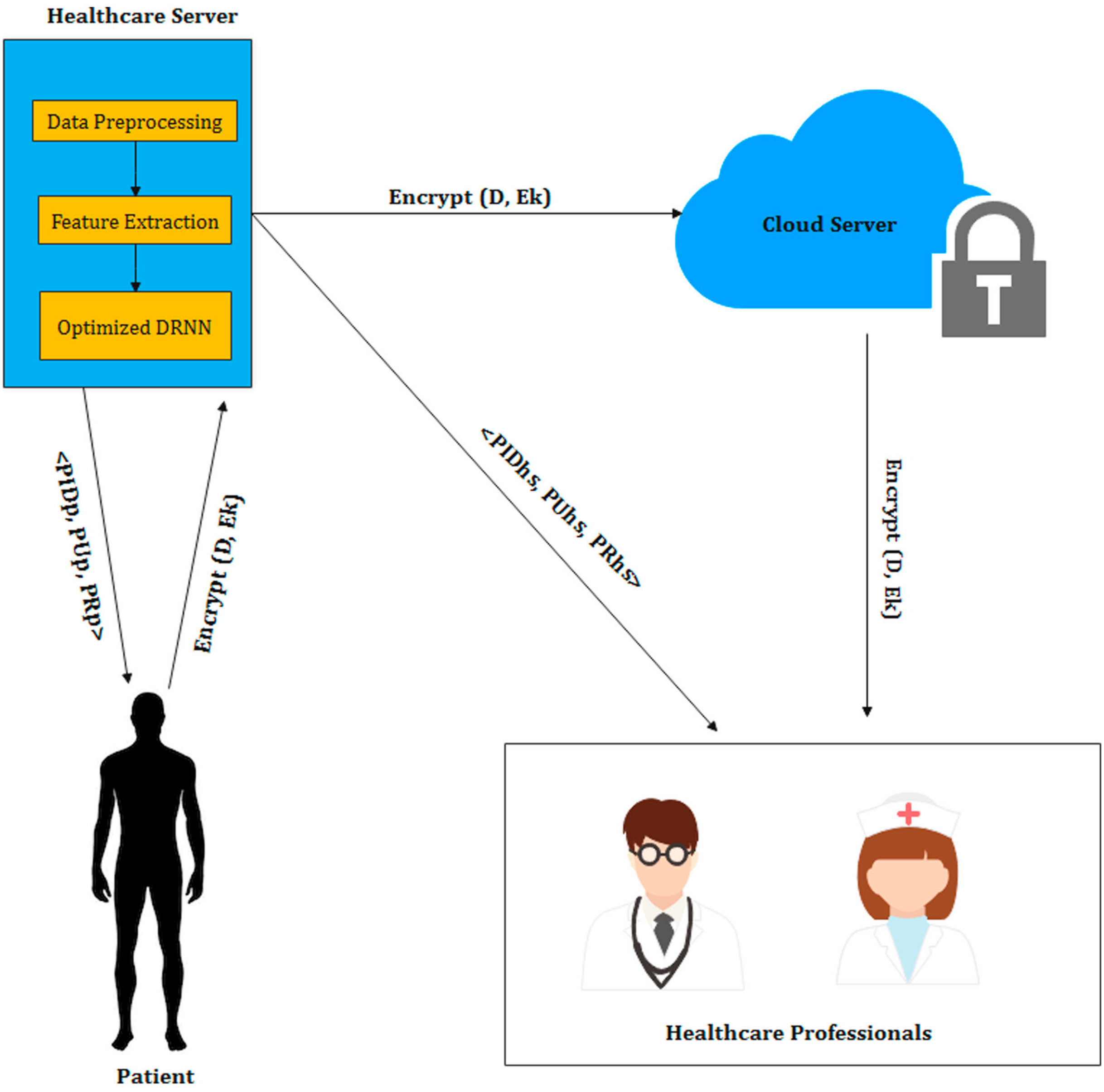

Figure 1. Process of the proposed model.

than the feature subset y. In this method, the diabetes attributes are mentioned as particles in the search space with the value 0 or 1.

