Healthcare Monitoring-Based IoT Framework for Heart Disease Detection and Classification

J. Shafiq Mansoor 1*, Kamalraj Subramaniam 2

Abstract

Background: Chronic diseases like diabetes, heart disease, and cancer pose significant global health challenges, contributing to a substantial portion of worldwide mortality. Diagnosing heart disease, with its diverse signs and symptoms, remains a complex task. The growing market for connected wearable devices presents opportunities for leveraging Internet of Things (IoT) technologies in healthcare. However, diagnosing and managing heart disease effectively remains a critical concern due to its high fatality rates. Integrating IoT into the traditional healthcare system holds promise for enhancing patient outcomes, particularly for those with heart disease.

Methods: A Healthcare Monitoring-based IoT framework (HM-IoT) has been developed to enable continuous monitoring of heart disease patients, eliminating the need for manual feature extraction. This framework facilitates real-time monitoring of heart failure patients through IoT-enabled devices. Data encryption using the Enhanced Encryption Standard algorithm ensures the security of patient information within the cloud platform. An Artificial Neural Network (ANN) model is employed to classify encrypted data, promptly alerting healthcare professionals to abnormal physiological conditions.

Results: Evaluation in Matlab revealed impressive processing capabilities, with decryption and encryption rates of 1085 milliseconds and 1075 milliseconds, respectively. Data protection level reached 91%, while the Security Rate level attained 99%. Performance metrics, including Accuracy (98%), Sensitivity (96%), Specificity (98%), and Precision (99.4%), demonstrated the reliability of the system in detecting potential instances of heart disease.

Conclusion: The Healthcare Monitoring-based IoT framework represents a significant advancement in smart healthcare solutions for heart disease management. By integrating IoT technologies with healthcare infrastructure, the framework enables real-time monitoring, enhancing prognostic capabilities and facilitating timely interventions.

Keywords: Healthcare Monitoring, Internet of Things, Artificial Neural Networks, Security, Enhanced Encryption Standard algorithm

1. Introduction

The IoT is a generalized and expanding pattern shared by all forms of emerging technology. IoT connects uniquely tagged smart objects and gadgets Haque et al. (2021). However, the IoT is limited by the numerous things that are being installed all over the world Malik et al. (2021); (Zhu, X., 2021). Healthcare systems quickly incorporate clinical data, which would increase the number of electronic health records available Marques et al. (2022); Adeniyi et al. (2021); Pai et al. (2021); Khowaja et al. (2023); Mishra et al. (2021). Devices like accelerometers, worn on the body or implanted, make up the body sensor networks (Sinha, A., Singh, S.,

Significance

The proposed Healthcare Monitoring based IoT framework (HM-IoT) is evaluated based on the security rate and classification accuracy.

*Correspondence. J. Shafiq Mansoor, Research Scholar, Department of ECE, Karpagam Academy of Higher Education, Coimbatore, India. E-mail: shafiqid@gmail.com

Editor Ashish Agarwal And accepted by the Editorial Board Mar 07, 2024

(received for review Jan 08, 2024)

Author Affiliation.
1 Department of ECE, Karpagam Academy of Higher Education, Coimbatore, India.
2 Department of Biomedical Engineering, Karpagam Academy of Higher Education, Coimbatore, India.

Please cite this article.

https://doi.org/10.25163/angiotherapy.839553
Body Sensor Network is essential for operating IoT devices in biomedical applications (Soni, M., Singh, D.K., 2022; Haleem et al. 2021). The embedded IoT gadgets and sensors used to track and manage the state of patients at risk for cardiovascular disease can generate a lot of information at any given time (Patro et al. 2021; Ihnaini et al. 2021). The sudden termination of heart function poses the pending threat of death for those suffering from such conditions (Alam, A., 2022; Jansi Rani et al. 2022; Domínguez-Gil et al. 2021; Fanara et al. 2021).

