Computer Systems Science & Engineering
DOI:10.32604/csse.2022.019976
Article

Tech Science Press

A Secure IoT-Cloud Based Healthcare System for Disease Classification Using Neural Network

M. Vedaraj* **and P. Ezhumalai**

Department of Computer Science and Engineering, R.M.D. Engineering College, Kavaraipettai, 601206, Tamilnadu, India
*Corresponding Author: M. Vedaraj. Email: vedaraj1983@gmail.com

Received: 04 May 2021; Accepted: 18 June 2021

Abstract: The integration of the Internet of Things (IoT) and cloud computing is the most popular growing technology in the IT world. IoT integrated cloud computing technology can be used in smart cities, health care, smart homes, environmental monitoring, etc. In recent days, IoT integrated cloud can be used in the health care system for remote patient care, emergency care, disease prediction, pharmacy management, etc. but, still, security of patient data and disease prediction accuracy is a major concern. Numerous machine learning approaches were used for effective early disease prediction. However, machine learning takes more time and less performance while classification. In this research work, the Attribute based Searchable Honey Encryption with Functional Neural Network (ABSHE-FNN) framework is proposed to analyze the disease and provide stronger security in IoT-cloud healthcare data. In this work, the Cardiovascular Disease and Pima Indians diabetes dataset are used for heart and diabetic disease classification. Initially, means-mode normalization removes the noise and normalizes the IoT data, which helps to enhance the quality of data. Rectified Linear Unit (RLU) was applied to adjust the feature weight to reduce the training cost and error classification. This proposed ABSHE-FNN technique provides better security and achieves 92.79% disease classification accuracy compared to existing techniques.

Keywords: Honey encryption; functional neural network; rectified linear unit; feature selection; classification

1 Introduction

The Internet of Things (IoT) is defined as a network of internet-linked physical devices that are interacting with each other over the internet. Cloud computing delivers various resources to users over the internet, such as software, networking, storage, etc. IoT integrated with cloud computing can increase performance capabilities and storage of resources to the fullest. Cloud computing is therefore used as a front-end for accessing the Internet of Things. The consumerization of the healthcare system has surged by developing and encouraging people to use connected devices such as smart phones, wearable, and hand-held devices to live life with comfort. IoT is the revolutionary innovation that bridges the challenges of interoperability to fundamentally change the way healthcare is provided, thereby driving improved results, increasing quality, and making healthcare accessible. The Internet of Things equips person-centered infrastructures to produce improved outcomes. The important IoT applications are detection of patient disease, detection of an earthquake, detection of smart home, and Smartphone. The important technologies used for IoT communication are WiFi, Bluetooth, RFID, Zigbee, etc. The health care system should be designed to handle an enormous amount of patient data. To handle enormous amounts of data, the cloud plays a prominent role in the healthcare system. Challenges are increasing due to increasing the usage of the health care system. IoT-Cloud-based health care systems have numerous advantages, such as efficient patient monitoring, improved management of patient data, easy to access patient data, cost-saving, etc. The IoT-cloud based health care system also faces a lot of issues like scalability, patient safety, privacy, and security [1].

Nowadays, the healthcare system uses many new advanced technologies to provide healthcare services to users. The important aspects of the healthcare system are confidentiality of patient data and accuracy of disease diagnosis. Patient information can be shared with multiple users in the hospital. Patient personal and disease diagnosis information must be protected from illegal access [2]. IoT system popularity has been promoting IoT technology development to include different scientific research and healthcare architectures. The IoT network enables the electronic medical system to share information related to the latest technology by linking devices, applications, and services. Continuous monitoring of patients and secure parent data transmission is an important aspect of the healthcare system which improves the performance of the healthcare system [3].

Early prediction of disease is one of the significant advantages of the healthcare system. Diabetes and heart disease are increasing among the middle aged people. Diabetes and heart disease have been the primary causes of death worldwide for the past 20 years So, An accurate early diagnosis of the disease is needed to reduce the death rate due to diabetes and heart disease. As per the European Society of Cardiology report, every year 3.6 million people were diagnosed with heart disease. Numerous supervised and unsupervised machine learning algorithms can be used to diagnosis diabetes and heart disease earlier. However, machine learning takes more time and less performance while classification. To overcome this issue, the functional neural network is proposed for accurate disease classification in the early stage.

Cryptography is the branch of information security that deals with protecting information by transforming the plaintext (ordinary text) into ciphertext (known as encryption) and then back again in the original form of text (known as decryption). In symmetric cryptographic techniques, the encryption and decryption keys are similar, i.e., an encipher key can be computed with the help of a deciphering key and vice versa, but in the asymmetric cryptographic technique, these keys are independent but correlated. The encipher and decipher keys are known as a public key and private key respectively, which are to be kept secret. These keys work as a key pair. In today's world, privacy and security are the major concern for technologies including e-commerce, healthcare, personal information over the internet, confidential Govt. reports, etc. Therefore, to solve the security issue, the cryptographic technique is a very useful and very popular tool for authorized users. The healthcare system handles very sensitive information that must be protected from unauthorized access. Cryptography encryption technique is performed before storing patient data into the cloud [4]. The important contributions of our research work are as follows:

- To use ABSHE technique to guarantee the security of patient-sensitive data stored in a cloud.
- To eliminate the noise from IoT data by using the mean-mode normalization process, which helps to improve the quality of data.
- For the effective classification of diabetic and heart disease, FNN-RLU techniques are used.
- The Rectified Linear Unit (RLU) is used to adjust the feature weight for reducing the classification errors.

