IEEE *Access*
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

An efficient IoT based patient monitoring and heart disease prediction system using Deep learning modified neural network

Simanta Shekhar Sarmah
[1]Alpha Clinical Systems Inc, New Jersey, USA ,08854

ABSTRACT The leading causes of death worldwide are chronic illnesses suchlike diabetes, Heart Disease (HD), cancer as well as chronic respiratory malady. It is remarkably intricate to diagnose HD with disparate symptoms or features. With the augmentation in popularity of smart wearable gadgets, a chance to render an Internet of Things (IoT) solution has turned out to be more. Unfortunately, the survival rates are low for the people suffering from sudden heart attacks. Consequently, a patient monitoring scheme intended for heart patients utilizing IoT centered Deep Learning Modified Neural Network (DLMNN) is proposed to assist in the HD diagnosis, and medication is given accordingly. This proposed technique is executed via '3' steps: I) Authentication, ii) Encryption, and iii) Classification. First, by utilizing the substitution cipher (SC) together with the SHA-512, the heart patient of the specific hospital is authenticated. Subsequently, the wearable IoT sensor device, which is fixed to the patient's body, concurrently transmits the sensor data to the cloud. This sensor data is encrypted and securely transmitted to the cloud utilizing the PDH-AES technique. After that, the encrypted data is finally decrypted, and by employing the DLMNN classifier, the classification is done. The classified outcomes comprise '2'types of data: i) normal and ii) abnormal. It denotes the patient's heart condition and if the outcome is abnormal, an alert text is passed to the physician for treating the patient. The investigational outcomes are estimated and the DLMNN for HD diagnosis shows improvement as compared to existing algorithms. Additionally, the proposed PDH-AES used in support of secure data transmission results in the highest level of security i.e. 95.87%, and it is achieved in the lowest time for encryption along with decryption when weighted against the existent AES.

INDEX TERMS Disease prediction, Healthcare Monitoring System, Internet of Things (IoT), Advanced Encryption Standard (AES), Modified Huffman Algorithm (MHA), Deep Learning Modified Neural Network (DLMNN), and Cuttlefish Optimization Algorithm (CFOA).

I. INTRODUCTION

IoT [1] is essentially a developing trend for all future-generation technology. It is the inter-connection of exclusively identified smart objects along with devices. IoT is bounded by numerous objects, which are being invisibly fixed all around the environment [2]. Health monitoring (HM) is the utmost common research application in wearable electronics. Smart HM is the amalgamation of smart computing in addition to the remote HM with IoT [3]. The body sensors networks (BSN) are formed of disparate wearable or implantable devices, say accelerometer, cardioverter-defibrillator, and pacemaker, which sense as well as monitor the breathing rates, blood pressures, pulse, together with body temperature [4] of users. BSN functions as a basic component of IoT [5, 6]. These devices are utilized to collect vital information like adequate alteration in wellbeing restraint and it refreshes the weightiness of the remedial parameters in a pre-said period [7]. The data amassed as of the IoT-centered wearable devices are stocked up in a clinical database for required action when the patients' health condition depreciates [8, 9]. IoT gives a drop in cost and widens the scope of attaining the medical facilities to a remote region and it ameliorates the services' quality [10].

Chronic HD patients can profit from this kind of device. There stands a hazard of demise for those patients with such diseases since their heart functionality might stop at any moment [11]. Obesity, stress, rigorous eating of salty and oily foods, no exercise along with genetic factors is the chief reason for the high occurrence of such diseases. Besides that, due to augmented hazard factors, like hypertension, diabetes, elevated blood fat, and weight gain caused amid menopause can make women suffer a heart attack. [12].

Studies conducted on heart failure patients show that around 30 percent of patients had been readmitted as a minimum of once within the timeframe of 90 days. Within 3-6 months, the readmission ranges had come athwart 25% to 54% [13]. Therefore, the key to augment the HD performance of the

healthcare (HC) and to decrease the death rate is changing the inert HC mode into an invasive one. The physicians should monitor the patient's physical status and decide the time the HC services should well be delivered to them, which could be attained with the assist of IoT [14].

Machine learning (ML) algorithms handle a very large quantity of data and play a chief part in the decision-making. To adopt data analysis methods, the data namely velocity, volume in addition to variety must be known [15]. ML-centered early diagnosis along with prediction design was established as an effective application on medical analysis. Numerous ML algorithms were devised for the disease prediction systems, which are discussed in the literature review section, but most of those techniques had only focused on the disease prediction. They didn't consider security as a prime concern. Also, the previous disease prediction techniques did not utilize a feature selection, which leads to the highest training time. To overcome such drawbacks, an ML algorithm called DLMNN based HD prediction system is proposed for envisaging the patient's heart condition. The proposed work uses the Hungarian HD in addition to the healthcare sensors to envisage the patients who suffer as of HD. The classification algorithms are utilized for the reason of classifying the patient data for the recognition of HD. The prediction is done by performing two phases i) training and ii) testing. In the training phase, the classifier is trained by utilizing the data from the benchmark dataset. During the testing phase, the actual patient data is utilized to recognize the disease's presence. The proposed work has the subsequent objectives.

- To render an efficient patient authentication scheme utilizing SHA-512.
- To propose a Modified Huffman algorithm for compressing the data of patient healthcare records.
- To propose a PDH-AES algorithm for encrypting the compressed patient data
- To propose a DLMNN for predicting the patient's heart condition
- To present a CFA optimization for the parameter tuning (weight optimization) of DLMNN

With the above-stated objectives, the patient's heart condition is identified accurately utilizing the DLMNN classifier that classifies the patient's heart condition into '2' classes (normal as well as abnormal). The required action should be rendered via the doctor as stated by the predicted class and to augment the patient data security level, the PDH-AES scheme is introduced in the proposed work. In this PDH-AES, the key for encrypting the patient data is generated by three factors, like patient id, doctor id, and healthcare-id. So, the key is unique for every patient data that increases the intricacy of the key. Hence, it is exceedingly tough for an attacker to steal patient data with an increased level of data security. By using these best encryption and classification algorithms, promising outcomes for the

proposed prediction and encryption techniques are achieved successfully.

The rest is pre-arranged as Section 2-critiques the associated work. Section 3 signifies a concise discussion. Section 4 analyses the experimental outputs. Lastly, a conclusion is written in section 5.