In observational studies, machine learning (ML) may help to assess cardiovascular risk, make predictions, and locate valuable biomarkers such as ECG signals (Dami, S., Yahaghizadeh, M., 2021; Ali et al. 2021; Vishwanadham et al. 2024). The IoT offers a logical framework for dealing with the challenges of portable health care and virtual patient monitoring (Mbunge, E., Muchemwa, B., 2022); Hartmann et al. (2022). The main goal of HM-IoT is to predict people with heart disease. The initial stage is the authentication of patient information, data encryption, and heart disease classification based on the data collected. The Enhanced Encryption Standard algorithm achieves the encryption of data. If the doctor receives an alert and the patient is expected to have abnormal cardiac disease, they will be informed immediately. LSTM is responsible for the sorting of heart disease. Several studies based on the detection of heart disease, the security measurement for encryption of medical data, and the prediction and classification of heart disease are briefly discussed in this section. Sekar et al. (2022) proposed a unique, efficient Internet-of-Things-based modified Tuned neuro-fuzzy inference system (TANFIS) classifier. As a result, the proposed method improves upon prior algorithms by as much as 5.4%, resulting in an accuracy of 99.76% for predicting cardiac issues. Elayan et al. (2021) developed a machine-learning classifier model for electrocardiogram heart rhythms detection. Mehmood et al. (2021) presented a deep learning algorithm called convolutional neural networks (CNN) to estimate the likelihood that a given patient has cardiovascular disease. However, based on the experimental findings, it is clear that the proposed strategy provides better performance with 97% of Accuracy. Kumar et al. (2021) optimized the number of qubits utilizing the pipelining technique after first normalizing the qubit count in terms of their characteristics by applying min-max, principal component analysis, and standard vector. Rani et al. (2021) suggested that the Synthetic Minority Oversampling Method (SMOTE) and industry-standard scalar approaches have been applied for data preprocessing. Alraja et al. (2021) offered a unified approach to empower regular IoT app users to guard their data better. Ru et al. (2021) learned about wearable health monitoring devices. The IoT-based human health monitoring system is crucial for improving the efficiency and standard of healthcare. Hu et al. (2022) presented a methodology for 5G-secure-smart healthcare monitoring (5GSS) with the specific goals: rapid and precise detection of the health status in a given environment, blockchain-based secure information exchange, and low-latency solutions for urgent patients. (Zhenya, Q., Zhang, Z., 2021). incorporated five types of classifiers, random forest, logistic regression, support vector machine, extreme learning machine, and k-nearest neighbour, into the proposed methodology. Verma et al. (2018) calculated the impact of student illnesses by periodically mining health metrics obtained from medical and other IoT devices to forecast the likelihood of sickness and its severity. An intelligent student healthcare system architectural framework has been developed to facilitate the practical analysis of student healthcare data. In this work, we mimic waterborne disease cases using a health dataset involving 182 kids suspected of being infected. (Ganesan, M., Sivakumar, N., 2019) employed the UCI Repository dataset and healthcare sensors to develop a reliable framework for predicting the population's susceptibility to cardiovascular illness. In addition, patient data is classified using classification algorithms to help diagnose cardiac disease. The benchmark dataset can be used to train the classifier in the stage of training. During testing, accurate patient information is used to determine whether or not illness is present.

The prediction and detection of heart disease diagnosis is a very tedious process. The usage of wearable sensors in IoT platforms leads to the highest survival rate. The HM-IoT framework enhances the difficulties based on heart disease detection.

2. Healthcare Monitoring based IoT framework

The HM-IoT framework has been developed to forecast people with heart disease using IoT and cloud computing technology. The data collected from the patient with the wearable sensor is stored in the Cloud by the router. The data collected and stored need to be encrypted. The encrypted data allows for classifying the disease as normal or abnormal. The alert message is given to the physician for the abnormal condition of the heart. The complete architecture of HM-IoT is shown in Figure 1.

