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

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)

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.,

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.
J. Shafiq Mansoor, Kamalraj Subramaniam. (2024). Healthcare Monitoring-Based Iot Framework for Heart Disease Detection and Classification, Journal of Angiotherapy, 8(3), 1-11, 9553

2021). 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). 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

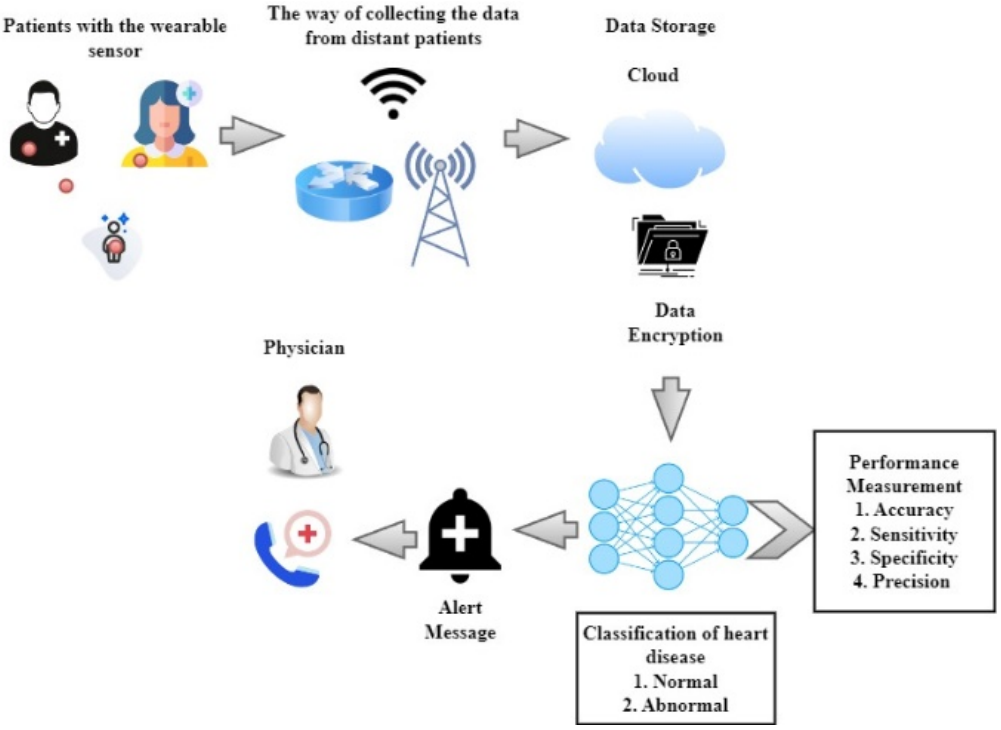

Figure 1. The Architecture of HM-IoT framework

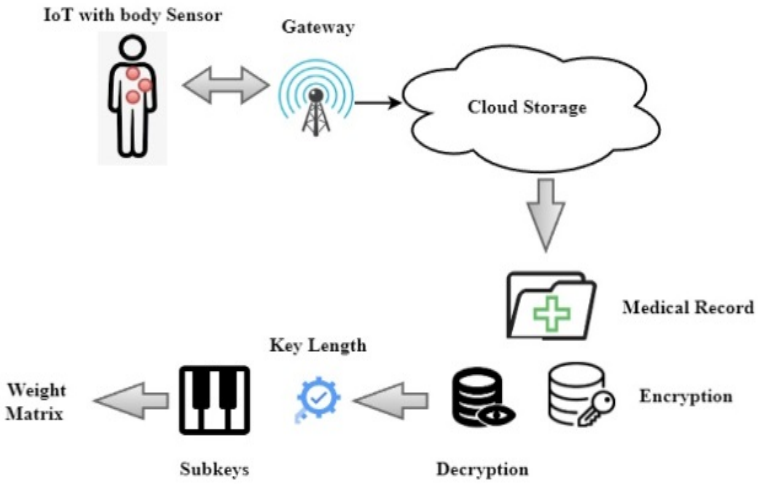

Figure 2. The data collection and storage of data with the data protection ways.

