electronics

MDPI

Review

Novel Hybrid Intelligent Secure Cloud Internet of Things Based Disease Prediction and Diagnosis

Ankit Verma [1], Gaurav Agarwal [2], Amit Kumar Gupta [1] and Mangal Sain [3,*]

[1] Department of Computer Applications, KIET Group of Institutions, Delhi-NCR, Ghaziabad 201206, India; ankit.verma@kiet.edu (A.V.); amit.gupta@kiet.edu (A.K.G.)
[2] Department of Computer Science & Engineering, Invertis University, Bareilly 243123, India; gaurav.a1@invertis.org
[3] Division of Computer Engineering, Dongseo University, 47 Jurye-Ro, Sasang-Gu, Busan 47011, Korea
* Correspondence: mangalsain1@gmail.com; Tel.: +82-1028591344

Abstract: Nowadays, more people are affected by various diseases such as blood pressure, heart failure, etc. The early prediction of diseases tends to increase the survival of affected patients by allowing preventive action. A key element for this purpose is the digitalization of the healthcare system through the Internet of Things (IoT) and cloud computing. Nevertheless, there are major problems in the cloud with the IoT due to false predictions and errors in medical data, which results in taking a longer time to receive patient details and not providing the best outcome. Data transfer through the cloud can also be hacked by attackers due to the lack of security. This leads to a challenge for medical experts to predict the diseases accurately for a specific patient. Therefore, a novel hybrid elapid encryption (HEE) method was proposed for improving the security of cloud systems. In addition, the affected person's disease and the severity risk level were predicted and classified using the proposed novel hybridization technique of the generalized-fuzzy-intelligence-based gray wolf ant lion optimization (GFI-GWALO) method. After the disease is predicted, the alert signal is provided to the patients. Moreover, this proposed research was implemented on MATLAB. Then the proposed simulation outcome was compared with various conventional methods and showed that the proposed method has the best outcomes in terms of its security and disease prediction with 80 ms of encryption time and 78 ms of decryption time, 100% accuracy, 99.50% precision and 8 ms of processing time.

Keywords: Internet of Things; generalized-fuzzy-intelligence-based gray wolf ant lion optimization; big data; healthcare system; cloud storage and hybrid elapid encryption

Citation: Verma, A.; Agarwal, G.; Gupta, A.K.; Sain, M. Novel Hybrid Intelligent Secure Cloud Internet of Things Based Disease Prediction and Diagnosis. *Electronics* **2021**, *10*, 3013. https://doi.org/10.3390/electronics10233013

Academic Editor: Shinichi Yamagiwa

Received: 19 October 2021
Accepted: 28 November 2021
Published: 2 December 2021

1. Introduction

In recent times, the human lifespan has increased due to the advances in the development of healthcare organization such as medical facilities, treatments and health data administration of patient care [1]. Nevertheless, unnecessary errors, transmission delays, security threats, the lack of proper medical data and fault diagnosis are major problems in advanced healthcare development [2]. Hence, the information of patients must be protected from unlicensed users using new strategies. Furthermore, the use of IoT-based wearable sensor technology has increased tremendously in healthcare applications for anticipated disease prediction [3]. Moreover, IoT devices are integrated with the cloud computing components and provide identical users [4]. IoT devices gather a huge amount of data from remote-area patients, which are stored in the cloud storage environment. Furthermore, this has the ability to broadcast the data of patients from the system without requiring computer communication from the patient [5]. Therefore, the availability of the cloud with the IoT allows logical and predictive tools for enhancing disease prediction accuracy. The unstructured medical statistics, semi-structured medical statistics and structured medical records of patients from the IoT on the cloud are arranged as big data of affected

patients [6]. From this, the cloud computing efficiency in the healthcare system is higher because it is used in disease forecast application, handling medical records of patients, recovering patients' data from big data and tele-medicine [7]. Moreover, IoT components are utilized to estimate various diseases such as breast cancer, heart disease, diabetes and so on [8]. Therefore, a robust monitoring scheme should be available to the patient while they move from one location to another or in situations with no or less network connection [9]. Real-time medical data processing has some difficulties with data storage in the cloud for data handling, disease diagnosis and health data management [10]. However, the main challenge of this technology is security threats to data transmission between the patient and management [11]. The confidential data can be captured by external attacks, eavesdropping, distortion and fraudulence. If there is no data security method, the information of patients may be leaked from the cloud server which can affect the disease estimation [12]. Furthermore, in the healthcare system, security supervision from illegal access is a challenging task. In the advanced cloud with IoT-based healthcare arrangement, the conventional security method is unfit for better performance [13].

Furthermore, the IoT collects an enormous amount of data in the medical care system, and data science technology can provide an essential method to develop more intelligent IoT devices [14]. Machine learning and data mining are a branch of data science, which is used to estimate new patterns and guidelines from data [15]. The enormous amount of data from the clinical system is significantly handled by the ordinary machine learning method [16]. Traditionally, various techniques have been utilized such as classification methods, the neural network (NN) approach, fuzzy methods, heuristic techniques and clustering techniques for disease prediction [17]. However, the conventional methods have not performed efficiently [18] because, if some of the data are missing, the accuracy of the conventional methods of disease forecasting is diminished and a high error rate is produced. Moreover, [19] used a lightweight encryption replica for analyzing the biological data of the affected people using IoT devices, but these analyzed data cannot provide accurate information about the affected people. In addition, an e-health system is provided for patients to reduce health problems [20]. However, this technology requires more security to protect the collected data in an efficient manner. Some recent heuristic algorithms have been used in the field of engineering such as particle swarm optimization [21], 2-Opt-based discrete ant lion optimization technique in routing issues [22], memetic genetic approach for traveling salesmen problems [23], arithmetic optimization method [24] and so on. Therefore, in this research, hybrid intelligent secure strategies were utilized to achieve the best outcomes in terms of improved security and prediction. Moreover, the developed technique aims to predict disease in the human body with the help of IoT-enabled devices. Conventional health support methods only forecast the chance of individual diseases, and security hazards are a major problem. Thus, the main scope of this research was developing a new hybrid encryption technique to protect the sensitive data of patients from the access of attackers. Moreover, the hybridization of a novel classifier based on neuro-fuzzy and optimization was performed for enhanced disease prediction with the best accuracy. Furthermore, the main aim of this research was to predict and analyze the severity of diseases.

The main contributions of this research are summarized below:

- We introduced a novel GFI-GWALO hybrid classifier for prediction and severity risk analysis.
- From the standard website, the human biological parameters were gathered and stored in the cloud database.
- The stored data were secured by a novel HEE-based security strategy.
- The HEE security protects the stored data from hackers, and a novel GFI-GWALO-based hybridization classifier technique was also proposed.
- A novel GFI-GWALO technique was developed to identify the disease and its severity. If the person has been affected by any diseases, the notice is provided via email or SMS, and then the person can consult medical experts.

- Finally, the proposed HEE with GFI-GWALO method was compared with various disease prediction approaches, which proved that the proposed HEE GFI-GWALO method achieves improvements in encryption and decryption time, accuracy, recall, precision, error rate and F-measure.

The structure of this paper is summarized as follows: The related work of this research is summarized in Section 1. The system model and the problem statement are explained in Section 2. The proposed security and classifier method is elaborated in Section 3. Consequently, the result and discussion along with the comparative analysis are described in Section 4. Finally, the paper is concluded in Section 5.

2. Related Work

Some of the recent works of literature related to this research are summarized below:

In advanced health and medical care, IoT-based systems play a significant part. Moreover, this methodology helps medical experts and patients predict diseases from the collection of disease forecasts and diagnoses. However, this method includes problems such as inaccurate diagnosis and security. Therefore, an optimized K-means-based adaptive neuro-fuzzy inference system (OKM-ANFIS) along with the distributed key-based advanced encryption standard (DK-AES) was introduced by Savitha et al. [25] for a breast cancer forecast system via IoT technology. The multiple data of disease are predicted using a genetic algorithm (GA). The alert signal informs the hospital if the patient has any critical conditions. However, security attacks are not detected by this method.

The association of health monitoring methods and the Internet of Health Things (IoHT) plays the main role in patient data gathering from remote areas using medical components and sensors because intelligent healthcare facilities are provided by this technology. However, for the best services, Lakshmanaprabu et al. [26] presented a cloud with an IoT-based deep neural network (DNN) method for chronic kidney disease (CKD) diagnosis and severity estimation. Moreover, the performance of this presented technique was enhanced for feature selection using particle swarm optimization (PSO). The accuracy of the estimated method was 99.25, specificity 98.03% and kappa value 98.40. Mainly, this method is complex in nature and lacks security.

In a healthcare system, cloud computing services provide more benefits for e-health applications. However, effective security is the main challenge in cloud computing. To resolve this problem, Karuppiah and Geetha [27] proposed a Twofish encryption method for security enrichment and a multi-kernel support vector machine (MKSVM) algorithm for distributing error data. The segmented data are encrypted and provided to the cloud server, which creates the best key. Then a modified whale optimization algorithm (MWO) is projected for the best key creation. Accuracy, F-measure and precision values are lower.

In smart cities, disease prediction by the cloud with the IoT plays an essential part in health care management. The digital sensors of the IoT collect CKD data; the gathered big data are stored in cloud storage. However, this cloud with the IoT method is facing more challenges in the crucial disease forecast of smart cities' health care management. Therefore, a new hybrid intelligent model was introduced by Abdelaziz et al. [28] for CKD prediction. Here, a linear regression (LR) with neural network (NN) method was developed as a hybrid model. The crucial features in CKD were estimated by LR, and the disease was predicted using an NN. Thus, 97.8% accuracy was achieved by this hybrid model. Nevertheless, the accuracy needs to be improved, and medical usage should be maximized.

Security is a major problem in storing medical information. For this reason, Dawid Polap et al. [29] projected a federated learning approach that utilizes blockchain security along with decentralized learning (particularly neural networks) by sharing only classifier parameters but not private data. However, the developed method fails to provide a good outcome.

The drawback of existing clustering is data transfer efficiency issues. To solve this problem, Taher and M. Ghazal [30] presented an IoT with artificial intelligence system (IoT-AIS) to bridge the digital world and IoT that encrypts patient records; the result

demonstrates that it has a high data transfer rate, delivery rate and less delay in estimation. However, it is not applicable in mobile-based applications.

