International Journal of Advanced Technology and Engineering Exploration, Vol 8(83)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2021.874436

Research Article

Optimized encryption based elliptical curve Diffie-Hellman approach for secure heart disease prediction

J. Vimal Rosy[1*] and S. Britto Ramesh Kumar[2]
Assistant Professor, Department of Computer Science, Soka Ikeda College of Arts and Science for Women, Chennai, Tamil Nadu, India[1]
Assistant Professor, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, India[2]

Received: 16-July-2021; Revised: 15-October-2021; Accepted: 19-October-2021

Abstract
Heart disease is considered one of the complex and global-wide diseases, and its early detection plays a vital role in healthcare and cardiology. The Big-data requires a cloud that provides expandable data storage that is accessed via the internet. Moreover, the out-sourcing data in the cloud for storage makes it easier to the management of user data and also decreases the maintenance cost of data. However, some organizations do not trust to store the data in the cloud due to privacy and security concerns. Though the existing encryption techniques can confidentially protect the data, it has few drawbacks, like the access pattern can leak sensitive data. In this paper, an efficient framework for heart disease prediction was developed using deep learning methods using heart disease datasets from University of California, Irvine (UCI) repository. The proposed method utilizes Optimized Encryption based Elliptical Curve Diffie-Hellman (OEECDH) approach for key generation. Elliptic Curve Cryptography (ECC) with Diffie-Hellman algorithm utilized for decryption and encryption of data for enhancing the security and privacy in the cloud. Additionally, this algorithm reduces the complexity in computations and also encrypts the data more efficiently. This system is followed by the classification using a deep convolution network performed in experimental analysis. The performance of the proposed method is calculated from the parameters like decryption time, key generation time and encryption time. The proposed method shows better performance compared with existing techniques like Methicillin-Resistant Staphylococcus Aureus (MRSA), Rivest, Shamir, Adleman (RSA), MRSA-Colonized (MRSAC) and Elliptic Curve with Diffie–Hellman (ECDH) on the basis of performance metrics. Additionally, the proposed algorithm can be applied in health care systems to identify cardiac disease effectively.

Keywords
Heart disease, UCI repository, Elliptical curve cryptography, Diffie –hellman, Deep CNN, Encryption, Decryption.

1.Introduction
Heart disease also termed congenital heart-disease that, means the abnormal function of the human heart. This abnormality is detected by many signs and symptoms like swelling legs, chest pain, weak feeling, palpitations, cyanosis and breathing trouble [1]. These signs are tough to detect in the initial stage and also varies from one person to another person. Furthermore, the surgical process also has alternates of bypass surgery, wrong valves of heart, pacemaker and angioplasty. However, these two surgical processes need to manage the difficulties like the diagnosis of coronary artery disease may be slower, leading to death, and some might take a much longer time to regain the problem.

To avoid these difficulties, cardiac problems are recognized at the early stages without making mistakes. Moreover, several automated systems are developed in medicine by using many techniques such as machine learning and data mining to predict coronary artery disease [2, 3]. Additionally, the efficient recognition of heart disease is evaluated utilizing analysis results that indicate the minimal number of disease-associated topographies which are further effectively classified.

Cloud computing is broadly implemented in several applications for data analytics and storage purposes. Cloud computing with significant data processing abilities is vital to almost every application that requires more processing cost, like machine learning. However, it may be inappropriate to keep trust in third-party cloud systems, particularly those that store

*Author for correspondence

sensitive data. Moreover, cloud computing systems suffer from various security problems [4]. Additionally, cloud computing provides cloud computing services utilizing on-demand, easy usage and elastic techniques. It also offers several resources, but it also owns critical security issues. Among several problems with cloud systems, verifying data integrity at untrustworthy servers is one of the main issues.

Homomorphic encryption plays a vital part in cloud computing, developing privacy for data providers [5]. This encryption stretches a way to accomplish many services in encrypted data and also enhances the privacy of cloud users. Therefore, the company's stock the encrypted data in the public cloud and performs services in the encrypted data. Moreover, homomorphic encryption has several properties that make the encrypted data much beneficial for companies, like re-randomized encryption, verifiable encryption and random self-reducibility [6].

Diffie-Hellman key exchange method securely exchanges the cryptography keys on a public channel, and it was the first public-key method as proposed by Whitfield Diffie & Martin Hellman in the year 1976. It utilizes 2 keys where one is the private key, and another key is a secret key. If a sender needs to communicate with the receiver, the encryption is performed by the private key and the public key of the sender. On the receiver side, the decryption process takes place by decrypting the sent message by utilizing the sender's private key and the public key. This method is performed based on the difficulty of calculating logarithmic functions. This is called Data Loss Prevention (DLP). The Deep Neural Network (DNN), methods are broadly utilized for several days, representing a reasonable improvement in the prediction process and analysis of coronary artery disease.

Expandable data storage, accessing through the internet is provided from big data, which in turn requires a cloud platform. Since, in managing the user data, the cloud platform has made easier maintenance and decreases the cost of data maintenance. However, due to security and privacy concerns, some organizations are not trusting to store the data. Though the existing encryption techniques can confidentially protect the data, it has few drawbacks, like the access pattern can leak sensitive data.

Hence the main contribution of the paper is,

- To develop an accurate and efficient deep learning model for the prediction of heart disease.
- To propose an effective privacy-preserving deep learning system with public verifiability.
- To delegate the data encryption and decryption with the same public key and private key.
- To reduce the key generation time, thereby reducing the time for the overall process.
- To perform effective classification with deep Convolutional Neural Networks (CNN) and compare the existing and proposed system following the corresponding parameters using four datasets such as Cleveland, Statlog, Switzerland heart disease dataset and Hungarian heart disease datasets from the University of California, Irvine (UCI) repository.
- To employ Optimized Encryption based Elliptical Curve Diffie-Hellman (OEECDH) approach for key generation. The proposed method utilizes Elliptic Curve Cryptography (ECC) with Diffie-Hellman algorithm for decryption and data encryption to enhance security and privacy in the cloud.

The initial section of the paper deals with the introduction of privacy preservation, the need for the rapid detection of heart disease and the process of ECC-Diffie-Hellman in cryptography. Section 2 deals with the existing works about the proposed method. Section 3 provides the comprehensive methodologies for the proposed cryptographic approach; section 4 deliberates the performance analysis of the proposed system, and Section 5 concludes the work.

2.Literature review

This section deals with the review of literature of the prevailing works.

In [7] an algorithm to verify the medical image assembly that could identify any changes made in size or the pixel value of the medical image was discussed. Meanwhile, it not only ensures the assembly of medical images, but also ensures the authentication of the sender, thereby making it beneficial to archive the medical images. Moreover, the algorithm consists of three modules such as hashing, image encryption and data embedding. Primarily, the hash signatures were extracted from the image and embedded into the medical image. In the data embedding, the image is said to be divided into unevenly sized blocks. Moreover, the signatures were extracted on the receiver side and could be utilized for verifying medical image assembly. The

algorithm's efficiency was verified concerning the SNR ratio, co-relation co-efficient and structurally similar index metrics.

In [8] a hybridized deep learning framework was introduced to analyze the features of coronary artery disease and earlier-stage prediction of heart disease. Furthermore, the coronary artery disease dataset was gathered from UCI repository, and the dimensionality was minimized by the suggested approach. The collected dataset was analyzed, and the inconsistent data were analyzed and were swapped by noise data utilizing standard feature details. After the data is processed and analyzed by the suggested approach, the study has stated that the efficient training process has gained the derived output and input. The study lacked in increasing the dimensionality of data to investigate the effective prediction of coronary artery disease.