For the x dimension, the particle position is given as y binary digits. Initially, the PSO algorithm is set with iteration size based on the number of features, population size depending on the feature set, acceleration factors c1 = c2 = 2 and the target is the optimal subset. The position of the particle is generated randomly with the values 0 or 1 and the velocity is 0 initially. The algorithm for feature selection using PSO is given in Table 1

Here, y_{pd}^{new} and y_{pd}^{old} are the updated and current particle positions, v_{pd}^{new} and v_{pd}^{old} are the new and old particle velocities respectively. The $rand_1$ and $rand_2$ are the random numbers generated between 0 and 1. After performing feature selection using PSO, obtained feature subset contains 9 attributes for the classification model.

3.4. Optimized deep recurrent neural network

LSTM blocks. The purpose of using Long Short Term Memory (LSTM) blocks for recurrent layers is to avoid the gradient vanishing problem. The LSTM layer is an intermittently connected layer with memory blocks. These blocks consist of three multiplicative components, such as forget, output, and input gates, which are interconnected memory cells used for reset, read and write operations of the memory cell [26]. The optimization of DRNN hyper-parameters are performed using Bayesian Optimization algorithm. Tuning the hyper-parameters in DNN is considered as black-box function [27]. The performance function in the Bayesian Optimization is modelled as Gaussian value over the hyper-parameter value. Initially, randomly generated hyper-parameter combinations are tested to form the model of the objective function. Then, the next combination is selected by taking the values near the highest observed value and then exploring to find another

Table 1. Pseudo-Code of PSO based feature selection.

```
Input: Dataset containing x attributes, samples and class labels.
Output: Optimized feature attributes y
Initialize population as number of features
While (number of particles as features) m, or stop rule is not fulfilled)
For $n = 1$ to number of articles
If $Y_p$'s fitness is greater than $P_{best}$'s fitness
Update $P_{best} = Y_p$
r $m$ ∈Neighborhood of$Y_p$
If the fitness of $Y_k > g_{best}$then
Update $g_{best} = Y_k$
Increment $m$. by 1
For each attribute $d$
$v_{pd}^{new} = \omega v_{pd}^{old} + C1rand_1(pbest_{pd} - y_{pd}^{old}) + C2rand_2(gbest_{pd} - y_{pd}^{old})$
If $v_{pd}^{new} \notin (V_{min}, V_{max})$ then
$v_{pd}^{new} = \max(\min(V_{max}, v_{pd}^{new}), V_{min})$
$S(v_{pd}^{new}) = (1/1 + e^{-v(new/pd)})$
If $(rand < S(v_{pd}^{new}))$ then $y_{pd}^{new} = 1$ else $y_{pd}^{new} = 0$
$y_{pd} = y_{pd} + v_{pd}$
Increase $d$ by 1
Increase $n$ by 1
Next generation till stop rule is fulfilled
Final optimal features $y$ selected
```

Table 2. Algorithm for Bayesian optimization.

```
Set a Gaussian process former on $p$
Observe $p$ at m0 according to a preliminary space-filling experimental design, points.
Set m = m0.
while m $\leq$ M perform
Using all relevant data, update the posterior probability distribution for $p$.
Let $y_m$ to maximize the acquisition function over y, where the acquisition function is calculated using the current posterior distribution.
Observe $x_n = g(y_n)$.
Increment m
end while
Return the solution as the point evaluated with the largest g(x) and with the largest posterior mean
```

hyper-parameter space to get the best optimal value [28]. This method combines both the exploration and exploitation trade-off. The acquisition function used is given in Equation (3) and the Algorithm for Bayesian Optimization is given in Table 2.

$$y_{n=}argmax_y b(Y/D_{1:m-1}) \tag{3}$$

The model is trained with the diabetes data from UCI repository before testing. The output of the model indicates the presence and the level of diabetes which is used for further analysis.