Enrollment, password, and confirmation are all part of the authentication system. Once a patient registers with the hospital’s portal, he or she will be given a username and password that will allow them to access their health records. The hospital’s system and the cloud server store this information about admitted patients.

The sensor device is initially attached to the patient’s body, marking the beginning of the suggested process. Next, the sensor on the IoT devices will read the patient’s vitals and send the data to the healthcare app. The verification stage is a crucial step in allowing authorized individuals access. When the application is first launched, the verification process is always successful. The verification stage is based on enrollment, access code, and confirmation. During enrolment, the patient creates an account on the healthcare application. The Healthcare platform’s operator
Figure 1. The Architecture of HM-IoT framework

Figure 2. The data collection and storage of data with the data protection ways.

Figure 3. The enhanced encryption standard algorithm with the encryption and decryption stage
Figure 4. The Data collection and the emergency alert message from the medical database

Figure 5. Overview of key sharing sequence and quadratic level representation

Figure 6. Schematic overview of classification stages by ANN
Figure 7. Overview of the Encryption and decryption rate

Figure 8. Overview of the DN and the SR level

Figure 9. Overall improvement analysis in terms of Accuracy

Figure 10. Overall improvement analysis in terms of Sensitivity

Figure 11. Overall improvement analysis in terms of Specificity

Figure 12. Overall improvement analysis in terms of Precision
Table 1. Performance evaluation of the proposed scheme in terms of Accuracy

<table>
<thead>
<tr>
<th>Epoch</th>
<th>SSHM</th>
<th>TANFIS</th>
<th>CNN</th>
<th>SMOTE</th>
<th>HM-IoT</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0.82</td>
<td>0.808</td>
<td>0.811</td>
<td>0.811</td>
<td>0.967</td>
</tr>
<tr>
<td>20</td>
<td>0.810</td>
<td>0.861</td>
<td>0.880</td>
<td>0.812</td>
<td>0.951</td>
</tr>
<tr>
<td>30</td>
<td>0.87</td>
<td>0.893</td>
<td>0.871</td>
<td>0.889</td>
<td>0.97</td>
</tr>
<tr>
<td>40</td>
<td>0.81</td>
<td>0.812</td>
<td>0.825</td>
<td>0.801</td>
<td>0.975</td>
</tr>
<tr>
<td>50</td>
<td>0.824</td>
<td>0.809</td>
<td>0.91</td>
<td>0.913</td>
<td>0.965</td>
</tr>
<tr>
<td>60</td>
<td>0.822</td>
<td>0.801</td>
<td>0.803</td>
<td>0.866</td>
<td>0.982</td>
</tr>
<tr>
<td>70</td>
<td>0.833</td>
<td>0.88</td>
<td>0.856</td>
<td>0.876</td>
<td>0.981</td>
</tr>
<tr>
<td>80</td>
<td>0.801</td>
<td>0.871</td>
<td>0.867</td>
<td>0.831</td>
<td>0.94</td>
</tr>
<tr>
<td>90</td>
<td>0.826</td>
<td>0.806</td>
<td>0.890</td>
<td>0.879</td>
<td>0.96</td>
</tr>
<tr>
<td>100</td>
<td>0.85</td>
<td>0.801</td>
<td>0.823</td>
<td>0.853</td>
<td>0.969</td>
</tr>
<tr>
<td>Mean</td>
<td>0.8266</td>
<td>0.8342</td>
<td>0.8536</td>
<td>0.8551</td>
<td>0.966</td>
</tr>
</tbody>
</table>