- The proposed ABSHE scheme provides better security and achieves lower encryption and decryption time compared to existing cryptography schemes.
- The proposed FNN-RLU disease classification technique achieves 92.79% accuracy compared to existing machine learning techniques.

The remaining research article can be organized into four sections. Security of data stored in the cloud, diabetic disease classification, and heart disease classification are briefly analyzed in Section 2. The proposed ABSHE scheme algorithm, mean mode normalization, and functional neural network with RLU algorithm for disease classification are discussed in Section 3, The experimental result analysis of both ABSHE and disease classification are analyzed in Section 4. The conclusion of the research work can be discussed in Section 5.

2 Literature Work

Zhou et al. [5] proposed an ICBN technique that addresses numerous security issues in the health care system. The significant benefit of the proposed ICBN technique is increased patient disease classification accuracy. The efficiency of the proposed work can be analyzed with average accuracy analysis, tracking performance, power conception analysis, and reliability ratio analysis. Xu et al. [6] proposed an ECG Monitoring system using LS-IOT and LAC which are used for secure data transmission. Sengupta et al. [7] implemented a medical data management program to store large amounts of health data and process queries to retrieve end-user health data. Wu et al. [8] suggested a sensor system that can send physiological measurements such as ECG, BT, BP, and Heart Rate. Data encryption technique is performed on both sensor patches and gateways to protect health-related sensitive information from illegal access for privacy and security purposes when it is sent.

Ismail et al. [9] developed a classification model called CNN-based health model for disease classification. The proposed model is used to classify three different types of disease such as obesity, diabetics, and BP. The effectiveness of the proposed classification technique is analyzed with existing models such as the LSTM model, SVM model, and neural network. The proposed CNN-based health model achieves better prediction accuracy than other classification models. Kolle et al. [10] developed automated meal detection system for diabetic patients based on the glucose level in blood. In this work, the binary classifier can be used to predict the glucose level. Saint-Pierre et al. [11] proposed a diabetic care by a collaboration team. This work analysis the team's role in the continuity of diabetic care. The important advantage of diabetics care by collaboration team is to increase the efficiency of treatment of diabetics. Syed et al. [12] proposed T2DM patient care. Experts evaluate the diet and begin with a retrospective evaluation. T2DM disease risk can be effectively diagnosed using machine learning approaches. Pima Indian Diabetes can be used in this work for the prediction of T2DM disease risk. The accuracy of the proposed decision forest model can be compared with existing machine learning approaches. The decision forest model achieves 82% accuracy for predicting T2DM disease risk. Islam et al. [13] developed a DiaNet model to predict diabetics with the help of retinal images. The DiaNet is based on a conventional neural network model. The proposed DiaNet model can predict diabetics with 84% accuracy. The proposed model uses QBB Retina-Image Dataset and EyePACS for the diagnosis of diabetic disease. In the Qatar population, the retinal image of diabetics is outstanding as we know it. Zaitcev et al. [14] proposed a new HbA_{1c} disease prediction model which is based on the CNN model and deep learning. The dataset used in this proposed prediction model was collected from Sheffield Teaching Hospitals. The HbA_{1c} disease prediction model achieves better accuracy compared to existing approaches.

Halabi et al. [15] suggested a Goal Question Metric (GQM) technique which uses a set of parameters to describe clouds' security–security level agreement quantitatively and uses it to assess CSPs' security levels.

The experimental result analysis of our proposed model shows that the federation model achieves more security and decreases the security SLA violation. Nassif et al. [16] described a ML technology that has been used in cloud technology to address various security issues. The usage of cloud technology has increased in recent days. But, the protection of data from illegal access is the most important issue. This work compares various mechanisms for protecting cloud data from attacks. Srinivas et al. [17] proposed a Cloud-based Authentication technique for protecting the privacy of patient data in the health care system. This research work describes the various benefits of wearable devices such as health care, business, law enforcement, and day-to-day activities. The proposed cloud based authentication technique uses seven different phases. The performance of the proposed model can be compared using the cost of communication, cost of computation, and different security features. Shabbir et al. [18] proposed a Modular Encryption Standard to guarantee the confidentiality of patient information in the health care system. The proposed MES techniques use three important measures such as IDN, CLF, and SC. The proposed MES technique can be compared with existing cryptographic techniques such as RC5, RC6, DES, 3DES, AES, and Blowfish. The proposed techniques have better memory utilization, space complexities, and processor utilization rate compared to existing techniques. Lee [19] proposed an RS-IBE technique to extend the concept of Identity-Based Encryption (IBE). The proposed RS-IBE technique can be modified using SUE. The proposed RS-IBE techniques have numerous benefits, such as feasible and cost-effective. Stergiou et al. [20] proposed a cache decision system that provides an efficient and safer browsing environment in the internet. In this work, the fog was used to manage and share a huge amount of data over 6G wireless networks. The proposed CDS system is energy efficient compared to existing techniques. Nguyen et al. [21] developed a ResNet disease classification model. The security of patient data in the health care system is ensured using block chain technology. The proposed ResNet classification model achieves higher sensitivity compared to the existing classification model.