II. LITERATURE REVIEW

Zafer Al-Makhadmeh and AmrTolba [16] presented an IoT-centered medical device for gathering prior and subsequent to HD information of patients' heart status. Utilizing the higher-order Boltzmann deep belief neural network, the information was processed after being incessantly transmitted to the HC center. The past HD aspects were learned by the deep learning technique, which led to the effectual manipulation of intricate data for achieving efficiency. Centered on these characteristics (specificity, f-measure, loss function, sensitivity, along with receivers operating characteristics (ROC)), the system's performance was computed. This existing technique had 99.03 percent accuracy with minimum time intricacy of 8.5s effectively; thus, brought about the minimized HD mortality via lessening the intricacy in diagnosing HD.

PavleenKaur et al. [17] presented disparate ML techniques that were aimed at real-time along with remote HM on IoT infrastructure and associated with cloud computing. The public data-set HC that was on the cloud was taken as the input. The system gave suggestions centered on the data (historical and empirical) that was present on the cloud. This existing framework was introduced to reveal knowledge on a database by enlightening the disguise patterns that could assist in convincing decision making. By using numerous input attributes associated with that disease, the prediction systems were employed in evaluating certain diseases, for instance, HD, breast cancer, liver disorders, diabetes, thyroid, dermatology, spect_heart, along with surgical data. Experimental outcomes were conducted utilizing some ML algorithms, say K-NN, Support Vectors Machine (SVM), Random Forests (RF), Decision Trees, along with MLP.

AKM Jahangir et al. [18] presented a multiple-sensory system via employing a smart IoT that gathered Body Area Sensor data to offer early caveat of an imminent cardiac arrest. The purpose of the existing work was to generate an integrated smart IoT that encompassed a lower power communication unit so that one could inconspicuously gather heart rates along with body temperatures utilizing a mobile phone without impeding their everyday life. The signal processing along with ML techniques was introduced for sensor data analytics for identifying and predicting sudden heart attack with higher accuracy.

SenthilKumar Mohan et al. [19] suggested a method that found significant features by applying ML techniques resulting in enhancing the accuracy on the forecast of cardiovascular disease. The hybrid RF with a linear model was utilized by joining the individuality of the RF in tandem

with the Linear Method (LM). This established to be quite accurate in the forecast of HD. This method gave an ameliorated performance level with an 88.7% accuracy level via the prediction model intended for HD.

ShadmanNashif*et al*. [20] suggested a cloud-centered HD prediction system to identify imminent HD utilizing ML techniques. Aimed at the precise detection of HD, effectual ML techniques ought to be employed that had been derived as of a distinctive analysis amongst numerous ML algorithms in a Java-centered Open Access Data Mining, WEKA. The algorithm was validated utilizing '2'extensivelyutilized open-access databases, wherein 10-fold cross-validation was executed to analyze the HD detection's performance. An accuracy level of 97.53% was found as of the SVM together with sensitivity accompanied by the specificity of 97.50% along with 94.94% correspondingly. Furthermore, an instantaneous patient monitoring system was developed utilizing Arduino that could sense some instantaneous parameters (such as body temperature, humidity, blood pressure, along with heartbeat) to make certain the HD patient non-stop via caretaker/doctor. The developed system sent the recorded data to the chief server every 10 sec. Consequently, the doctors could view the patient's real-time status by employing this application and start live video streaming on the off chance that an instant medication was needed.

Sambit Satpathy*et al*. [21] presented an IoT- centered analysis system that was employed to model a customer electronic device. This system disregarded the user if the parameters related to their health were above or below the standard range. The data amassed was uploaded to the cloud via an application and after that sent to the field-programmable gates array (FPGA). The unprocessed data were calculated as well as processed by means of the FPGA; in addition, pathological conditions were established on the patient's wearable IoT device. The method laid in the fuzzy classifier development that implied the pathological situation of diseases with high accuracy. The FPGA execution of the fuzzy classifier gave low execution time compared to KNN, SVM, decision tree, as well as Naive Bayes.

YosufElSaadany*et al*. [22] presented a multi-sensory system utilizing IoT that gathered heart rates along with body temperature. An embedded sensory system with a Low Energy Bluetooth communication module was employed to gather ECG along with body temperature data utilizing a smartphone in common surroundings. The utilization of signal processing along with ML aimed at sensor data analytics was introduced for the forecast of a sudden heart attack. The outcomes as of sensors' data were as well presented to illustrate that this approach gave a high rate of classification correctness in distinguishing the normal from abnormal ECG patterns. The system also found abundant applications in heart behavior detection for the populace with a range of disabilities who were at a high risk of a heart attack. Seven works were surveyed in this paper. The work projected in [16] HOBDBNN was an intellectual as well as an advanced classification model to predict the HD that gave the highest accuracy and reduced the mortality rate. [17] Projected an intellectual diagnosing framework recognized as the RF classifier to predict the different deadly diseases. Another work projected toward this path, an efficient RF in addition to the Linear Method (LM) was highlighted by [19], and this was quite accurate in the HD prediction. The HD prediction using [20] obtained the best accuracy and worst miss rate. The FPGA presented in [21] attains the accuracy as well as lower execution time but the technique was only apposite for the prediction of the pathological setting of cardiovascular diseases. The work was rendered in [18] and [22] suggested another online healthcare services diagnosis framework for observing remote heart patients utilizing a cell phone and wearable sensors. All these techniques prove their efficiency in their ways, but none of them stress on the significance of IoT data security. Moreover, none of them used a feature selection framework while classifying the data with a number of features to augment the systems training time, which will be overcome by the proposed work. The comparison table for the techniques reviewed in related works is evinced in table 1.

Table 1: Comparison of techniques used in Literature review

Author	Dataset used	Technique used	Advantages	Disadvantages
Zafer Al-Makhadmeh and AmrTolba [16]	UCI - ML repository	HOBDBNN	1. utmost recognition accuracy and lowest time complexity 2. Minimized the HD mortality	The algorithm did not employ any optimization algorithm aimed at feature selection, which increased the training time of the algorithm and that brought up some difficulties in dataset management for prediction.
PavleenKaur*et al*. [17]	Public datasets	RF classifier and IoT	1. Applicable for the prediction of multiple diseases, like HDs,	Security of the IoT data was not considered

			breast cancer, diabetes, etc. 2. Provided accurate outcomes for each considered dataset	
AKM Jahangir *et al*. [18]	-	Multisensory system utilizing a smart IoT	Combination of signal processing along with ML algorithms effectively identified the sudden heart attack with higher accuracy	The algorithm did not point out data security in addition to the system is not cost effective
Senthilkumar Mohan *et al*. [19]	Cleveland UCI repository	HRFLM	Having the ameliorated performance level with 88.7% accuracy level	The system did not have the capability of monitoring the HD in real time
ShadmanNashif*et al*. [20]	Cleveland HD dataset and Statlog HD dataset	SVM	Attained Highest accuracy	Lowest miss rate. The Photoplethysmography (PPG) centered blood pressure sensor or electronic sphygmomanometer were not fixed to the modeled patient monitoring system so the real time patient data cannot be predicted.
Sambit Satpathy*et al*. [21]	UCI repository database	FPGA	High accuracy, and low execution time	It was only applicable for the prediction of pathological conditions of cardiovascular diseases, not for all sorts of diseases and did not cover the data security
YosufElSaadany*et al*. [22]	-	Multisensory system	provided a high rate of classification correctness	The system was not tested foraged population who suffer from chronic heart problems.

