Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.030098
Article

Tech Science Press

An Intelligent Cardiovascular Diseases Prediction System Focused on Privacy

Manjur Kolhar* **and Mohammed Misfer**

Department of Computer Science, College of Arts and Science, Prince Sattam Bin Abdulaziz University 11990, Saudi Arabia
*Corresponding Author: Manjur Kolhar. Email: m.kolhar@psau.edu.sa
Received: 18 March 2022; Accepted: 09 June 2022

Abstract: Machine learning (ML) and cloud computing have now evolved to the point where they are able to be used effectively. Further improvement, however, is required when both of these technologies are combined to reap maximum benefits. A way of improving the system is by enabling healthcare workers to select appropriate machine learning algorithms for prediction and, secondly, by preserving the privacy of patient data so that it cannot be misused. The purpose of this paper is to combine these promising technologies to maintain the privacy of patient data during the disease prediction process. Treatment of heart failure may be improved and expedited with this framework. We used the following machine learning algorithms to make predictions: Logistic Regression (LR), Naive Bayes (NB), K-Nearest Neighbors (KNN), Decision Tree (DT) and Support Vector Machines (SVM). These techniques, combined with cloud computing services, improved the process of deciding whether to treat a patient with cardiac disease. Using our classifiers, we classified cardiac patients according to their features, which are grouped into single features, combinations of selected features, and all features. In experiments using all clinical features, machine learning classifiers SVM, DT, and KNN outperformed the rest, whereas in experiments using minimal clinical features, SVM and KNN were the most accurate. Internet of Things (IoT) devices allow family physicians to share diagnostic reports on the cloud in a secure manner. Ring signatures are particularly useful for verifying the integrity of data exchange. Our system keeps the physician's identity confidential from all authorized users, who can still access medical reports publicly. Our proposed mechanism has been shown to be both effective and efficient when it comes to obtaining patient reports from cloud storage.

Keywords: IoT; cloud computing; edge computing; cryptography; privacy

1 Introduction

Patients' privacy is at risk when using cloud storage services offered by third parties. Therefore, cryptographic data sharing is a good solution to privacy concerns [1–4]. Additionally, all research papers on health-based prediction systems to date do not address the security and privacy concerns fully. Keeping patient information private is always crucial to making accurate predictions. Nevertheless, medical reports or data can be shared geographically. As a result, medical data should be accessible from

multiple sources and have privacy protections. The use of machine learning algorithms for healthcare prediction has great promise, especially for cardiovascular patients, if they are combined with devices such as computerized tomography (CT) scans, an electrocardiogram (ECG) monitors, and Internet of Things (IoT) handheld devices.

In patients with Myocardial Infarction (MI), the continuous monitoring of Heart Rate (HR) is of utmost importance due to the risk of sudden cardiac arrest, which occurs following MI. Our proposed framework can not only process raw HR data streams on the app, but it can also share raw HR data to the cloud for optimization through machine learning modules. As a result of this approach, it has achieved low latency response time, and it does not require a large amount of data transmission. Additionally, the machine learning module provides feedback on how the machine learning process performed to the user, stores that feedback and shares it on the cloud. As a result of this strategy, we have been able to provide ML computing power in the cloud by utilizing feedback from all HR nodes at the edge. We also enable elasticity on the cloud storage capabilities in addition to local data caching by allowing users to choose whether to store HR raw data or aggregated HR data on the edge node, particularly the smart phone application that stays connected to the watch at all times. Through the use of data virtualization, it is possible to access data at the edge nodes on demand. With the addition of mesh and Ad-hoc networking to existing data virtualization, the amount of network traffic into the cloud can be reduced even further. Consequently, we have developed a machine learning-based system for predicting Cardiovascular Diseases using cloud computing architecture. Through homomorphic cryptographic algorithms, cloud data transactions are secured. Using homomorphic encryption, this paper presents an algorithm for securing machine learning. The PBC library, which utilizes multiplicative cyclic groups of primes, safeguards the model training under the best optimized hyper parameters. During the member inference attack, ML models were trained on plaintext gradients, putting others' data at risk. Thus, homomorphic encryption can be used to perform calculations on encrypted data without decryption. In addition, the homomorphic operation after decryption is equivalent to the operation on plaintext data. As part of the framework, we proposed a multi-party privacy protected machine learning framework that combines homomorphic encrypting and machine learning tools to ensure the confidentiality of data and model security in consultations.

Following is an outline of the remainder of the paper. Section two describes the proposed sections, whereas section three describes how the proposed framework for predicting cardio-vascular disease will be implemented using a homomorphic authentication scheme to ensure privacy. Experimental observations and analyses of the data are presented in the third section. Finally, conclusions are drawn and suggestions for further research are made.

2 Literature Review

ML algorithms provide complex rules and reduce the need to develop and test the system from scratch in addition to reading and predicting data directly from IoT sensors, such as biosensors [5]. A further problem with ML algorithms is the noise present in the datasets. Datasets are also not collected under real-world clinical conditions. Numerous papers [6–11] have suggested using AI-based applications to detect cardio vascular disease. One such system assessed heart conditions using a hybrid recommendation engine, wireless Sensors collected cardiovascular data, which was used to generate personalized medical reports. The authors of [11] have demonstrated that machine-learning algorithms are capable of forecasting cardiovascular disease cases correctly. Through extensive research and development in cardiovascular prediction systems, deep learning is a major factor. Furthermore, deep learning has not yet fully been incorporated into imaging due to file format issues [11]. A distributed computing technology known as edge computing, aka fog computing, is based on multiple IoT that are linked to a cloud. The amount of