Table 2. Performance evaluation of the proposed scheme in terms of Sensitivity

<table>
<thead>
<tr>
<th>Epoch</th>
<th>SSHM</th>
<th>TANFIS</th>
<th>CNN</th>
<th>SMOTE</th>
<th>HM-IoT</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0.808</td>
<td>0.877</td>
<td>0.809</td>
<td>0.89</td>
<td>0.91</td>
</tr>
<tr>
<td>20</td>
<td>0.816</td>
<td>0.821</td>
<td>0.816</td>
<td>0.876</td>
<td>0.967</td>
</tr>
<tr>
<td>30</td>
<td>0.821</td>
<td>0.824</td>
<td>0.814</td>
<td>0.888</td>
<td>0.94</td>
</tr>
<tr>
<td>40</td>
<td>0.833</td>
<td>0.844</td>
<td>0.901</td>
<td>0.876</td>
<td>0.96</td>
</tr>
<tr>
<td>50</td>
<td>0.847</td>
<td>0.802</td>
<td>0.911</td>
<td>0.812</td>
<td>0.951</td>
</tr>
<tr>
<td>60</td>
<td>0.890</td>
<td>0.822</td>
<td>0.887</td>
<td>0.854</td>
<td>0.901</td>
</tr>
<tr>
<td>70</td>
<td>0.867</td>
<td>0.867</td>
<td>0.871</td>
<td>0.817</td>
<td>0.912</td>
</tr>
<tr>
<td>80</td>
<td>0.801</td>
<td>0.87</td>
<td>0.831</td>
<td>0.883</td>
<td>0.922</td>
</tr>
<tr>
<td>90</td>
<td>0.817</td>
<td>0.881</td>
<td>0.833</td>
<td>0.813</td>
<td>0.956</td>
</tr>
<tr>
<td>100</td>
<td>0.826</td>
<td>0.828</td>
<td>0.831</td>
<td>0.842</td>
<td>0.967</td>
</tr>
<tr>
<td>Mean</td>
<td>0.8326</td>
<td>0.8436</td>
<td>0.8504</td>
<td>0.8551</td>
<td>0.9386</td>
</tr>
</tbody>
</table>

Box 1. Enhanced Encryption standard Algorithm for data protection and heart disease detection

Input: Data collected from wearable sensors, \(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m\)

Output: \(H_l, H_m\); heart disease detection and classification

step 1: Data normalization, \(D = \alpha_1 + \alpha_m\),

\[\begin{align*}
\alpha &= \alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m \\
M &= (\alpha_1 \ast \alpha_m) \\
N &= 1
\end{align*}\]

Else repeat step 1

step 2: Encryption stage

For \(D = 1; D \leq 1; D + 1)\)

\[\begin{align*}
\mu &= N_t + M_{j+1} \\
\nu &= 1
\end{align*}\]

Else go to Step 3

end

Go to step 4

Step 3: Decryption stage

for \(M_j = 1; M_j \geq 1; \nu + M_j\)

\[\begin{align*}
\mu &= N_t + M_{j+1} \\
\nu &= \text{end}
\end{align*}\]

Go to step 4

Step 4 Heart disease classification and detection

Initialization \(H_l, H_m\)

if \(H_l \leq 1\) Classification as normal;

if \(H_m \geq 1\) classification as abnormal;

end
Table 3. Performance evaluation of the proposed scheme in terms of Specificity