In [9] an idea for the prediction of heart disease was suggested. Coronary artery disease is on major area for utilizing DNN so that it could enhance the total quality of classifications of coronary artery disease. Furthermore, these classifications could be conducted in several ways: Support Vector Machine (SVM), Random Forest (RF), and K-Nearest Neighbour (KNN). Moreover, the study has stated that this dataset would be utilized for the optimization of Talos hyperparameter that is said to be more effective than others. The study has deployed optimized DNN with the employment of Talos and has compared it to others. When comparing them with other algorithms, the study has stated that the suggested model was more effective. The paper needs to improve the accuracy in terms of deep learning neural networks utilizing Talos optimization.

In [10] an optimum kernel function was suggested to improve the accuracy of SVM for Medical Data Classification (MDC). The study has stated that the key target of the MDC process was the Sequential Minimal Optimization (SMO) needed to elevate the linear kernel in SVM. Moreover, with a final objective to achieve the promising results in MDC, the study has utilized the UCI machine learning coronary artery disease database. From the results, the Optimal Kernel SVM (OKSVM) has accomplished more accuracy. Furthermore, the paper also denotes that the suggested technique could improve in works compared to existing approaches.

In [11] a novel e-health care to monitor the level of a deadly disease by utilizing the technologies like cloud and IoT with the support of deep learning techniques was suggested. The study has stated that the medical data was recovered from several patients using e-health care devices. Furthermore, the encrypted data were applied to a novel suggested cloud storage system, and it was stored in the cloud. The data that were stored could be recovered as original by implementing the decrypting process. Moreover, the cloud system was introduced to predict the rate of diabetes and heartbeat levels by utilizing medical data. The study has denoted that the analysis outcomes were obtained by performing several experiments, and from those outcomes, the suggested system surpasses the existing methods based on prediction. The further analysis deals with introducing the cryptographic algorithm, as an alternative to ECC and could determine in CNN for effective decision making.

In [12] a novel 5-layer deep neural network called HEARO-5 to produce the best heart rate prediction was deliberated. In order to tune and evaluate the architecture, the study has utilized Matthews Correlation Coefficient (MCC) and Kway cross-validation. Furthermore, the study has made their developments open source to facilitate more research and analysis on DNN in medicine. From the investigation, the study has found that the heart evaluation of algorithmic risk-reduction and optimization-5 architecture has produced 99% of accuracy, which substantially outperforms other existing studies. Furthermore, the study has failed to improve the process of the algorithm's ability and also has failed to develop a user-friendly software interface.

In [13] authors have intended to obtain a password from complex credentials during the integration of servers. The paper suggests that the properties of tetrahedron were used along with the Diffie-Hellman algorithm to defy malicious attacks. Furthermore, the noteworthy feature of the suggested 3D password authenticated and key exchange protocol is that end-user complexity has been significantly decreased with respect to communication and computation. Moreover, the recommended protocol is a novel noticeable protected 2-server protocol that shatters the expectations of some studies. The study has also denoted that the two server protocols should not be integrated. The parameters such as communication complexity, computational complexity and security principles are said to be evaluation parameters. The further analysis deals with strengthening the

protocols by the constant addition of surplus parameters.

In [14] a deep learning method utilizing Deep Convolutional Neural Network (DCNN) on Electrocardiogram (ECG) and Galvanic Skin Response (GSR) in a dataset for Affect, Mood and Personality and Mood Research on Groups and Individuals (AMIGOS) dataset was utilized. Furthermore, the identification of emotions is performed by comparing the physiological signals with data of valence and arousal of the dataset. The study has stated that this application utilizes CNNs for the extraction of physiological signals as well as Fully Connected Network (FCN) layers. The analysis outcomes of the suggested dataset have represented a substantial improvement in classifications of emotional states than the other existing studies. The further analysis deals with the implementations of the computational models in wearable devices to identify the emotional status.

In [15] authors have suggested an Internet of Things framework for accurately evaluating coronary artery disease utilizing a Modified Deep Convolutional Neural Network (MDCNN). Furthermore, the blood pressure and ECG of patients are monitored by the smartwatches attached to the heart monitoring device. Moreover, the performance was examined by comparing the suggested MDCNN to existing DNN techniques. From the outcomes, the study has denoted that the recommended method outperforms the existing studies in terms of accuracy. The further analysis deals with performing extensive experiments for enhancing the performance, and the suggested work will be tested with wearable in the upcoming days.

In [16] a robust homomorphic encryption model for non-Abelian rings followed by the definition of homomorphic mechanism in the ciphertext was suggested. The system could obtain one-way security following the conjugacy search problem. Then a homomorphic system was employed over the matrix ring. The system supported the encryption of real numbers in accordance with a homomorphism of second-order displacement matrix function and obtained fast ciphertext.

The [17] a proofed and trusted method offering an authenticated encryption for mapping and encoding a message to the curve was suggested. The tests utilized in this work are INDistinguishable Under Chosen Plain Text Attack (IND–CPA), INDistinguishable under Chosen Cipher text Attack (IND–CCA) etc., which are regarded as indistinguishable under Chosen-Plaintext Attack (CPA) and Chosen-Ciphertext Attack (CCA) attacks. In general, Computer Aided Design (CAD) might be useful in the automatic identification of myocardial infarction on ECG signals.

The [18] a deep learning method with an end-to-end system on the standardized 12 lead ECG signal for Myocardial Infarction (MI) diagnosis was elaborated. The system utilized a more generalized method of deep CNN that obtained efficient sensitivity and accuracy performance of 99% for diagnosing MI on all the ECG signals.

In [19] an Enhanced Deep Learning Assisted Convolutional Neural Network (EDCNN) to support and enhance the cardiac disease prognosis of patients was suggested. Furthermore, the enhanced deep learning assisted convolutional neural network mainly concentrates on deep architecture that includes multi-layer perceptron with regularized learning techniques. The accuracy has been precisely analyzed and executed. From the obtained outcomes, the study has shown represented a precision of 99.1%. The further analysis deals with the implementation of advanced Artificial Intelligence for improving precision. For proper classification, there is a requirement to efficiently process the raw heart disease dataset, which can be resulted in saving human lives. For the performance improvement of heart disease prediction models, various researchers are utilized machine learning algorithms to build the different models. By considering an example [20], the authors developed an approach to improve prediction accuracy in detecting the substantial features and classification performed using the hybrid RF classifier. The accuracy obtained was 88.47%. Furthermore, in [21] the researchers developed a context for predicting the heart disease in which the reduction of features was performed, resulted in a performance impact of various classifiers like support vector machines with 88 percent accuracy. Likewise, in [22], an approach was developed which creates decision rules for the risk level of heart disease classification, and accuracy resulted as 86.7 percent. For further improvements in accuracy, other newly developed methods should be utilized [23, 24].

2.1Challenges

The existing techniques in the encryption of data have some limitations in the cloud. The issues with the existing methods of data encryption are discussed

here. The automated coronary artery disease detection system needs to be developed by implementing DNN techniques. Various novel techniques efficiently analyze every data in cardiac disease and also predict the abnormalities in data in an efficient manner [25, 26]. The computer-aided traditional coronary artery disease prediction system also analyses heart data and classifies the abnormality features [27, 28]. However, the dimensionality of the topographies reduces the accuracy of the prediction process of cardiac diseases. Furthermore, the overly fitting data increases the complexity in calculations and maximizes the prediction time. To minimize these issues, techniques such as the hybridized and effective feature must be introduced to pick and predict from the feature set. Additionally, effective training methods support identifying the abnormalities in cardiac disease. The existing techniques of encryption do not secure the access patterns, and that eventually creates an impact on cloud privacy.