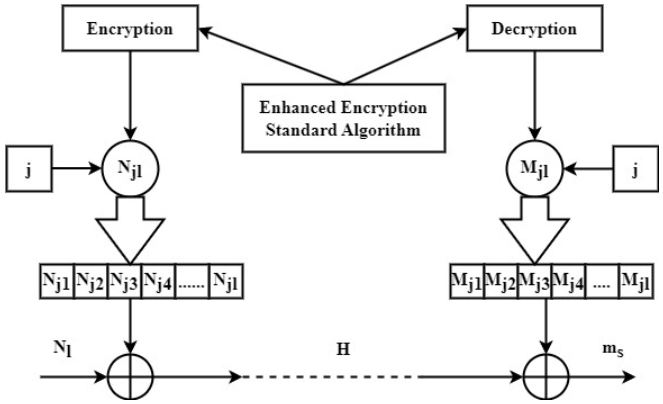

Figure 3. The enhanced encryption standard algorithm with the encryption and decryption stage

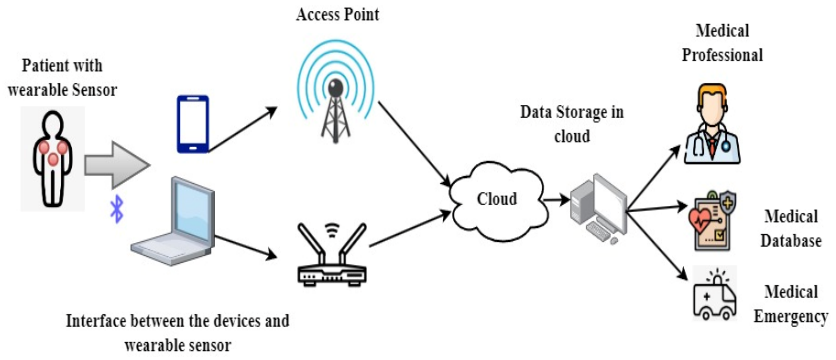

Figure 4. The Data collection and the emergency alert message from the medical database