3.5. Multitier data security system model

In our proposed model the security for data transmission is implemented at a multitier security level. Basically, the implementation of multitier security is done by performing the multilevel encryption process between the patient end and the doctor end. Wireless devices can provide secure communication by employing the ECC encryption technique. Our proposed system consists of four basic components. They are patients, edge devices or healthcare servers, cloud servers and healthcare professionals such as doctors, nurses, etc. Each component in the proposed system is initially allocated with its own key pair using Elliptic Curve Key Agreement Scheme. For generating the group key for efficient data transmission, the bilinear mapping technique has been used. To provide multilevel encryption for a single user it's obligatory to produce distributed group key to an established route. For generating the input for key generation, the following properties of bilinear mapping should get satisfied.

- Property 1:

$$e(x + z, y) = e(x, y) * e(z, y)$$

where,

$$e(y, x + z) == e(x + z, y)$$

Here *x*,*y*,*z* are random positive values generated on the curve c.

- Property 2:

Choose any two points on curve as *i*,*j*

$$e(i, j) = (i - j) * (i + j)$$

where random positive value is multiplied in the above equation,

$$e(i * x, j * x) == e(x, j * x)^i$$

$$e(x, j * x)^i == e(i * x, x)^j$$

$$e(i * x, x)^j == e(x * x)^{i*j}$$

The points which are agreeable to these two properties are considered for the key generation process as the ECC points. We presume that the communication paths between the patient, HS, cloud servers and HP are secured because of using various security protocols. But unfortunately, cloud storage and wireless transmission are liable to attack at any time. So data encryption should begin with data collection itself. The proposed security model operates in four major phases: Setup Phase, Registration Phase and Encryption and Decryption Phase.

(1) Setup Phase

This phase initializes the essential parameters of the following phases in secured data transmission.

Step 1 : The health care server initiates the process of initialization by choosing an elliptic curve EC and the cyclic additive group G with generator X and order p.

Step 2 : Step 2:The healthcare server generates the public key (PU) and private key (PR) pair.

Step 3 : A pair of one-way hash functions $H_1()$ and $H_2()$ are chosen which are supposed to be collision resistant.

Step 4 : At the end, made the following parameters public $< G, EC, X, p, H_1(), H_2(), PU >$.

(2) Registration Phase

In this phase, the patients and doctors will register in the healthcare server (HS) and HS will allocate the public-private key pair (PU_p & PR_p) and pseudo-identity value (PID). The processes involved in these computations are detailed below:

Step 1 : The patient selects the identity (ID_p) value and forwards it to the healthcare server through the secured channel.

Step 2 : The secret key is established between the patient and cloud ($SK_{p)}$. And HS performs the hash function by combining the IDp and Group key value R_u ie., $h_p = H_1(ID_p||R_u)$. At the end, HS calculates PID_p by using the above-calculated value and HS's private value PR.

Step 3 : Then HS computes PU_p & PR_p for the patient p. The computed PIDp, PU_p & PR_p values are transmitted through the secured channel to the patient p.

Step 4 : The received values of patient p are stored safely for the future secret key establishment process. At the same time $< PID_p, PU_p, R_u >$ values are displayed as public.

The same procedure is applicable to healthcare professionals' registration also. The only difference in registration is generating the different parameters such as the public-private key pair (PU_{hp} & PR_{hp}) and pseudo-identity value (PID_{hp}).

(3) Encryption Phase

In this phase, the data collected from the patient's end will get encrypted as cipher text before starting its transmission to the HS. The detailed process is explained below:

Step 1 : The secret key E_k for converting patient health data (D) to cipher text is generated by combining the Private key of the patient PR_p with the public key of the healthcare serve PU. ie., $E_k = PR_p.PU$

Step 2 : After generating the secret key, the encryption process begins between the patient and HS. D' = Encrypt (D, E_k)

Step 3 : The encrypted data is transmitted from the patient's end to HS.

(4) Decryption process:

In this phase, the received cipher text at HS will get decrypted to original health data for disease prediction process. The detailed process is explained below:

Step 1 : The secret key D_k for converting cipher text (D') to patient health data (D) to is generated by combining the Public key of the patient PU_p with private key of the healthcare server PR. ie., $D_k = PU_p.PR$

Step 2 : After generating the secret key, the decryption process begins at the HS end. D = Encrypt (D', D_k)

Step 3 : Original health data is decrypted at HS end for further processing.