data generated by IoT devices is likely to remain high for a long time. As opposed to sending this data to cloud storage for processing, IoT devices would instead be processing this data using edge devices in order to reduce the load on the cloud architecture as well as bandwidth requirements. Due to this, increasing the proximity of storage and computing system architectures to IoT and other networking components, such as software defined networks, that are required for processing is easier and shorter processing latency can be achieved. The implementation of these aforementioned methods has already begun in a few countries, like Canada, for predicting mortality in heart failure patients [12]. In a study conducted in the United States, the authors of reference [13] used neural networks to predict cardiovascular events. As a result of the findings in [14], the authors concluded that the use of artificial intelligence for the prediction of coronary heart disease is superior to coronary calcium measurements and clinical risk assessments. In the vast majority of countries of the world, machine learning is a powerful tool for predicting diseases such as cardiovascular disease on an enormous scale. Even though technology has improved greatly in recent years, there is no technology framework which is adequate for the prediction of patients with heart disease. Our paper presents a three layer architecture for the development of a cardiovascular system that preserves privacy of patient data while ensuring accuracy and efficiency.

The first step in our study was to select ML algorithms to predict cardiovascular diseases. Additionally, the algorithms can be implemented on any platform with minimal requirements for hardware. According to their respective hyper-parameters, the aforementioned machine learning models have been trained to yield the most accurate results under privacy protection. ML algorithms have the following advantages, based on which we selected them as the primary algorithm in our methodology:

- With the suggested algorithms, there is a strong margin of separation between the datasets.
- High-dimensional spaces are best suited for them.
- The decision function uses only a subset of the training dataset, so they are memory-efficient.

3 Proposed Framework

The figure in Fig. 1 illustrates the proposed smart health care framework for cardiac patients. There are four main modules that make up the framework: smart watch, edge application and cache manager, fog data analysis layer, and intelligence system. There are also smart watches with both Android and iOS operating systems on board. Our study presents a framework for the detection of heart rate which can be used for smart watches that can be worn like wrist watches and can be connected to the internet. An edge application and cache manager (EACM) detects the heart rate sensor on the smart watch and sends it to the edge application. EACM is composed of an edge layer module called application and cache manager. This module allows a single-sided caching of heart rate measurements. In addition to the cloud layer, other layers, such as the fog layer and the intelligence system, are built with high storage and processing power to allow better data analysis and management for better results.

There can be grave consequences resulting from an abnormal variation in HR [15,16]. In our smart cardio watch, we have tightly containerized all models for each example of real-time data so they can be encapsulated in their own data container [17,18], allowing real-time data to be updated from the client devices as required. Due to this, the Machine Learning modules had to be rebuilt every time the watch received data from the container. Alternately, you can find commercial solutions that can take care of your edge node deployment without requiring additional storage resources [19,20]. Moreover, healthcare applications, namely the monitoring of edge nodes, are not directly connected to the storage containers, which means that unprocessed data will have to be processed by third parties. EACM manages locally built applications, but it can also manage data from IoT sensors. The HR data is stored directly in the cloud, so that it can be analyzed and predicted later on.

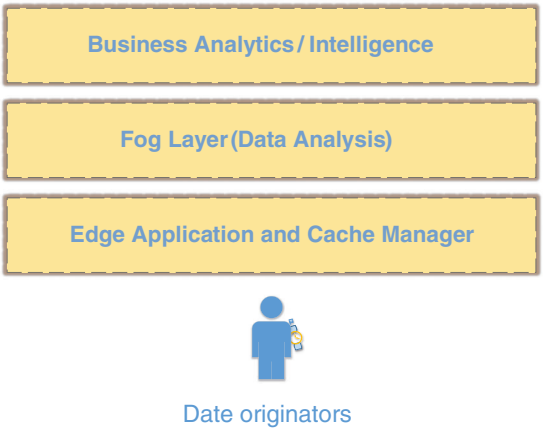

Figure 1: Proposed cardiac care system using heart rate, consists of smart watch, edge computing application and business layers for decision making

As part of our proposed framework, the fog layer is one of the most important layers, due to its close relationship to the data originators. A framework such as this is a public resource that is available at a relatively high level of information. This can be done by pushing data to the upper layer, and then the upper layer data can be analyzed locally at the edge. Data from the smartwatch is pushed to the fog layer which responds to events as they occur to allow health care workers to make decisions or monitor for emergency cases by using real-time heart beat data. As a result of this setup, the transfer of data between a smart watch and a storage place where it needs to go becomes more seamless and convenient. Furthermore, it also has two more software and hardware modules, which are called software defined networks and self-organizing modules. Our proposed frame reaps the benefits of these two services with the deployment of machine learning modules. Whenever real-time data is received, these modules keep the record for further processing. In addition to the performance of all resources within the fog layer and pushes the data to other layers for decision-making data to be used by other layers. Communication, routing, traffic type, status of the communication channel, and storage-related issues are solely network-based issues. It also plays a crucial role in selecting ML modules and parameters based on the inputs of healthcare workers [21]. The dataflow diagram is shown in Fig. 2. The dataflow diagram is divided into three layers: edge, fog, and intelligence.