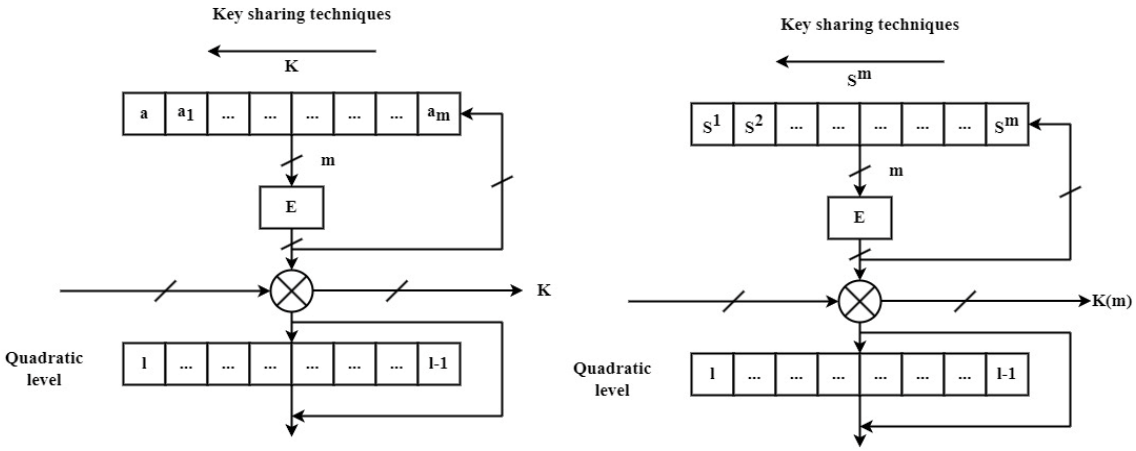

Figure 5. Overview of key sharing sequence and quadratic level representation

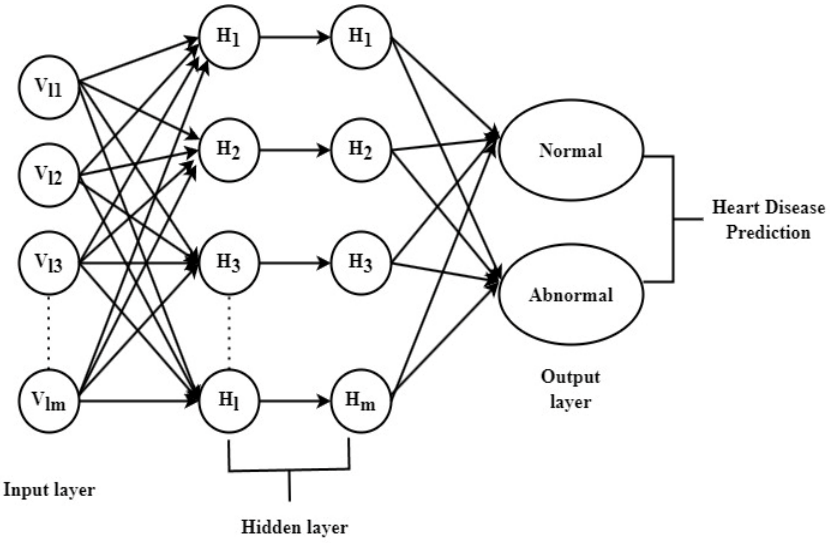

Figure 6. Schematic overview of classification stages by ANN

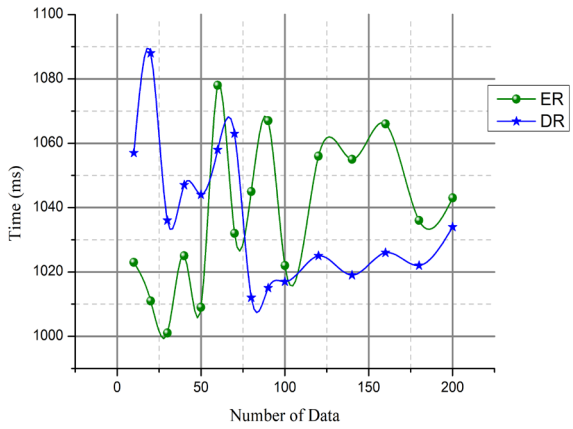

Figure 7. Overview of the Encryption and decryption rate

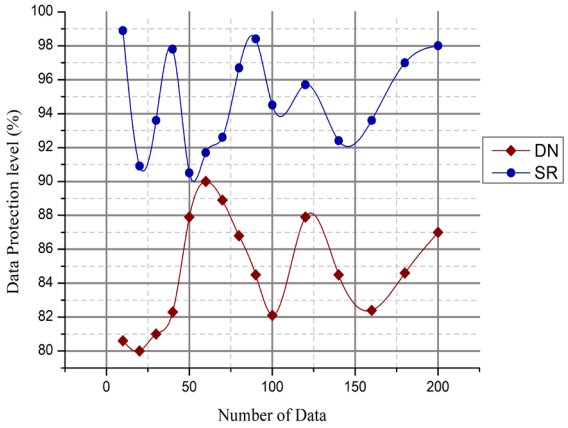

Figure 8. Overview of the DN and the SR level

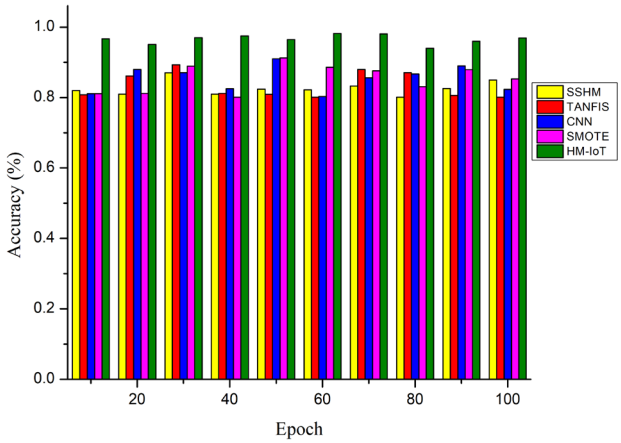

Figure 9. Overall improvement analysis in terms of Accuracy

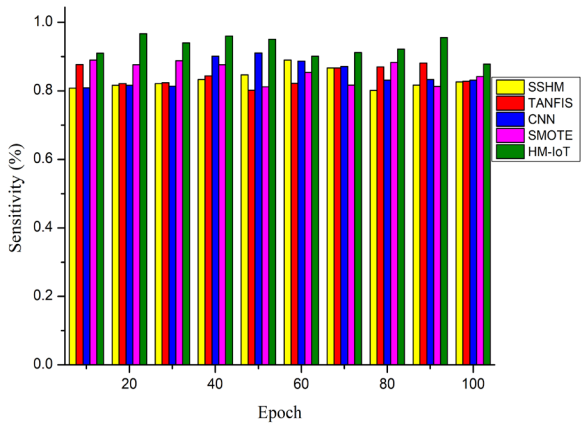

Figure 10. Overall improvement analysis in terms of Sensitivity

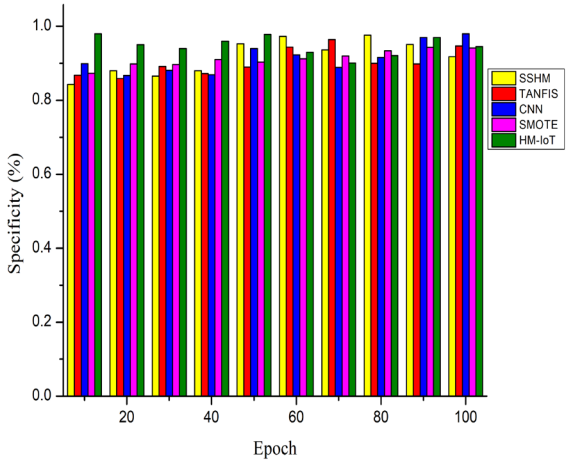