III. PROPOSED METHODOLOGY

Nowadays, HD is the leading reason for deaths worldwide. Predicting the heart attack is an extremely intricate process. It can well be done only if the doctor is well-experienced and have good knowledge concerning the disease. The effectiveness of the remote HM system of the aged patients who need long-standing care has enhanced a lot attributable to the augmentation of the IoT along with its medical applications. The core technology of IoT on the HC system is the wireless body sensors network (WBSN). It utilizes a compilation of little-powered along with light wireless sensor nodes meant for scrutinizing a patient. Since this technology doesn't regard security, patient privacy is at risk. The existing works presented for the HC sector provides low security. A framework is proposed to trounce such drawback; thus, the data are transmitted more securely as of WBSN and the HD of the patients is predicted more accurately. The proposed work encompasses '3' phases i) Authentication, ii) Encryption, and iii) Classification. The authentication stage encompasses '3' steps: a) registration, b) login, and c) verification. After registering their details

into the hospital website or app, the patient will login to the website with his/her unique username and password. This registered patient detail is saved on the cloud server (CS) and the hospital database. Once the patient is registered, the cipher-based hash code is created using an SC as well as the SHA-512, which is employed for the verification of the patient. Amid verification, the server corroborates whether the patient is an authenticated one or not using the code created at the registration phase. If the patient is the right individual, then access is granted. After registration, the patient could upload previous and current medical reports. Modified Huffman algorithm (MHA) is employed for compressing the report, and it can well be stored on the CS for further use. The sensor that is fixed to the body (human) gathers the entire data as well as transfers the data to the cloud via a gateway. Using the PDH-AES method, the sensor data as of the sensor device is encrypted; later this information is transmitted to the cloud. Simultaneously, the hospital CS attains the encrypted sensor data and decrypts it. DLMNN classifier starts classification centered on the attained sensor data for the reason of envisaging the HD. To perform classification, the system goes through training

along with testing. Hungarian HD dataset is employed as an input to envisage the disease. In training, preprocessing is done, and classification is performed on the pre-processed data. After training, the sensor information as of the CS is tested and classified as a) normal and b) abnormal. In the instances of an abnormal outcome, an alert message is transmitted to the doctor to tend the patient. The proposed work is primarily concentrated on authentication, high security, DPS along with Monitoring. The proposed work's architecture is evinced in fig 1.

A. PATIENTS WITH IOT

This is the starting phase of the proposed word where the sensor device is fixed to the patient's body. The IoT device will sense the values as of the patient's body using the sensor as well as transmits the values to the HC application.

B. AUTHENTICATION

This is an imperative step in giving access to authorized users. The authentication procedure always functions at the beginning of the application. Disparate systems may need disparate sorts of qualifications to ascertain a user's identity. The credential frequently takes the form of a password that is confidential and known just to the individual together with the system.

To sustain high-secure authentication, the proposed work utilizes the cipher text-centered hashing technique. This phase encompasses '3' steps (i) Registration, (ii) Login, and (iii) Verification.
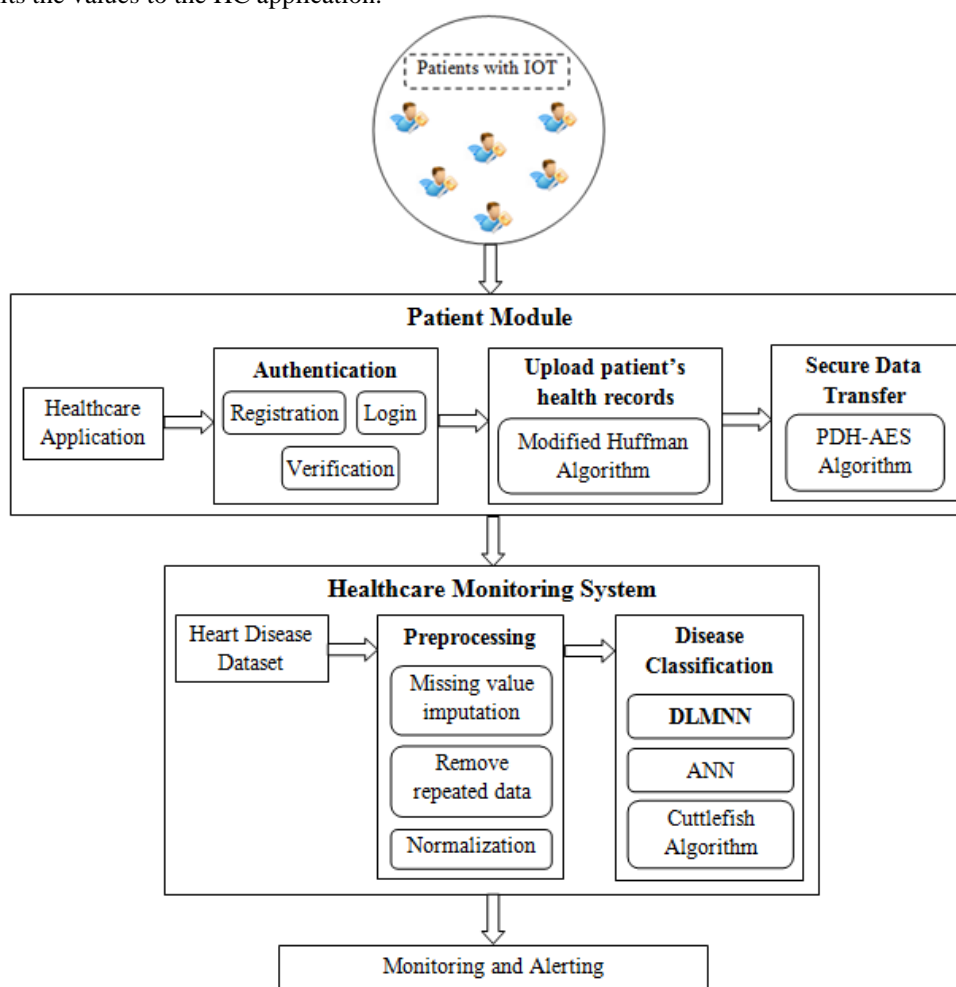

Figure 1 ⦂ **Block diagram for the proposed methodology**

1) REGISTRATION

In this phase, the patient registers their information in the HC application (hospital app) or website. After that, the server,

by utilizing an SC unites the username together with the password of the registered patient. An SC is an encryption technique in cryptography via which the units of plain

text are swapped with ciphertext, as per a fixed system. The "units" might be single letters, two letters, three letters, blend of the precedent, et cetera. The receiver, by doing the inverse substitution deciphers the text. Next, the Hash value of substation ciphertext is found utilizing SHA 512 algorithm.