<table>
<thead>
<tr>
<th>Epoch</th>
<th>SSHM</th>
<th>TANFIS</th>
<th>CNN</th>
<th>SMOTE</th>
<th>HM-IoT</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0.832</td>
<td>0.878</td>
<td>0.90</td>
<td>0.863</td>
<td>0.981</td>
</tr>
<tr>
<td>20</td>
<td>0.87</td>
<td>0.849</td>
<td>0.877</td>
<td>0.878</td>
<td>0.956</td>
</tr>
<tr>
<td>30</td>
<td>0.875</td>
<td>0.881</td>
<td>0.871</td>
<td>0.887</td>
<td>0.943</td>
</tr>
<tr>
<td>40</td>
<td>0.879</td>
<td>0.892</td>
<td>0.879</td>
<td>0.911</td>
<td>0.961</td>
</tr>
<tr>
<td>50</td>
<td>0.943</td>
<td>0.88</td>
<td>0.93</td>
<td>0.923</td>
<td>0.978</td>
</tr>
<tr>
<td>60</td>
<td>0.963</td>
<td>0.954</td>
<td>0.913</td>
<td>0.922</td>
<td>0.935</td>
</tr>
<tr>
<td>70</td>
<td>0.926</td>
<td>0.944</td>
<td>0.899</td>
<td>0.923</td>
<td>0.901</td>
</tr>
<tr>
<td>80</td>
<td>0.956</td>
<td>0.91</td>
<td>0.906</td>
<td>0.944</td>
<td>0.911</td>
</tr>
<tr>
<td>90</td>
<td>0.971</td>
<td>0.881</td>
<td>0.96</td>
<td>0.953</td>
<td>0.971</td>
</tr>
<tr>
<td>100</td>
<td>0.908</td>
<td>0.957</td>
<td>0.978</td>
<td>0.931</td>
<td>0.945</td>
</tr>
<tr>
<td>Mean</td>
<td>0.9123</td>
<td>0.9026</td>
<td>0.9113</td>
<td>0.9135</td>
<td>0.9482</td>
</tr>
</tbody>
</table>

Table 4. Performance evaluation of the proposed scheme in terms of Precision

<table>
<thead>
<tr>
<th>Epoch</th>
<th>SSHM</th>
<th>TANFIS</th>
<th>CNN</th>
<th>SMOTE</th>
<th>HM-IoT</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0.866</td>
<td>0.868</td>
<td>0.881</td>
<td>0.943</td>
<td>0.941</td>
</tr>
<tr>
<td>20</td>
<td>0.907</td>
<td>0.908</td>
<td>0.884</td>
<td>0.962</td>
<td>0.975</td>
</tr>
<tr>
<td>30</td>
<td>0.947</td>
<td>0.967</td>
<td>0.971</td>
<td>0.916</td>
<td>0.994</td>
</tr>
<tr>
<td>40</td>
<td>0.860</td>
<td>0.973</td>
<td>0.970</td>
<td>0.920</td>
<td>0.931</td>
</tr>
<tr>
<td>50</td>
<td>0.79</td>
<td>0.897</td>
<td>0.967</td>
<td>0.957</td>
<td>0.968</td>
</tr>
<tr>
<td>60</td>
<td>0.906</td>
<td>0.909</td>
<td>0.98</td>
<td>0.944</td>
<td>0.924</td>
</tr>
<tr>
<td>70</td>
<td>0.916</td>
<td>0.882</td>
<td>0.91</td>
<td>0.935</td>
<td>0.978</td>
</tr>
<tr>
<td>80</td>
<td>0.911</td>
<td>0.914</td>
<td>0.90</td>
<td>0.939</td>
<td>0.992</td>
</tr>
<tr>
<td>90</td>
<td>0.85</td>
<td>0.917</td>
<td>0.94</td>
<td>0.920</td>
<td>0.944</td>
</tr>
<tr>
<td>100</td>
<td>0.84</td>
<td>0.945</td>
<td>0.92</td>
<td>0.911</td>
<td>0.991</td>
</tr>
<tr>
<td>Mean</td>
<td>0.918</td>
<td>0.9323</td>
<td>0.9347</td>
<td>0.9638</td>
<td>0.978</td>
</tr>
</tbody>
</table>
validates individuals by examining their data. The medical status of the patients is collected utilizing a wearable sensor. The organized medical data is stored in the Cloud for future use. Data normalization analysis DN along with the data prediction model $D_m$ is shown in Equation (1)

$$ DN = a_1 + a_m N + \varepsilon_m + (a_1 \ast a_m)^m \sum_{m=1}^{M} (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m) $$

(1)