Figure 11. Overall improvement analysis in terms of Specificity

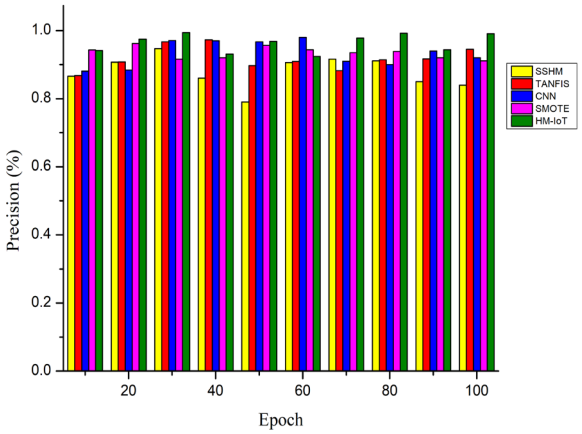

Figure 12. Overall improvement analysis in terms of Precision

Table 1. Performance evaluation of the proposed scheme in terms of Accuracy

Epoch	SSHM	TANFIS	CNN	SMOTE	HM-IoT
10	0.82	0.808	0.811	0.811	0.967
20	0.810	0.861	0.880	0.812	0.951
30	0.87	0.893	0.871	0.889	0.97
40	0.81	0.812	0.825	0.801	0.975
50	0.824	0.809	0.91	0.913	0.965
60	0.822	0.801	0.803	0.886	0.982
70	0.833	0.88	0.856	0.876	0.981
80	0.801	0.871	0.867	0.831	0.94
90	0.826	0.806	0.890	0.879	0.96
100	0.85	0.801	0.823	0.853	0.969
Mean	0.8266	0.8342	0.8536	0.8551	0.966