In our present case, the data originator is the patient with cardio vascular agent who pushes data to the edge layer and the edge layer sends data notify requests to higher intelligence layers through the fog layer in order to initiate communication channels so that these data will be available for subsequent reference. During this initial communication, the authentication process will be conducted between the intelligence layer and the fog layer. After the authentication process has been successfully completed, the next course of action will be to execute it. By means of the fog layer, the HR raw data is processed and sent to the intelligence layer for further processing. Through the intelligence layer, the most complex analysis and interpretation of the proposed system can be carried out. With the use of the intelligence layer, the distribution of work can be managed on the basis of the preferred machine learning algorithm. In order to process the real-time data for the purpose of pre-prediction, this preference can only be set by the health care workers. Once the result is obtained by the intelligence layer, then the result is passed along to the health care system for prescription or any other appropriate action that can be taken. Once the health care system issues the prescription, then the prescription reaches the patient so that the next step can be taken. It seems that its principal concern is that if a patient requires urgent medical attention, then the health care provider should take all necessary steps to ensure that the patient is brought to the hospital as early as possible. In

addition, the intelligence layer is built with a multilevel scheduling algorithm to be able to offer HR data in real-time. Additionally, it carries secured tunneled data transmission between the fog and edge layers. In Fig. 3, you can see the block diagram of the ML dynamic settings, which is very important when selecting ML modules. Through edge and fog layers, real-time HR data is fed into the intelligence layer's storage containers. The data is divided into three dimensions that are equal in size. For the experiments, training and testing are performed using a specific patient. Data can be directly fed into ML modules to produce predictions based on real-time data. We have only used different set classifiers, such as LR, NB, KNN, DT and SVM. A deep learning algorithm has also been used for the comparison.