The same process is repeated between HS, cloud server and HP for further data transmission in a secured way. The data is encrypted and decrypted between these multiple ends for more secure data transmission. At the beginning of our architecture, each and every patient is provided with a login id and randomly generated unique group key values.

Similarly, caregiver is also provided with login credential details to access the patient detail from the cloud server for remote monitoring of the patient's health status. Multitier security is provided between the users and the healthcare professionals to provide security for data. In our proposed architecture, we have introduced various levels of encryption and decryption processes.

The first level of encryption is happening between the patient and the edge device or healthcare server. Once the data is received at HS, immediately cipher text is decrypted and detailed data analysis is done for diabetics prediction using the Optimized DRNN model. After the analysis, the predicted data will be encrypted and forwarded to the cloud server. Similar encryption and decryption process is done between the cloud server and the healthcare professional. Hence the proposed system ensures data security in both transmission and cloud storage.

3.6. Experimental analysis for optimized DRNN scheme

The efficiency of the model was investigated for with and without diabetes patients to analyse the presence of diabetes. The data are obtained from the UCI repository that contains 520 instances with 17 attributes.

During implementation, the dataset was partitioned in a 70:30 ratio for training and testing the model. Nearly 1500 records were analysed and obtained the following result.

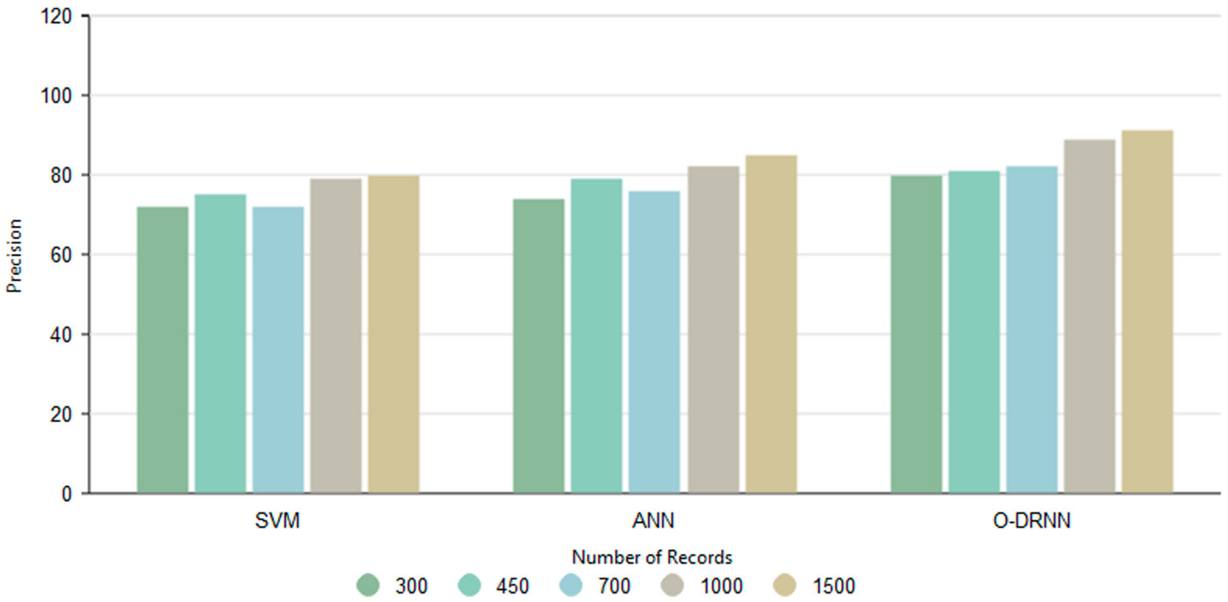

Figure 2. Precision analysis.