From the above literature review, it is identified that the authors have not focused on various attributes for heart disease prediction. Most of the researchers focus on general characteristics. For increasing the accuracy, the size of the attributes is reduced. However, this reduction does not predict accurate heart disease. All kinds of factors influencing cardiovascular disease should be considered. Thus, effective dataset should be utilized. Only a few studies have used larger datasets, and however, they did not consider the proper error handling mechanism in the classification approach. The error handling mechanism suggested as reconstruction error reduction, removal of rows, filling empty values using global values and mean factor consideration. Some researchers have been justified their proposed model with minimum comparison, and thus several effective comparative analysis is required. The above-listed challenges such as dimensionality reduction, overfitting, security in storage, improving accuracy are addressed using deep CNN and proposed OEECDH for enhancing security.

3.Proposed methodology

The following flow diagram (*Figure 1*) depicts the overall architecture of the proposed framework. The successful encryption and decryption of the obtained heart disease dataset, such as UCI heart disease datasets, have been introduced in this paper for improving the heart disease prediction. The file uploaded has been encrypted with ECC based Diffie-Hellman cryptographic method and stored in the corresponding cloud storage. From the cloud storage, the proposed method utilizes the same ECC-Diffie-Hellman method for the decryption of the encrypted key. Then this process is followed by the corresponding file download. These files are pre-processed for the removal of noise and feature selection with statistical analysis. These features are classified with deep CNN. The results are predicted and analyzed for their performance analysis.

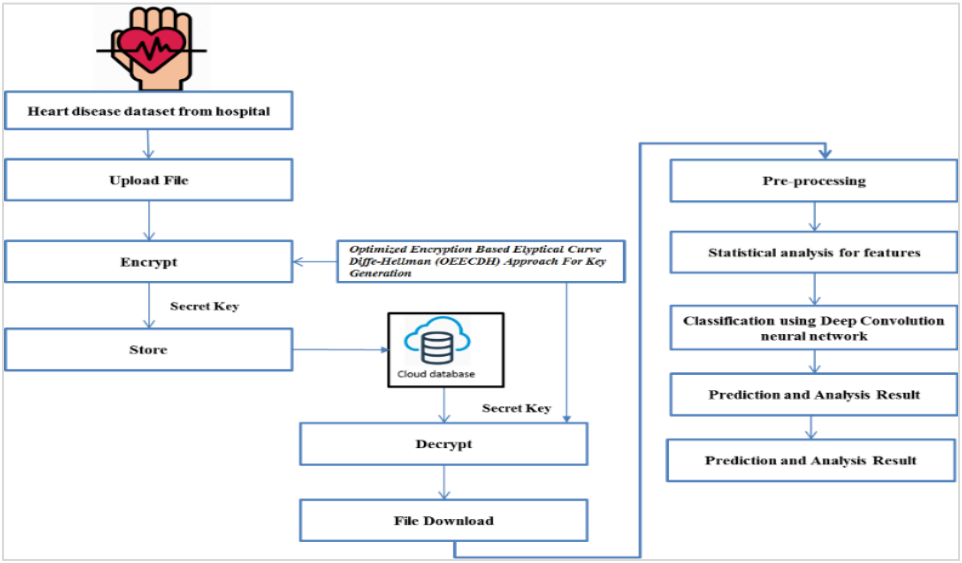

Figure 1 Overall architecture of the proposed system

This process is explained in detail in the following. In the proposed system, the heart disease dataset providers encrypt the data sets with the use of the Unidirectional Proxy Re-Encryption (UPRE) method that comprises initialization, key generation, rekey generation, encryption, re-encryption and decryption. This data has been loaded to the proxy server. Here the multi-data providers can decide their desired, and sensitive data be encrypted. This is followed by the re-encryption of the ciphertext obtained from the data providers under the appropriate public key of the data analyst. The server includes the encrypted and noised data to the ciphertext with ECC–Diffie-Hellman homomorphic scheme. After the addition of the encrypted noise, the cloud server forwards the noised ciphertext to the corresponding data analyst. Here, the data analyst decrypts the noised ciphertext for obtaining the noise dataset. This step is followed by a performance of deep CNN architecture algorithms by the data analyst for his extrapolative analytics. The data analyst decrypts the noise ciphertext initially to obtain a noise dataset with his private key followed by privacy preservation of the entire data without the leakage of privacy to the individual users.

3.1Elliptic curve Diffie-Hellman (ECD) cryptography

In this section, the study illustrated the computational Diffie-Hellman assumption concerning the difficulty of estimating the discrete logarithm in the cyclic groups.

ECD is a key exchange method for the determination of private and public keys. Both the recipient and sender will perform the same operation with a similar public key and different private key and produce similar results. EDH is a well-known algorithm for resolving the logarithmic problems of elliptic curve discretion based on complicated mathematics.

The operational group in ECD has been divided into two kinds of process which are an addition and point labelling.

Step 1)ECC $= \{(a, b \mid b2 = a3 + ra + s)\{\theta\}\}$,
$where\ \theta = \text{Point at infinity}$

Step 2) $\text{SEnc} = \frac{b_Y - b_X}{a_Y - a_X} \bmod \text{Prime}$

Step 3) $aT = (\text{SEnc}^2 - (a_X + a_Y)) \bmod \text{Prime}$

Step 4)$b_T = (\text{SEnc}^2(a_X - a_T)) - b_X$

Step 5) $X + X = T = 2X$

Step 6) $\text{SEnc} = \frac{3a^2 X + r}{2b_X} \bmod \text{Prime}$

Step 7) $a_T = (\text{SEnc}^2 - 2a_X) \bmod \text{Prime}$

Step 8) $b_T = (\text{SEnc}\,(a_X - a_T) - b_X) \bmod \text{Prime}$

Step 9) $X + Y = \theta$ if $(a_X = a_Y)$

Step 10) $X + Y = \theta$ if $(a_X = 0)$

Step 11) $Y = \text{key}\, X$

Step 12) $Y = X + X + X + \ldots + X$ key ε Z

3.2Diffie-Hellman

Diffie-Hellman key exchange method securely exchanges the cryptography keys on a public channel, and it was the first public-key method as proposed by Whitfield Diffie & Martin Hellman in the year 1976. It utilizes 2 keys where one is the private key, and another key is a secret key. If a sender needs to communicate with the receiver, the encryption is performed by the private key and the public key of the sender. On the receiver side, the decryption process takes place by decrypting the sent message by utilizing the sender's private key and the public key. This method is performed based on the difficulty of calculating logarithmic functions. This is called DLP. The DNN, deep learning neural network methods are broadly utilized for several days, representing a reasonable improvement in the prediction process and analysis of coronary artery disease.

In this study a setup has been proposed that could be processed and implemented in the cloud environment by considering the merits of linear cryptography for establishing a secured connection and cryptography for data encryption. The Diffie-Hellman key exchange and the ECC are integrated by following the four steps. The first step is the establishment of a secured connection; the next is the account creation, followed by the authentication and data exchange. The study utilized ECC mainly due to its computational cost and easy processing. Further, it possesses a sub exponential time complexities that make the complexity of cracking. The study used Diffie-Hellman to offer the better establishment of the corrections during encryption and decryption.

3.3Optimized encryption based elliptical curve Diffie Hellman (OEECDH) approach for key generation

OEECDH is an approach for generating a secured key for Encryption based Elliptical Curve (EEC) as well as the Advanced Encryption Standard (AES) algorithm. Generally, in the AES algorithm, a random key will be generated on the sender side, then through a secured channel, it is sent to the destination site. So far, the encryption key is being a plain text key [29]. Since it is not much efficient, this approach of generating and sharing a random key to the destination site through a secured channel may not be

much secured. So the effective method of generating key on the sender side and destination side and using it for decryption and encryption of the data. This OEECDH approach is shown in *Figure 2*.