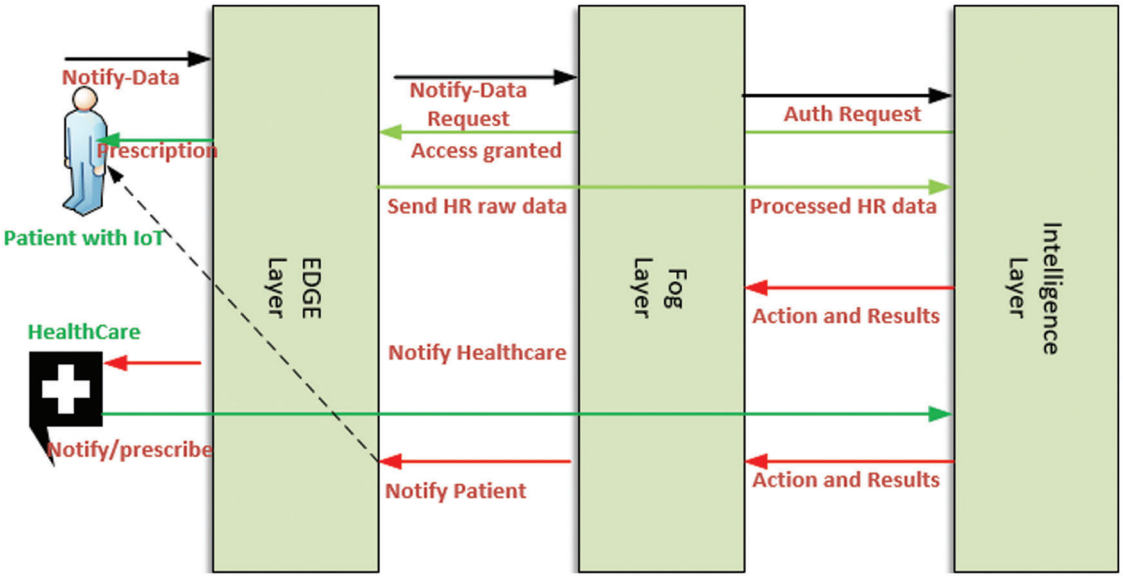

Figure 2: Dataflow diagram between various entities of the proposed framework

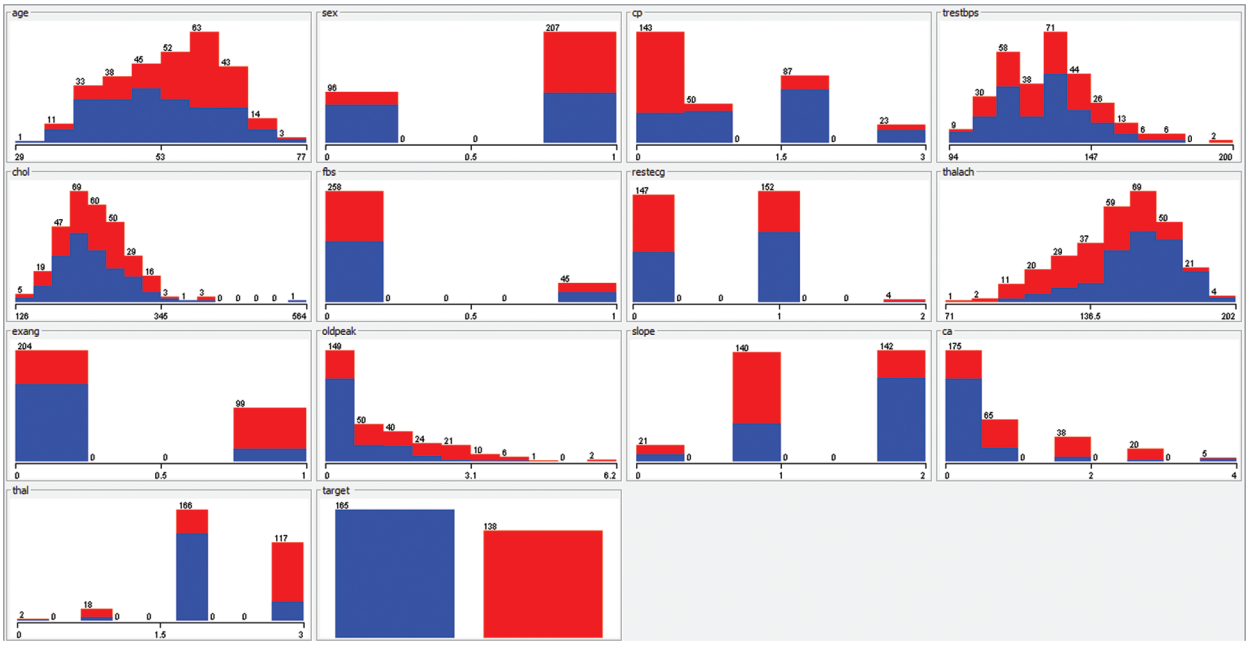

Figure 3: The various attributes of dataset UCI

3.1 Privacy Preservation

To keep sensitive patient data private, we have used an efficient method called homomorphic message authentication code (MACs) along with a group signature called elliptic curves [22,23]. In light of the fact that patient data is shared with many healthcare workers, maintaining the identity anonymity of patient data during prescription process is appreciated. As the main consultant, he or she is considered to be the owner of the patient data and the keeper of data integrity. They can keep the identities of other consultants who can sign if needed. In addition, we have achieved the privacy of patient data by imposing the data masking technique in conjunction with short signatures and homomorphic MAC. Using this technique, we were able to create constant-sized public secret keys that reduced the amount of communications and computation required [24,25]. Margins: set to 1.0" (2.54 cm) (top, bottom, left, and right). We have used pairing-based cryptography libraries to ensure that all transactions between consultants are private. To accomplish privacy preservation [26], we have used three cyclic group [27] namely $G_1, G_2,$ *and* G_T of order of the group r, we have also used bilinear map e which produces an element of G_T using G_1 *and* G_2. The framework allows the main consultant to publish transfer patients report along with the system parameter g which is a random element of G_2. When the main consultant wishes to invite other consultant for the purpose of prescription then the consultant should generate public and private keys. The private key of the main consultant is a random element x of Z_r, and public key is g^x [28]. T invite the other consultant, the main consultant hashes the invitation the message to some number h of G_1, the gives back h^x. Additionally, this invitation can be verified by the other consultant. To verify the signature σ, the invited consultant can check that using Eq. (1).

$$e(h, g^x) = e(\sigma, g) \tag{1}$$

Furthermore, to get computable isomorphism we have utilized the following equation.

$$\psi(g_2) = g_1$$

whereas g_1 *and* g_2 is generated from G_1 *and* G_2 respectively. The bilinear map can be had from

$e: G_1 X\ G_2 \rightarrow G_T$ By computability map e, the two mostly used properties such as Bilinearity and non-degeneracy:

Bilinearity: $u \in G_1$ and $v \in G_2$ and $m, n \in Z_P$, $(u^m, v^n) = e(u, v)^{mn}$

Non-degeneracy: $e(g_1, g_2)$.

GenKey, SignRing, and VerifySign are three signature types supported by public hashing along with ring signatures. For example, a family doctor or main consultant wishes to consult another specialist doctor, so he initializes the GenKey algorithm and produces private and public keys as follows.

GenKey Steps

Step 1:- Generate a random variable.

$$x\ R \rightarrow Z_p \tag{2}$$

Step 2:- Generate Public Key

$$v \leftarrow g_2^x \tag{3}$$

Step 3:- Generate secrete Key

$$x \leftarrow Z_p \tag{4}$$

Sign Steps

According to the Eq. (1), the consultant uses a public key generated in step 2 to begin the process of securely transferring patient reports.

$$v_1, v_2, v_3, \ldots, v_n \in G_2 \tag{5}$$

Step 4:- Public and Secrete keys of the all the consultant who are currently working on patient report (message) $m \in Z_R$ v_i and x_i respectively.

Step 5:- The main consultant chooses a random variable a_i and computes the following Eq. (6).

$$\alpha \leftarrow H(m)g_1^m \in G_1 \tag{6}$$

$$m_i * m_i * m_i, \ldots m_n = m$$

Whereas ***m*** is the report which is generated from the different

Step 6:- Calculate the following Eq. (7), to form ring signature.

$$\sigma_s = \left(\alpha/\psi\left(\prod_{i\neq s} v_i^{a_i}\right)\right) \tag{7}$$

VerifySign

In this process, verification of message by the receiver can be had by using the public keys generated during Eq. (5), the patient report $m \in Z_R$ v_i and the ring signature σ_s from the Eq. (7). Therefore, the patient report can be had by the following Eq. (8).

$$\prod_{i=0}^{n} e(\sigma_i, v_i) \tag{8}$$

3.2 Security Analysis

As we discussed in the previous section, we will now discuss the properties of privacy in the context of computational infeasibility of the untrusted cloud share and how to post an invalid message or medical report to pass the verification phase of the cloud server.

Proof

Since the co-computational Diffie-Hellman assumption (co-CDH) holds then G1, G2, and GT are hard [29], it is computationally infeasible to verify and compute on invalid message blocks [30]. Game 1: Main consultant generates the proof for the message or medical report should you Eq. (7) with the parameters $\{\alpha, \psi, id, v_i\}$. The untrusted entity generated wrong message or medical report $\{\alpha, \psi^I, id, v_i\}$, when there is change in ψ^I for all the values less than 1. If this message is verified with cloud server then untrusted entity wins game. To prove this untrusted transaction to crack the message then it means that this contradicts the Discrete Logarithm assumption, which is believed to be intractable. According to Eq. (7), for the all the elements such as *g and h* which belongs to G_1 and there also exist $x \epsilon Z_p$, we can also conclude that $g = h^x$ because G_1 is cyclic group, Hence, Eq. (7) is computable by the untrusted entity, but it is clear that DPL problem is hard under G_1.