SHA-512 stands as an advancement of the renowned SHA-1, and also it is basically a function of the cryptographic algorithm (SHA-2). It is extremely close to SHA-256 except that this one employs 1024 bits "blocks" and accepts 2^{128} bits maximum length string as input. With reference to Sha-256, the SHA-512 has other algorithmic modifications. The SC text is padded with extra bits to form a manifold of 1024 bits. After that, this block is bifurcated into smaller parts of 1024 bits. The 1st block is united with the initializing vector, and the hash code is created. The succeeding blocks are united with the formerly generated hash codes.

2) LOGIN

Generally, login is basically the procedure utilized to attain access to an application, typically on a remote computer. It is basically the process wherein an individual gains admission to a computer system via identifying along with authenticating themselves. Every system login phase needs the username together with the password of the user (registered). User's authentication is checked by carrying out the verification when the users log into the system.

3) VERIFICATION

The system verifies if the user is a registered one or not. By means of analyzing the user data, the administrator of the HC application verifies the users. In this phase, the entered username is joined with the password and the SC is applied. Subsequently, this ciphertext is converted utilizing SHA 512 into a Hash code, and this generated hash code is contrasted to save hash code value. If both hash values are equivalent, then user access to the system is allowed. Or else, the user is signified as the illegal user and their access is repudiated.

3.3 Upload Patient's Health Records

This is the 3rd phase, wherein the patient uploads their preceding and present health records suchlike X-Ray, Prescription details, MRI scan report, et cetera, to the HC application. However, the patient's health records (PHR) encompass a vast extent of data with a gamut of sizes. Thus, prior to sending it to the server, the PHR is compressed utilizing the MHA to lessen the file size and this compressed PHR is saved in a CS. The meticulous explanation of the MHA is rendered in section 3.3.1.

3.3.1   Modified Huffman Algorithm

Huffman coding is an algorithm that is employed for the loss-less compression of files centered upon the frequency of the symbol's incidence on the file, i.e., on the course of compression; this is labeled as Huffman encoding. The small code is given to the most produced character together with the large code is given to the least produced character. Huffman tree (HT) is basically a certain technique

by which every symbol is signified. The total bits that are needed for the representation of every character rely mainly on the total characters that are required to be signified in the instance of the binary representation. This technique makes sure to generate a code where that codeword is in no way will be the prefix for any other code-word. These codes are termed prefix codes.

The largest drawback that is present in the Huffman is that even a little change that occurs in any bit of the encoded string will shatter the whole message. Especially if the text is longer, then the level of the binary tree (BT) will be more, therefore more time will be taken for traversing through the BT. The MHA is proposed to trounce such drawbacks. In the proposed MHA, every character on the message is transmuted into ASCII codes. After that, the BT is built for those ASCII codes. Subsequent to building a tree, traverse the nodes to obtain an encoded text of every character. The instance of MHA is elucidated as follows.

Consider the input message that is required to be compressed as "Huffman".

- ➤ Initially for every character, the ASCII on the message are found. The ASCII for every character that is present on the input message are
  H -72, u - 117, f -102, m -109, a -97, and n -110.
- ➤ After that, the hash tree is formed for the attained ASCII values, which are exhibited below.
- ➤ After generating a hash tree, the hash tree is traversed to generate codes for every input character on the message. The code for the character is presumed as,
  (a) Beginning at the top, if the route is left, then appends 0 to the encoded text. If the route is right, then append 1.
  (b) Stop when the Leaf nodes are reached. The string of zeros and ones generated till now is the encoded text of that specific node in the tree. The encoded text of every character on the message is obtained as of the tree is written as H - 000, u - 011, f - 0, f - 0, m - 010, a - 00, and n – 01. The binary tree for the obtained ASCII values is exhibited in figure 2.
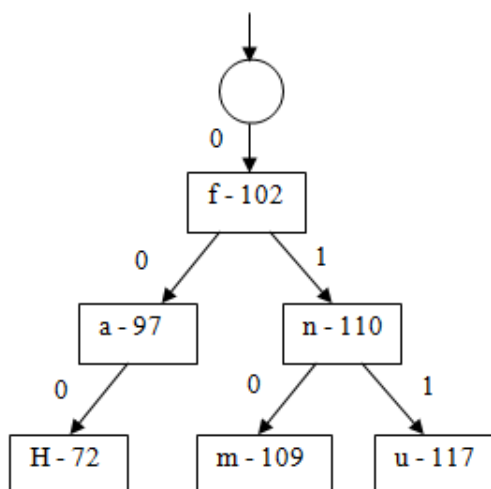
Figure 2: **Binary tree for given input**

> ➢ The final encoded text of the complete input message is written as 000011000100001. Amid decoding, produce the traits of every leaf traversed by the above-encoded text in the HT.

3.4 Secure Data Transfer

Here, the sensed data as of the patient are encrypted utilizing Patient id, Doctor Id, Hospital Id-Advanced Encryption Standard (PDH-AES) Algorithm. In the proposed work, the hospital CS generates a 128bit key. By uniting the '3' IDs i.e., Patient id, Doctor Id, Hospital id, this 128bit key is produced. If the key is produced centered on this notion, then every single patient encompasses a disparate key. By utilizing this 128-bit key, the sensed values are encrypted utilizing the AES.

3.4.1 AES Algorithm

AES is basically a symmetric-key block cipher that takes 128-bit blocks of data and a key and gives ciphertext as an output. AES treats these 128 bits of a data block as 16bytes, which are prearranged in '4' columns and '4' rows to process as a matrix. 128, 192, along with 256 bits are the '3' disparate key lengths that are allowed. For these three key lengths, AES performs 10, 12, in addition to 14 rounds correspondingly. Each round utilizes a disparate 128-bit round key that is computed centered on PDH. Every round of AES repeats these '4' major functions that follow to encrypt the data, which are (a) Sub Bytes, (b) Shift Rows, (c) Mix Columns, along with (d) Add Key.

(a) Sub Bytes

The sixteen input bytes are swapped by the fixed table. The outcome is in a'4' rows and '4' columns matrix.