Zhang et al. [22] proposed a LDVAS method which is used to protect sensitive medical data from quantum-computing attacks. The performance of the LDVAS technique can be compared with existing techniques such as PPPA, CIPPPA, and CLPA. The proposed LDVAS cost of communication is much less compared to existing approaches. The performance of the LDVAS can be examined using Storage Correctness Guarantee, Robustness, and Privacy Preservation. El-Sappagh et al. [23] described various mobile health technologies used in DM are briefly analyzed. The relationship between MH and cloud computing, MH and big data, and MH and CDSS are briefly discussed. The challenges of diabetic Mellitus are also described. Masud et al. [24] proposed a MASK protocol to guarantee the security of patient health data using cryptography primitives. The proposed MASK protocol has some significant advantages, such as limited resource usage, and protection against device loss. The performance of the proposed MASK protocol was evaluated using the AVISPA tool. Ali et al. [25] proposed a PBCV framework for component-based healthcare applications. The proposed PBCV enhances the quality of the CB based Healthcare system with the help of regression testing. The performance analysis of the PBCV framework shows an increased detection rate.

3 Proposed Methodology

The proposed searchable honey encryption algorithm is a security tool that safeguards data from illegal access. The proposed Cryptographic algorithm provides two layers of security that address numerous security issues of existing cryptography techniques. Attribute-Based Searchable Honey Encryption (ABSHE) authenticates the user key and encrypts the IoT data. This cryptography algorithm uses attribute-based encryption for verifying the user policy and attributes. The proposed Functional Neural Network with Rectified Linear Unit (FNN-RLU) method analyzes the disease from a given IoT data.

Functional Neural Network is an unsupervised learning algorithm to provide a less training rate. It presents a preprocessing task to remove noise and inconsistent data from various sources using a Mean-Mode Normalization. The architecture of the proposed ABSHE-FNN is shown in Fig. 1. The data trains to each input layer and estimates the weight of each neuron. The Rectified Linear Unit is applied to adjust the neuron's feature weight, reducing the training cost and error classification.

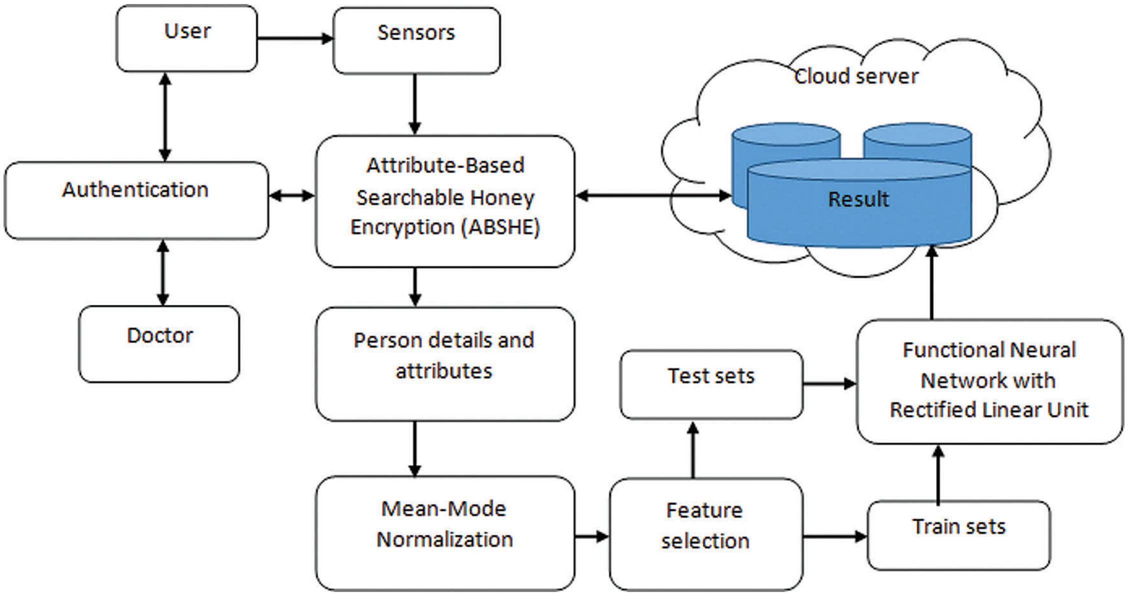
User
Sensors
Cloud server
Authentication
Attribute-Based Searchable Honey Encryption (ABSHE)
Result
Doctor
Person details and attributes
Test sets
Functional Neural Network with Rectified Linear Unit
Mean-Mode Normalization
Feature selection
Train sets

Figure 1: Proposed ABSHE-FNN framework

3.1 Attribute-Based Searchable Honey Encryption (ABSHE)

The attribute-based searchable honey encryption (ABSHE) is proposed to encrypt and authenticate valid users to allow the cloud server. It is 128/256 cryptographic algorithm that performs two layers of encryption for added security. The user's private key is a collection of custom attributes in the system that is associated with space attribute access policies. The user attributes cannot be decrypted by the user only if they meet the corresponding ciphertext policy. The user attributes set is defined as {A, B, C, and D}; the first user receives the {A, B} key attribute based on the user policy attribute. If an input text is encrypted concerning the policy (A^C) ^D, then the second user {D} cannot decrypt the original data; the 1st user only decrypts it. Three different groups run the basic design of the algorithm.