4 Result and Discussion

The aforementioned algorithms are set up in Tab. 1 according to their environment. The hyper parameters play a very important role in controlling the overall performance of a machine learning model. The ultimate goal was to find an optimal combination of hyper parameters that diminishes a predefined loss function in order to get better results. Our analysis is based on the UCI ML Repository Heart

Disease Dataset. Dataset contains more than five most important attributes, namely sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal. According to Fig. 2, all of these features are of heart related parameters, these parameters are dependent on each other and in some cases, and all are independent from each other. In fact, most of the study shows they are highly dependent on each other and provide insight into cardiovascular disease. The proposed system utilizes a special file format for the dataset. For feeding into any of the ML models, each of these features is not resized or skewed in any way. The aforementioned algorithm used five ML classifiers in addition to deep learning ML. In order to classify the dataset, the SVM, DT, KNN, NB, and deep learning classifiers are applied. The SVM classifier was implemented because of its ability to find intricate relationships within a given dataset without the need for time-consuming and challenging transformations. Furthermore, deep learning has the proven ability high rated accurate classification. Additionally, these algorithms consume longer computational CPU time when measured with NB and DT, which consumes less CPU time and has the ability to provide acceptable performance. As shown in Fig. 3, the proposed method was evaluated for accuracy, precision, and the F-measure using the aforementioned techniques for all attributes.

Table 1: Parameters settings to yield best results

Classifiers	Parameters
LR	Class for building and using a multinomial logistic regression model with a ridge estimator. Parameters:seed, dontReplaceMissing, dontNormalize, Epochs, lambda, numDecimalPlaces, batchSize Debug, lossFunction learningRate, doNotCheckCapabilities and epsilon.
NB	Class for a Naive Bayes classifier using estimator classes. Numeric estimator precision values are chosen based on analysis of the training data, useKernelEstimator, numDecimalPlaces, batchSize, displayModelInOldFormat, doNotCheckCapabilities), useSupervisedDiscretization
KNN	K-nearest neighbours classifier. Can select appropriate value of K based on cross-validation. numDecimalPlaces, batchSize, KNN, distanceWeighting, nearestNeighbourSearchAlgorithm, windowSize, doNotCheckCapabilities, meanSquared, crossValidate
DT	Class for generating a pruned or unpruned C4.5 decision tree. Seed, unpruned, confidenceFactor, numFolds, numDecimalPlaces, reducedErrorPruning useLaplace, doNotMakeSplitPointActualValue, subtreeRaising binarySplits doNotCheckCapabilities, minNumObj, useMDLcorrection collapseTree
SVM	Implements stochastic gradient descent for learning various linear models (binary class SVM, binary class logistic regression, squared loss. buildCalibrationModels numFolds, randomSeed, c – The complexity parameter C. numDecimalPlaces, kernel – The kernel to use., checksTurnedOff, filterTypetolerance Parameter, calibrator, doNotCheckCapabilities, epsilon

The accuracy is the ratio of true values to the total observations, expressed as a percentage. The proposed system can only be accepted if accuracy is high, otherwise it rejects. F is the weighted average of P (precision) and R (recall); P is the number of correctly predicted attributes and R is the number of positive values or predictions from the dataset. A confusion matrix is a two by two matrix containing four outcomes as a result of a binary classifier. We have used five data mining techniques, Tabs. 2–4 show the results of these techniques, and all the attributes were fed to the framework in a batch wise so

as to maintain experimental settings. Following Tabs. 2–4, show the accuracy, precision and F-measure of all attributes, respectively.

Table 2: F-measure with respect to all the features of the dataset

Classifiers	F-measures	Features
SVM	0.933	sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal
LR	0.821	sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal
KNN	0.866	sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal
NB	0.827	sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal
DT	0.895	sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal

Table 3: Recall with respect to all the features of the dataset

Classifiers	Recall	Features
SVM	0.935	sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal
LR	0.822	sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal
KNN	0.862	sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal
NB	0.828	sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal
DT	0.875	sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal

Table 4: Precision with respect to all the features of the dataset

Classifiers	Precision	Features
SVM	0.941	sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal
LR	0.823	sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal
KNN	0.861	sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal
NB	0.830	sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal
DT	0.865	sex, cp, fbs, restecg, exang, oldpeak, slope, ca, and thal

Tabs. 2–4 show that only the SVM classifier achieved the highest F-measure, Recall and precision, however, NB was the second most successful classifier in all performance matrices. KNN and decision trees were able to achieve much less proficiency than SVM and LR classifiers. These results used all features from the dataset, and these features are considered to be more significant in detecting cardiovascular illnesses. We also used minimum features to obtain results, and there were recommended and most important while detecting cardiovascular disease. In contrast, we chose minimum features since smart cardio watches or any other IoT devices could provide very basic information about cardio vascular events. Therefore, we have considered risk factors for patients with physical inactivity, age, male sex, heart rate, and lipid levels. In Tabs. 5–7, we demonstrate how our framework identifies cardiovascular risk based on minimal feature selection. In these Tabs. 5–7, we learn that SVM, LR, and NB have predicted the cardio vascular issues and have performed better than the rest of the machine learning classifiers.