(b) Shift rows

Every single one of the '4' rows of the matrix is shifted to the left side. The entries that 'fall off' are re-inserted to the row's right side. The shift is performed as follows −

- The I row is doesn't shift.
- The II row is shifted '1' (byte) spot to the left.
- The III row is shifted '2'spot to the left.
- The IV row is shifted '3'spot to the left.

The outcome is a unique matrix comprising the same sixteen bytes; however, shifted regarding one another.

(c) Mix Columns

By utilizing a mathematical function, every column of the '4' bytes is changed. The '4' bytes of one column is regarded as the input for this function, and then it outputs completely '4' different bytes. This replaces the original column. It ought to be recorded that this step is not performed in the last round.

(d) Add round Key

The round key is attached to the block of data by this transformation. The sixteen bytes of the matrix is regarded as 128 bits. These bits are XOR-ed with the 128bits of the rounds key.

The decryption of AES is to be done in the inverse order of the encryption process. Every round comprises '4' processes performed in the inverse order. i.e., i) Add round key, ii) Mix columns, iii) Shift rows, along with iv) Byte substitution.

3.5 Disease Prediction System

The sensor information is decrypted by the CS and transmitted to the hospital management after the process of encryption. On the Hospital side, the sensed data values by utilizing the DPS are monitored. The patient's HD can be predicted in the proposed work utilizing a DLMNN. For this, the system goes through training along with testing. For training, the Hungarian HD dataset is considered as the input. The DLMNN classifier trains the system. More time is taken for the detection of disease if the value is directly taken as of the IoT, thus there is a likelihood of inaccurate results. So, the system undergoes training. The steps are briefly elucidated as follows.

- ✓ Data collection
- ✓ Preprocessing
- ✓ Disease Classification

3.5.1 Data Collection

The classified result, i.e. normal as well as abnormal, is present in the Hungarian HD dataset. From the dataset, a total of 294 numbers of records or rows are taken for the proposed work. Each row contains the health records of different patients. The health records of the patients contain details like blood pressure level, heart rate, breathing rate, pulse et cetera, and these are all regarded as a feature of the dataset. To acquire an accurate result, the system should well be trained before disease classification. The Hungarian dataset is inputted for training which encompass76 attributes of HD patients. Initially, the data are gathered for the classification of HD as of this database. The gathered data is additionally

processed to obtain the classification outcomes, which are elucidated as follows

3.5.2   Preprocessing

Three steps are included in the preprocessing of the Hungarian HD dataset. They are i) replacing of missing attributes, ii) removal of redundancy, and iii) normalization. The taken Hungarian HD dataset encompasses 1314 missing values, which are represented by zero. These missing attributes are swapped by utilizing the maximal number of recurring attribute values. Subsequent to checking the whole patients' age group, blood pressure, along with cholesterol, the missing value of the specific attribute is replaced. If most of the attribute values of any patient are matched, then the value is swapped by the same position. Next, the data size is reduced by eradicating redundant or irrelevant attributes, and data normalization are done.

3.5.3   Disease Classification

It is the final and major step in DPS. Here, the DLMNN classifies the preprocessed data. The hidden layers in ANN are increased for deep learning and the Cuttlefish optimization algorithm (CFOA) was hybridized with this to lessen the backpropagation (BP) process. So, the proposed work is labeled as DLMNN. A brief explanation of DLMNN is rendered in the section below.

3.3.3   Classification using DLMNN Classifier

In this, the preprocessed data values are rendered as the input to the DLMNN. The weights are the haphazardly assigned values that are joined with every input [23]. The subsequent one is the hidden layer where nodes from this layer are labeled as hidden nodes. These nodes carry out the operation of adding up the input value's product in addition to the weight vector of every input node that is linked to it.

The weight values in DLNN are being optimized by the CFOA that is labeled as DLMNN. Arbitrary weight values provide more BP process to attain the outcome. Thus, optimization is done. So, the DLNN is labeled as DLMNN. In DLMNN, the activation operation is implemented in the hidden layer; in addition, the layer's output is transferred to the successive layer. These have an utmost effect on the classifier's output. The algorithmic steps in the DLMNN classification are,

➢ Initialize the pre-processed data values together with their corresponding weights utilizing equ (1) and (2)

$$P_{di} = \{ P_{d1}, P_{d2}, P_{d3}.....P_{dn} \} \ (1)$$

$$w_i = \{ w_1, w_2, w_3.....w_n \} \tag{2}$$

➢ Wherein P_{di} implies the input value that signifies the n number of pre-processed data values for instance $P_{d1}, P_{d2}, P_{d3}.....P_{dn}$ and w_i implies the weight value of

P_{di} that encompasses the n number of weights explicitly $w_1, w_2, w_3.....w_n$ for equivalent $P_{d1}, P_{d2}, P_{d3}.....P_{dn}$.

➢ The input preprocessed data is multiplied with the randomly chosen weight vectors, and after that, sum up that values fully [23], which is mathematically written as,

$$G = \sum_{i=1}^{n} P_{di} w_i \ (3)$$

Wherein G implies the summed value

➢ Ascertain the activation function (AF) by utilizing the equ (4),

$$F_{Ai} = S_i (\sum_{i=1}^{n} P_{di} w_i)$$

$$(4)$$

$$S_i = e^{-P_{di}^2}$$

$$(5)$$

Where F_{Ai} implies the Gaussian AF and S_i indicates the exponential of P_{di}. The proposed DLMNN uses Gaussian AF and also the proposed DLMNN is capable of working with other types of activation function, such as Sigmoid Activation function, Hyperbolic Tangents function, etc.

➢ Utilizing the equ (6), calculate the subsequent hidden layer's output

$$Y_i = B_{ai} + \sum S_i w_i \ (6)$$

Where, B_{ai} denotes the bias value, w_i specifies the weight betwixt the input and the hidden layers.

➢ Perform the precedent 3 steps for every layer of DLMNN. Lastly, estimate the output by summing the whole input signals' weights to attain the output layer neurons' value that is written as

$$V_i = B_{ai} + \sum O_i w_j$$

$$(7)$$

Where, O_i denotes the layer's value that precedes the output one, w_j specifies the hidden layer's weights, in addition, V_i indicates the output unit.

➢ The network output is contrasted with the target value. The difference betwixt these '2' values is termed as the error signal. This value is mathematically implied by utilizing (8) as,

$$E_s = T_i - V_i \text{ (8)}$$

Where, E_s implies the error signal, T_i specifies the aimed target output.