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

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

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

Input: Data collected from wearable sensors, $\alpha_1, \alpha_2, \alpha_3, \dots\dots\dots \alpha_m$
Output: H_l, H_m; heart disease detection and classification
step 1: Data normalization, $DN = \alpha_1 + \alpha_m$;
$\alpha = \alpha_1, \alpha_2, \alpha_3, \dots\dots\dots \alpha_m$
If (M=$(\alpha_1 * \alpha_m)\frac{N}{m}$)
Else
$(\varepsilon = \varepsilon_1, \varepsilon_2, \dots\dots\dots \varepsilon_M)$
$N = \frac{\varepsilon_M}{\gamma_M} > 1$
Else repeat step 1
end
step 2: Encryption stage
For $(D = 1; D \leq 1; D++)$
If $(l = N_{j1}, N_{j2}, \dots\dots\dots N_{jl})$
If $(m_s = N_l + M_{jl-1}, \dots\dots\dots M_{jl+1})$
Else
Go to Step3
end
end
Step 3: Decryption stage
for $(M_{jl} = 1; M_{jl} \geq 1; ++M_{jl})$
$m_s = N_l + M_{jl-1}, \dots\dots\dots M_{jl+1}$
end
end
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
end

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

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

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

Epoch	SSHM	TANFIS	CNN	SMOTE	HM-IoT
10	0.866	0.868	0.881	0.943	0.941
20	0.907	0.908	0.884	0.962	0.975
30	0.947	0.967	0.971	0.916	0.994
40	0.860	0.973	0.970	0.920	0.931
50	0.79	0.897	0.967	0.957	0.968
60	0.906	0.909	0.98	0.944	0.924
70	0.916	0.882	0.91	0.935	0.978
80	0.911	0.914	0.90	0.939	0.992
90	0.85	0.917	0.94	0.920	0.944
100	0.84	0.945	0.92	0.911	0.991
Mean	0.918	0.9323	0.9347	0.9638	0.978

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)

$$\left.\begin{array}{c} DN = \alpha_1 + \alpha_m N + \varepsilon_M + (\alpha_1 * \alpha_m)\frac{N}{m} \\ D_m = \alpha_1 + \alpha_m + \varepsilon_M - (\alpha_1 * \alpha_m - N)\sum_{m=1}^{M}(\varepsilon_1, \varepsilon_2, \dots\dots\dots\dots\varepsilon_M) \end{array}\right\} \quad (1)$$

From Equation (1), $\alpha_1$represents data values with the variability and α_mRepresent the error calculation rate. ε_MStand for the least squares figures. The first step in Heart Disease detection is data preparation $(\alpha_1, \alpha_2, \alpha_3, \dots\dots\dots\dots\alpha_m)$. There are several outliers D_m and gaps in the information that hinder the Accuracy of the classifier ε_M. The leftover number is represented as N. The variance is used to determine the mean and sampling information in the form of $(\varepsilon_1, \varepsilon_2, \dots\dots\dots\dots\varepsilon_M)$.The sampling data α_1, α_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).

$$\left.\begin{array}{c} M = \sum_{m=1}^{l} N + m_s + (\alpha_1 * \alpha_m)\frac{N}{m} \\ N = \frac{\varepsilon_M}{\gamma_M} + \alpha_m N - (\alpha_1 * \alpha_m) + (\varepsilon_1 * \varepsilon_M) \end{array}\right\} \quad (2)$$

From Equation (2), N stands for the number of times the data values α_1 are used. Standardization of data is denoted as m_s.m denote the number of data. ε_1 represent the leftover value, ε_M denote the statistical values. The sampling data is given as α_1, α_m. γ 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).

$$\left.\begin{array}{c} N_j = N_1, N_2, N_3 \dots\dots N_m + (S_1, S_2, \dots\dots\dots S_N) \\ (M_{j1}(l), M_{j2}(l), M_{j3}(l) \dots\dots M_{jN}(l)) \\ D^1 + D^2 + D^3 = D \end{array}\right\} (3)$$

The quantity of chosen sources is denoted by N_j, N_m represent the total amount of selected options. where D^1 represent the single encryption value, D^2 represent the double encryption values, D^3 denote the triple encryption value, and D represents the corresponding Encryption component. $(M_{j1}(l), M_{j2}(l), \dots\dots M_{jN}(l))$ 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.