Table 5: F-measure with minimal features of the dataset

Classifiers	F-measures	Features
SVM	0.908	sex, cp, fbs, exang, ca, and thal
LR	0.794	sex, cp, fbs, exang, ca, and thal
KNN	0.864	sex, cp, fbs, exang, ca, and thal
NB	0.812	sex, cp, fbs, exang, ca, and thal
DT	0.834	sex, cp, fbs, exang, ca, and thal

Table 6: Recall with minimal features of the dataset

Classifiers	Recall	Features
SVM	0.913	sex, cp, fbs, exang, ca, and thal
LR	0.812	sex, cp, fbs, exang, ca, and thal
KNN	0.864	sex, cp, fbs, exang, ca, and thal
NB	0.812	sex, cp, fbs, exang, ca, and thal
DT	0.867	sex, cp, fbs, exang, ca, and thal

Table 7: Recall with minimal features of the dataset

Classifiers	Precision	Features
SVM	0.910	sex, cp, fbs, exang, ca, and thal
LR	0.809	sex, cp, fbs, exang, ca, and thal
KNN	0.862	sex, cp, fbs, exang, ca, and thal
NB	0.809	sex, cp, fbs, exang, ca, and thal
DT	0.844	sex, cp, fbs, exang, ca, and thal

Experimental results revealed that the SVM machine learning classifier outperformed all the other ML classifiers using 10-fold CV fairly well. The F-measure was 84%, recall was 93%, and precision was 94.92% with SVM. In the case of the KNN ML classifier, a large number of experiments were conducted with various K values. Consequently, KNN has produced its best performance at k = 7 and has a best accuracy of 86.55%, 86.93% precision, and 86.17% recall. Accordingly, the F-measure of DT ML is 89.82%, recall is 87.73%, and precision is 86.76%. In terms of precision, recall, and F-measure, the SVM Classifier outperformed all other ML algorithms. When compared to other classifiers, NB has the lowest performance. A ROC curve for the SVM algorithms is shown in Fig. 4. The healthcare system has been unable to predict which patients are at risk of developing cardiovascular disease in the future, and prevent that from happening. Presently, healthcare workers can perform a number of tests that can provide clues about patients who are already developing heart diseases years before they show symptoms. The use of these ML classifiers along with sophisticated medical equipment such as a CT scan can help healthcare workers to diagnose a patient's risk factors such as high blood pressure, lipid profile and other conditions before they become extremely high.

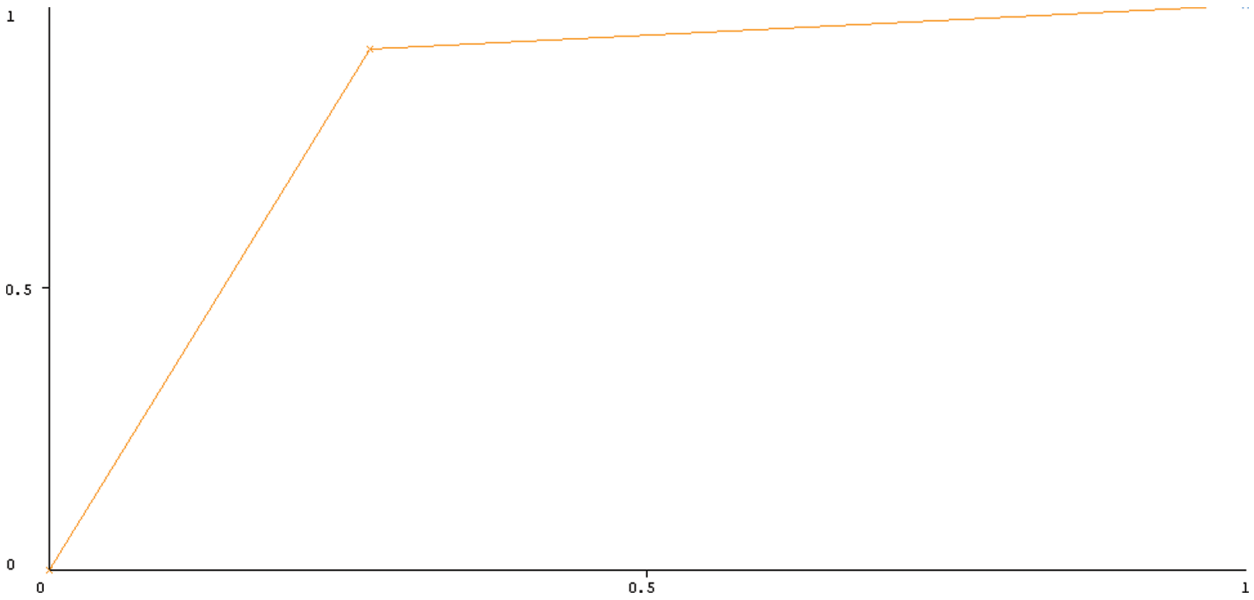

Figure 4: ROC curves of all SVM on full feature using 10-fold cross-validation

Our proposed privacy framework includes addition, product of elliptic curves, exponentiation, which is repeated multiplication of the elliptic curves, hashing, and pairing operations. Because they are easy to operate and won't load the CPU much, we don't evaluate additions in our evaluation process.

4.1 Communication Cost

Our proposed privacy framework includes addition, product of elliptic curves, exponentiation, which is repeated multiplication of the elliptic curves, hashing, and pairing operations. Because they are easy to operate and won't load the CPU much, we don't evaluate additions in our evaluation process.

As part of the cloud architecture privacy operation [31], the main consultant generates some random numbers to create encrypted messages. The random number generation operation requires little CPU power. On the other hand, the cloud server must prove that the messages are encrypted.