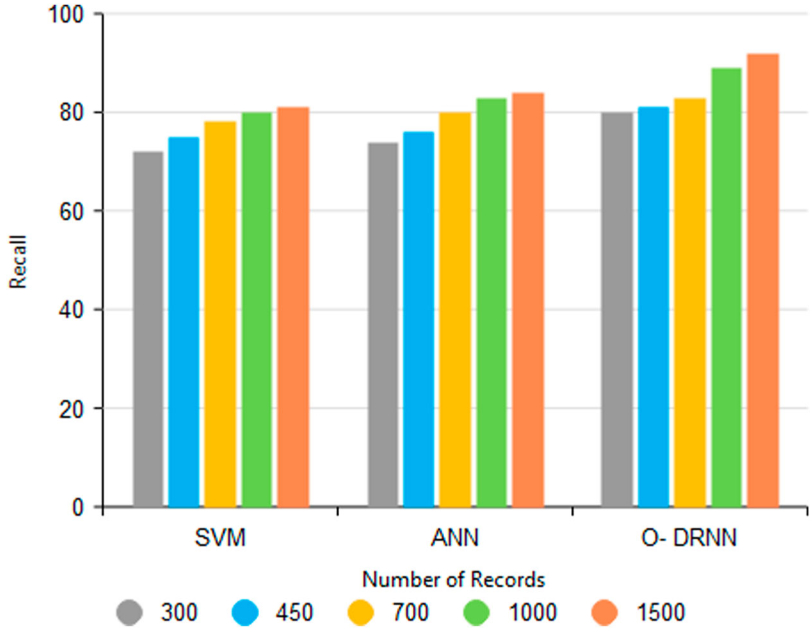

Figure 3. Recall analysis.

3.7. Precision

The ratio of the relevant data to the data that were obtained is called precision. From the Figure 2, the model proposed provides better precision of 0.91 than other existing classification methods SVM and ANN which obtained values of 0.80 and 0.85.

3.8. Recall

The efficiency of the proposed paradigm is examined using recall. It is the ratio of relevant data that are retrieved among all the existing relevant data. Figure 3. shows that the proposed model has a better recall value of 0.92 than the existing algorithm SVM and ANN with values of 0.81 and 0.84 respectively.

3.9. Specificity

Specificity is also termed as a true negative rate. This is the percentage of true negatives among the total data. From Figure 4, the proposed model-optimized DRNN has a better specificity rate of 90% when compared with the other two algorithms SVM and ANN. SVM obtained 81% and ANN obtained 85% of specificity.

3.10. F-Measure

The harmonic mean of accuracy and recall value is known as the F-Measure or F-score. Optimized DRNN obtained an F-Score value of 0.90 when compared to the other two algorithms SVM with 0.83 and ANN with 0.87 as shown in Figure 5.

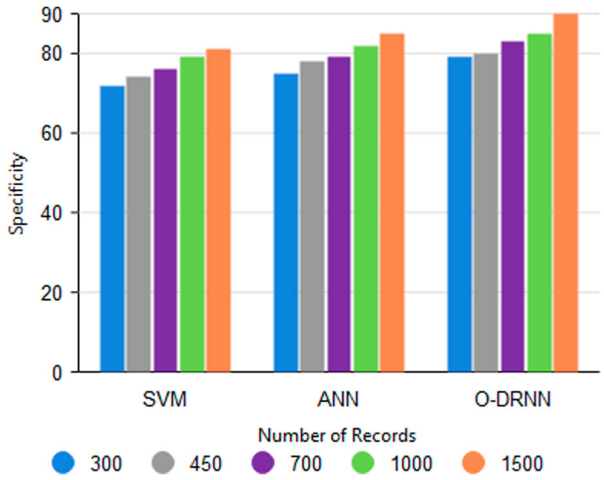

Figure 4. Specificity analysis.