Moreover, artificial intelligence (AI)-enabled wearable device and sensor analyses were used for IoT-based healthcare applications in COVID-19 screening, prevention and treatment [31,32]. During the COVID-19 pandemic, the use of IoT technology is increasing in health monitoring systems [33]. The IoT technology instantly detects the health problems of people by using sensors [34]. Moreover, during the COVID-19 pandemic, the IoT helps to improve patient care [35]. However, effective IoT monitors can also work well and save the lives of patients with problems such as heart failure, blood pressure, diabetes, etc. [36]. For this, a modified disease prediction technique is necessary.

Medical devices and the IoT improve the health care system and condition at any time. Moreover, H. Fouad et al. [37] proposed a novel Internet of Nano-Things technology to achieve perfect disease prediction. Moreover, this technology was utilized in several medical applications such as the bio-therapeutic and internal body sensing fields.

Abualigah and Mohammad Qasim [38] proposed a krill herd algorithm for the clustering of text data for feature selection enhancement. This framework was utilized as a monitor device and smartwatch for observing the parameters and selecting the features of data from the patients. Moreover, the proposed approach attained better accuracy compared with existing techniques. Nevertheless, it takes more time to receive information about the patient's health condition.

Abualigah, Laith and Ali Diabat [39] developed hybrid optimization algorithms to overcome task-scheduling problems based on cloud computing systems. Here, an ant lion algorithm was used to minimize the local optima problems and to also improve the ability of the system. The outcomes of the proposed technique were compared with other optimization techniques.

Abualigah [40] introduced the group search optimization (GSO) technique to manage numerous optimization issues. Moreover, the common process of the GSO algorithm is to give details about fundamental versions, customized versions and separate versions. Moreover, the function of the GSO approach has more problems such as networking, benchmark application and engineering issues. The conventional methods have less accuracy and less security. Thus, the survival of patients can be affected due to the influence of faulty analysis. Hence, a novel intelligent secured HEE with GFI-GWALO strategy was proposed in this work.

3. System Model and Problem Statement

The modern cloud with an IoT-based disease prediction method utilizes IoT-based biosensors. The sensors are interconnected with the human body via wearable or inbuilt devices [41]. The collected data from the human are transferred to the cloud computing for storage, handling and predicting. The data from the cloud system are passed to the analytical tools, which means data processing and classification of the disease prediction and severity risk level of the affected person [42]. Throughout this chain, outside unauthorized attackers can hack the data of patients.

Therefore, an accurate prediction is affected by this lack of data security and leads to incorrect medical support. This increases the prediction time, potency and the cost of medical treatments [43]. Moreover, the improper cataloging of disease and severity analysis of a conventional classifier can cause faulty prediction. Errors from traditional methods are high, and this affects the accuracy along with sensitivity of the system [44]. These reasons inspired this research to design an improved healthcare support system with the base of worthy security and best classification by means of a novel hybridization technique. Consequently, this enhances the scope of ordinary healthcare support and helps the affected patients and medical experts more effectively. Conventional health support methods only forecast the chance of individual disease. Thus, the main scope of this research was to develop a new hybrid encryption technique to protect patients' data from

attackers by proposing the hybridization of a novel classifier based on neuro-fuzzy and optimization, achieving higher precision in disease prediction.

4. Proposed HEE with GFI-GWALO

Initially, IoT-based biosensors collect significant human body parameters such as blood sugar, pressure, heart rate, respiratory, temperature, etc., from an area of the population and provide them to the cloud storage for handling, storage, etc. Consequently, the UCI dataset and other medical records were considered for data testing purposes. However, while sending the data for health monitoring, the attackers may hack the data of a large number of people. Therefore, a novel HEE security encryption method was developed for securing the data from hackers by ciphering the plain text from the cloud for removing the unwanted data and normalizing the featured data. Consequently, the featured data were entered into the proposed novel GFI-GWALO classifier for disease estimation and severity prediction. Various types of diseases are predicted such as heart disease, hypertension, high cholesterol, kidney failure and diabetes. Moreover, the severity level of the disease is categorized into normal, low and high. If the people are affected by the diseases, then the warning message is provided via email or SMS. Then, the people can seek medical advice from the hospital. Consequently, performance evaluation was analyzed for the best performance of the healthcare system. The advanced medical support system covers the cloud with IoT-based disease diagnosis for remote and urban areas.

Numerous IoT-based biosensors were connected to different people. The sensors can collect the person's glucose level in the blood, heartbeat rate, blood pressure, temperature, cholesterol, respiratory rate, etc. These collected data from the people are gathered and stored in cloud data storage. In this cloud storage system, the different types of data are collected in the cloud unit. Moreover, the affected person's data are protected by a novel HEE security method. Here, a novel GFI-GWALO-based classification method was proposed for classifying the predicted disease and severity level of the illness.

4.1. Dataset Collection

This research used four categories of data—cholesterol, glucose level, blood pressure and heart rate—to obtain the disease diagnosis. Initially, the data from the IoT-based biosensors were recorded and compared with the actual data along with medical data. Moreover, the UCI data source and the hospital medical data were used for mapping with the real data. In the cloud storage, the data were stored, which involved mobile networks for the disease prediction system. Moreover, from the Kaggle site (available at https://www.kaggle.com/nareshbhat/health-care-data-set-on-heart-attack-possibility; accessed on 28 December 2020), the dataset was obtained, and different respiratory system diagnoses were collected and stored in the cloud.

4.2. HEE for Cloud Security

In general, IoT-based healthcare systems collect as much patient data as possible from sensors and store them in the cloud. The cloud storage stores the details of patients and their backgrounds, etc. However, if the storage system has a lack of security, the details of patients can be hacked by attackers. This leads to a faulty diagnosis of disease, and the hackers may blackmail the patients about the information. For this reason, a proper efficient security method was developed based on the hybridization approach. In this research, an HEE-based security encryption method was proposed, which is based on the combination of elapid and multiplication models. Therefore, the data from the cloud are encrypted for the next level to avoid hacking and unlicensed users.

The data from the cloud are represented as y_i^j, d_k, r. Where y_i^j are the affected people, d_k is the particular disease of patients, r is the data-handling round number, and j is the overall symptoms. Consequently, G is the plain text key, and b is the affine transformation sequences of encryption as well as decryption. These data are encrypted by HEE for

security enhancement. The algorithm of secure HEE in IoT-enabled disease prediction is demonstrated in Algorithm 1.

Algorithm 1. HEE for security.

int y_i^j, d_k

$y_i^j, d_k \rightarrow r$ for 128-bit keys — *// r is the data handling round number; where r=10*

Key collaborating

$G \vee y_i^j, d_k$

$G \rightarrow$ 128-bit key plain text — *// XOR-ed with four keys* $y_i^j, d_k \rightarrow 128bit$

Rijndael S-Box — *// multiplication model*

$G \rightarrow 4\ AND\ 32\ bit$ — *// 128-bit plain data are allocated into four shares of 32 bits*

Affine transformation

$$b = y_i^j, d_k \oplus \left(y_i^j, d_k <<< 1\right) \oplus \left(y_i^j, d_k <<< 2\right) \oplus \left(y_i^j, d_k <<< 3\right) \oplus \left(y_i^j, d_k <<< 4\right) \oplus G$$

// summation of numerous cycles of the byte as a trajectory

$\oplus$, bitwise XOR operative; b, multiplicative inverse; $<<<$, left bitwise circular move

Equivalent transformation

$$b = y_i^j, d_k \oplus \left(y_i^j, d_{k(i+1)}\right)_{\text{mod8}} \oplus \left(y_i^j, d_{k(i+1)}\right)_{\text{mod8}} \oplus \left(y_i^j, d_{k(i+1)}\right)_{\text{mod8}} \oplus \left(y_i^j, d_{k(i+1)}\right)_{\text{mod8}} \oplus G$$

Encrypted $\rightarrow$ 128-bit cyber text

Encryption **stop**

Decryption $\rightarrow$ Inverse the transform

Estimate the encrypted key value

Inverse affine transformation

$$b = \left(y_i^j, d_k <<< 1\right) \oplus \left(y_i^j, d_k <<< 3\right) \oplus \left(y_i^j, d_k <<< 6\right) \oplus G$$

// decryption

Key mingling $\rightarrow$ Plain text

4.3. Pre-Processing

The pre-processing of data is performed for the removal of unwanted data, exchanging missing features along with normalization. The unwanted data from the group are removed, which diminishes the size of the data. Consequently, the missing features are replaced by the mean estimation using Equation (1).

$$m_f = \sum_{i=1}^{T} \frac{b_n}{t} \tag{1}$$

where the missing features are denoted as m_f, t is the time taken for processing, and the overall feature count is denoted as b_n. Moreover, normalization is executed to normalize the raw data, which is in the range of 0 to 1.

4.4. Proposed GFI-GWALO Classifier

The proposed disease prediction classifier is the hybridization of novel advanced intelligent neuro-fuzzy along with the gray wolf and ant lion algorithm. These algorithms were combined due to their significant advantages. The neuro-fuzzy method has comprehensible and returnable characteristics of knowledge, and thus it effectively trained the patient data. Moreover, the gray wolf technique significantly contributes to the competitive consequences and supreme performance which improves the accurate prediction of diseases. Consequently, the ant lion algorithm has the features of fast computation and high efficiency, and characteristics are provided for the risk-level prediction of the disease. Therefore, due to the advanced significant merits, this neuro-fuzzy along with the gray wolf and ant lion algorithm were combined in this work. The problem with the proposed secured HEE with GFI-GWALO disease monitoring is illustrated in Figure 1, and

its algorithm is explained in Algorithm 2. Initially, the collected data from the IoT-based biosensors are given as the input of the GFI-GWALO algorithm.