During auditing, the cloud server generates some random values to construct the auditing message, which introduces only a small computation cost. Then, after receiving the auditing message, the cloud server needs to compute a proof $\{\alpha, \psi, id, v_i\}$. According to the group homomorphism computation can be calculated as follows.

$$k_p = k_{11}p + k_{12}[\lambda_1] + k_{21}p + k_{22}[\lambda_2]p \tag{9}$$

where, k_p is multiple of a point or order n on an elliptic curve and the integers $k_{11}, k_{12,} k_{21}, and\ k_{22}$ are resolved by solving the vector problem in lattice. Hence the following equation is used to calculate the cloud server's privacy proof generation initiated by the main consultant.

$$k_{11}G_1 + k_{12}G_1 + k_{21}\ Z_r + k_{22}\ hash\ function \tag{10}$$

Cloud server uses the above Eq. (10) to calculate the correctness of the Eq. (8).

In Fig. 5, the privacy preservation graph, it is shown that data transfer within stipulated time is always possible if privacy preservation is applied. In the proposed system, the communication cost is brought on by very important processes such as file transmission and proof generation within health care workers. Each message sent between health care workers and patients contains $m \in Z_R\ v_i$, the cost of this

communication is message length of an element of Z_R and index length of the message. There each message cost will be consists of $\{\alpha, \psi, id, v_i\}$.

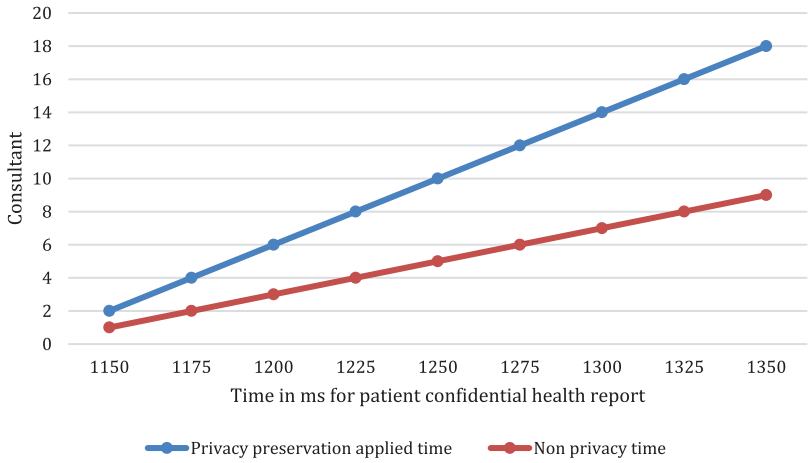

Figure 5: Application of ring privacy algorithm with and without privacy preservation time in ms

5 Conclusion

According to reports, heart disease is both life-threatening and prevalent both in developed and underdeveloped countries. To deal with such dreaded diseases successfully, one must seek treatment as soon as possible. A major challenge in this region of the kingdom is detecting the disease at an early stage and diagnosing the cardiovascular onset, which in turn will improve the cardiovascular outcomes, thereby reducing cardiovascular morbidity. Our paper proposes a three-layered, smart, connected health care system that preserves the privacy of patient medical data stored in the cloud. Our proposed framework was able to predict heart disease using machine learning algorithms. In order to predict the risk of heart disease, we utilized two datasets from the UCI heart disease database. The purpose of this paper is to develop two test cases, namely full feature and minimal feature, using the same dataset to train and evaluate classifiers. In the future, other forms of machine learning classifiers will be investigated, such as Boltzmann machines and Convolutional Neural Networks. Furthermore, we have raised concerns about the security of patient data when transmitted over untrusted cloud services. In published clinical trials, machine learning has not been compared with laboratory reports or datasets. In addition, the impact of machine learning algorithms on clinical practice can also be assessed in clinical laboratories where actual outcomes will be compared with predicted outcomes.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Kolhar, M. M. Abu-Alhaj and S. M. Abd El-atty, "Cloud data auditing techniques with a focus on privacy and security," *IEEE Security & Privacy*, vol. 15, no. 1, pp. 42–51, 2017.

[2] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei *et al.,* "Towards secure and privacy-preserving data sharing for covid-19 medical records: A blockchain-empowered approach," *IEEE Transactions on Network Science & Engineering*, vol. 9, no. 1, pp. 271–281, 2021.

[3] G. Kaissis, A. Ziller, J. Passerat-Palmbach, T. Ryffel, D. Usynin *et al.,* "End-to-end privacy preserving deep learning on multi-institutional medical imaging," *Nature Machine Intelligence*, vol. 3, no. 6, pp. 473–484, 2021.

[4] C. Zhang, C. Xu, K. Sharif and L. Zhu, "Privacy-preserving contact tracing in 5G-integrated and blockchain-based medical applications," *Computer Standards & Interfaces*, vol. 77, no. 103520, pp. 1, 2021.

[5] R. N. Kazi, M. Kolhar and F. Rizwan, "Smart cardiowatch system for patients with cardiovascular diseases who live alone," *CMC-Computers, Materials & Continua*, vol. 2, no. 66, pp. 1237–1250, 2021.

[6] S. F. Weng, J. Reps, J. Kai, J. M. Garibaldi and N. Qureshi, "Can machine-learning improve cardiovascular risk prediction using routine clinical data," *PLOS ONE*, vol. 12, no. 4, pp. 1–4, 2014.

[7] K. C. Siontis, P. A. Noseworthy, Z. I. Attia and P. A. Friedman, "Artificial intelligence-enhanced electrocardiography in cardiovascular disease management," *Nature Reviews Cardiology*, vol. 18, no. 7, pp. 465–478, 2021.

[8] A. Haleem, M. Javaid, R. P. Singh and R. Suman, "Applications of artificial intelligence (ai) for cardiology during covid-19 pandemic," *Sustainable Operations and Computers*, vol. 2, no. 1, pp. 71–78, 2021.