The honey encryption flow diagram is shown in Fig. 2. The seed area is used to find the bits n prefix values, and finally, the DTE is encoded, and the message is decrypted using the seed values. In the Honey encryption process, select the file to be encrypted, and then select the attributes from the file. After selecting attributes, set the rules/policies. Input file 'f' is encrypted according to these rules. Also, the encrypted files are password protected again for more security. Generated honey words are given to the user. In the proposed algorithm ABSHE, the only expected group of users with <attribute, password> decrypts the data. At the time of decryption, the user must enter a valid password; then only the user is allowed to decrypt a file. Otherwise, the user is not allowed to decrypt the file. The user is treated as an attacker. If the password entered is valid, the user must enter a private key created at the time of encryption. Otherwise, the user is not allowed to access a file.

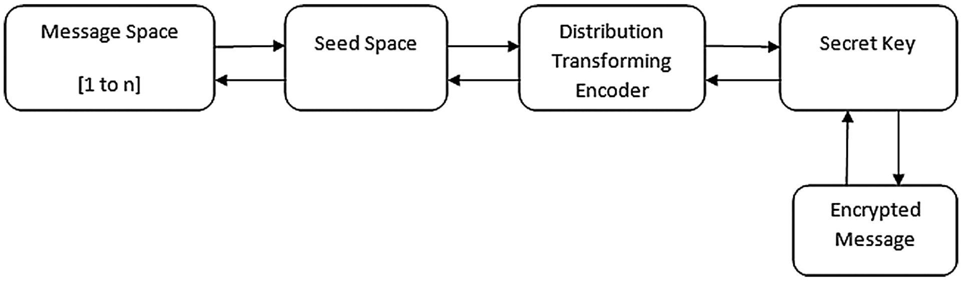

Figure 2: Honey encryption process

3.2 ABSHE Algorithm

Step 1: To analyses the message space length of characters. In this distribution, Message is denoted as ω_m to taken $\omega_{m(n-1)}$ length of the message.

Step 2: Seed space S are some of the space of binary strings of all n bits of a given n. Each message in m, the seed's size is mapped to S seed, which is directly proportional to the likelihood of how certain messages are sent. The distribution map S →[0,1] such as ∑ map(s) = 1.

Step 3: Encode the ω_m to apply the DTE (encode, decode) message DTE ($m_i \in m_j$). The encoding method to take the input message $m_i \in m_j$ and output set of the seed value $S_i \in S_j$ and the decoding process is the reverse format of encoding values.

Step 4: Encryption (ABSHE encryption algorithm takes file 'f' along with policy 'p' as input and produces ciphertext (CT) as output)

a. Select files and settings whose attributes are encrypted to encrypt files 'f' with attributes that occur in the set of policies 'P', Keywords also encrypted which are extracted from the file.
b. Securing the encrypted file once more with the help of a password.
c. Created honey words are given to the user, followed by steps 1 to step 3.

Step 5: Decryption (The decryption algorithm takes password-protected encrypted file as input. The encryption algorithm produces a cipher text (CT), and the access policy "P" is under the text being encrypted).

a. If the password matches, then the ciphertext CT will be decrypted; otherwise, its processes stopped.
b. If the keys match decrypts the original information and prints the corresponding original file "F"; otherwise, the file prints NULL.

3.3 Mean-Mode Normalization

The preprocessing technique improves the data quality and minimizes the irrelevant information and redundant information from the list. The preprocessing process includes noise elimination and the normalization process, which completely reduces the irrelevant data from the data list. Due to the preprocessing importance, the Mean-Mode Normalization process is used to eliminate the noise from IoT data in this work. If a particular row consists of any missing value, which is filled by computing the mean value of a specific row. The mean esteem is evaluated as

$$Mean(M) = \sum_{i=0}^{n} x_i \qquad (1)$$

The missing values are replaced continuously, and the data set is normalized according to the scaling process that is performed as

$$v' = \frac{(v - min)}{max - min} \tag{2}$$

Above the equation, data is represented as V, the minimum value of diabetes data is denoted as min, maximum diabetes value is represented as max. V′ is the normalized data that consists of values 0 to 1. The first check for the existence of outliers is performed in these two variables and their dependent variables. It needs to modify some anomalous variables and use means to convert them to a normal distribution. From the quality improved data, various features, namely, mean, minimum, variance, correlation, maximum, and the other features are extracted.

3.4 Functional Neural Network with Rectified Linear Unit

The proposed functional neural network is a recurrent learning method to assign the feature weight to classify the disease randomly. The FNN-RLU structure is shown in Fig. 3. The network helps to analyze false patterns from the set of features by covering the local minimum. The network structure consists of a unit set, normally represented in a binary threshold unit that does not exceed the threshold value. The units are represented as 1 or −1. In general, the network has a weight value between node i and j. The connection between nodes is formed as an undirected graph, and the weight value has to be updated for each neuron. To use the Rectified Linear Unit (RLU) to handle the unsupervised learning data and classification error to adjust the feature weight. The weight value is used to compute the estimated output for a particular pattern recognition problem. During the output computation process, the unit value is updated as follows,

$$s_i \leftarrow \begin{cases} +1 & if \sum_{i=1}^{n} j\, w_{i,j} x_j \geq \theta_i \\ -1 & otherwise \end{cases} \tag{3}$$

$w_{i,j}$ is denoted as the connection between two nodes or units, s_i is a state of the unit, and θ_i is the threshold of unit i. According to the discussion, the generalized neural network structure is shown in Fig. 3.