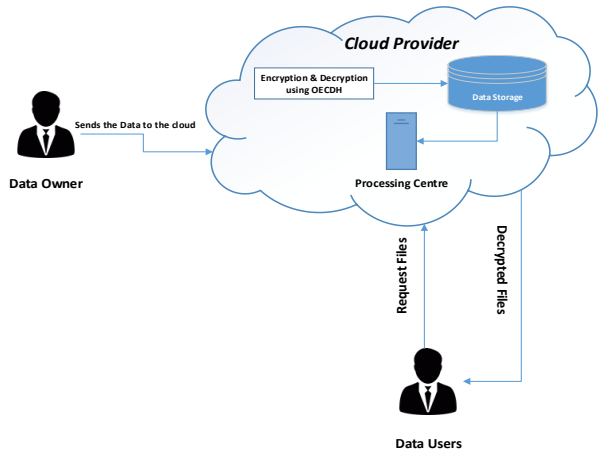

Figure 2 Optimized encryption based elliptical curve Diffie-Hellman (OEECDH) approach

3.4Pseudocode

EECDH method for common key generation on sender and receiver side shown in *Figure 3.*

At the sink node:

(i) Select a private key 'a'**(1<a<n-1)**

(ii) Multiply the generator point H with private key 'a', **X= a. H**

(iii) Exchanging the results to the destination side. "No need for the channel to be secure"

(iv) To calculate the final key," key"

'Key' must be multiplied with the private key 'a' and the received values from the other side, **key= a. b. H**

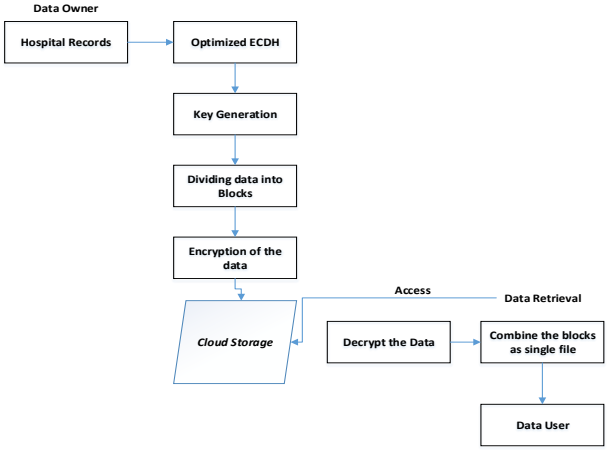

Figure 3 OEECDH method for common key generation on sender and receiver side

At base station node:

(i) Select a private key 'b'**(1<b<n-1)**

(ii) Multiply the generator point H with private key 'b', **S= b. H**

(iii) Exchanging the results to the destination side. "No need for the channel to be secure"

(iv) To calculate the final key," key"

"Key" must be multiplied with the private key 'b' and the received value from the other side, **key= a.b.H**

Sliding window scalar multiplication

$1.R \leftarrow \infty \; and \; j \leftarrow (1-1)$
$2.while \; j \geq 0 \; do$
$3.if \; p_j = 0 \; then \; R \leftarrow [2]R \; and \;\; j \leftarrow (j-1)$
$4.else$
$5.A \leftarrow max(j-m+1,0)$
$6.while \; p_a = 0 \; do$
$7.A \leftarrow A+1$
$8.end \; while$
$9.for \; h = 1 \; to \; j-A+1 \; do$
$10.R \leftarrow [2]R$
$11.end \; for$
$12.v \leftarrow [p_j \dots \dots \dots p_a]_2 \;\; [p_j = p_a = 1 \; and \; j-a+1 \leq m$
$13.R \leftarrow R \oplus [v]S \; [u \; is \; odd \; so \; that \; [v]S \;\; is \; pre-computed$
$14.j \leftarrow A-1$
$15.return \; R$
$16.end \; while$

Sliding widow scalar method

In this method, more memory has been added to the WSN nodes in recent years. When the node size decreases, the size of the battery becomes much constrained [30]. In this technique, it needs a certain amount of memory to store pre-computations, which results in decreased mathematical operations and proved to be an energy-efficient method.

Preprocessing

Preprocessing is the initial step of the cardiac disease prediction since the data collected comprise various information like chest pain type and location, age, serum cholesterol, cigarette habits, diabetic level, betablocker, exercise protocol, usage of nitrates, depression level etc. These collected data has been stored and forms the database for every patient through a normal monitoring process. It is to be noted that few data are interrupted or missing by the activities of patients and technician mistakes. Hence, before technical processing, it is necessary to prepare

the data to be free of noise and other criteria discussed.

Deep CNN classification

The CNN utilizing Keras library that runs over Tensor Flow, the study has built a consecutive model. The CNN here is a two-layer deep architecture with an output prediction layer as well as a fully associated layer. The code extracts of the implementation are shown in the following algorithm. The comprehensive flow of CNN is described in *Figure 4*. The primary convolutional layer consists of 32 filters of size 3×3 with activation of Rectified Linear Unit (ReLU). Furthermore, it is shown that 32 feature maps are produced by an intermediate layer. The max-pooling size of 2×2 was utilized to decrease the unnecessary dimensionality of filter and data in feature maps. The secondary layer consists of 64 filters of size 3×3 with the activation of ReLU. The similar-sized max-pooling was again utilized in the secondary hidden layer. To avoid the data overfitting, 50% of the dropout probability was used to create a co-adaption amid the hidden layers. Before the information had passed to the fully connected layer, the features were flattened to form a one-dimensional feature vector. A fully connected layer that contains 128 ReLU activations are utilized to process the feature vectors. Furthermore, the prediction layer is a soft-max layer used to predict the final class [31].

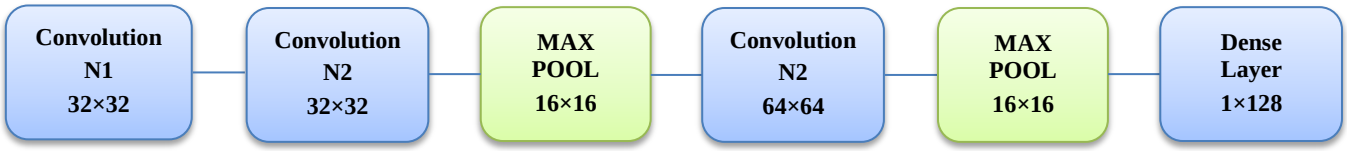

Figure 4 Comprehensive flow of CNN

Model definition

Sequential Model

- The addition of two-dimensional convolutions with the employment of 32 filters and 3×3 size until the filter reaches 64 ReLU and linear activations till the dense layer 128 layers.
- Addition of fully connected layers with dense class.
- Computing Softmax activation via Adam optimized to prevent decaying of the model.
- Definition of accuracy metrics followed by the compilation of the model.

View of model configuration

- Viewing of output and input shape
- Assignation of weight to an individual layer
- Once the weights are updated, the models are ready to train

Training

- Performs model fitting utilizing the size of the batch and also epochs. The data validation is tested until the training gets completed.

Performance

- Represents the validation loss and model loss with accuracy till epochs reach 15.