From Equation (1), $a_1$ represents data values with the variability and $a_m$ represents the error calculation rate. $\varepsilon_m$ stand for the least squares figures. The first step in the Heart Disease detection is data preparation $(a_1, a_2, a_3, \ldots, a_m)$. There are several outliers $D_m$ and gaps in the information that hinder the Accuracy of the classifier $\varepsilon_m$. The leftover number is represented as $N$. The variance is used to determine the mean and sampling information in the form of $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m)$. The sampling data $a_1, a_m$ detects heart disease in the form of $\varepsilon_1, \varepsilon_2, \varepsilon_3$. Finally, the typical approximation of data $M$ is given by equation (2).

$$ M = \sum_{m=1}^{M} N + m + (a_1 \ast a_m)^m \sum_{m=1}^{M} \varepsilon $$

$$ N = (\varepsilon_1 + \varepsilon_2 + \varepsilon_3) $$

(2)

From Equation (2), $N$ stands for the number of times the data values $a_1$ are used. Standardization of data is denoted as $m$, $m$ denote the number of data. $\varepsilon_i$ represents the leftover factor, $\varepsilon_m$ denote the statistical values. The sampling data is given as $a_1, a_m$, $\varepsilon$ denote the scaling parameter.

The Enhanced Encryption Standard algorithm is recommended to protect vast amounts of data in the Cloud, particularly data used in medical programs. The input information is viewed as a group of characters, and the process of the data encryption stage is shown in Equation (3).

$$ N_j = N_1, N_2, N_3, \ldots, N_m + (S_1, S_2, \ldots, S_m) $$

$$ (M_{j1}(l), M_{j2}(l), M_{j3}(l), \ldots, M_{jm}(l)) $$

$$ D^1 + D^2 + D^3 = D $$

(3)

The quantity of chosen sources is denoted by $N_j, N_m$ represent the total amount of selected options. Where $D^1$ represents the single encryption value, $D^2$ represents the double encryption value, $D^3$ denote the triple encryption value, and $D$ represents the corresponding Encryption component. $(M_{j1}(l), M_{j2}(l), \ldots, M_{jm}(l))$ represent the critical length of the encrypted data. Since medical records are highly confidential, the data must be encrypted and decrypted with the total key length for security purposes. The total key length is divided into subkeys with the weight matrix illustrated in Figure 2.

$$ f = N_{j2} + M_{j2} \ast (N_{j1}(l)) $$

$$ f = M_{j2} $$

(4)

The combination function is represented as $f, N_{j3}$ triple encryption stage with $j$ keys and key length $l$. $N_{j2}$ represent the single encryption stage, $N_{j1}$ represent the double encryption stage, $N_{j2}$ represent the l number of encryption stages, $M_{j2}$ represent the triple decryption stage, $N_{j2}$ denote the double decryption stage with the key length $M_{j1}$ represent the l number of decryption stages.

The enhanced encryption standard algorithm has the encryption $N_{j1}$ and decryption stage $M_{j1}$ with $j$ keys is shown in Figure 3. The original preprocessed information is given as $H$ with the selected weight matrices $m_s$ and the weighted quantity $N_{j1}$.

The numerical value representation is given in Equation (5)

$$ H = \sum_{j=1}^{M} M_{jm} + m_s + N_{j1} $$

$$ m_s = N_{j1} + M_{j1-1} \ldots, M_{jm+1} $$

(5)

From Equation (5), the weighted quantity is represented as $M_{jm}, m_s$ denote selected weight matrices, input information of the patient is given as $M_{j1}, N_{j1}$ stands for the weighted quantity. $M_{j1-1}, M_{jm+1}$ represent the decryption stages. $M_{jm+1}$ denote the numerical values with subkeys length. Cloud-based pharmacy databases also keep track of the latest heart disease treatments developed, ensuring that patients and doctors have access to the most up-to-date information.

The data from the medical database is given as alert messages for the medical professional and illustrated in Figure 4.