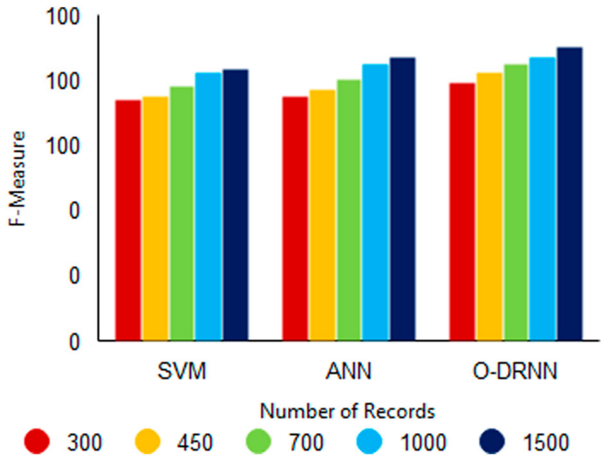

Figure 5. F-Measure analysis.

3.11. Experimental analysis for security analysis

In this part, the suggested security scheme's security aspects are discussed in detail with the existing methodologies using the following evaluation parameters such as Data Encryption and Decryption Time, Key Computation Time, and Security Overhead.

3.12. Data encryption & key computation time

In this proposed system, the time taken to encrypt the data as per request from HS is called the data encryption time. Data encryption time will differ as per the vary in file size from 1 MB to 500 MB. The Figure 6 shows the time taken for encryption is increasing when the file size is increasing. The diagram shows how the length of time it takes to finish encrypting a file grows linearly as the file size increases. This diagram also shows that file size and calculation time are unrelated. Because key computation time is almost stable even if the file size is getting increased. The computation of an encryption key takes a total of between 0.011 and 0.0193 s.

3.13. Data decryption & key computation time

The amount of time it takes to decrypt data upon HS's request is referred to as the data decryption time. Data decryption time is directly proportional to the size of the file. Because the decryption time consumes extremely high when compared to the encryption time. Encryption requires around 0.2 and 0.4 s to complete, whereas decryption takes around 0.2 and 0.9 s. But decryption key computation time is stable even though the increase in file size as shown in Figure 7.

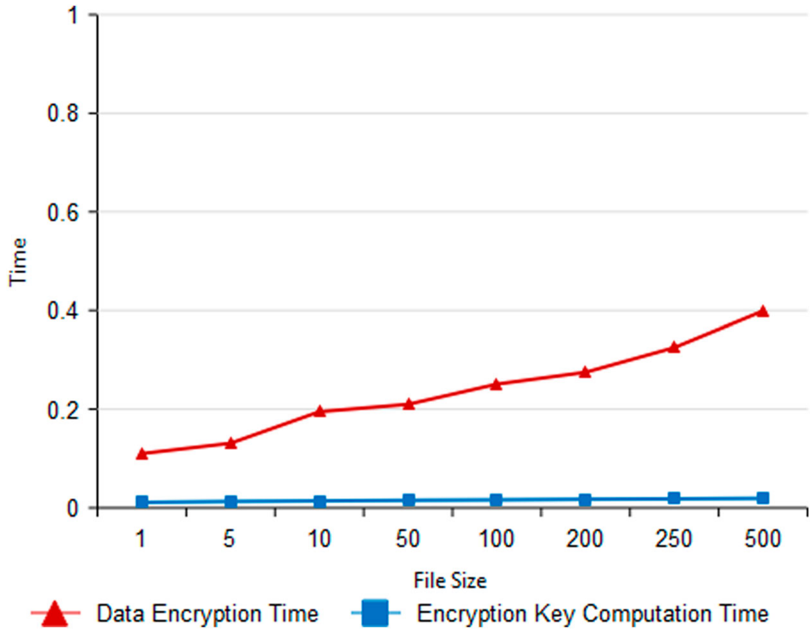

Figure 6. Data encryption and key computation time.