[9] S. Shu, J. Ren and J. Song, "Clinical application of machine learning-based artificial intelligence in the diagnosis prediction, and classification of cardiovascular diseases," *Circulation Journal*, vol. 85, no. 9, pp. 1416–1425, 2021.

[10] N. Kagiyama, S. Shrestha, P. D. Farjo and P. P. Sengupta, "Artificial intelligence: Practical primer for clinical research in cardiovascular disease," *Journal of the American Heart Association*, vol. 8, no. 17, pp. 1–12, 2019.

[11] X. Zhang, J. Zhou, W. Sun and S. K. Jha, "A lightweight cnn based on transfer learning for covid-19 diagnosis," *CMC-Computers, Materials & Continua*, vol. 72, no. 1, pp. 1123–1137, 2022.

[12] P. C. Austin, J. V. Tu, J. E. Ho, D. Levy and D. S. Lee, "Using methods from the data-mining and machine-learning literature for disease classification and prediction: a case study examining classification of heart failure subtypes," *Journal of Clinical Epidemiology*, vol. 66, no. 4, pp. 398–407, 2013.

[13] R. Narain, S. Saxena and A. K. Goyal, "Cardiovascular risk prediction: A comparative study of Framingham and quantum neural network based approach," *Patient Preference and Adherence*, vol. 10, no. 1, pp. 1259–1270, 2016.

[14] A. Kilic, "Artificial intelligence and machine learning in cardiovascular health care," *The Annals of Thoracic Surgery*, vol. 109, no. 5, pp. 1323–1329, 2020.

[15] M. Shiotani and K. Yamaguchi, "Research on an anomaly detection method for physical condition change of elderly people in care facilities," *Advanced Biomedical Engineering*, vol. 11, no. 1, pp. 10–15, 2022.

[16] H. K. Hammond and V. F. Froelicher, "Normal and abnormal heart rate responses to exercise," *Progress in Cardiovascular Diseases*, vol. 27, no. 4, pp. 271–296, 1985.

[17] J. Mellado and F. Núñez, "Design of an IoT-PLC: A containerized programmable logical controller for the industry 4. 0," *Journal of Industrial Information Integration*, vol. 25, no. 1, pp. 100–250, 2022.

[18] Y. Liu, S. Mousavi, Z. Pang, Z. Ni, M. Karlsson *et al.,* "Plant factory: A new playground of industrial communication and computing," *Sensors*, vol. 22, no. 1, pp. 7–14, 2022.

[19] C. Jian, L. Bao and M. Zhang, "A high-efficiency learning model for virtual machine placement in mobile edge computing," *Cluster Computing*, vol. 11, no. 17, pp. 1–16, 2022.

[20] X. Ren, S. Vashisht, G. S. Aujla and P. Zhang, "Drone-edge coalesce for energy-aware and sustainable service delivery for smart city applications," *Sustainable Cities and Society*, vol. 77, no. 1, pp. 1–15, 2022.

[21] H. Zhu, Y. Chen, T. Tang, G. Ma, J. Zhou *et al.,* "ISP-Net: Fusing features to predict ischemic stroke infarct core on ct perfusion maps," *Computer Methods and Programs in Biomedicine*, vol. 215, no. 1, pp. 1–15, 2022.

[22] M. Anastasova, R. Azarderakhsh and M. M. Kermani, "Fast strategies for the implementation of SIKE round 3 on ARM Cortex-M4," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 10, pp. 4129–4141, 2021.

[23] A. M. Hilal, J. S. Alzahrani, I. Abunadi, N. Nemri, F. N. Al-Wesabi *et al.,* "Intelligent deep learning model for privacy preserving iiot on 6g environment," *CMC-Computers, Materials & Continua*, vol. 72, no. 1, pp. 333–348, 2022.

[24] D. Boneh, B. Bünz and B. Fisch, "Batching techniques for accumulators with applications to IOPs and stateless blockchains," in *Proc. CRYTO*, Santa Barbara, USA, pp. 561–586, 2019.

[25] J. Kim and H. Oh, "FAS: Forward secure sequential aggregate signatures for secure logging," *Information Sciences*, vol. 47, no. 1, pp. 115–131, 2019.

[26] R. K. Ajeena and H. Kamarulhaili, "Analysis on the elliptic scalar multiplication using integer sub-decomposition method," *International Journal of Pure and Applied Mathematics*, vol. 87, no. 1, pp. 95–114, 2013.

[27] S. Azhar, N. A. Azam and U. Hayat, "Text encryption using pell sequence and elliptic curves with provable security," *CMC-Computers, Materials & Continua*, vol. 71, no. 3, pp. 4971–4988, 2022.

[28] J. Guo, J. Huang and J. Hou, "A scalable computing resources system for remote sensing big data processing using geopyspark based on spark on k8s," *Remote Sensing*, vol. 14, no. 3, pp. 5–21, 2022.

[29] R. K. Ajeena, "The soft graphic integer sub-decomposition method for elliptic scalar multiplication," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 6, pp. 1751–1765, 2021.

[30] C. Wang, S. Wang, X. Cheng, Y. He, K. Xiao *et al.,* "A privacy and efficiency-oriented data sharing mechanism for IoTs," *IEEE Transactions on Big Data*, vol. 99, no. 1, pp. 1–15, 2022.

[31] A. A. Aldujaili, M. Dauwed and A. Meri, "Wearable sensors and internet of things integration to track and monitor children students with chronic diseases using arduino uno," *Journal on Internet of Things*, vol. 3, no. 4, pp. 131–137, 2021.