2.1 Protection of Data

A patient’s information $(l_1, l_2, l_3, \ldots, l_m)$ is stored in a database labeled $K$, broken into two sections with varying degrees of protection. The following requirements must be completed for the data table to be segmented properly.

$$ S^3 \cup S^3 \cup S^3 = K $$

$$ l_1 + l_2 + l_3, \ldots, l_m = l $$

$$ S^1, S^2, S^3, \ldots, S^m $$

(6)

The segmented stages are obtained from Equation (6), and the contents of the database are represented as $S^3, S^2, S^3$, the information storage of the patient is denoted as $K$, $S^l$ represent the varying degrees, $\omega$ denote the relevant data pieces. These $m$ parts are kept apart on several encrypted cloud servers. Choose $l_1$ coefficients $(l_1, l_2, l_3, \ldots, l_m)$ and give the coefficient $l_m$ as a deterministic value. A quadratic of level $(l – 1)$ is shown in Equation (7).

$$ K(m) = S^1(a_1), S^2(a_2), \ldots, S^m(a_m) $$

$$ (l_1, l_2, l_3, \ldots, l_m) \ast \omega $$

(7)

By plugging in the numbers of $S^1, S^2, \ldots, S^m$, the system calculates and stores each cloud provider’s portion as $l_m$. The data collected, verified, and protected is classified based on the condition of details available in the cloud server. The quadratic level 1 and 1-1 with key
The output of heart disease classification is in the form of $H_l$, obtained by Equation (9) for the patient condition of heart in the form of normal and abnormal.

### 2.2 Heart disease classification

The input layer of ANN is represented as $V_{l1} \ldots V_{lm}$. The hidden layer is represented as $H_{l1} \ldots H_{l1}, H_{lm}$. The output classification is based on normal and abnormal conditions. Heart disease prediction is based on the normal and abnormal classification of heart disease. The classification stages are illustrated in Figure 6.

If the output layer unit’s value is denoted by $l$, then $m$ is revised following Equation (8) and can be adjusted if the weight of the buried layer unit is denoted as $l$.

$$
\begin{align*}
\epsilon_l &= H_l(1 - H_l)(S_l - H_l) \\
\epsilon_m &= H_m(1 - H_m) \sum_{i \in \alpha_m} X_{im} \epsilon_l
\end{align*}
$$

(8)

$H_l$ and $H_m$ are the outputs obtained regarding $l$ and $m$, respectively. $S_l$ is the output-unit-goal symbol. The way of classification of the patient condition of heart in the form of normal and abnormal is obtained by Equation (9)

$$
\begin{align*}
H_l &= 1 + X_{lm} \leq 0; \textit{normal} \\
H_m &= 1 - H_{lm} \geq 0; \textit{abnormal}
\end{align*}
$$

(9)

The output of heart disease classification is in the form of $H_l$ and $H_m$: $X_{lm}$ and $H_{lm}$ is represented as reference symbols for the classification stage (Box 1). The complete process of the Enhanced Encryption standard Algorithm for data protection and heart disease detection is described in Table 1. The collected data from the wearable sensor is processed for data normalization with the encryption and decryption stages. The input is in the form of data collected from wearable sensors. The initial step of the algorithm is data normalization (DN); DN is in the form of $\alpha 1$ that represents data values with the variability and $\alpha_m$ represents the error calculation rate. The data normalization is followed by data preparation $\alpha$. If $N$ stands for the number of times the data values $\alpha 1$ are used with $m$ number of data. If the condition is not satisfied, the process continues to step 2. Step 2 is based on the Encryption stage D. If the condition is implemented for different encryption stage ($l = N_{j1}, N_{j2}, \ldots, N_{jk}$), ($m_s = N_{ij} + M_{ij-1} \ldots M_{ij+1}$) and depending upon the condition, step 3 is implemented. Step 3 is the decryption stage with the number of $M_{ij}$ decryption stage. The selected weight matrices $m_s$ is obtained from the decryption stage. The final step is the classification of the heart as if ($H_l \leq 1$) then the classification is stated as normal if ($H_l \geq 1$), then the classification is stated as abnormal.