Algorithm 2. GFI-GWALO classifier

Input: Normalized data (Pre-processed data)
Begin
Initialize the feature data and convergence
Stage 2 $\rightarrow \alpha_{aN,aL,aH}(m)$ // *feature condition normal, low and high*

$$\alpha_{aN,aL,aH}(m) = \begin{cases} 1 - |m - r|/aL & m \in [Low] \\ 1 - |m - r/aH| & m \in [High] \\ 0 & m \in [Normal] \end{cases} \quad // \textit{ actual data}$$

weight
if
$\theta_c = \frac{\sum_k \alpha_k a^{-h\alpha_k}}{\sum_k a^{-h\alpha_k}}$ // *differential softmin-rule-based operation*
Learning parameter applied
end if
${\alpha^{-1}}_{aN,aL,aH}(\theta_c) \rightarrow$ Collected data and actual data mapping
while $\{ z : \mu_w(z) \geq \omega_\tau \}$ **do**
$\mu_w^{-1}(\omega_\tau)$ // *infrequent data removed*
Estimate ψ_a for disease prediction outcome
Calculate P for predicted diseases data // *rule asset weights*
Arrange the predicted data arbitrarily using $D(x)$
Severity prediction:
Predicted data are stored in D_P
Corresponding objective function D_s
Threshold estimation:

$$H_1 = H_\beta - V_1 \cdot M_\beta \text{ // } \textit{high risk}$$
$$L_1 = H_\gamma - V_2 \cdot M_\gamma \text{ // } \textit{low risk}$$
$$N_1 = H_\phi - V_3 \cdot M_\phi \text{ // } \textit{medium risk}$$

Condition for severity risk level from the predicted data
$D_p = D_s$
if $f(D_s) > f(D_p)$
Condition satisfied **stop**
else Repeat the process
end if
Output: Disease prediction and severity analysis (normal, low and high)

The input such as the person's gender, age, respiratory rate, heartbeat rate, overall cholesterol, high along with low cholesterol rate, systolic and diastolic blood pressure rate, temperature and the possibility of diseases is identified. Then, the input data are provided for finding the possible values. The three conditions are taken for each feature such as normal, low and high. The function of this layer is defined by Equation (2) as

$$\alpha_{aN,aL,aH}(m) \tag{2}$$

where aN, aL and aH are the normal, low and high expansion of the fuzzy system of actual data a, and m is the function of data. The smooth triangular membership function is applied in this stage using Equation (3).

$$\alpha_{aN,aL,aH}(m) = \begin{cases} 1 - |m - r|/aL & m \in [Low] \\ 1 - |m - r/aH| & m \in [High] \\ 0 & m \in [Normal] \end{cases} \tag{3}$$

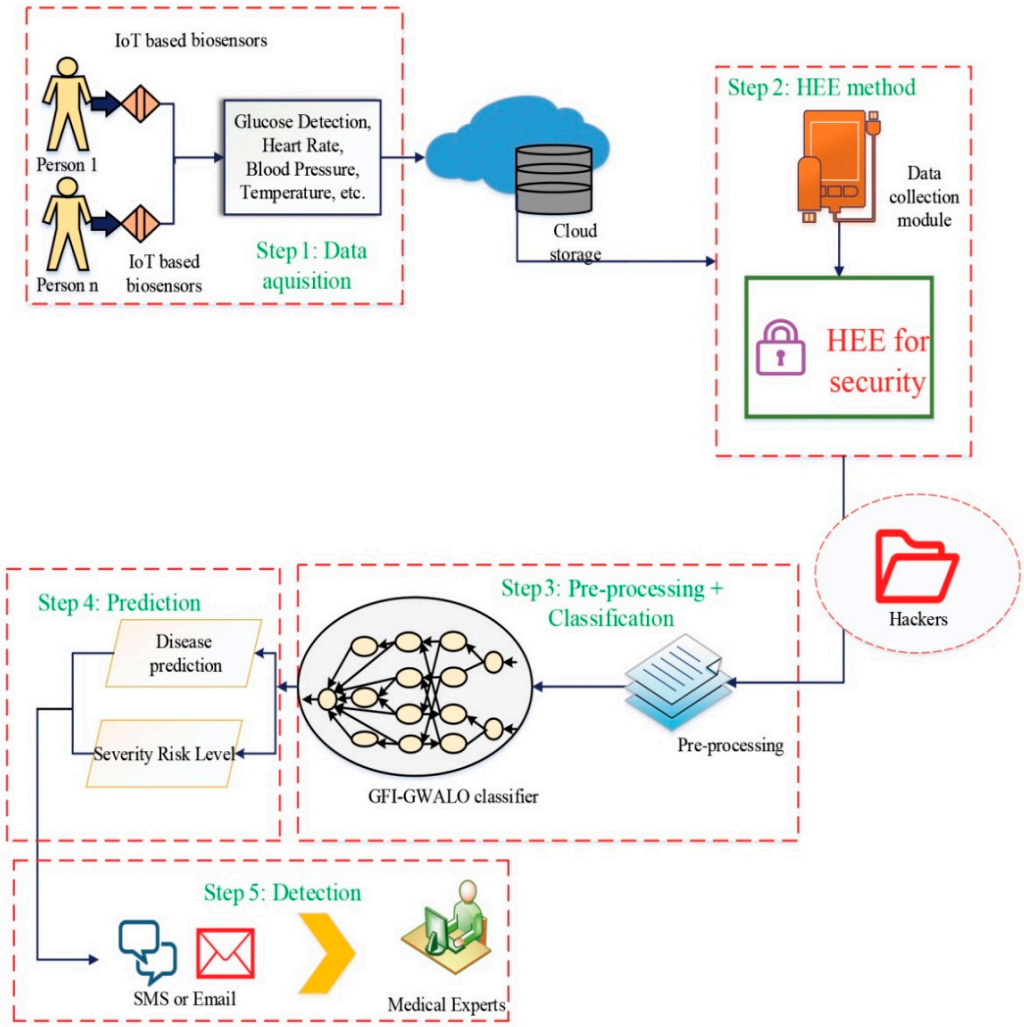

Figure 1. Problem with proposed solution.

The weights of the input actual data are considered in this layer using Equation (3). Moreover, the output from the previous layer is fed to the third phase, and the process is validated on the basis of if condition. The differential softmin-rule-based operation is applied in the phase using Equation (4):

$$\theta_c = \frac{\sum_k \alpha_k a^{-h\alpha_k}}{\sum_k a^{-h\alpha_k}} \tag{4}$$

where the relationship between the fuzzy point and the condition k is denoted as α_k. The softmin smoothening function can be regulated by h. Moreover, the gradient descent strategy is applied for the learning improvement of the classifier training parameters. The training of the data is carried out based on the reference data and the collected data. The output of predicted data is suggested by the condition k. Therefore, the mapping of collected data and the actual data are computed by Equation (5).

$$\alpha^{-1}{}_{aN,aL,aH}(\theta_c) \tag{5}$$

The inverse function is considered for the applicable output from the data to a single rule. The degree of θ_c is satisfied, and the rule k condition is expressed by the coordination of the expression in Equation (6).

$$\alpha_k^{-1}(\theta_c) \text{ While } \{ m : \alpha_k(m) \geq \theta_c \} \tag{6}$$

The infrequent feature of a healthcare unit is removed in this stage, and all the rules are provided at this level. This creates the consistent output that is given to the next phase. Consequently, for the triangular process, the exact values are provided in the computation of Equation (7).

$$\psi_a = \left(aN + \left(\frac{aH - aL}{2}\right)\right)\left(\sum_k \theta_k\right) - \left(\frac{aH - aL}{2}\right)\left(\sum_k \theta_k^2\right) \tag{7}$$

where θ_k is the trained data degree. The predicted disease outcomes are obtained from all the stages of rule using the resulting overall weight. The rule asset weights are estimated by Equation (8).

$$P = \frac{\sum\limits_k \theta_k \alpha^{-1}(\theta_k)}{\sum\limits_k \theta_k} \tag{8}$$

The proposed GFI-GWALO classifier flow chart is represented in Figure 2. The predicted disease data are provided to the hybrid gray wolf and ant lion optimization for disease severity analysis. Initially, the data are arranged arbitrarily using Equation (9).

$$D(x) = [0, g(2s(x_1) - 1, g(2s(x_2 - 1, \ldots, g2s(x_2) - 1] \tag{9}$$

where the stochastic feature is denoted as $s(x)$. The predicted trained featured data position is stored in the matrix form using Equation (10).

$$D_P = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdot & g_{1,i} \\ g_{2,1} & g_{2,2} & \cdot & g_{2,}i \\ \cdot & \cdot & \cdot & \cdot \\ g_{i,1} & g_{i,2} & \cdot & g_{i,i} \end{bmatrix} \tag{10}$$

where the predicted data are stored in D_P, $B_{1.i}$ specifies the value of the first variable of i^{th} data, $g_{i,i}$ is the group of i^{th} data, and n is the number of feature data. The corresponding data are computed by Equation (11).

$$D_s = \begin{bmatrix} d[g_{1,1} & g_{1,2} & \cdot & g_{1,i}] \\ d[g_{2,1} & g_{2,2} & \cdot & g_{2,}i] \\ \cdot & \cdot & \cdot & \cdot \\ d[g_{i,1} & g_{i,2} & \cdot & g_{i,i}] \end{bmatrix} \tag{11}$$

Moreover, the threshold value is estimated for severity analysis using Equations (12)–(14) as:

$$H_1 = H_\beta - V_1 \cdot M_\beta \tag{12}$$

$$L_1 = H_\gamma - V_2 \cdot M_\gamma \tag{13}$$

$$N_1 = H_\phi - V_3 \cdot M_\phi \tag{14}$$

where H_1, L_1 and N_1 are the high risk, low risk and normal, M is the predicted data symptom, and V is the vector. Moreover β, γ, and φ are the search agents. From that, the predicted data symptom is estimated by Equation (15).

$$M_\beta = C_1.H_\beta - H,\ M_\gamma = C_2.H_\gamma - H,\ M_\phi = C_3.H_\phi - H \tag{15}$$

where the vectors of V and C are estimated for the position of data. The vectors are calculated by Equations (16) and (17) as:

$$V = D_p + V_t \tag{16}$$

$$C = D_p + C_t \tag{17}$$

where t is the present iteration, and D_p is the predicted data. The condition for the severity risk level evaluation uses the rule in Equation (18) as:

$$D_p = D_s; \ldots \textbf{ if } f(D_s) > f(D_p) \tag{18}$$

where D_s is the corresponding objective data. The predicted severity estimated value is considered for the normal-, high- and low-state severity of the disease. If the severity and the affected person's disease are predicted, then the warning signal is provided to the patient who can seek the advice of medical practitioners.