4.Performance analysis

4.1Dataset description

The Cleveland coronary artery disease dataset is deliberated for testing in the study. Four different datasets are used in the proposed research. They are Statlog, Cleveland, Switzerland and Hungarian heart disease datasets from the UCI machine learning repository [32]. At the time of designing the dataset, there were 75 attributes and 303 instances, though all the published experiments are referred to utilize 14 subsets of them. In this paper, the pre-processing on the dataset and six samples were eliminated because of the missing values. The rest of the samples from 297 and 13 datasets is left with an output label of 1. The output label has two classes to determine the presence as well as the absence of heart disease. Therefore, the matrix 297×13 was formed from the extracted features. The dataset features information is given in *Table 1*. The environmental configuration of the proposed system is shown in *Table 2*.

4.2Performance analysis

Table 3 shows the key generation time of the current cryptographic techniques along with the proposed approach. The minimum time is taken by the proposed algorithm to generate keys and compared to other currently existing methods. The existing algorithms such as Methicillin-Resistant Staphylococcus Aureus (MRSA), Elliptic Curve with Diffie–Hellman (ECDH), Rivest, Shamir, Adleman

(RSA) and MRSA-Colonized (MRSAC) takes maximum time for the key generation. Furthermore, the proposed technique gives a small encrypted key that needs small power for computation and processing time. So, the existing technique has a higher computation time of 8925ms for 2048-bit key length, while the proposed method has a computation time of 780ms that seems much lower.

Table 1 UCI machine learning repository- heart disease dataset attributes

Features	Description
Age	Age (in years)
Sex	The male is indicated as 1 The female is indicated as 0
Restecg	Results of resting electrocardiographs Normal: Value 0 Having an ST-T wave abnormality (inverting T wave or elevating ST or depression rate>0.05mV): Value 1 Discovering probable or definite LVH (Left Ventricular Hypertrophy) by estes' criteria: Value 2
Trestbps	RBP (Resting Blood Pressure) – mm Hg on hospital admittance
Condition	No disease: 0 Disease: 1
Thalach	HRR (High Heart Rate) achieved
Thal	Normal: 0 Fixed defect: 1 Reversible defect and label: 2
CP	Kind of chest pain Typical-angina: Value 0 Atypical-angina: Value 1 Non-angina pain: Value 2 Asymptomatic: Value 3
Chol	Serum cholesterol (mg/dl)
Exang	Use prompted angina (no: 0, yes: 1)
FBS	Blood sugar>120mg/dl False: 0 True: 1
CA	Number of major vessels (0-3) coloured by fluoroscopy
Oldpeak	ST depression instigated based on rest
Slope	Peak slope applying ST segment Up-sloping: Value 0 Flat: Value 1 Down-sloping: Value 2

Table 2 Hardware and software configuration

Hardware configuration	Software configuration
CPU - Intel Core i7 – 7700 @ 2.80 GHz	Windows 10
GTX 1050	Python 3.7
16GB RAM	Anaconda Spyder

Table 3 Key generation time of existing and proposed system

Key length (in bit)	RSA [33]	ECDHC [33]	MRSA [33]	MRSAC [33]	Proposed approach
100	72	78	110	158	70
128	92	79	144	244	72
256	469	94	484	584	86
512	140	110	172	192	100
1024	469	391	625	1625	381
2048	2453	781	8125	8925	780
4096	91,542	7637	93,899	123,899	7,620

Table 4 and *Table 5* shows the encryption time and decryption time for output and input data respectively. The performance of proposed and existing techniques is calculated based on diverse key lengths like 128, 100, 512, 256, 4096, 1034 and 2048 in bits. When comparing to the existing techniques, the proposed algorithms represent better results. Moreover, the proposed technique requires minimal decryption and encryption time. The proposed method is a key exchange protocol that quickly exchanges the key between server and client. Furthermore, the existing techniques are dependent on the RSA algorithms, which need a number key for encryption and also need more time for computation. The proposed technique generates a lesser number of keys as well as the computation time for the encryption process is reduced. The existing design has a decryption time of 10,957 ms, and the proposed technique has 180 ms. Therefore, the computation time is reduced because of the less utilization of the number key generation. The proposed method decreases the information delay between the server and client. And also, it is faster than existing techniques such as MRSA, RSA ECDH and MRSAC. *Table 6* depicts the performance parameters of the proposed system in accordance with the Accuracy, Specificity, Sensitivity and MCC. The proposed method has been compared with Logistic Regression (LR), Artificial Neural Network (ANN), KNN, SVM (linear and Radial basis Function (RBF)), Decision Tree (DT) and Navies Bayes (NB). It is shown that our proposed system exhibited 92 % accuracy and specificity, 90% sensitivity and 85% MCC. These measures are greater, and hence the proposed system proved to be efficient in terms of accuracy, specificity, sensitivity and MCC value.

Table 4 Encryption time

Key length (in bit)	ECDHC [33]	MRSA [33]	MRSAC [33]	Proposed approach
100	10	222	188	9
128	12	205	305	10
256	15	329	409	12
512	19	1672	2762	19
1024	30	11,625	13,625	28
2048	50	99,891	10,880	46
4096	92	110,907	21,887	86

Table 5 Decryption time

Key length (in bit)	ECDHC [33]	RSA [33]	MRSA [33]	MRSAC [33]	Proposed approach
100	16	88	107	212	12
128	31	188	122	188	29
256	47	62	156	203	42
512	63	218	968	688	60
1024	78	1453	6938	7038	70
2048	109	15,203	53,609	83,709	100
4096	187	18,381	10,957	10,957	180

Table 6 Comparative analysis of the proposed and the existing system with the performance parameters on Cleveland dataset

Parameters	LR [34]	KNN [34]	ANN [34]	SVM (RBF) [34]	SVM (Linear) [34]	NB [34]	DT [34]	Proposed approach
Accuracy (%)	88	84	82	85	87	79	78	92
Specificity (%)	98	96	93	93	95	95	88	92
Sensitivity (%)	76	70	78	74	72	79	89	90
MCC (%)	87	85	82	85	86	84	83	85

From the *Figure 5*, *Figure 6* and *Figure 7* shows the proposed study result based on encryption, decryption time and key size evaluation based on reference [35]. Generally, if the file size increases, the encryption time increases, but for the proposed lightweight OEECDH approach, it reaches minimum encryption and decryption time compared with the existing study. Increased key size achieved

compared with current studies ECC, Homomorphic Encryption (HE) and Optimal Homomorphic Encryption (OHE), thus the security also increased. The graphs visualized the optimal security achieved in the proposed model compared to other techniques.

From *Table 7*, it is found that existing methods such as RF, LR, SVM, Extreme Learning Machine (ELM) and KNN showed better precision, recall, G-mean, Misclassification Cost (MC), Area under Curve (AUC), specificity and the Effective Performance (E) value based on reference [36]. However, the proposed system showed a high rate of E with 95.01%, precision with 97.03%, recall with 96.36%, G-mean with 95.09%, MC with 17.43%, specificity with 96.63% and AUC with 97.63%. This proved its efficacy than conventional systems [36].

In addition, proposed and conventional systems are analyzed in the Hungarian dataset. The obtained outcomes are shown in *Table 8*. From the results, it is found that existing methods like RF showed the E value as 80.43%, precision as 75.52%, recall as 60.19%, G-mean as 71.04, MC as 87.93%, specificity as 86.34% and AUC as 74.07%. On the other hand, traditional methods like LR, SVM, ELM, KNN and [36] showed better results concerning all the metrics. However, in comparison with the proposed system, existing methods showed lower performance. From *Table 7*, it is found that the proposed system showed E as 95.62%, precision as 96.32%, recall as 94.85%, G-mean as 93.68%, MC as 20.96%, specificity as 23.47% and AUC as 96.99%. Hence, the proposed system is effective in predicting heart disease than conventional [36].