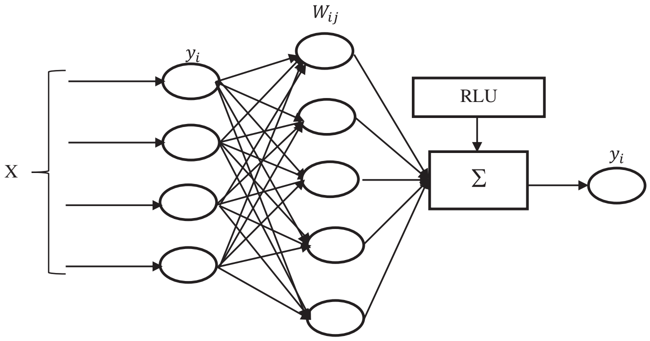

Figure 3: Functional neural network structure

The incoming disease features are fed into the neural network in n-dimensional space in binary components −1 and 1. The binary components represent the output of the neural network. During the input process, each node has specific weights, which is mentioned as

$$w = \frac{1}{n}\left(\sum_{i=1}^{c} \sigma_i^c \omega_i\right) \tag{4}$$

c is class patterns, ω_i is the vectors. According to the feature weight, network output is computed as

$$x(t+1) = sign(w * x(t)) \tag{5}$$

where the $x(t)$ is the input feature state time. This process is endless to get the outcome of every incoming patient feature. At the time of the above classification procedure, the network has an error rate that completely reduces the disease prediction system's efficiency and maximizes the miss-classification rate. The system's performance is enhanced by optimizing the network with a Rectified Linear Unit algorithm.

3.5 FNN-RLU Algorithm

Step 1: Initialize the W_{ij} form samples s are randomly selected from normal distribution then bias terms $(x_i \mid c_i)$ to zero.

Step 2: Similarly, update all the hidden units using Eqs. (4) and (5).

Step 3: If the probability is greater than a threshold selected from a uniformly distributed random variable, which takes value in the range [0,1].

Step 4: Update the weight and biases $(w_{ij},\ x_i,\ c_j)$,

$$w_{ij}^{t} = w_{ij}^{t}(x) + \eta \triangle w_{ij}^{t+1}$$

$$\triangle w_{ij}^{t+1} = \mu \triangle w_{ij}^{t} + \alpha\left[v_j P(h_i|) - v_j' P(h_i' \mid v')\right] \tag{6}$$

where η is the learning parameter, μ is the momentum term, and α is the parameter that decides weight on the corresponding gradient value. Initial weights of the FNN model are set up randomly. The weights adoption used mean square error (MSE) between target and output of FNN. The training and test data sets were generated from the given dataset. Before training, the data sets were scaled in (−1, +1) to each row of input and output matrix for an easier learning process.

The activation gate or function is defined as a non-linear Rectified Linear Unit (RLU) function. This activation function receives any input which is less than zero, it returns zero. Otherwise, it returns value back when it receives any positive input. The significant advantages of the Rectified Linear Unit activation function are its ability to be used similar to the human nervous system, simple and fast for training large networks.

$$f(x) = \max(0, x) \tag{7}$$

The linear unit for configuration is the activation function most commonly used in deep learning models. In case of negative input is received, it returns the output as 0. This is primarily a classification used by fully connected networks. In neural networks, a fully connected layer connects all the neurons in one layer to all the neurons in the next layers. The Fully connected layer computes the prediction class by identifying the data. The hierarchy uses the "Rectified Linear Unit" activation function to classify features generated based on the input data of various training data categories received from the previous layer.

4 Results and Discussions

4.1 ABSHE Performance Analysis

The proposed ABSHE methodology performance can be examined by using performance metrics such as encryption and decryption time. The effectiveness of the proposed ABSHE technique is compared with existing techniques such as VPKE-HE [26], HERDE [27]. The proposed ABSHE technique can be implemented in the java language.

4.1.1 Encryption Time

Encryption Time is the time taken for transferring an input text to ciphertext. Fig. 4 shows the encryption time comparison of proposed ABSHE and Existing approaches such as VPKE-HE and HERDE. The existing technique VPKE-HE takes 52.25, 103.59, 154.58, 392.71, and 712.59 s for the encryption of file size 64, 128, 256, 512, and 1024 MB respectively. HERDE technique takes 39.25, 74.61, 147.37, 225.25, and 645.81 s for the encryption of file size 64, 128, 256, 512, and 1024 MB respectively. The proposed ABSHE takes 1.45, 9.9, 23.52, 80.04, and 362.58 s for the encryption of file size 64, 128, 256, 512, and 1024 MB with respectively. From these simulation results, the proposed ABSHE takes less encryption time compared to existing approaches.