$N_j(l)$ and $M_j(l)$are encrypted and decrypted utilizing the j keys of Enhanced Encryption Standards. As a combination function of the encryption and decryption standards of Enhanced Encryption standard algorithm derivation is shown in Equation (4)

$$\left.\begin{array}{c} f = N_{j3} + M_{j2} * \left(N_{j1}(l)\right) \\ f = M_{j2} \\ f = M_{j2} + N_{j2} * (M_{j3}(l)) \end{array}\right\} \quad (4)$$

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

The enhanced encryption standard algorithm has the encryption N_{jl} and decryption stage M_{jl} 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_l .

The numerical value representation is given in Equation (5)

$$\left.\begin{array}{c} H = \sum_{j=1}^{m} M_{jm} + m_s * M_{jl} + N_l \\ m_s = N_l + M_{jl-1}, \dots\dots\dots M_{jl+1} \\ N_l = M_{jm} + M_{jm-1}, \dots\dots M_{jm+1} \end{array}\right\} \quad (5)$$

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_{jl}, N_l Stands for the weighted quantity. M_{jl-1}, M_{jl+1} represent the decryption stages. M_{jm-1}, 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.

2.1Protection of Data

A patient's information $(l_1, l_2, l_3 \dots\dots l_m)$ 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.

$$\left.\begin{array}{c} S^1 \cup S^2 \cup S^3 = K \\ S^l \cup s^l = \omega \\ l_1, l_2, l_3 \dots\dots l_m = l \\ S^1, S^2, S^3 \dots\dots S^m = m \end{array}\right\} \quad (6)$$

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

$$\left.\begin{array}{c} K(m) = S^1(a), S^2(a_1), \dots\dots S^m(a_m) \\ (l_1, l_2, l_3 \dots\dots l_m) * \omega \end{array}\right\} \quad (7)$$

By plugging in the numbers of $S^1, S^2 \dots\dots S^m$, 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 l and l-1 with key

sharing for each sequence $a, a_1, \ldots \ldots\ a_m$ is given by K, and the key-sharing sequence of $S^1, S^2 \ldots\ldots S^m$ is given by k(m) is illustrated in Figure 5.

2.2Heart disease classification

The input layer of ANN is represented as $V_{l1} \ldots \ldots V_{lm}$. The hidden layer is represented as $H_1 \ldots \ldots H_l, H_m$. 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.

$$\left.\begin{aligned} \epsilon_l &= H_l(1-H_l)(s_l-H_l) \\ \epsilon_m &= H_m(1-H_m)\textstyle\sum_{l\in o/p} X_{lm}\epsilon_l \end{aligned}\right\} \quad (8)$$

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)

$$\left.\begin{aligned} H_l &= 1 + X_{lm} \le 0; normal \\ H_m &= 1 - H_{lm} \ge 0; abnormal \end{aligned}\right\} \quad (9)$$

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 α_mRepresent the error calculation rate. The data normalization is followed by data preparation α. If N stands for the number of times the data values α_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 $(l = N_{j1,}N_{j2}, \ldots \ldots \ldots N_{jl})$, $(m_s = N_l + M_{jl-1}, \ldots \ldots \ldots M_{jl+1})$ and depending upon the condition, step 3 is implemented. Step 3 is the decryption stage with the l number of M_{jl} 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 $(H_l \le 1)$ then the classification is stated as normal if $(H_l \ge 1)$, 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.

$$\left.\begin{aligned} ER &= E_S - E_E \\ DR &= D_S - D_E \end{aligned}\right\} \quad (10)$$

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)

$$AC = \frac{t_p+t_n}{t_p+t_n+f_p+f_n} \quad (11)$$

The Accuracy is calculated utilizing true positive t_p, true negative t_n, false positive f_p, false negative f_n. (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

$$\text{Sen} = \frac{t_p}{t_p+f_n} \quad (12)$$

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

$$sp = \frac{t_p}{f_p+t_n} \quad (13)$$

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

$$pre = \frac{t_p}{t_p+f_p} \quad (14)$$

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

Adeniyi, E.A., Ogundokun, R.O., & Awotunde, J.B. (2021). IoMT-based wearable body sensors network healthcare monitoring system. IoT in healthcare and ambient assisted living, 103-121.