The comparison is also carried out with another dataset named the Switzerland dataset. The obtained results are tabulated in *Table 9*. Various traditional methods such as Adaptive Genetic Algorithm with Fuzzy Logic (AGAFL), Linear Programming (LPP) with Rule-Based Fuzzy Classifier (LPP+RBFL), Rough Set with Fuzzy Logic (RS+FL) are employed for analysis. Accuracy, sensitivity and specificity are taken as performance metrics. The analytical outcomes revealed that the traditional methods like AGAFL explored 89% accuracy, LPP+RBFL showed 72% accuracy, and RS+FL exhibited a 63.4% accuracy rate. Moreover, the sensitivity and specificity rates of existing methods were better. But the proposed system showed a high accuracy rate (97.51%) than the existing system. Accordingly, the accuracy rate of the proposed method is found to be high that reveals its suitability in disease prediction.

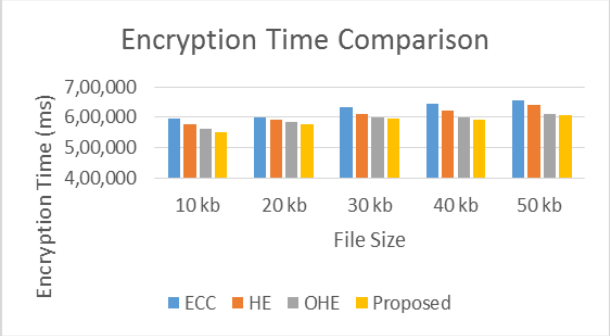

Figure 5 Encryption time comparison of proposed and existing study

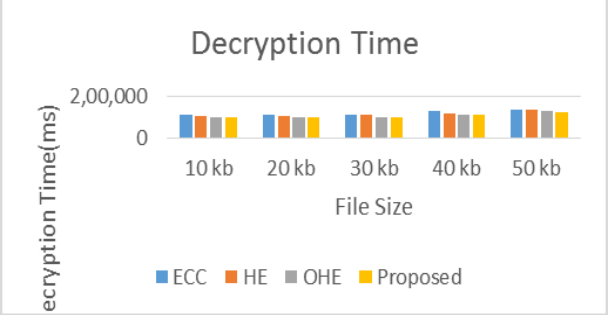

Figure 6 Decryption time comparison of proposed and existing study

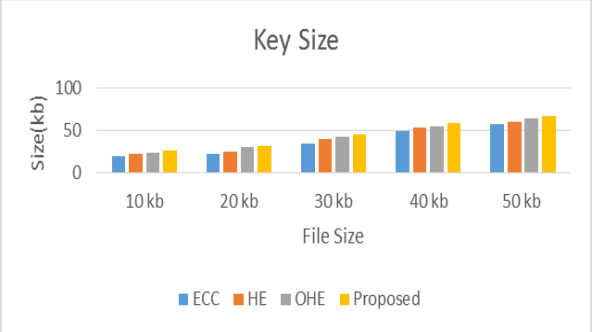

Figure 7 Key size evaluation of proposed and existing

Table 7 Comparative analysis of the existing and proposed methods in Statlog dataset

Metrics	RF [36]	LR [36]	SVM [36]	ELM [36]	KNN [36]	Existing [36]	Proposed approach
E (%)	87.53	87.87	88.67	82.81	76.94	94.44	95.01

Precision (%)	83.7	84.07	84.81	78.15	70	92.59	97.03
Recall (%)	80.64	82.08	83.85	70.65	62.85	92.15	96.36
G-mean	83.14	83.79	84.41	76.65	68.4	92.56	95.09
MC (%)	51.85	50	44.81	75.19	96.67	22.22	17.43
Specificity (%)	86.13	86	85.45	84.29	75.18	93.21	96.63
AUC (%)	83.75	83.92	85.07	80.17	68.42	92.08	97.63

Table 8 Comparative analysis of the proposed and existing methods in Hungarian dataset

Metrics	RF [36]	LR [36]	SVM [36]	ELM [36]	KNN [36]	Existing [36]	Proposed approach
E (%)	80.43	82.07	78.91	80.40	75.43	89.47	95.62
Precision (%)	75.52	77.93	74.48	75.86	66.55	89.31	96.32
Recall (%)	60.19	62.08	53.38	59.42	61.36	82.39	94.85
G-mean	71.04	73.72	67.55	70.97	59.97	82.95	93.68
MC (%)	87.93	82.76	100.00	90.34	94.14	38.28	20.96
Specificity (%)	86.34	88.99	89.10	88.13	70.92	92.02	93.47
AUC (%)	74.07	76.31	71.96	74.59	69.07	88.38	96.99

Table 9 Comparative analysis of the proposed and existing methods in Switzerland dataset

Methods	Accuracy	Sensitivity	Specificity
AGAFL [37]	89	97	75
LPP + RBFL [37]	72	76	67
RS + FL [37]	63.4	67	72
Proposed approach	97.51	98.09	97.86

Additionally, analysis has been undertaken with respect to memory consumption, and the obtained outcomes are provided in *Table 10*. Generally, memory consumed in less amount is found to be a good algorithm. Accordingly, the proposed system explored minimum memory consumption than existing methods such as Elliptical Curve Cryptography with Chinese Remainder Theorem (ECC-CRT), RSA and EIGamal. This explores the efficacy of the proposed system in predicting heart disease.

Table 10 Analysis in terms of memory consumption

Algorithm	5000 kb	10000 kb	15000 kb
Proposed	12678	15269	25685
ECC-CRT [38]	19855	36458	56981
ElGamal [38]	37587	69458	124589
RSA [38]	52896	120000	155683

4.3Comparative analysis of all datasets (Cleveland, Statlog, Hungarian and Switzerland)

Lastly, all the datasets (Cleveland, Statlog, Switzerland and Hungarian) have been analyzed with respect to hidden neurons, epochs, client bench time and server bench time, as shown in *Table 11*. Cleveland dataset showed 89.3ms as client bench time and 98.78ms as server bench time for 100 epochs with ten hidden neurons. Similarly, the Statlog dataset showed 78.26 ms as client bench time and 85.96 ms as server bench time for 120 epochs with 15 hidden neurons. Moreover, the Switzerland dataset showed 95.89ms as client bench time and 124.32 ms as server bench time for 100 epochs with 15 hidden neurons. Hungarian dataset showed 74.95 ms as client bench time and 90.54 ms as server bench time for 150 epochs with 20 hidden neurons. It has been found that the Hungarian dataset showed minimum client bench time and more bench time. On the contrary, the Statlog dataset explored high client bench time and minimum server bench time. Thus, each of these datasets is better in accordance with the hidden neurons, epochs, client and server bench time.

Table 11 Comparative analysis of all datasets

Dataset	Hidden Neurons	Epochs	Client bench time (ms)	Server bench time (ms)
Cleveland	10	100	89.3	98.78
Statlog	15	120	78.26	85.96
Switzerland	15	100	95.89	124.32
Hungarian	20	150	74.95	90.54

Analysis has been carried out in terms of computational time excluding network communication, and results are shown in *Table 12* [39]. It has been found that the Cleveland dataset showed a computational time of client with 82.62 ms and cloud server with 75.96 ms and bandwidth 102.63 kB with 100 epochs and ten hidden neurons. Statlog dataset showed the computational time of client with 81.75 ms and cloud server with 71.85 ms and bandwidth 114.45 kB with 120 epochs and 15 hidden neurons. Switzerland dataset showed the computational time of client with 90.89 ms and cloud server with 84.79 ms and bandwidth 101.365 kB with 100 epochs and 15 hidden neurons. Hungarian dataset showed the computational time of client with 81.26 ms and cloud server with 74.81 ms and bandwidth 98.15 kB with 150 epochs and 20 hidden neurons.