➢ Here, the output unit is weighted against the targeted value. Ascertain the associated error. Compute δ_i centered on this error, in addition, it is employed to allot the error at the output back to all other units on the network.

$$\delta_i = E_s [\ f(T_i)] \text{ (9)}$$

➢ Assess the weight correction by employing the BP methodology that is calculated utilizing

$$w_{ci} = \lambda \delta_i (P_{di}) \text{ (10)}$$

Where wc_i implies the weight correction, λ signifies the momentum term, and δ_i implies the error that is distributed in the network. The weight values are optimized using a CFOA. The explanation for CFOA is rendered in section 3.3.1.1.

3.3.1.1 Cuttlefish Optimization Algorithm

The CFOA is a meta-heuristic optimizations algorithm. It was inspired as of the cuttlefish's color-changing activities to locate the optimal numerical worldwide optimization issues [24]. Cuttlefishes disguise themselves by changing their colors to be invisible or visible in their environment. The colors along with patterns are generated via the light reflection on their '3' disparate layers of cells.
The cuttlefish algorithm regards chiefly '2' processes: i) reflection and ii) visibility. The reflection of the light mechanism that was adopted by these cuttlefish's cell layers are simulated as the reflection process, and its visibility of the matching patterns are simulated as the visibility process. By utilizing these '2' process, the worldwide optimum solution is obtained. It is centered on the division of cells into '4' groups, they are groups 1 (G1), groups 2 (G2), groups 3 (G3), and groups 4 (G). These groups work autonomously as well as share the best solution. The CFOA begins with arbitrary solutions for initializing the populace and functions until the stop criteria are met. The new solution in the CFOA is computed utilizing the equ (11)

$$N = R + V \text{ (11)}$$

Where N denotes the new solution, R and V denotes the reflection in addition to visibility.

➢ Let's initialize the populace of F (elements) having N initial solutions as $F = \{k_1, k_2, ... k_N\}$. This populace spread over the d dimensional problem space at random positions (k) using the below equation

$$F(p) \cdot k(q) = Rd * (Ul - Ll) + Ll\ (\ p = 1,2,.....N\ , \\ q = 1,2,.....d\ ) \text{ (12)}$$

Where U_l and L_l implies the upper as well as the lower limit of the issue domain, and Rd implies an haphazard number in gamut (0, 1). Here, in the proposed method, the upper limits in addition to the lower limits of the CFA problem domain are set as 5 and 0.5. Each individual k_p within the populace represents a single cell, and it is associated with '2' values: fitness and a vector of d-dimension continuous values. Next, the best solution is kept in bp, and also the average of bp is computed and saved in AV_{bp}, after that the populace is bifurcated in mentioned '4' groups of cells for six cases, which are elucidated as follows.

G1 (case 1 and case 2): InG1, cases 1 along with 2 are implemented (the interaction betwixt chromatophores and iridophores) to generate a new solution centered upon the reflection together with the visibility of pattern [25], additionally, these cases are viewed as a global search that is mathematically estimated utilizing (13) and (14).

$$R(q) = r * G_1(p) \cdot k(q) \text{ (13)}$$

$$V(q) = v * (bp(q) - G_1(p).k(q)) \text{ (14)}$$

Wherein p is the p th cell in group G_1, $k(q)$ represents the q th point of p th element, bp implies the best solution and it gives the best points' average value, and r and v are two arbitrary numbers in the gamut (-1, 1),

G2 (case 3 and case 4): In G2, the CFOA utilizes case 3 along with case 4 (iridophores cells operators) to compute new solutions centered upon the reflected light that is coming as of the best solution together with the visibility of the matching pattern [26]. These cases are regarded as a local search, and they are calculated using equation (15) and (16)

$$R(q) = r * bp(q) \tag{15}$$

$$V(q) = v * \left(bp(q) - G_2(p).k(q) \right) \tag{16}$$

G3 (case 5): In G3, the CFOA applies case 5 (leucophores cells operator) as a local search to form a new solution via reflecting light as of the region about the best solution along with pattern's visibility [27] that is computed as

$$R(q) = r * G_1(q) \cdot k(q) \tag{17}$$

$$V(q) = v * \left(bp(q) - AV_{bp} \right) \tag{18}$$

Where AV_{bp} specifies the bp 's average value

G4 (case 6): In G4, case '6' is used (leucophores cells operator) as a global search for an arbitrary solution via reflecting the incoming light, which is evaluated in equation (12). The CFOA pseudo-code is evinced in fig 3.

The outcome of the training contains '2' classes centered upon the heart condition of the patient as i) normal and ii) abnormal. After training, the testing phase is performed. The sensor device that is fixed on the patient simultaneously transmits the sensor values. These sensor values are classified and centered on the training results, that means the sensor values as of IoT, are compared with the training phase's values. The system compares both values, furthermore, gives the classified results. If the classified results of the patient data are abnormal, then the system alerts the doctor for further treatments.