Alam, A. (2022). Cloud-based e-learning: scaffolding the environment for adaptive e-learning ecosystem based on cloud computing infrastructure. In Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021, Volume 2. Singapore: Springer Nature Singapore, 1-9.

Ali, M.M., Paul, B.K., Ahmed, K., Bui, F.M., Quinn, J.M., & Moni, M.A. (2021). Heart disease prediction using supervised machine learning algorithms: Performance analysis and comparison. Computers in Biology and Medicine, 136, 104672.

Alraja, M.N., Barhamgi, H., Rattrout, A., & Barhamgi, M. (2021). An integrated framework for privacy protection in IoT—Applied to smart healthcare. Computers & Electrical Engineering, 91, 107060. https://doi.org/10.1016/j.compeleceng.2021.107060

Dami, S., & Yahaghizadeh, M. (2021). Predicting cardiovascular events with deep learning approach in the context of the internet of things. Neural Computing and Applications, 33, 7979-7996.

Domínguez-Gil, B., Ascher, N., Capron, A.M., Gardiner, D., Manara, A.R., Bernat, J.L., & Delmonico, F.L. (2021). Expanding controlled donation after the circulatory determination of death: statement from an international collaborative. Intensive care medicine, 47, 265-281.

Elayan, H., Aloqaily, M., & Guizani, M. (2021). Digital twin for intelligent context-aware IoT healthcare systems. IEEE Internet of Things Journal, 8(23), 16749-16757.

Fanara, S., Aprile, M., Iacono, S., Schirò, G., Bianchi, A., Brighina, F., & Salemi, G. (2021). The role of nutritional lifestyle and physical activity in multiple sclerosis pathogenesis and management: a narrative review. Nutrients, 13(11), 3774. https://doi.org/10.3390/nu13113774

Ganesan, M., & Sivakumar, N. (2019). IoT based heart disease prediction and diagnosis model for healthcare using machine learning models. In IEEE international conference on system, computation, automation and networking (ICSCAN), 1-5.

Haleem, A., Javaid, M., Singh, R.P., & Suman, R. (2021). Telemedicine for healthcare: Capabilities, features, barriers, and applications. Sensors international, 2, 100117. https://doi.org/10.1016/j.sintl.2021.100117

Haque, M.S.M., Hassan, M.R., & Hossain, M.K. (2021). Underlying Concepts and Understandings of Internet of Things (IoT). Manchester Journal of Artificial Intelligence and Applied Sciences, 2(2), 101-110.

Hartmann, M., Hashmi, U. S., & Imran, A. (2022). Edge computing in smart health care systems: Review, challenges, and research directions. Transactions on Emerging Telecommunications Technologies, 33(3), e3710. https://doi.org/10.1002/ett.3710

https://doi.org/10.1016/j.compbiomed.2021.104672

https://www.kaggle.com/code/cdabakoglu/heart-disease-classifications-machine-learning

Hu, J., Liang, W., Hosam, O., Hsieh, M. Y., & Su, X. (2022). 5GSS: A framework for 5G-secure-smart healthcare monitoring. Connection Science, 34(1), 139-161.

Ihnaini, B., Khan, M.A., Khan, T.A., Abbas, S., Daoud, M.S., Ahmad, M., & Khan, M.A. (2021). A smart healthcare recommendation system for multidisciplinary diabetes patients with data fusion based on deep ensemble learning. Computational Intelligence and Neuroscience, 2021. https://doi.org/10.1155/2021/4243700

Jansi Rani, S.V., Chandran, K.S., Ranganathan, A., Chandrasekharan, M., Janani, B., & Deepsheka, G. (2022). Smart wearable model for predicting heart disease using machine learning: Wearable to predict heart risk. Journal of Ambient Intelligence and Humanized Computing, 13(9), 4321-4332.