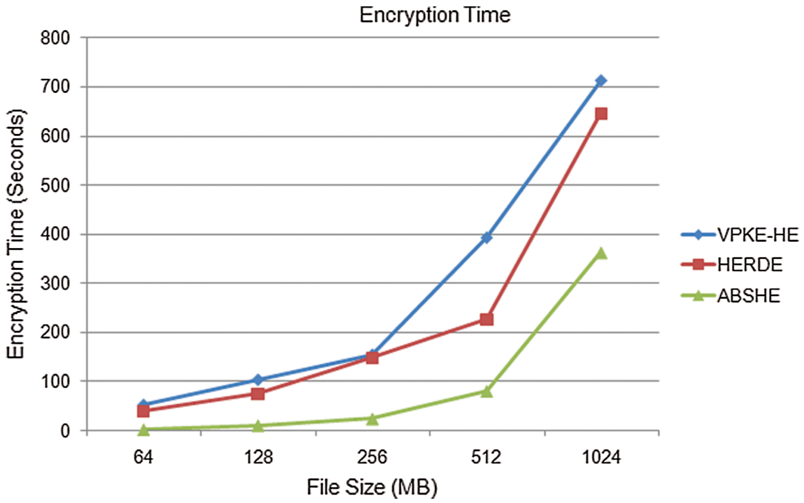

Figure 4: Encryption time comparison

4.1.2 Decryption Time

Decryption time is the time taken for transferring encrypted text (ciphertext) to original text (plain text). Fig. 5 shows the encryption time comparison of proposed ABSHE and Existing approaches VPKE-HE and HERDE. The existing technique VPKE-HE takes 78.33, 131.1, 171.84, 536.94, and 845.04 s for the decryption of file size of 64, 128, 256, 512, and 1024 MB respectively. HERDE technique takes 65.7, 99.36, 159.38, 392.19 s, and 732.66 for the file size of 64, 128, 256, 512, and 1024 MB respectively. The proposed ABSHE takes 1.81, 10.08, 27.3, 81.24, and 403.8 s decrypts the file size of 64, 128, 256, 512, and 1024 MB respectively, From this simulation results, The proposed ABSHE takes less decryption time compared to existing approaches.

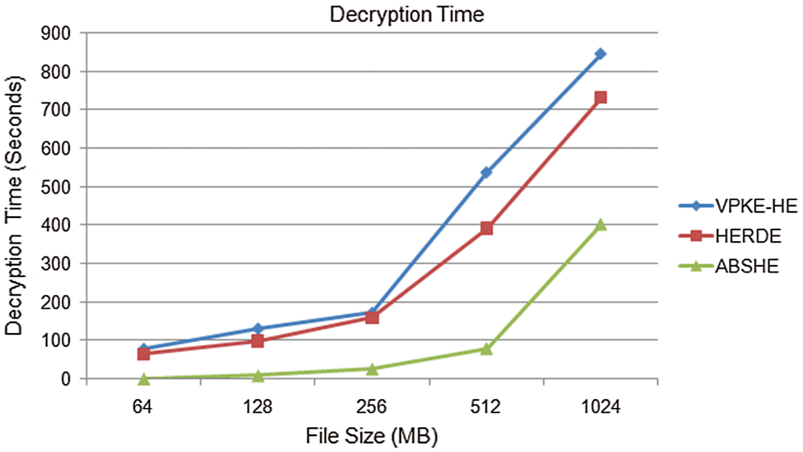

Figure 5: Decryption time comparison

4.2 FNN-RLU Performance Analysis

This section presents the results of a work that proposed a technique for predicting disease using a neural network. Statistics are the strong basic background for quantifying and assessing results. Different components and parameter values are considered in the simulation. These parameters include data collected for the Online Basic Medical Information Website and Medical Pima Indian dataset. Tab. 1 presents the proposed method IoT healthcare framework simulation parameter and dataset detail.

Table 1: Simulation parameter

Parameter	Value
Dataset name	Cardiovascular Disease, Pima Indians diabetes
Tools	Visual Studio framework
Total number of data	5000, 2000

4.2.1 Disease Classification

This Heart disease result analysis shows, the KNN method has 76.87%, RF method has 83.5%, MLP has 83.89%, MSNB has 93.33% F-measure compares to the proposed classifier FNN-RLU methods have 95.39% better F-measure rate. The analysis result of heart disease prediction performance of the proposed method and existing method f-measure, sensitivity, specificity, and accuracy is present in Tab. 2. The proposed method FNN-RLU method has 93.66% accuracy, 92.3% specificity, 95.18% of sensitivity, and 95.39% F-measure which is better than other techniques. The heart disease performance comparison of FNN-RLU and existing classification techniques are shown in Fig. 6.

Tab. 3 presents the analysis result of diabetes disease prediction of the proposed FNN-RLU method and existing KNN, RF, and MSNB method f-measure, sensitivity, specificity, and accuracy rate. The Diabetes disease performance comparison of FNN-RLU and existing classification techniques are shown in Fig. 7. The proposed FNN-RLU method diabetes prediction provides 91.92% accuracy, 87.05% specificity, 95.5% of sensitivity, and 96.50% of F-measure which is better performance than other machine learning techniques.

Table 2: Performance analysis of heart disease prediction

Methods	F-Measure (%)	Sensitivity (%)	Specificity (%)	Accuracy (%)
KNN	76.87	78.47	70.63	74.1
RF	83.5	82.47	79.51	81.48
MLP	83.89	84.46	80.17	82.22
MSNB [27]	93.33	93.33	91.67	92.59
FNN-RLU	95.39	95.18	92.3	93.66

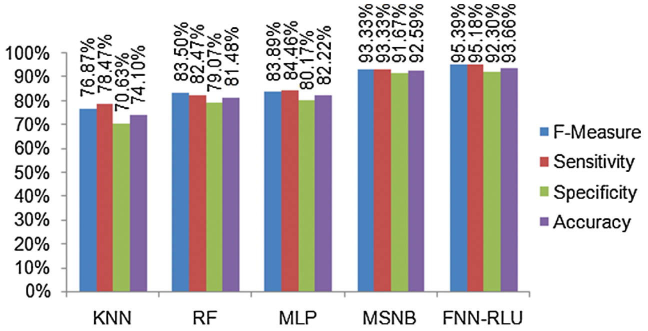

Figure 6: Heart disease prediction

Table 3: Performance analysis of diabetes prediction

Methods	F-Measure (%)	Sensitivity (%)	Specificity (%)	Accuracy (%)
KNN	71.76	73	33.21	63.4
RF	83.83	98	46.25	75.39
MLP	82.59	81	58.33	76.82
MSNB [27]	93.58	93.44	68.12	88.93
FNN-RLU	96.5	95.5	87.05	91.92