Figure 3 exhibits the CFA pseudocode for getting the optimized weight values of DLMNN. Initially, the weight values of every neuron in the DLMNN are given as the input to the CFA. In CFA, first, the populace initialization of F elements is done with an arbitrary solution for performing the optimization, and the fitness value is gauged for every element in the populace. The element with the highest fitness value is considered as the best, and it is kept in bp . After that, the population is split into '4' groups, such as G1, G2, G3, along with G4. Each group applies different cases to attain the best solution. The average value of bp is computed if the stopping conditions is not met and that computed average value is saved in AV_{bp}. For every constituent in G1, G2, G3, G4, '6' cases are performed in total. For the entire constituent in G1, cases 1 and 2 are applied and the solution is found. Next for the constituent in G2, cases 3 and 4 are applied and the solution is found. Similarly, for the constituent in G3 as well as G4, cases 5 and 6 are implemented and the new solutions are found. From those 4 solutions, the best solution is finally derived centered on their fitness values, and that is considered as an optimized one. Likewise, the iterations will be continued to get optimized weight values aimed at the entire neurons on the classifier.
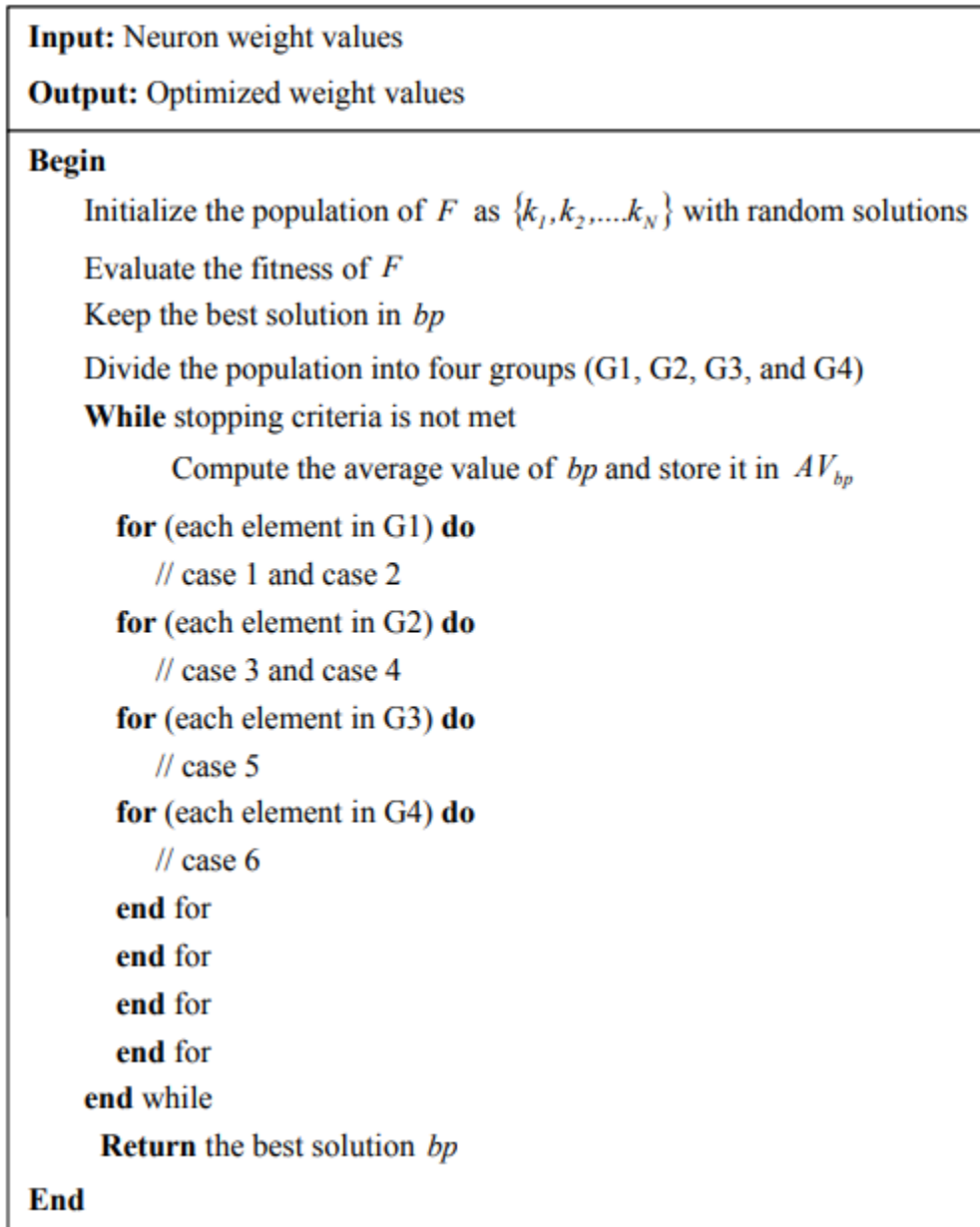

Input: Neuron weight values

Output: Optimized weight values

Begin

    Initialize the population of F as $\{k_1, k_2, \ldots k_N\}$ with random solutions

    Evaluate the fitness of F

    Keep the best solution in bp

    Divide the population into four groups (G1, G2, G3, and G4)

    While stopping criteria is not met

        Compute the average value of bp and store it in AV_{bp}

    for (each element in G1) **do**

      // case 1 and case 2

    for (each element in G2) **do**

      // case 3 and case 4

    for (each element in G3) **do**

      // case 5

    for (each element in G4) **do**

      // case 6

    end for

    end for

    end for

    end for

   end while

    Return the best solution bp

End

Figure 3:**Pseudocode for CFA**

IV. RESULT AND DISCUSSION

The proposed IoT based HD prediction system using DLMNN is implemented in the working platform of JAVA. In this phase, the performance rendered by the proposed methods utilized in data compression (DC), disease prediction, and data transfer is assessed by means of comparing the proposed methods with the existing works regarding some performance metrics. The meticulous explication of the proposed methods' analysis is evinced in the below sections

A. Performance Analysis of data compression

In the proposed work, the MHA is utilized in DC. Once the patients upload their PHR in the hospital app or website, each patient record is compressed and stored in a CS using MHA. Here, the proposed MHA's performance is weighted against the existing Huffman algorithm in respects of the compression time and compression ratio (CR).

The DC ratio is a gauge of the relative decrease in the size of data representation that is generated by a DC algorithm. This also labeled as compression power, which is evaluated by dividing the uncompressed size by means of the compressed size as

$$C_r = \frac{U_s}{C_s} \quad (19)$$

Where

C_r - CR,

U_s - Uncompressed file size

C_s - Compressed file size

The performance analysis table for the proposed and existing Huffman algorithms is proffered in table 2.

TABLE 2
PERFORMANCE COMPARISON OF MHA AND HA

File Size (MB)	Proposed MHA		Existing HA	
	Compression Time (ms)	CR	Compression Time (ms)	CR
5	10224	3.8892	10324	2.4542
10	21225	3.8901	21448	2.6887
15	30578	3.8904	30822	2.5534
20	40870	3.8907	41187	2.7535
25	50785	3.8909	50887	2.8843