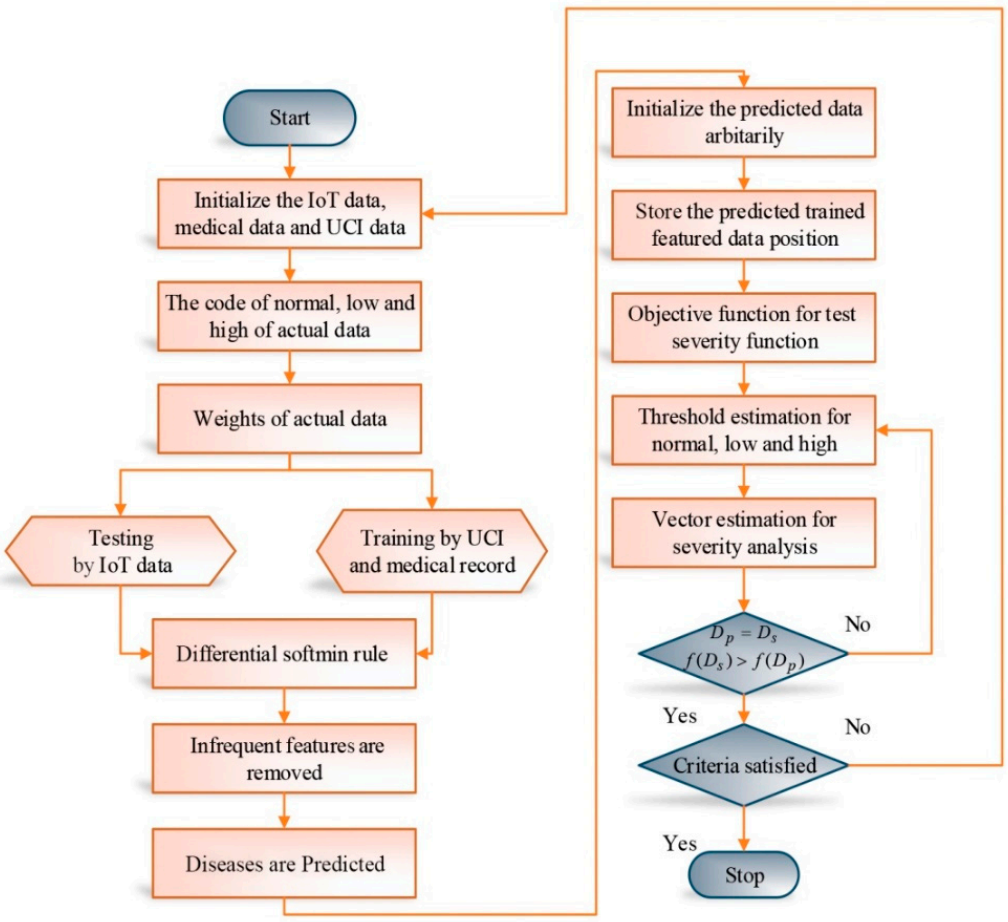

Figure 2. The flowchart of the proposed GFI-GWALO classifier.

The health monitoring stages of the proposed cloud with the IoT-based HEE and GFI-GWALO method for healthcare systems are illustrated in Figure 3. In the health monitoring stages, the unwanted data are removed which normalizes the data. After pre-processing, the proposed technique is implemented to predict and analyze the severity level of the disease. Then it sends messages to the patient to seek medical support.

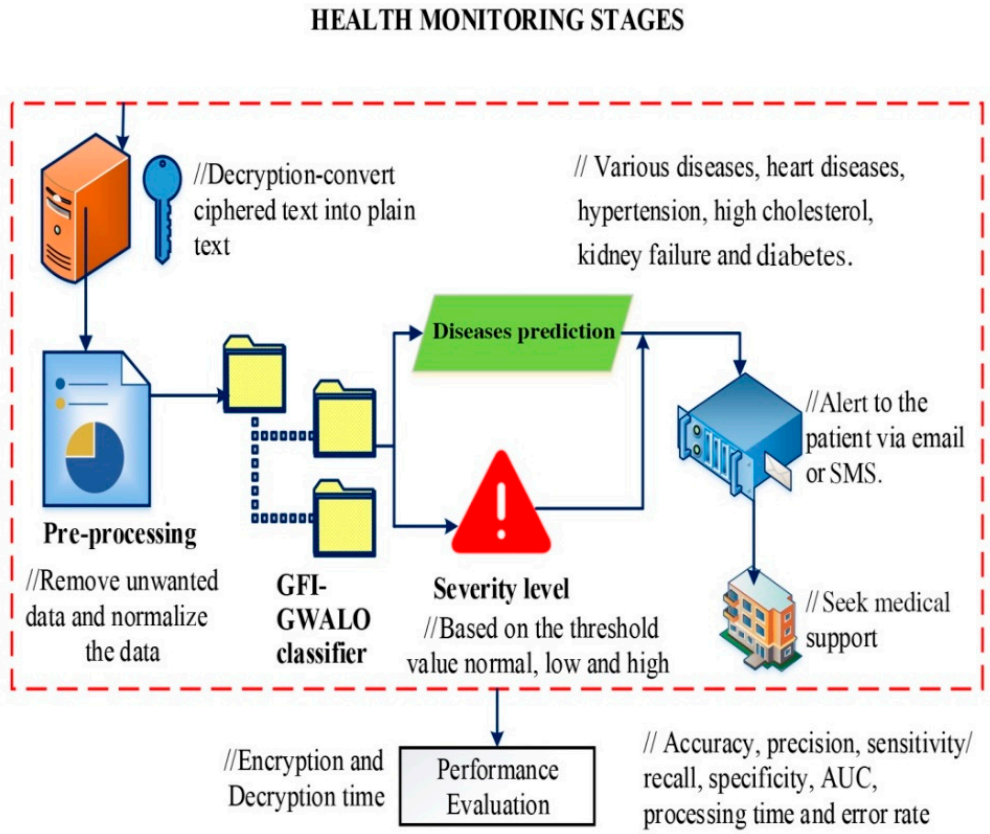

Figure 3. Health monitoring stages of the proposed method.

5. Result and Discussion

In this section, the efficiency of the proposed cloud with IoT-based HEE and GFI-GWALO is simulated in the MATLAB R2018b platform, Windows 7 operating system running 64 bit with an Intel 5 processor and 4 GB RAM. Moreover, computation metrics such as specificity, sensitivity, precision, recall, etc., are utilized to evaluate the accuracy of prediction. To determine the effectiveness of the proposed scheme, the metrics were compared with other existing schemes.

5.1. Case of Study

We consider R as a remote area with a population of 250 since the datasheet selected for the evaluation has 250 inhabitants. From that, the IoT-based sensors are placed to the human body and collect the body parameters from various people. The collected data are sent to the cloud storage system for handling, storing and monitoring the affected people. In the input, the data handling round number is considered as 10. Therefore, the plain text key of 128 bits takes 10 rounds. Moreover, the XOR function is applied to split the 128-bit plain data into four sections of keys. The Rijndael S-Box is applied in the elapid encryption for the association of the multiplication model. The four sections of the key are multiplied (AND) with a 32-bit key for 128 bits of plain text. Consequently, the affine transformation is applied for the security purpose in encryption, and the equivalent transformation encrypts the data into 128-bit cyber text. The encrypted data are sent to the health monitoring arrangement. After reaching the healthcare management, the data are decrypted by the HEE method. In pre-processing, unusual data are removed, the missing features are estimated by Equation (1), and m_f is obtained as 3.

The remaining data collected from the people are name, age, gender, both systolic and diastolic blood pressure, blood sugar level, low, high and overall cholesterol rate, body temperature and the possible diseases. The connected IoT sensors collected the body parameters of both males and females. The age of the IoT-sensor-connected person is

categorized into four groups. Moreover, the features of collected data are categorized based on their severity such as normal, low and high. The outputs of possible diseases are classified as heart disease, hypertension, high cholesterol, kidney failure and diabetes. The risk features and their encoded value consideration are demonstrated in Table 1.

Table 1. Risk features and codes.

S. No	Risk Features	Standard Range and Codes
1	Gender	Male (1), Female (2)
2	Age	15–35 (1), 36–55 (2), 56–75 (3) and >76 (4)
3	Heart rate (h)	60–100 beats/min, normal (1); >60–100 beats/min high (2); and <60–100 beats/min, low (3)
4	Respiratory rate (r)	12–18 breaths/min, normal (1); <12–18 breaths/min high (2); and >12–18 breaths/min low (3)
5	Diastolic blood pressure (dbp)	60–90 mmHg, normal (1); >60–90 mmHg, high (2); and <60–90 mmHg, low (3)
6	Systolic blood pressure (sbp)	90–120 mmHg, normal (1); >90–120 mmHg, high (2); and <90–120 mmHg, low (3)
7	LDL cholesterol (lc)	100–129 mg/dL, normal (1) and >129 mg/dL, high (1)
8	HDL cholesterol (hc)	41–59 mg/dL, normal (0) and >59 mg/dL, high (1)
9	Overall cholesterol (oc)	200 mg/dL, normal (0) and >200 mg/dL, high (1)
10	Body temperature (bt)	97–99 F, normal (0) and >99 F, high (1)
11	Output (possible diseases)	Heart disease (1); hypertension (2); high cholesterol (3); kidney failure (4) and diabetes (5)

Moreover, the triangular membership smooth function is evaluated by Equation (3) and achieved as in Equation (19).

$$\alpha_{aN,aL,aH}(250) = \begin{cases} 1 - |250 - r|/3 & 250 \in [3] \\ 1 - |250 - r|/2 & 250 \in [2] \\ 0 & 250 \in [1] \end{cases} \quad (19)$$

The encoded values from the feature data are compared for the trained data with tested data. The observation of data shows that when the iteration level increases, then the GFI-GWALO classifier training error level slopes down and enhances the GFI-GWALO classifier test accuracy rate. Consequently, the GFI-GWALO model training stage is stable at the 60th iteration, and the GFI-GWALO test process is steady after 70 iterations. Therefore, the number of iterations is set to be 70. Moreover, the training performance is shown in Figure 4.

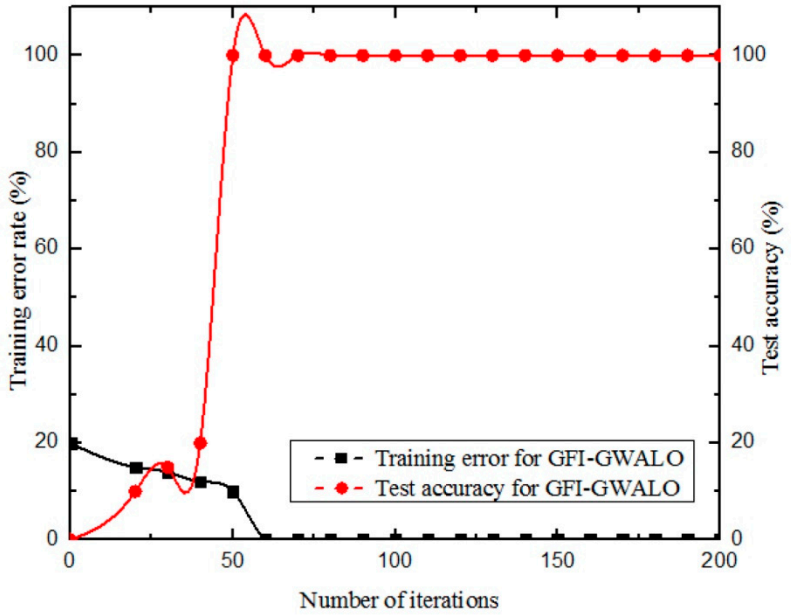

Figure 4. Training performance.