Table 12 Comparative analysis of user threshold protocol

Uses threshold protocol			Computational time (excluding network communication) (ms)		
Dataset	**Hidden neurons**	**Epochs**	**Client**	**Cloud server**	**Bandwidth (kB)**
Cleveland	10	100	82.62	75.96	102.63
Statlog	15	120	81.75	71.85	114.45
Switzerland	15	100	90.89	84.79	101.36
Hungarian	20	150	81.26	74.81	98.15

4.4Discussion

From the results, outcomes, it shows that the encryption and decryption time is reduced from the proposed model compared with existing works. Key size is increased, and hence the security is improved. Computation time is reduced. Thus, reliability is increased. Prediction time for classification is decreased, and the results are accurate. The proposed study has optimized the encryption and decryption process, making the algorithm more efficient and reliable. The major aim is to make data more secure because it's a hospital patient record. The proposed algorithm will perform the process more securely. And for the classification, the proposed study has implemented deep CNN, which will extract more features from its layers and classify them more accurate than the traditional algorithms. This study proposed a lightweight OEECDH approach to secure hospital records. The traditional methods have less security compared to our proposed methodology, and it takes time to process the huge data. Though efficient outcomes were obtained, the security has to be further enhanced in addition to the system performance. The present study proposed Optimized encryption and Decryption methodologies to increase the system security on big data. For performance evaluation, this study utilized four datasets such as UCI Cleveland, Hungarian, Switzerland and Statlog dataset. It has been found that the Hungarian dataset showed minimum client bench time and more bench time. On the contrary, the Statlog dataset explored high client bench time and minimum server bench time. Thus, each of these datasets is better in accordance with the hidden neurons, epochs, client and server bench time. Significantly, the statlog dataset shows better results by using the proposed system with an accuracy of 97.63% compared with the Switzerland dataset as 97.54%, Hungarian dataset as 96.6% and Cleveland dataset as 92%.

Hence, through comparative analysis, it is clear that the proposed system is more effective than the existing methods with respect to the considered significant metrics such as accuracy, specificity, precision, recall, computational time, memory consumption, encryption and decryption time. This outstanding performance of the proposed system has made it gain high suitability in heart disease prediction. A complete list of abbreviations is shown in *Appendix I*.

5.Conclusion

The cloud computing paradigm has recently become popular because of its flexible computation and the capacity to store a large amount of data. To gain

these beneficial impacts, several data owners will out-source their data and data analysis operations such as data insertion, data modifying and data queries in the cloud. For security reasons, the owner of the data encrypts the data before it gets outsourced. In this article, the proposed method is utilized for data security in the cloud. The user has encrypted the data utilizing the algorithm and has stored the data in cloud storage. Furthermore, the data that has been stored can easily be retrieved using the decryption method. The proposed technique can process the data faster with a larger key size than the existing methods. An experimental analysis of the proposed method is evaluated by various evaluation metrics like decryption time, key generation time and encryption time, memory consumption, computational time. The processing time of the ECDH algorithm seems to be better than the other existing cryptographic techniques. Four datasets, such as UCI Cleveland heart disease datasets such as Cleveland, Statlog, Hungarian and Switzerland datasets, are used in this study. Significantly, the statlog dataset shows better results by using the proposed system with an accuracy of 97.63% compared with the Switzerland dataset as 97.54%, Hungarian dataset as 96.6% and Cleveland dataset as 92%. In future, a much-secured data retrieval mechanism could be implemented in cloud storage.

Acknowledgment
None.

Conflicts of interest
The authors have no conflicts of interest to declare.

References
[1] Amin MS, Chiam YK, Varathan KD. Identification of significant features and data mining techniques in predicting heart disease. Telematics and Informatics. 2019; 36:82-93.
[2] Khan A, Ramsey K, Ballard C, Armstrong E, Burchill LJ, Menashe V, et al. Limited accuracy of administrative data for the identification and classification of adult congenital heart disease. Journal of the American Heart Association. 2018; 7(2).
[3] Singh P, Singh S, Pandi-jain GS. Effective heart disease prediction system using data mining techniques. International Journal of Nanomedicine. 2018:121-4.
[4] Kumar PM, Lokesh S, Varatharajan R, Babu GC, Parthasarathy P. Cloud and IoT based disease prediction and diagnosis system for healthcare using fuzzy neural classifier. Future Generation Computer Systems. 2018; 86:527-34.
[5] Prasetya FM, Sari AK. Pneumonia risk assessment on data encrypted using a homomorphic cryptosystem. In international conference on bioinformatics, biotechnology and biomedical engineering (BioMIC)-bioinformatics and biomedical engineering 2019 (pp. 1-6). IEEE.
[6] Aldossary F. Health observation system using cloud computing. International Journal of MC Square Scientific Research. 2017; 9(4):8-16.
[7] Agarwal S, Ranjani JJ. Image integrity verification via reversible predictive hiding and elliptic curve diffie-hellman. International Journal of Innovative Computing and Applications. 2019; 10(3-4):154-63.
[8] Vijayashree J, Sultana HP. Heart disease classification using hybridized ruzzo-tompa memetic based deep trained neocognitron neural network. Health and Technology. 2020; 10(1):207-16.
[9] Sharma S, Parmar M. Heart diseases prediction using deep learning neural network model. International Journal of Innovative Technology and Exploring Engineering. 2020; 9(3): 2244-8.
[10] Rath SK. Kernel classifier for heart disease data classification. International Journal of Information Technology. 2020; 6(4):57-63.
[11] Munirathinam T, Ganapathy S, Kannan A. Cloud and IoT based privacy preserved e-healthcare system using secured storage algorithm and deep learning. Journal of Intelligent & Fuzzy Systems. 2020; 39(3):3011-23.
[12] Tomov NS, Tomov S. On deep neural networks for detecting heart disease. arXiv preprint arXiv:1808.07168. 2018.
[13] Kumari KA, Sadasivam GS. An efficient 3D diffie-hellman based two-server password-only authenticated key exchange. Journal of Applied Research and Technology. 2018; 16(1):9-21.
[14] Santamaria-granados L, Munoz-organero M, Ramirez-gonzalez G, Abdulhay E, Arunkumar NJ. Using deep convolutional neural network for emotion detection on a physiological signals dataset. IEEE Access. 2018; 7:57-67.
[15] Khan MA. An IoT framework for heart disease prediction based on MDCNN classifier. IEEE Access. 2020; 8:34717-27.
[16] Li J, Kuang X, Lin S, Ma X, Tang Y. Privacy preservation for machine learning training and classification based on homomorphic encryption schemes. Information Sciences. 2020; 526:166-79.
[17] Almajed HN, Almogren AS. SE-ENC: a secure and efficient encoding scheme using elliptic curve cryptography. IEEE Access. 2019; 7:175865-78.
[18] Baloglu UB, Talo M, Yildirim O, San TR, Acharya UR. Classification of myocardial infarction with multi-lead ECG signals and deep CNN. Pattern Recognition Letters. 2019; 122:23-30.
[19] Pan Y, Fu M, Cheng B, Tao X, Guo J. Enhanced deep learning assisted convolutional neural network for heart disease prediction on the internet of medical things platform. IEEE Access. 2020; 8:189503-12.
[20] Mohan S, Thirumalai C, Srivastava G. Effective heart disease prediction using hybrid machine learning techniques. IEEE Access. 2019; 7:81542-54.
[21] Haq AU, Li JP, Memon MH, Nazir S, Sun R. A hybrid intelligent system framework for the prediction of