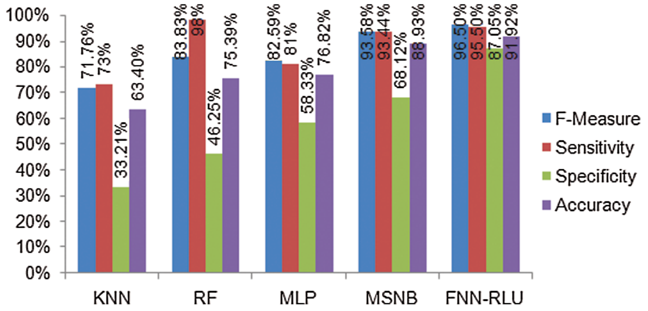

Figure 7: Diabetes disease prediction

Table 4: Performance analysis of FNN-RLU disease classification

FNN-RLU	F-Measure (%)	Sensitivity (%)	Specificity (%)	Accuracy (%)
Heart disease classification	95.39	95.18	92.3	93.66
Diabetes disease classification	96.5	95.5	87.05	91.92
Overall disease classification	95.94	95.34	89.675	92.79

The performance analysis of FNN-RLU disease classification (both heart and diabetes) is presented in Tab. 4. In this analysis, FNN-RLU has achieves 92.79% of classification accuracy, 95.94% of F-measure, 95.34% of sensitivity, and 89.67% of specificity. The proposed FNN-RLU method feature parameters are randomly trained neurons to predict the feature weight and predict the disease efficiently. The performance of the proposed FNN-RLU classification model can be compared with existing machine learning techniques. The FNN-RLU overall disease classification performance is shown in Fig. 8. From the result comparison, the proposed method FNN-RLU overall performance is higher than other existing MSNB, KNN, and RF methods.

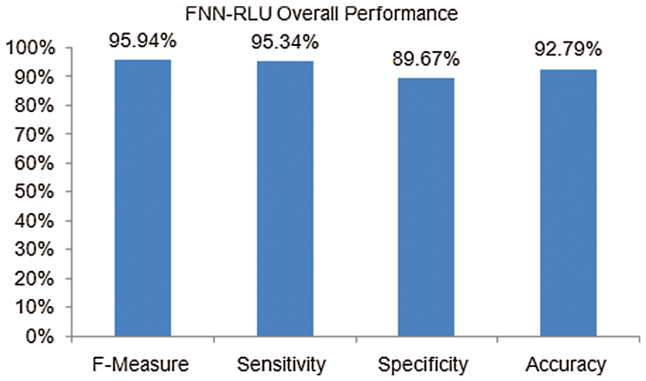

Figure 8: Comparison of overall disease classification performance

5 Conclusion

In this research work, Attribute Based Searchable Honey Encryption with Functional Neural Network (ABSHE-FNN) provides an efficient disease classification and IoT data security over cloud users. The attribute-based searchable honey encryption (ABSHE) is proposed which allows encryption and decryption of sensitive patient data over cloud storage. The encrypted data is retrieved by applying the corresponding proposed key to provide security to the data. The proposed Functional Neural Network with Rectified Linear Unit (FNN-RLU) method analyzes the disease from a given IoT data. In this research work, Cardiovascular Disease and Pima Indians diabetes dataset are used for heart and diabetic disease classification respectively. The means-mode normalization is used to remove noise and inconsistent data from various sources, which helps to enhance the quality of data. The data trains to each input layer and estimates the weight of each neuron. The Rectified Linear Unit is applied to adjust the neuron's feature weight, reducing the training cost and error classification. With the help of an optimized learning concept, the heart and Diabetes features are classified with maximum accuracy. The performance analysis of the ABSHE scheme shows that lower encryption and decryption time compared to existing cryptography schemes. The overall accuracy of the FNN-LRU technique for diagnosing diabetes and heart disease is 92.79%, which is higher than the existing machine learning technique.

In the future, this work could be extended to improve the security of patient data stored in cloud storage using some advanced cryptography algorithms. The FNN-RLU classification model effectively predicts heart and diabetes disease. In the future, the same disease classification model will be implemented with a real time dataset to improve the accuracy of disease classification.

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] K. Jaiswal, S. Sobhanayak, A. K. Turuk, S. L. Bibhudatta, B. K. Mohanta *et al.,* "An IoT-cloud based smart healthcare monitoring system using container based virtual environment in edge device," in *Int. Conf. on Emerging Trends and Innovations in Engineering and Technological Research*, Ernakulam, India, 2018.

[2] K. Bouelmehdi, A. Beni-Hessane and H. Khaloufi, "Big healthcare data: Preserving security and privacy," *Journal of Big Data*, vol. 5, no. 1, pp. 38, 2018.

[3] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun *et al.,* "Secure healthcare data aggregation and transmission in IoT—a survey," *IEEE Access*, vol. 9, pp. 16849–16865, 2021.

[4] Mamta, B. B. Gupta, K. C. Li, V. C. M. Leung, K. E. Psannis *et al.,* "Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system," *IEEE/CAA Journal of Automatica Sinica*, 2021.