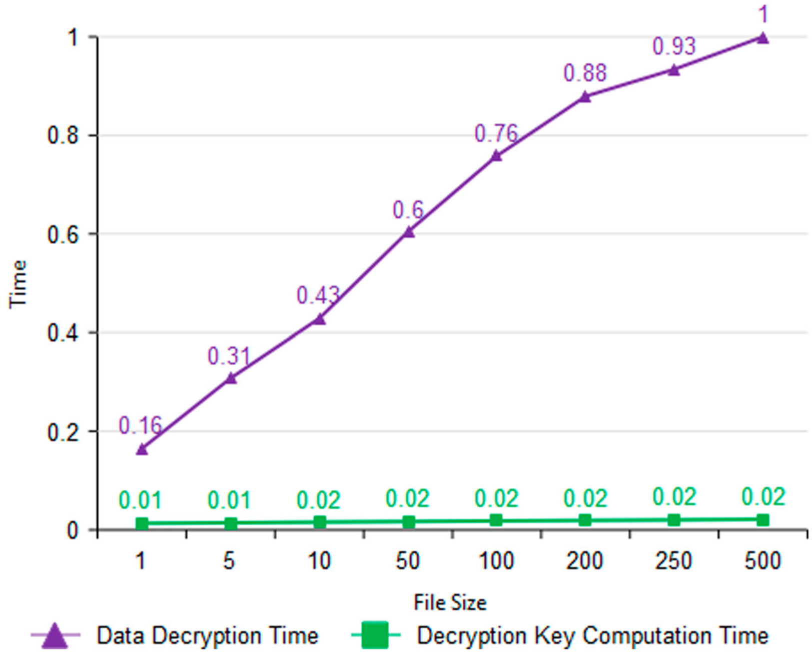

Figure 7. Data decryption and key computation time.

Table 3. Performance analysis for security overhead.

File size (MB)	Security overhead (%)
1	20
5	19.5
10	19
50	15
100	14
200	12
250	12
500	12

3.14. *Security overhead*

The ratio of protected operation time to file transmission time is known as security overhead. Table 3 clearly depicts that the security overhead percentage is becoming constant when the file size increases and it is not more than 12%. For smaller-size files, security overhead is 20% and 12% for larger files. The difference in Security overhead percentage for files from 1 MB to 100 MB is 6% but for 50 MB to 100MB files its only 1%. The overall outcome of the security overhead percentage is smaller for larger files.

4. Conclusion

In this paper, secured and optimized DRNN is used for sending the processed data from the patient remotely to the healthcare professionals. The remote data obtained from the patient is encrypted and sent to the healthcare server in edge computing, where the data is preprocessed for further analysis. The optimal feature set is extracted from the data obtained using the Particle Swarm Optimization algorithm that improves the performance of the classification model. After feature extraction, the data is processed by the Optimized DRNN model for identifying the presence and level of diabetes. In the O-DRNN model, the LSTM-based deep recurrent neural network is used with a Bayesian optimization algorithm for optimizing the hyper-parameter of the DRNN. The output of the model is sent to the cloud server by encrypting the data. Healthcare professionals can retrieve the data from the cloud server for further analysis using their authentication details. Multilevel security is implemented at all levels from the transmission to storage. According to experimental research, the suggested approach outperforms other current models to enable securely processed distant data transfer in edge computing. In the future, the model can be analysed for multiple disease prediction with more security.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

[1] Malasinghe LP, Ramzan N, Dahal K. Remote patient monitoring: a comprehensive study. J Ambient Intell Human Comput. 2019;10:57–76. doi:10.1007/s12652-017-0598-x.

[2] Stankovic JA. Research directions for cyber physical systems in wireless and mobile healthcare. ACM Trans Cyber Phys Syst. 2016;1(1):1–12.

[3] Chen M, Mao S, Zhang Y, et al. Big data related technologies, challenges and future prospects. Inf Technol Tour. 2014;15:283–285.

[4] Tang B, Chen Z, Hefferman G, et al. Incorporating intelligence in fog computing for big data analysis in smart cities. IEEE Trans Ind Inform. 2017;13:2140–2150.

[5] Wan J, Zou C, Ullah S, et al. Cloud-enabled wireless body area networks for pervasive healthcare. IEEE Netw. 2013;27:56–61.

[6] Sunny AD, Kulshreshtha S, Singh S, et al. Disease diagnosis system by exploring machine learning algorithms. Int J Innovations InEng Technol (IJIET). 2018;10(2):14–21.