heart disease using machine learning algorithms. Mobile Information Systems. 2018.
[22] Saxena K, Sharma R. Efficient heart disease prediction system. Procedia Computer Science. 2016; 85:962-9.
[23] Dutta A, Batabyal T, Basu M, Acton ST. An efficient convolutional neural network for coronary heart disease prediction. Expert Systems with Applications. 2020.
[24] Ambekar S, Phalnikar R. Disease risk prediction by using convolutional neural network. In fourth international conference on computing communication control and automation 2018 (pp. 1-5). IEEE.
[25] Shah D, Patel S, Bharti SK. Heart disease prediction using machine learning techniques. SN Computer Science. 2020; 1(6):1-6.
[26] Fitriyani NL, Syafrudin M, Alfian G, Rhee J. HDPM: an effective heart disease prediction model for a clinical decision support system. IEEE Access. 2020; 8:133034-50.
[27] Khan MA, Abbas S, Atta A, Ditta A, Alquhayz H, Khan MF, et al. Intelligent cloud based heart disease prediction system empowered with supervised machine learning. CMC-Computers Materials & Continua. 2020; 65(1):139-51.
[28] Gárate-escamila AK, El HAH, Andrès E. Classification models for heart disease prediction using feature selection and PCA. Informatics in Medicine Unlocked. 2020.
[29] Tirthani N, Ganesan R. Data security in cloud architecture based on diffie hellman and elliptical curve cryptography. IACR Cryptography ePrint Archive. 2014.
[30] Kim T, Lee MK. Efficient and secure implementation of NTRUEncrypt using signed sliding window method. IEEE Access. 2020; 8:126591-605.
[31] Khamparia A, Gupta D, Nguyen NG, Khanna A, Pandey B, Tiwari P. Sound classification using convolutional neural network and tensor deep stacking network. IEEE Access. 2019; 7:7717-27.
[32] https://www.kaggle.com/ronitf/heart-disease-uci. Accessed 24 August 2021.
[33] Subramanian EK, Tamilselvan L. Elliptic curve diffie–hellman cryptosystem in big data cloud security. Cluster Computing. 2020:3057-67.
[34] Li JP, Haq AU, Din SU, Khan J, Khan A, Saboor A. Heart disease identification method using machine learning classification in e-healthcare. IEEE Access. 2020; 8:107562-82.
[35] Kalyani G, Chaudhari S. An efficient approach for enhancing security in internet of things using the optimum authentication key. International Journal of Computers and Applications. 2020; 42(3):306-14.
[36] Qi Z, Zhang Z. A hybrid cost-sensitive ensemble for heart disease prediction. BMC Medical Informatics and Decision Making. 2021; 21:1-18.
[37] Reddy GT, Reddy MP, Lakshmanna K, Rajput DS, Kaluri R, Srivastava G. Hybrid genetic algorithm and a fuzzy logic classifier for heart disease diagnosis. Evolutionary Intelligence. 2020; 13(2):185-96.
[38] Begum BR, Chitra P. ECC-CRT: an elliptical curve cryptographic encryption and Chinese remainder theorem based deduplication in cloud. Wireless Personal Communications. 2021; 116(3):1683-702.
[39] Wang C, Wang A, Xu J, Wang Q, Zhou F. Outsourced privacy-preserving decision tree classification service over encrypted data. Journal of Information Security and Applications. 2020.

J. Vimal Rosy has completed her Masters in Computer Science, Masters in Philosophy Computer Science, and is currently pursuing her Ph.D in Computer Science in the Field of Cloud Computing. She currently serves as a Head & Assistant Professor in the Department of Computer Science, Soka Ikeda College of Arts and Science for Women, Chennai, Tamil Nadu, India.
Email: vimalrosy07@gmail.com

Dr. S. Britto Ramesh Kumar is an Assistant Professor of Computer Science at St. Joseph's College (Autonomous), Tiruchirappalli. His research interests include software architecture, wireless and mobile technologies, information security and Web Services. He has published many journal articles and book chapters on the topics of Mobile payment and Data structure and algorithms. His work has been published in the International journals and conference proceedings, like JNIT, IJIPM, IEEE, ACM, Springer and Journal of Algorithms and Computational Technology, UK. He was awarded as the best researcher in the year 2008 in Bishop Heber College, Tiruchirappalli. He has completed a minor research project. He has visited countries like China, South Korea and Singapore.
Email: brittork@gmail.com

Appendix I

S. No.	Abbreviation	Description
1	AES	Advanced Encryption Standard
2	AGAFL	Adaptive Genetic Algorithm with Fuzzy Logic
3	AMIGOS	A dataset for Mood, personality and affect research on Individuals and GrOupS
4	ANN	Artificial Neural Network
5	AUC	Area Under Curve
6	CAD	Computer Aided Design
7	CCA	Chosen-Ciphertext Attack
8	CNN	Convolutional Neural Networks
9	CPA	Chosen-Plaintext Attack
10	DCNN	Deep Convolutional Neural Network
11	DLP	Data Loss Prevention
12	DNN	Deep Neural Networks
13	DT	Decision Tree
14	ECC	Elliptic Curve Cryptography
15	ECC-CRT	Elliptical Curve Cryptography with Chinese Remainder Theorem

16	ECD	Elliptic Curve Diffie-Hellman
17	ECG	Electrocardiogram
18	ECDH	Elliptic Curve with Diffie–Hellman
19	ECDHC	Elliptic Curve Diffie–Hellman Cryptosystem
20	ECG	Electrocardiogram
21	EDCNN	Enhanced Deep Learning Assisted Convolutional Neural Network
22	EEC	Encryption based Elliptical Curve
23	EECDH	Enhanced Elliptic Curve Diffie - Hellman
24	E	Effective Performance
25	ELM	Extreme Learning Machine
26	FCN	Fully Connected Network
27	GSR	Galvanic Skin Response
28	HE	Homomorphic Encryption
29	HEARO-5	Heart Evaluation for Algorithmic Risk-reduction and Optimization Five
30	HRR	High Heart Rate
31	IND – CCA	INDistinguishable under Chosen Cipher text Attack
32	IND – CPA	INDistinguishable Under Chosen Plain Text Attack
33	KNN	K-Nearest Neighbour
34	LPP+RBFL	LPP with Rule-Based Fuzzy Classifier
35	LR	Logistic Regression
36	LVH	Left Ventricular Hypertrophy
37	MC	Misclassification Cost
38	MCC	Matthews Correlation Coefficient
39	MDC	Medical Data Classification
40	MDCNN	Modified Deep Convolutional Neural Network
41	MI	Myocardial Infarction
42	MRSA	Methicillin-Resistant Staphylococcus Aureus
43	MRSAC	MRSA-Colonized
44	NB	Navies Bays
45	OEECDH	Optimized Encryption Based Elliptical Curve Diffie-Hellman
46	OHE	Optimal Homomorphic Encryption
47	OKSVM	Optimal Kernel SVM
48	RBF	Radial basis Function
49	RBP	Resting Blood Pressure
50	ReLU	Rectified Linear Unit
51	RF	Random Forest
52	RS+FL	Rough Set with Fuzzy Logic
53	RSA	Rivest, Shamir, Adleman
54	SMO	Sequential Minimal Optimization
55	SNR	Signal-to-Noise Ratio
56	SVM	Support Vector Machine
57	UCI	University of California Irvine
58	UPRE	Unidirectional Proxy Re-Encryption