The consistent output was obtained using Equation (7), and the considered value was $\sum_k \theta_k = 2$; after the value substitution, the predicted output is obtained by Equation (20).

$$\psi_a = \left(1 + \left(\frac{3-2}{2}\right)\right)(2) - \left(\frac{3-2}{2}\right)(4) = 1 \tag{20}$$

Based on the featured value variation, the consistent diseases are predicted. Mainly, the overall weights of predicted disease are estimated by Equation (8) and achieved by Equation (21).

$$P = \frac{\sum_{11} 2\alpha^{-1}(2)}{\sum_{11} 2} = 15 \tag{21}$$

The predicted disease data are arranged arbitrarily and the stored data value obtained in Equation (10) is expressed in Equation (22) as:

$$D_P = \begin{bmatrix} 1 & 5 & . & 2 \\ 3 & 4 & . & 5 \\ . & . & . & . \\ 2 & 1 & . & 3 \end{bmatrix} \tag{22}$$

Moreover, the severity threshold value is estimated using Equations (12)–(14) and is obtained in Equations (23)–(25) as:

$$H_1 = 7 - 1 \times 4 = 3 \tag{23}$$

$$L_1 = 5 - 3 \times 1 = 2 \tag{24}$$

$$N_1 = 3 - 1 \times 2 = 1 \tag{25}$$

The rule-based condition value of severity is estimated in Equation (18) for disease prediction. After the severity level is obtained, the alert will be sent to the person who is affected by critical diseases such as heart disease, hypertension, high cholesterol, kidney failure and diabetes.

5.2. Performance Evaluation

The efficiency of the proposed security-enhanced cloud with IoT-based HEE and GFI-GWALO is validated by the performance evaluation in terms of encryption time, decryption time, security analysis, accuracy, specificity, sensitivity, precision, area of curve (AoC),

recall, misclassification and error percentage. The proposed secured method efficiency is compared with various conventional methods such as DE-KS with OKM-ANFIS [25], PSO with DNN [26], MKSVM-MWO [27], LR-NN [28] and MDCNN [45].

5.2.1. Encryption Time

The time taken to encrypt the plain text to ciphered text is calculated for the proposed HEE, and this is compared with the existing techniques of MKSVM-MWO [27] and DK-AES [25], which is shown in Figure 5.

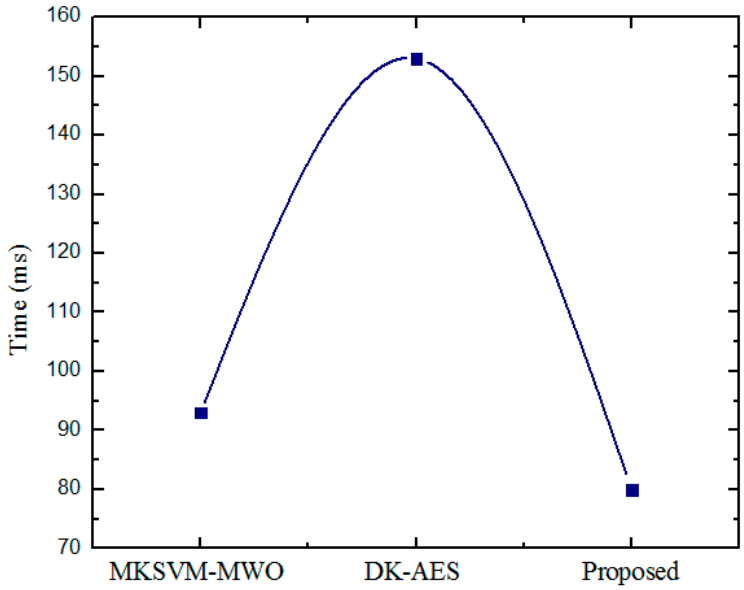

Figure 5. Encryption time comparison.

The conventional MKSVM-MWO achieved 93 ms, and DK-AES achieved 153 ms. However, the proposed HEE method achieved 80 ms; compared to other methods, the proposed method took less time.

5.2.2. Decryption Time

Consequently, the time taken for the decryption of the ciphered text into plain text is calculated for the proposed HEE, and this is compared with the existing techniques of MKSVM-MWO and DK-AES as shown in Figure 6.

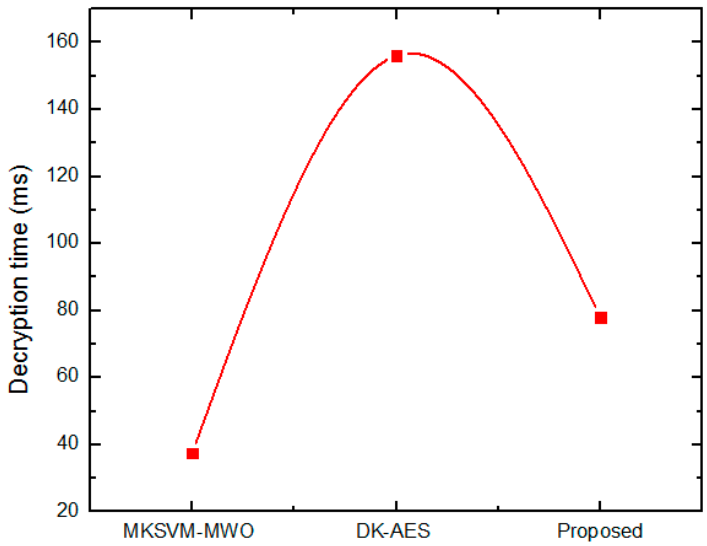

Figure 6. Decryption time comparison.

The conventional MKSVM-MWO achieved 37.458 ms, and DK-AES achieved 156 ms. However, the proposed HEE method achieved 78 ms; compared to other methods, the proposed method took less time. The present research attained the best accuracy and reduced encryption time. However, the main drawback of this model is maximum decryption time, which will be addressed in the future. This happened because of high security and more encryption procedures, and thus it took more time to decrypt the data.

5.2.3. Sensitivity and Recall

In primary disease prediction, both sensitivity and recall are necessary because the function of both recall and sensitivity metrics are similar. Both these metrics have the ability to estimate the risk level of numerous diseases in a patient. The performance metrics were evaluated based on the following parameters: the true negative (P_{tn}), true positive (P_{tp}), false negative (P_{fn}) and false positive (P_{fp}) of the system.

Moreover, sensitivity specifies the number of specific positives and was classified suitably as optimistic, which is evaluated by Equation (26).

$$\text{Sensitivity} = \frac{P_{tp}}{P_{tp} + P_{fn}} = 100 \tag{26}$$

The proposed secured HEE with GFI-GWALO sensitivity/recall is compared with the conventional DE-KS with OKM-ANFIS, PSO with DNN, LR-NN and MDCNN, which is shown in Figure 7.

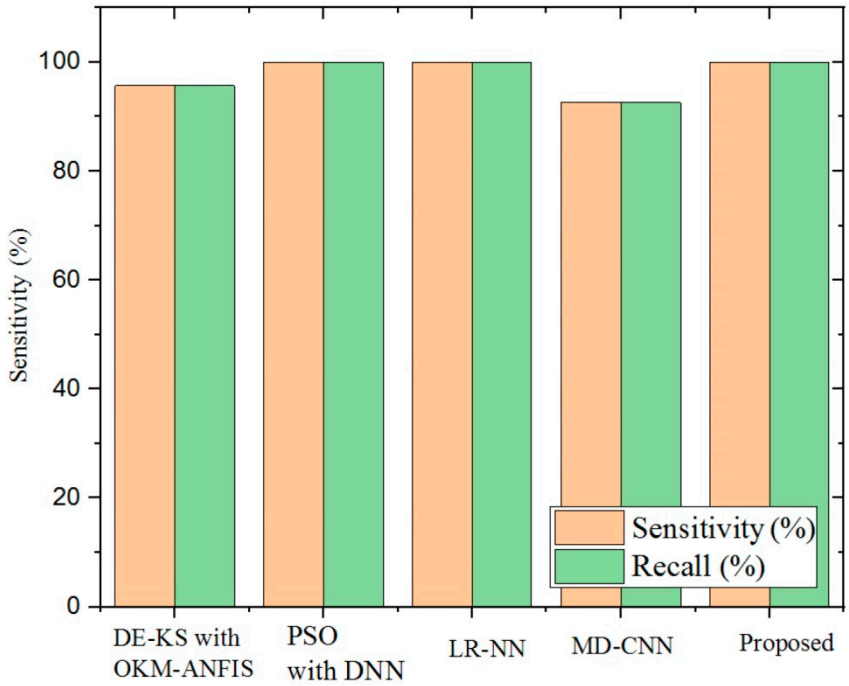

Figure 7. Comparison of sensitivity and recall with existing methods.

The sensitivity value of the conventional DE-KS with OKM-ANFIS (95.7%), PSO with DNN (99.99%), LR-NN (99.97%) and MDCNN (92.6%) was obtained. However, the proposed HEE with GFI-GWALO has 100% sensitivity. Moreover, the recall and sensitivity have the same estimation. Thus, the outcomes show that the proposed method sensitivity/recall is higher than the other prediction method, which is detailed in Table 2.

Table 2. Comparison of sensitivity/recall and specificity.

Methods	Sensitivity	Recall
DE-KS with OKM-ANFIS	95.7	95.7
PSO with DNN	99.99	99.99
LR-NN	99.97	99.97
MDCNN	92.6	92.6
Proposed (HEE with GFI-GWALO)	100	100

5.2.4. Specificity

Specificity states the number of specific negatives and was classified suitably as an undesirable rate, which is evaluated by Equation (27).

$$\text{Specificity} = \frac{P_{tn}}{P_{tn} + P_{fp}} = 99.98 \quad (27)$$

Moreover, the specificity value of the conventional DE-KS with OKM-ANFIS (94.2%), PSO with DNN (98.03%), LR-NN (99%) and MDCNN (91.3%) was obtained. However, the proposed HEE with GFI-GWALO has 99.98 % specificity. Moreover, a comparison of specificity is shown in Figure 8 and Table 3.