[7] Leoni Sharmila S, Dharuman C, Venkatesan P. Disease classification using machine learning algorithms -a comparative study. Int J Pure Appl Mathetics. 2017;1114(6):1–10.

[8] Shraddha SS. Disease prediction using machine learning over big data. Int J Innovative Res Sci. June 2018;7(6):1–8.

[9] Gudadhe M, Wankhade K, Dongre S. Decision support system for heart disease based on support vector machine and artificial neural network. in Proceedings of International Conference on Computer and Communication Technology (ICCCT), September 2010: 741–745.

[10] Kahramanli H, Allahverdi N. Design of a hybrid system for the diabetes and heart diseases. Expert Sys Appl. 2008;35:82–89.

[11] Palaniappan S, Awang R. Intelligent heart disease prediction system using data mining techniques. in Proceedings of IEEE/ACS International Conference on Computer Systems and Applications (AICCSA 2008), Doha,Qatar, March-April 2008: 108–115.

[12] He D, Chan S, Tang S. A novel and lightweight system to secure wireless medical sensor networks. IEEE J Biomed Health Inform. 2014;18:316–326. (PMID: 24403430).

[13] Zhao Z. An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. J Med Syst. 2014;38:1–7.

[14] Han ND, Han L, Tuan DM, et al. A scheme for data confidentiality in cloud-assisted wireless body area networks. Inf Sci. 2014;284:157–166.

[15] Barua M, Lu R, Shen X. SPS: Secure personal health information sharing with patient-centric access control in cloud computing. In Proceedings of the Global Communications Conference (GLOBECOM), Atlanta, GA, USA, 9–13 December 2013: 647–652.

[16] Divi K, Liu H. Modeling of WBAN and cloud integration for secure and reliable healthcare. In Proceedings of the BodyNets, UMass Club, MA, USA, 30 September–2 October 2013: 128–131.

[17] Drira W, Renault E, Zeghlache D. A Hybrid authentication and key establishment scheme for WBAN. In Proceedings of the TrustCom, Liverpool, UK, 25–27 June 2012: 78–83.

[18] Van Pham H, Son LH, Tuan LM. A proposal of expert system using deep learning neural networks and fuzzy rules for diagnosing heart disease. In: Frontiers in intelligent computing: theory and applications. Singapore: Springer; 2020. p. 189–198.

[19] Mehmood A, Iqbal M, Mehmood Z, et al. Prediction of heart disease using deep convolutional neural networks. Arab J Sci Eng. 2021;46:3409–3422.

[20] Jabeen F, Maqsood M, Ghazanfar MA, et al. An IoT based efficient hybrid recommender system for cardiovascular disease. Peer Peer Netw Appl. 2019;12:1263–1276.

[21] Muzammal M, Talat R, Sodhro AH, et al. A multisensor data fusion enabled ensemble approach for medical data from body sensor networks. Inf Fusion . 2020;53:155–164.

[22] Khan MA. An IoT framework for heart disease prediction based on MDCNN classifier. IEEE Access. 2020;8:34717–34727.

[23] Zhang D, Chen Y, Chen Y, et al. Heart disease prediction based on the embedded feature selection method and deep neural network. J Healthc Eng. 2021;2021:6260022.

[24] Pavithra D, Jayanthi AN. An improved adaptive neuro fuzzy interference system for the detection of autism spectrum disorder. J Ambient Intell Humaniz Comput. 2021;12:6885–6897.

[25] Xue B, Zhang M. Browne WN particle swarm optimisation for feature selection in classification: novel initialisation and updating mechanisms. Appl Soft Comput 18. 2014: 261–276.

[26] Graves A, Schmidhuber J. Framewise phoneme classification with bidirectional LSTM and other neural network architectures. Neural Netw. 2005;18(5-6):602–610.

[27] Nguyen V. Bayesian optimization for accelerating hyper-parameter tuning. In 2019 IEEE Second International Conference on Artificial Intelligence and Knowledge Engineering (AIKE) June 2019: 302–305.

[28] Frazier PI. A tutorial on Bayesian optimization. arXiv Preprint ArXiv:1807.02811. 2018: 1–22.