[5] Z. Zhou, H. Yu and H. Shi, "Human activity recognition based on improved bayesian convolution network to analyze healthcare data using wearable IoT device," *IEEE Access*, vol. 8, pp. 86411–86418, 2020.

[6] G. Xu, "IoT-assisted ECG monitoring framework with secure data transmission for healthcare applications," *IEEE Access*, vol. 8, pp. 74586–74594, 2020.

[7] S. Sengupta and S. S. Bhunia, "Secure data management in cloudlet assisted IoT enabled e-health framework in smart city," *IEEE Sensors Journal*, vol. 20, no. 16, pp. 9581–9588, 2020.

[8] T. Wu, F. Wu, C. Qiu, J. M. Redoute and M. R. Yuce, "A rigid-flex wearable health monitoring sensor patch for IoT-connected healthcare applications," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6932–6945, 2020.

[9] W. N. Ismail, M. M. Hassan, H. A. Alsalamah and G. Fortino, "CNN-based health model for regular health factors analysis in internet-of-medical things environment," *IEEE Access*, vol. 8, pp. 52541–52549, 2020.

[10] K. Kolle, T. Biester, S. Christiansen, A. L. Fougner and O. Stavdahl, "Pattern recognition reveals characteristic postprandial glucose changes: Non-individualized meal detection in diabetes mellitus type1," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 2, pp. 594–602, 2020.

[11] C. Saint-Pierre, F. Prieto, V. Herskovic and M. Sepulveda, "Team collaboration networks and multidisciplinary in diabetes care: Implications for patient outcomes," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 1, pp. 319–329, 2020.

[12] H. Syed and T. Khan, "Machine learning-based application for predicting risk of type2 diabetes mellitus (T2DM) in saudi arabia: A retrospective cross-sectional study," *IEEE Access*, vol. 8, pp. 199539–199561, 2020.

[13] M. T. Islam, H. R. H. Al-Absi, E. A. Ruagh and T. Alam, "Dianet: A deep learning-based architecture to diagnose diabetes using retinal images only," *IEEE Access*, vol. 9, pp. 15686–15695, 2021.

[14] A. Zaitcev, M. R. Eissa, Z. Hui, T. Good, J. Elliott *et al.,* "A deep neural network application for improved prediction of HbA1c in type1 diabetes," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 10, pp. 2932–2941, 2020.

[15] T. Halabi and M. Bellaiche, "Towards security-based formation of cloud federations: A game theoretical approach," *IEEE Transactions on Cloud Computing*, vol. 8, no. 3, pp. 928–942, 2020.

[16] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani and F. M. Dakalbab, “Machine learning for cloud security: A systematic review,” *IEEE Access*, vol. 9, pp. 20717–20735, 2021.

[17] J. Srinivas, A. K. Das, N. Kumar and J. J. P. C. Rodrigues, “Cloud centric authentication for wearable healthcare monitoring system,” *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 942–956, 2020.

[18] M. Shabbir, A. Shabbir, C. Iwendi, A. R. Javed, M. Rizwan *et al.,* “Enhancing security of health information using modular encryption standard in mobile cloud computing,” *IEEE Access*, vol. 9, pp. 8820–8834, 2021.

[19] K. Lee, “Comments on secure data sharing in cloud computing using revocable-storage identity-based encryption,” *IEEE Transactions on Cloud Computing*, vol. 8, no. 4, pp. 1299–1300, 2020.

[20] C. L. Stergiou, K. E. Psannis and B. B. Gupta, “IoT-based big data secure management in the fog over a 6G wireless network,” *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5164–5171, 2021.

[21] G. N. Nguyen, N. H. L. Viet, M. Elhoseny, K. Shankar, B. B. Gupta *et al.,* “Secure blockchain enabled cyber-physical systems in healthcare using deep belief network with ResNet model,” *Journal of Parallel and Distributed Computing*, vol. 153, no. 2, pp. 150–160, 2021.

[22] X. Zhang, C. Huang, Y. Zhang, J. Zhang and J. Gong, “LDVAS: Lattice-based designated verifier auditing scheme for electronic medical data in cloud-assisted WBANs,” *IEEE Access*, vol. 8, pp. 54402–54414, 2020.

[23] S. El-Sappagh, F. Ali, S. El-Masri, K. Kim, A. Ali *et al.,* “Mobile health technologies for diabetes mellitus: Current state and future challenges,” *IEEE Access*, vol. 7, pp. 21917–21947, 2019.

[24] M. Masud, G. S. Gaba, S. Alqahtani, G. Muhammad, B. B. Gupta *et al.,* “A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care,” *IEEE Internet of Things Journal*, 2020.

[25] S. Ali, Y. Hafeez, N. Z. Jhanjhi, M. Humayun, M. Imran *et al.,* “Towards pattern-based change verification framework for cloud-enabled healthcare component-based,” *IEEE Access*, vol. 8, pp. 148007–148020, 2020.

[26] D. N. Wu, Q. Q. Gan and X. M. Wang, “Verifiable public key encryption with keyword search based on homomorphic encryption in multi-user setting,” *IEEE Access*, vol. 6, pp. 42445–42453, 2018.

[27] M. Vedaraj and P. Ezhumalai, “HERDE-MSNB: A predictive security architecture for IoT health cloud system,” *Journal of Ambient Intelligence and Humanized Computing*, 2020.