### 3. Experimental analysis

The experimental analysis is based on the data collected from the open-source dataset to predict and classify heart diseases (heart-disease-classifications-machine-learning). The experimental section is divided into data security levels for protecting patients’ medical data in the cloud environment, collected through IoT-based devices. The other part is the classification of heart diseases, and the classification is evaluated utilizing Accuracy, Sensitivity, Specificity, and Precision. The encryption level is compared in the form of encryption rate, security level, and decryption rate of Enhanced Encryption standard Algorithm with those of the proposed HM-IoT technique for application in safe data transfer.

Calculating the Decryption rate $DR$ involves subtracting the timing information from when the decryption initiated $D_s$ and completed $D_e$ and it is shown in Figure 7. The encryption and decryption rate are calculated using the formula in Equation (10). The data normalization (DN) and the security level (SR) of the enhanced encryption standard algorithm are shown in Figure 8.

$$
\begin{align*}
ER &= E_s - E_r \\
DR &= D_s - D_e
\end{align*}
$$

(10)

The Accuracy of HM-IoT is shown in Figure 9. The Accuracy of HM-IoT Vs. with the existing approaches. The Accuracy (AC) of HM-IoT is obtained from Equation (11)

$$
AC = \frac{tp + tn}{tp + tn + fp + fn}
$$

(11)

The Accuracy is calculated utilizing true positive $tp$, true negative $tn$, false positive $fp$, false negative $fn$. (Table 1).

Sensitivity is defined as the rate at which insignificant characteristics are extracted and labeled from a given dataset utilizing the classification of heart disease, as shown in Equation (12). The Sensitivity of HM-IoT is shown in Table 2 and Figure 10

$$
Sen = \frac{tp}{tp + fn}
$$

(12)

The Specificity (sp) of HM-IoT is calculated from Equation (13)

$$
sp = \frac{tp}{tp + fp}
$$

(13)

The classification of heart diseases is based on the Specificity of true negative values. The Specificity of HM-IoT is shown in Table 3 and Figure 11.

The Precision of HM-IoT is obtained from Equation (14), and the values are shown in Table 4 and Figure 12

$$
pre = \frac{tp}{tp + fp}
$$

(14)
The proposed HM-IoT is compared with the Synthetic Minority Oversampling Method (SMOTE) Rani et al. (2021), convolutional neural networks (CNN) Mehmood et al. (2021), Tuned neuro-fuzzy inference system (TANFIS) Sekar et al. (2022), secure-smart healthcare monitoring (SSHM) Hu et al. (2022).

4. Conclusion
Although there are many potential causes and manifestations of cardiac disease, diagnosing heart disease is challenging. Providing an IoT service in healthcare is becoming increasingly feasible, along with the usage of wearable devices. Traditional healthcare must be converted to smart healthcare using IoT to continuously monitor patients with heart disease. HM-IoT improves life predictions for persons with heart disease without relying on human-driven feature development. By continuously monitoring patients with data gathered from linked devices, the smart IoT-based framework provides efficient and high-quality care to those with heart failure. The decryption rate is 1085 ms, encryption rate is 1075 ms. The data protection level in DN is 91%, SR level is 99%, Accuracy is 98%, Sensitivity is 96%, Specificity is 98%, and Precision is 99.4%.

Author contribution
J.S.M. conceptualized, investigated, collected and presented data, and wrote the original content. K.S. supervised, planned the study, collected data, conceptualized, analyzed, and interpreted results.

Acknowledgment
The authors were grateful to the department for this study.

Competing financial interests
The authors have no conflict of interest.

References


https://doi.org/10.1016/j.compeleceng.2021.107060

https://doi.org/10.1016/j.compeleceng.2021.107060

https://doi.org/10.25163/angiotherapy.839553