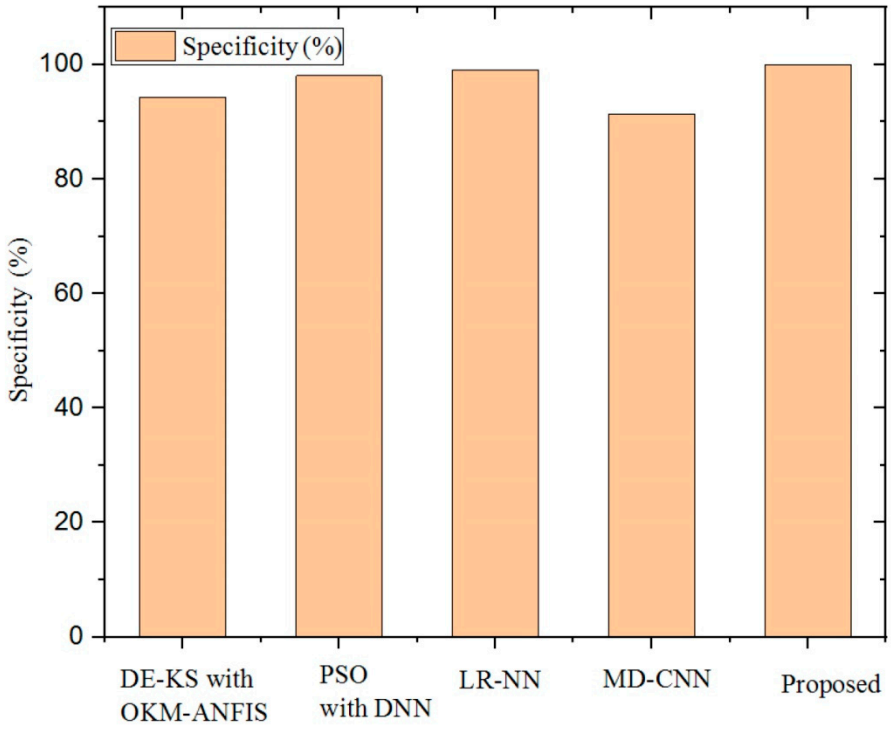

Figure 8. Comparison of specificity with existing methods.

Table 3. Comparison of specificity with existing methods.

Methods	Specificity
DE-KS with OKM-ANFIS	94.2
PSO with DNN	98.03
LR-NN	99
MDCNN	91.3
Proposed (HEE with GFI-GWALO)	99.98

5.2.5. Precision

Precision is another important metric for the performance estimation of proposed secured healthcare monitoring. This is estimated by the ratio of specific forecast positive disease to the total forecast positive disease, expressed by Equation (28).

$$\text{Precision} = \frac{P_{tp}}{P_{tp} + P_{fp}} = 99.86 \tag{28}$$

The precision value of the proposed HEE with GFI-GWALO (99.50%) is compared with the conventional DE-KS with OKM-ANFIS (95.7%), PSO with DNN (99.25%), LR-NN (96.2%) and MDCNN (95.1%), which is illustrated in Figure 9.

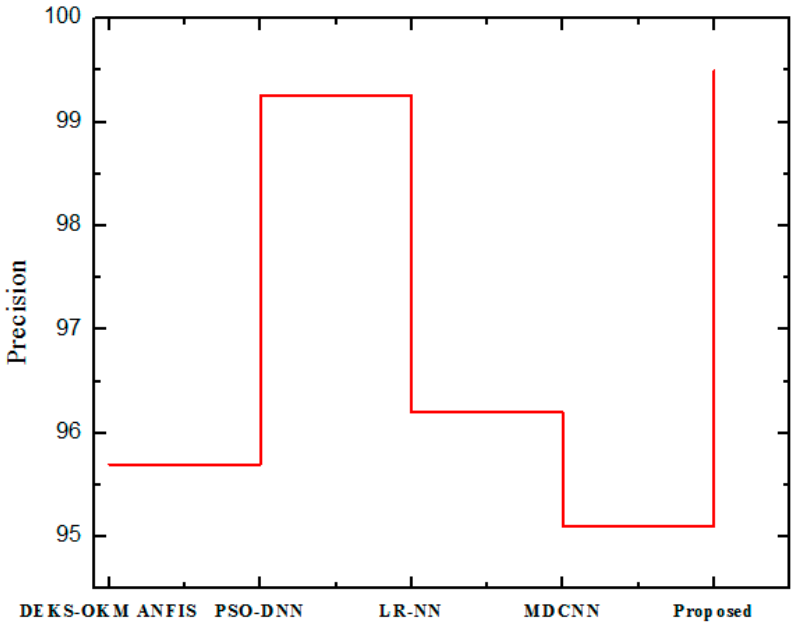

Figure 9. Comparison of precision with other techniques.

Furthermore, the comparison of estimated precision with existing methods is detailed in Table 4. The table shows that the traditional methods have less precision when compared with the proposed HEE with GFI-GWALO secured method.

Table 4. Comparison of precision.

Methods	Precision
DE-KS with OKM-ANFIS	95.7
PSO with DNN	99.25
LR-NN	96.2
MDCNN	95.1
Proposed (HEE with GFI-GWALO)	99.50

5.2.6. Accuracy

Accuracy is a significant parameter for the estimation of classification performance. It characterizes the percentage of exactly classified diseases and is denoted by percentage (%). When the accuracy reaches 100%, then the classification is considered the best. The computation of accuracy is in Equation (29).

$$\text{Accuracy} = \frac{P_{tp} + P_{tn}}{P_{tp} + P_{tn} + P_{fp} + P_{fn}} = 100 \tag{29}$$

The accuracy value of the proposed HEE with GFI-GWALO (100%) is compared with the conventional DE-KS with OKM-ANFIS (94%), PSO with DNN (98.03%), LR-NN (97.8%) and MDCNN (98.2%), which is shown in Figure 10.

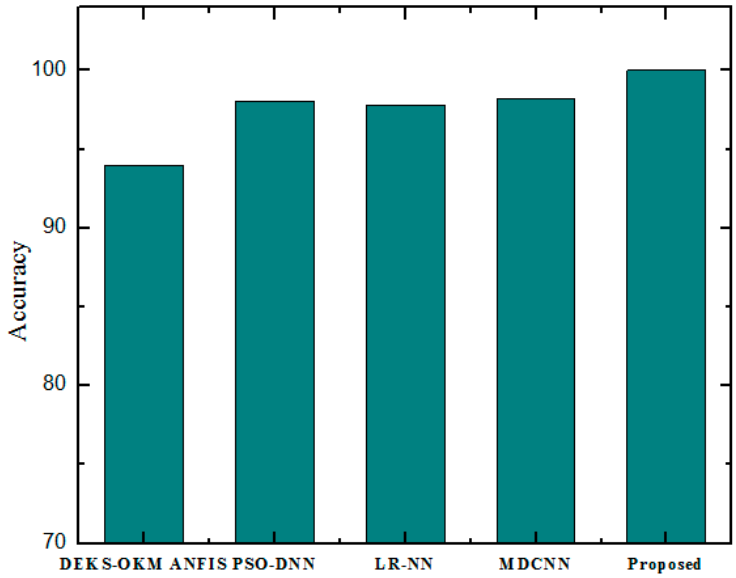

Figure 10. Comparison of accuracy with other techniques.

The accuracy of the proposed disease forecast obtains higher accuracy than other existing methods. The detailed values are shown in Table 5.

Table 5. Comparison of accuracy.

Methods	Accuracy
DE-KS with OKM-ANFIS	94
PSO with DNN	98.03
LR-NN	97.8
MDCNN	98.2
Proposed (HEE with GFI-GWALO)	100

5.2.7. F-Measure

The F-measure parameter is represented as the average weight of recall and precision, and the value is calculated by Equation (30).

$$\mathrm{F-Measure} = \frac{2P_{tp}}{2P_{tp} + P_{fp} + P_{fn}} = 99 \tag{30}$$

The F-measure value of the proposed HEE with GFI-GWALO (99%) is compared with the conventional DE-KS with OKM-ANFIS (97.8%), PSO with DNN (99.39%), LR-NN (98.1%) and MDCNN (95%), which is illustrated in Figure 11. This shows that the HEE with GFI-GWALO achieved a higher F-measure than existing methods and is detailed in Table 6.

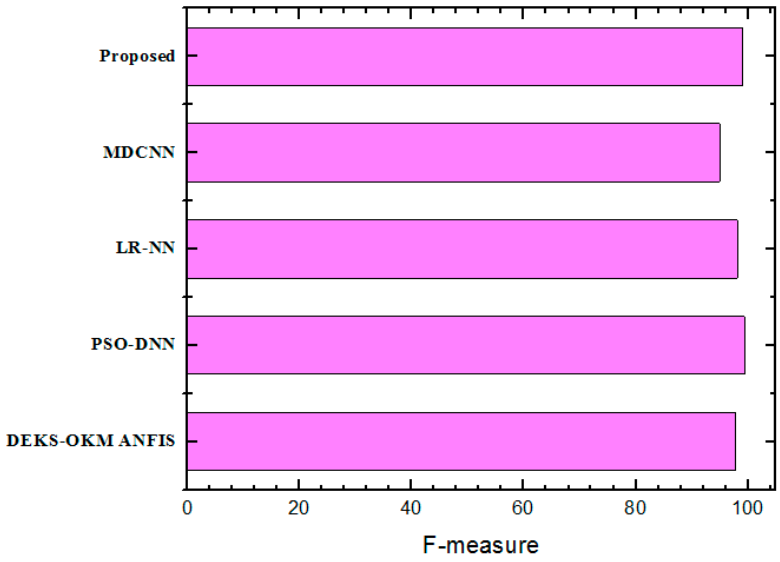

Figure 11. Comparison of F-measure with other techniques.

Table 6. Comparison of F-measure.

Methods	F-Measure
DE-KS with OKM-ANFIS	97.8
PSO with DNN	99.39
LR-NN	98.1
MDCNN	95
Proposed (HEE with GFI-GWALO)	99

5.2.8. Area under Curve (AUC)

The high value of the Area of curve (AOC) suggests that the proposed classifier has the best performance. Consequently, the HEE with GFI-GWALO secured classification obtained 99.05% of AUC. The obtained AUC value is better than other existing classifiers and is described in Table 7.

Table 7. Comparison of AUC.