Khowaja, S.A., Khuwaja, P., Dev, K., & D'Aniello, G. (2023). VIRFIM: an AI and Internet of Medical Things-driven framework for healthcare using smart sensors. Neural Computing and Applications, 35(22), 16175-16192.

Kumar, Y., Koul, A., Sisodia, P. S., Shafi, J., Kavita, V., Gheisari, M., & Davoodi, M.B. (2021). Heart failure detection using quantum-enhanced machine learning and traditional machine learning techniques for internet of artificially

intelligent medical things. Wireless Communications and Mobile Computing, 2021, 1-16.

Malik, P.K., Sharma, R., Singh, R., Gehlot, A., Satapathy, S.C., Alnumay, W.S., & Nayak, J. (2021). Industrial Internet of Things and its applications in industry 4.0: State of the art. Computer Communications, 166, 125-139.

Marques, J.A.L., Gois, F.N.B., Da Silveira, J.A.N., Li, T., & Fong, S.J. (2022). AI and deep learning for processing the huge amount of patient-centric data that assist in clinical decisions. In Cognitive and Soft Computing Techniques for the Analysis of Healthcare Data. Academic Press, 101-121.

Mbunge, E., & Muchemwa, B. (2022). Towards emotive sensory Web in virtual health care: Trends, technologies, challenges and ethical issues. Sensors International, 3, 100134. https://doi.org/10.1016/j.sintl.2021.100134

Mehmood, A., Iqbal, M., Mehmood, Z., Irtaza, A., Nawaz, M., Nazir, T., & Masood, M. (2021). Prediction of heart disease using deep convolutional neural networks. Arabian Journal for Science and Engineering, 46(4), 3409-3422.

Mishra, S., Thakkar, H.K., Mallick, P.K., Tiwari, P., & Alamri, A. (2021). A sustainable IoHT based computationally intelligent healthcare monitoring system for lung cancer risk detection. Sustainable Cities and Society, 72, 103079. https://doi.org/10.1016/j.scs.2021.103079

Pai, M.M., Ganiga, R., Pai, R.M., & Sinha, R.K. (2021). Standard electronic health record (EHR) framework for Indian healthcare system. Health Services and Outcomes Research Methodology, 21(3), 339-362.

Patro, S.P., Padhy, N., & Chiranjevi, D. (2021). Ambient assisted living predictive model for cardiovascular disease prediction using supervised learning. Evolutionary intelligence, 14(2), 941-969.

Rani, P., Kumar, R., Ahmed, N.M.S., & Jain, A. (2021). A decision support system for heart disease prediction based upon machine learning. Journal of Reliable Intelligent Environments, 7(3), 263-275.

Ru, L., Zhang, B., Duan, J., Ru, G., Sharma, A., Dhiman, G., & Masud, M. (2021). A detailed research on human health monitoring system based on internet of things. Wireless Communications and Mobile Computing, 2021, 1-9.

Sekar, J., Aruchamy, P., Sulaima Lebbe Abdul, H., Mohammed, A.S., & Khamuruddeen, S. (2022). An efficient clinical support system for heart disease prediction using TANFIS classifier. Computational Intelligence, 38(2), 610-640.

Sinha, A., & Singh, S. (2021). Detailed analysis of medical IoT using wireless body sensor network and application of IoT in healthcare. Human Communication Technology: Internet of Robotic Things and Ubiquitous Computing, 401-434.

Soni, M., & Singh, D.K. (2022). LAKA: lightweight authentication and key agreement protocol for internet of things based wireless body area network. Wireless Personal Communications, 127(2), 1067-1084.

Verma, P., Sood, S.K., & Kalra, S. (2018). Cloud-centric IoT based student healthcare monitoring framework. Journal of Ambient Intelligence and Humanized Computing, 9(5), 1293-1309.

Zhenya, Q., & Zhang, Z. (2021). A hybrid cost-sensitive ensemble for heart disease prediction. BMC medical informatics and decision making, 21, 1-18.

Zhu, X. (2021). Complex event detection for commodity distribution Internet of Things model incorporating radio frequency identification and Wireless Sensor Network. Future Generation Computer Systems, 125, 100-111.