Methods	AUC (%)
DE-KS with OKM-ANFIS	92.8
PSO with DNN	99
LR-NN	97
MDCNN	95
Proposed (HEE with GFI-GWALO)	99.05

The Area of Curve (AOC) value of the proposed HEE with GFI-GWALO (99.05%) is compared with the conventional DE-KS with OKM-ANFIS (92.8%), PSO with DNN (99%), LR-NN (97%) and MDCNN (95%), which is illustrated in Figure 12.

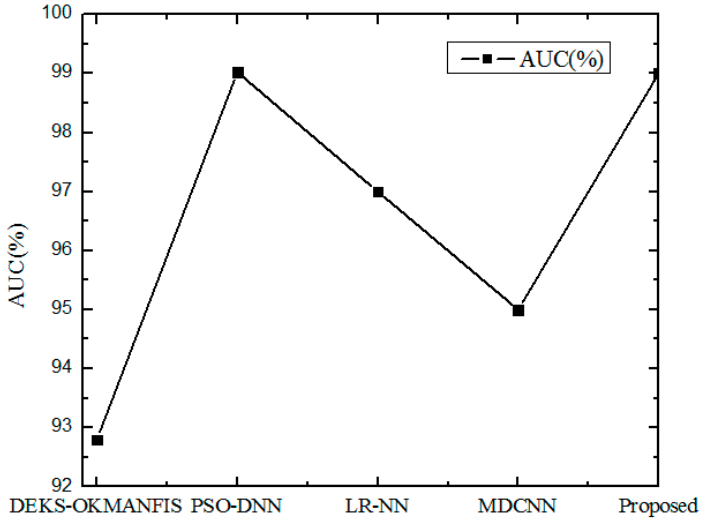

Figure 12. Comparison of AOC with other techniques.

5.2.9. Processing Time

The processing time analysis is the main part of this research because a shorter processing time is more efficient than a longer time. The achieved processing time of the proposed HEE with GFI-GWALO (50 ms) is compared with the conventional DE-KS with OKM-ANFIS (45 ms), PSO with DNN (20 ms), LR-NN (96.2%) and MDCNN (15 ms), which is shown in Figure 13 and Table 8.

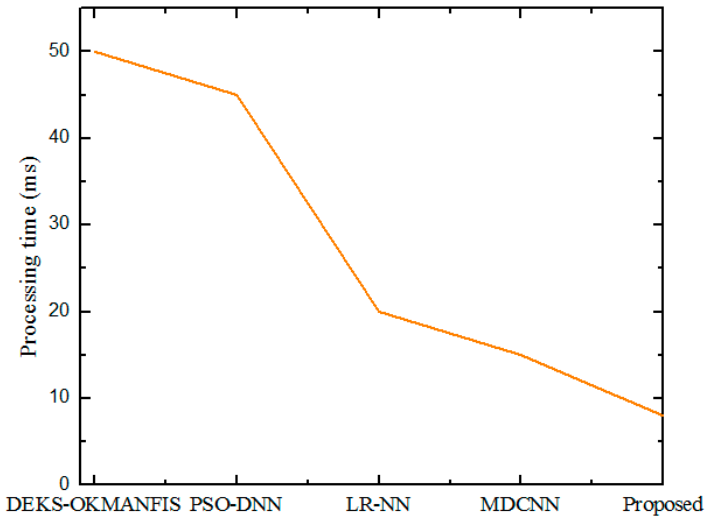

Figure 13. Comparison of processing time with other techniques.

Table 8. Comparison of processing time with existing methods.

Methods	Processing Time (ms)
DE-KS with OKM-ANFIS	50
PSO with DNN	45
LR-NN	20
MDCNN	15
Proposed (HEE with GFI-GWALO)	8

When compared with the existing DE-KS with OKM-ANFIS, PSO with DNN, LR-NN and MDCNN, the proposed HEE with GFI-GWALO took less time (8 ms). This shows the proposed method is more efficient in disease prediction.

5.2.10. Error Rate

The error rate of the proposed approach is estimated by Equation (31).

$$Error = 1 - Accuracy = 0 \quad (31)$$

The error rate of the proposed HEE with GFI-GWALO (0%) is compared with the conventional DE-KS with OKM-ANFIS (1.40%), PSO with DNN (0.98%), LR-NN (0.25%) and MDCNN (1.8%), which is illustrated in Figure 14.

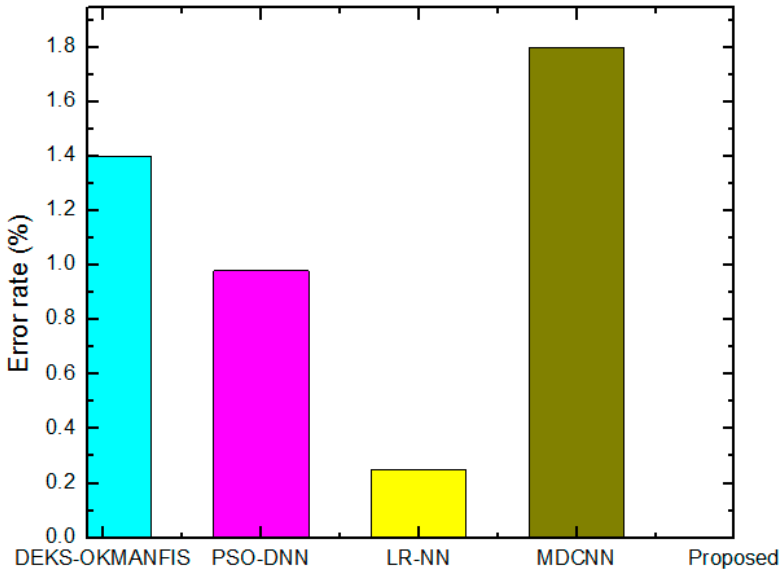

Figure 14. Comparison of error rate with other techniques.

The obtained error rate of HEE with GFI-GWALO is zero because of 100% accuracy. This comparison shows that the proposed strategy attained the best result and is described in Table 9.

Table 9. Comparison of error rate with other methods.

Methods	Error Rate
DE-KS with OKM-ANFIS	1.40
PSO with DNN	0.98
LR-NN	0.25
MDCNN	1.8
Proposed (HEE with GFI-GWALO)	0

Thus, the overall outcomes and comparison demonstrated that the projected IoT with cloud secured HEE with GFI-GWALO method achieved high sensitivity, specificity, accuracy, F-measure, high AUC and less processing time as well as a lower error rate. The confidentiality rate of the presented model is compared with existing techniques such as LMDS [45] and lightweight security scheme [46]. The comparison of the confidentiality rate is shown in Table 10.

Table 10. Comparison of confidentiality rate.

Methods	Confidentiality Rate (%)
LMDS	96
Lightweight security scheme	98
Proposed (HEE with GFI-GWALO)	99

The comparison results demonstrate that the presented model has a high confidentiality rate. Moreover, the proposed model attained a 99% confidentiality rate.

5.3. Discussion

The proposed HEE with GFI-GWALO performance was validated by the comparison with exiting state-of-the-art methods in terms of accuracy, precision, recall, F-measure, specificity, sensitivity, AOC, error rate, time of encryption and decryption and processing time. This factor of the projected method was compared with conventional methods such as DE-KS with OKM-ANFIS [25], MDCNN [45], PSO with DNN [26], MKSVM-MWO [27], LMDS [45], lightweight security scheme [46] and LR-NN [28]. The encryption and decryption time were compared with the MKSVM-MWO and DK-AES approaches. Moreover, the presented model has high encryption; the high encryption increases the security of data. Furthermore, the merits and limitations of the state-of-the-art methods are detailed in Table 11.

Table 11. Merits and limitations of state-of-the-art methods.

Reference	Methods	Advantages	Limitations
[25]	DE-KS with OKM-ANFIS	Security analysis and adaptive self-adjusted framework	Computational burden, require more knowledge of function
[45]	MDCNN	Adapts to unidentified conditions and able to function complex data	Complexity of the algorithm model is high and needs more processing time; achieved less accuracy
[27]	MKSVM-MWO	Minimized the health risk framework and secured the data significantly	The parameter achieved uncertainty and overfitting problems
[28]	LR-NN	Applicable for huge number of data and design for non-uniform data	Initialization is complex and restrictive situation of secure data
[26]	PSO with DNN	The solution attained of high quality and simple constraints	Convergence is slow and complex to find the primary parameter
[45]	LMDS	It ensures higher security and minimum computational overhead and computational time	The data delivery rate is lower
[46]	Lightweight security scheme	It ensures resiliency against jamming-based attack	The trustworthiness of nodes in network does not secure the data
[47]	Artificial intelligence (deep neural network)	It shares only classifier parameters but not private data	It fails to provide best outcome, and the processing time is high
[30]	IoT-AIS	It has high data transfer rate, delivery rate and less delay in estimation	It is not suitable in mobile-based applications
Proposed	HEE with GFI-GWALO	• The security of the data enhanced significantly with less decryption and encryption time and high confidential rate • Predicted diseases with high accuracy, precision, recall, F-measure, specificity • Fast processing rate with zero error	Real-time validation is required

The discussion shows that the proposed technique attained a lower error rate, high accuracy, precision, recall, F-measure, specificity, sensitivity, AOC and encryption and decryption time. Furthermore, the proposed model has a high confidentiality rate, and the projected HEE

with GFI-GWALO method attained superior performance over other conventional methods due to its effective security improvement and accurate disease prediction.

6. Conclusions

The proposed method provides the best possible results and also predicts assaults in the IoT fields. The proposed MATLAB simulation outcome was compared with other traditional methods in terms of encryption and decryption time and other important quantity metrics. The effective comparison showed that the proposed secured disease estimation and severity analysis attained better outcomes. Moreover, the findings of this technique are summarized below:

- The proposed HEE with GFI-GWALO attained 100% accuracy, sensitivity and recall. The proposed model secured the data and classified the diseases effectively. Thus, it attained the accuracy of 100%.
- Consequently, the proposed technique achieved zero error, 99% F-measure, 99.98% specificity and 99.50% precision rate.
- Moreover, the encryption and decryption time was reduced to 80 ms and 78 ms when compared with existing security methods.

Finally, the outcomes show that the HEE with GFI-GWALO classifier in the IoT with cloud-based disease prediction obtained the best performances in terms of its overall metrics. However, real-time validation was not achieved in this algorithm for disease prediction. Thus, in the future, a real-time experiment will be developed for the effective verification of the system performance. For further investigation in this area, the work will be developed based on new innovative algorithms with more signified parameters.

Funding: This work was supported by Dongseo University, "Dongseo Cluster Project" Research Fund of 2021 (DSU-20210004).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ferlie, E.B.; Shortell, S.M. Improving the quality of health care in the United Kingdom and the United States: A framework for change. *Milbank Q.* **2001**, *79*, 281–315. [CrossRef] [PubMed]
2. Javadi, S.S.; Razzaque, M.A. Security and privacy in wireless body area networks for health care applications. In *Wireless Networks and Security*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 165–187.
3. Farahani, B.; Firouzi, F.; Chang, V.; Badaroglu, M.; Constant, N.; Mankodiya, K. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Gener. Comput. Syst.* **2018**, *78*, 659–676. [CrossRef]
4. Díaz, M.; Martín, C.; Rubio, B. State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. *J. Netw. Comput. Appl.* **2016**, *67*, 99–117. [CrossRef]
5. Ren, Y.; Werner, R.; Pazzi, N.; Boukerche, A. Monitoring patients via a secure and mobile healthcare system. *IEEE Wirel. Commun.* **2010**, *17*, 59–65. [CrossRef]
6. Giacalone, M.; Scippacercola, S. Big Data: Issues and an Overview in Some Strategic Sectors. *J. Appl. Quant. Methods* **2016**, *11*, 1–17.
7. Das, N.; Das, L.; Rautaray, S.S.; Pandey, M. Big data analytics for medical applications. *Int. J. Mod. Educ. Comput. Sci.* **2018**, *11*, 35. [CrossRef]
8. Joubert, J.; Norman, R.; Lambert, E.V.; Groenewald, P.; Schneider, M.; Bull, F.; Bradshaw, D. Estimating the burden of disease attributable to physical inactivity in South Africa in 2000. *S. Afr. Med. J.* **2007**, *97*, 725–731. [PubMed]
9. Zhang, Y.; Qiu, M.; Tsai, C.W.; Hassan, M.M.; Alamri, A. Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. *IEEE Syst. J.* **2015**, *11*, 88–95. [CrossRef]
10. Lorincz, K.; Welsh, M. Motetrack: A robust, decentralized approach to rf-based location tracking. In *International Symposium on Location-and Context-Awareness*; Springer: Berlin/Heidelberg, Germany, 2005.
11. Kotz, D. A threat taxonomy for mHealth privacy. In Proceedings of the 2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011), Bangalore, India, 4–8 January 2011.
12. Liu, X.; Lu, R.; Ma, J.; Chen, L.; Qin, B. Privacy-preserving patient-centric clinical decision support system on naive Bayesian classification. *IEEE J. Biomed. Health Inform.* **2015**, *20*, 655–668. [CrossRef]
13. Yeh, K.H. A secure IoT-based healthcare system with body sensor networks. *IEEE Access* **2016**, *4*, 10288–10299. [CrossRef]
14. Swan, M. The quantified self: Fundamental disruption in big data science and biological discovery. *Big Data* **2013**, *1*, 85–99. [CrossRef]

15. George, G.; Osinga, E.C.; Lavie, D.; Scott, B.A. Big data and data science methods for management research. *Acad. Manag. J.* **2016**, *59*, 1493–1507. [CrossRef]
16. Kononenko, I. Machine learning for medical diagnosis: History, state of the art and perspective. *Artif. Intell. Med.* **2001**, *23*, 89–109. [CrossRef]
17. Karlik, B.; Tokhi, M.O.; Alci, M. A fuzzy clustering neural network architecture for multifunction upper-limb prosthesis. *IEEE Trans. Biomed. Eng.* **2003**, *50*, 1255–1261. [CrossRef]
18. Rutledge, R.; Osler, T.; Emery, S.; Kromhout-Schiro, S. The end of the Injury Severity Score (ISS) and the Trauma and Injury Severity Score (TRISS): ICISS, an International Classification of Diseases, ninth revision-based prediction tool, outperforms both ISS and TRISS as predictors of trauma patient survival, hospital charges, and hospital length of stay. *J. Trauma Acute Care Surg.* **1998**, *44*, 41–49.
19. Akhbarifar, S.; Javadi, H.H.S.; Rahmani, A.M.; Hosseinzadeh, M. A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment. *Pers. Ubiquitous Comput.* **2020**, 1–17. [CrossRef]
20. Jagadeeswari, V.; Subramaniyaswamy, V.; Logesh, R.; Vijayakumar, V. A study on medical Internet of Things and Big Data in personalized healthcare system. *Health Inf. Sci. Syst.* **2018**, *6*, 14. [CrossRef]
21. Ganguly, S. Multi-objective distributed generation penetration planning with load model using particle swarm optimization. *Decis. Mak. Appl. Manag. Eng.* **2020**, *3*, 30–42. [CrossRef]
22. Barma, P.S.; Dutta, J.; Mukherjee, A. A 2-opt guided discrete antlion optimization algorithm for multi-depot vehicle routing problem. *Decis. Mak. Appl. Manag. Eng.* **2019**, *2*, 112–125.
23. Roy, A.; Manna, A.; Maity, S. A novel memetic genetic algorithm for solving traveling salesman problem based on multi-parent crossover technique. *Decis. Mak. Appl. Manag. Eng.* **2019**, *2*, 100–111. [CrossRef]
24. Abualigah, L.; Diabat, A.; Mirjalili, S.; Abd Elaziz, M.; Gandomi, A.H. The arithmetic optimization algorithm. *Comput. Methods Appl. Mech. Eng.* **2021**, *376*, 113609. [CrossRef]
25. Savitha, V.; Karthikeyan, N.; Karthik, S.; Sabitha, R. A distributed key authentication and OKM-ANFIS scheme based breast cancer prediction system in the IoT environment. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *12*, 1757–1769. [CrossRef]
26. Lakshmanaprabu, S.K.; Mohanty, S.N.; Krishnamoorthy, S.; Uthayakumar, J.; Shankar, K. Online clinical decision support system using optimal deep neural networks. *Appl. Soft Comput.* **2019**, *81*, 105487.
27. Karuppiah, S.V.; Gurunathan, G. Secured storage and disease prediction of E-health data in cloud. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *12*, 6295–6306. [CrossRef]
28. Abdelaziz, A.; Salama, A.S.; Riad, A.M.; Mahmoud, A.N. A machine learning model for predicting of chronic kidney disease based internet of things and cloud computing in smart cities. In *Security in Smart Cities: Models, Applications, and Challenges*; Springer: Cham, Switzerland, 2019; pp. 93–114.
29. Połap, D.; Srivastava, G.; Jolfaei, A.; Parizi, R.M. Blockchain technology and neural networks for the internet of medical things. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020.
30. Ghazal, T.M. Internet of Things with Artificial Intelligence for Health Care Security. *Arab. J. Sci. Eng.* **2021**. [CrossRef]
31. Barnes, R.; Zvarikova, K. Artificial Intelligence-enabled Wearable Medical Devices, Clinical and Diagnostic Decision Support Systems, and Internet of Things-based Healthcare Applications in COVID-19 Prevention, Screening, and Treatment. *Am. J. Med Res.* **2021**, *8*, 9–22.
32. Morrison, M.; Lăzăroiu, G. Cognitive Internet of Medical Things, Big Healthcare Data Analytics, and Artificial intelligence-based Diagnostic Algorithms during the COVID-19 Pandemic. *Am. J. Med. Res.* **2021**, *8*, 23–36.
33. Riley, A.; Nica, E. Internet of Things-based Smart Healthcare Systems and Wireless Biomedical Sensing Devices in Monitoring, Detection, and Prevention of COVID-19. *Am. J. Med. Res.* **2021**, *8*, 51–64.
34. Scott, R.; Poliak, M.; Vrbka, J.; Nica, E. COVID-19 response and recovery in smart sustainable city governance and management: Data-driven Internet of Things systems and machine learning-based analytics. *Geopolit. Hist. Int. Relat.* **2020**, *12*, 16–22.
35. Lyons, N.; Lăzăroiu, G. Addressing the COVID-19 crisis by harnessing Internet of Things sensors and machine learning algorithms in data-driven smart sustainable cities. *Geopolit. Hist. Int. Relat.* **2020**, *12*, 65–71.
36. Rommer, D. Artificial Intelligence-based Decision-Making Algorithms, Industrial Big Data, and Smart Connected Sensors in Cloud-based Cyber-Physical Manufacturing Systems. *Econ. Manag. Financ. Mark.* **2020**, *15*, 40–46.
37. Fouad, H.; Hashem, M.; Youssef, A.E. A Nano-biosensors model with optimized bio-cyber communication system based on Internet of Bio-Nano Things for thrombosis prediction. *J. Nanopart. Res.* **2020**, *22*, 177. [CrossRef]
38. Abualigah, L.M.Q. *Feature Selection and Enhanced Krill Herd Algorithm for Text Document Clustering*; Springer: Berlin, Germany, 2019.
39. Abualigah, L.; Diabat, A. A novel hybrid antlion optimization algorithm for multi-objective task scheduling problems in cloud computing environments. *Clust. Comput.* **2020**, *24*, 205–223. [CrossRef]
40. Abualigah, L. Group search optimizer: A nature-inspired meta-heuristic optimization algorithm with its results, variants, and applications. *Neural Comput. Appl.* **2020**, *33*, 2949–2972. [CrossRef]
41. Letafati, M.; Kuhestani, A.; Wong, K.K.; Piran, M.J. A lightweight secure and resilient transmission scheme for the Internet of Things in the presence of a hostile jammer. *IEEE Internet Things J.* **2020**, *8*, 4373–4388. [CrossRef]
42. Bates, D.W.; Saria, S.; Ohno-Machado, L.; Shah, A.; Escobar, G. Big data in health care: Using analytics to identify and manage high-risk and high-cost patients. *Health Aff.* **2014**, *33*, 1123–1131. [CrossRef] [PubMed]

43. Carter, P.J. Potent antibody therapeutics by design. *Nat. Rev. Immunol.* **2006**, *6*, 343–357. [CrossRef] [PubMed]
44. Liu, H.; Darabi, H.; Banerjee, P.; Liu, J. Survey of wireless indoor positioning techniques and systems. *IEEE Trans. Syst. Man Cybern. Part C* **2007**, *37*, 1067–1080. [CrossRef]
45. Khan, M.A. An IoT Framework for Heart Disease Prediction Based on MDCNN Classifier. *IEEE Access* **2020**, *8*, 34717–34727. [CrossRef]
46. Maity, S.; Das, D.; Sen, S. Wearable health monitoring using capacitive voltage-mode human body communication. In Proceedings of the 2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Jeju, Korea, 11–15 July 2017.
47. Alzubi, J.A. Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare. *Comput. Commun.* **2021**, *170*, 200–208. [CrossRef]