Table 2 exhibits the performance comparison of the proposed MHA with prevailing HA showing the compression time and CR. Totally '5' different kinds of file sizes are taken for analyzing the MHA technique's performance. For the 5MB file, the proposed MHA takes 10224ms compression time, but the prevailing HA takes 10324ms for compressing the same 5MB file, which is higher than the MHA. In the same way, the MHA and HA take 50785ms and 50887ms to compress the 25mb file. For both the file sizes, MHA takes lesser time for compression when contrasted to the existing HA, and for the remaining file sizes, such as (10, 15, and 20MB), the compression time of MHA is lesser than HA. By comparing the CR of two methods (MHA and HA), it is inferred that the MHA gives the highest values for the CR. For 5, 10, 15, 20, and 25MB files, the MHA gives 3.8892, 3.8901, 3.8904, 3.8907, and 3.8909 of CR whereas the existing HA gives 2.45425, 2.6887, 2.5534, 2.7535, and 2.8843 of CR. For the best compression technique, the compression time ought to be low and the CR should be high. Both are achieved by MHA. So, from the comparison, it is established that the proposed MHA works well for DC in the HD prediction system. Table 1 could be graphically evinced in figure 4.
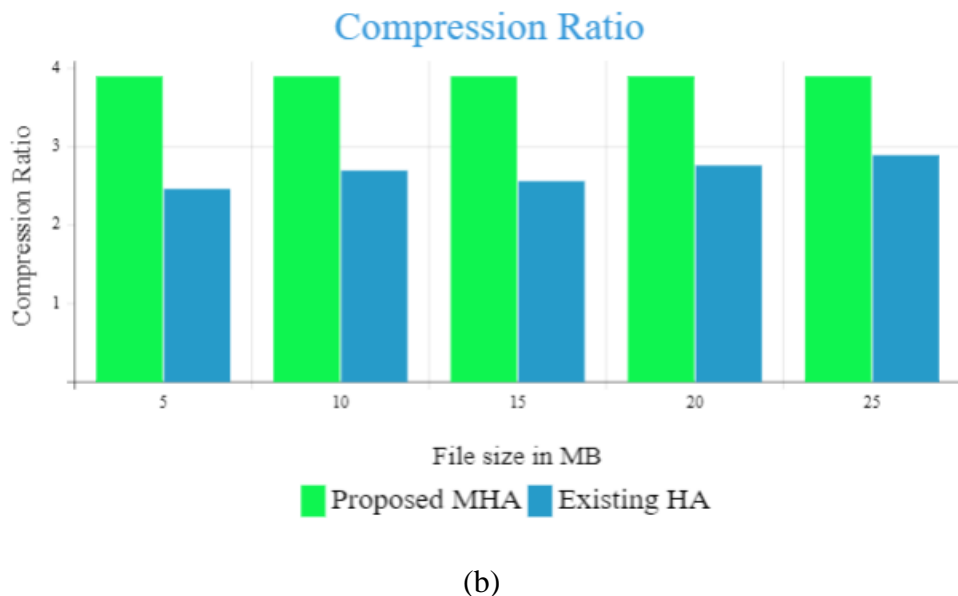

(a)

(b)
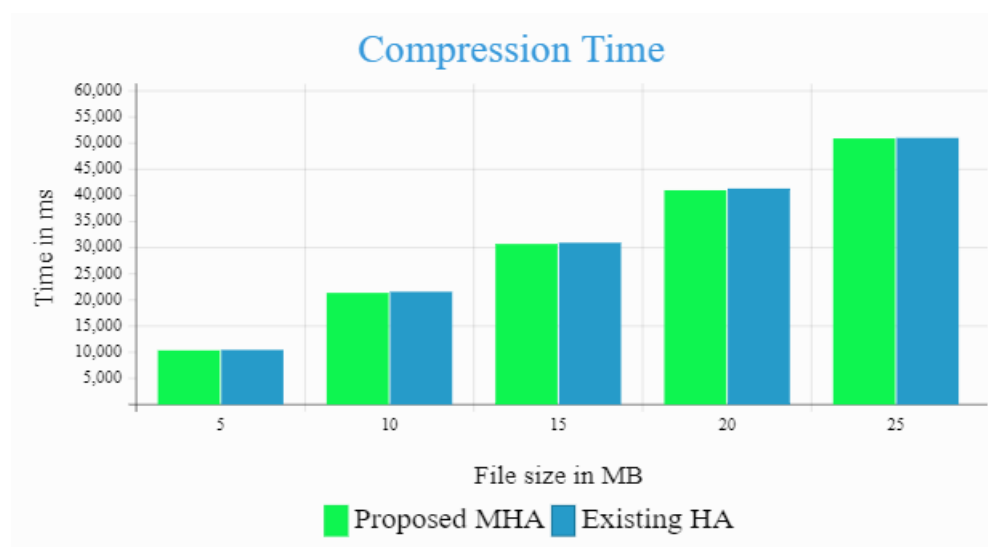
Figure 4: Comparison graph of the proposed MHA and existing HA

B. Performance analysis data transfer technique

The sensed data of the patient from the IoT device is securely sent to hospital admin using the PDH-AES encryption technique to avert the data of the user as of various attacks. Here, the proposed PDH-AES technique's performance used in secure data transfer is compared with the AES regarding encryption time (E_t), security level (S_l), and decryption time (D_t), which is plotted as graph as evinced in figure 5. The E_t and D_t are calculated as follows

➤ *Encryption Time (E_t)* - E_t is the time taken by the encryption algorithm to generate a ciphertext as of the plain text. It is calculated by taking the difference betwixt the encryption's ending time and the encryption's starting times and is expressed as,
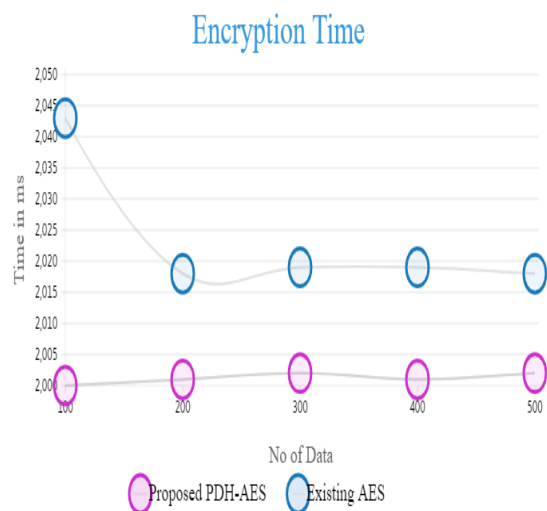
$$E_t = E_{et} - E_{st} \quad (20)$$

Where E_{et} denotes the encryption ending time, E_{st} signifies the encryption starting time.

➤ Decryption Time *(D_t)* - D_t is computed by taking the difference of the decryption's ending and starting times and is expressed as,

$$D_t = D_{et} - D_{st}$$
$$(21)$$

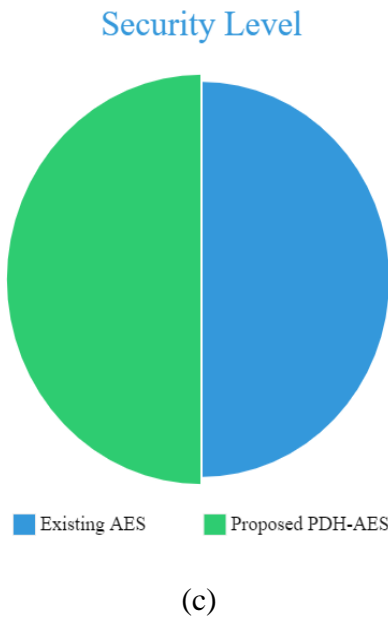Where D_{et} denotes the decryption ending time and D_{st} implies the decryption starting time.

(a)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI
10.1109/ACCESS.2020.3007561, IEEE Access

IEEE *Access*

Author Name: Preparation of Papers for IEEE Access (February 2017)

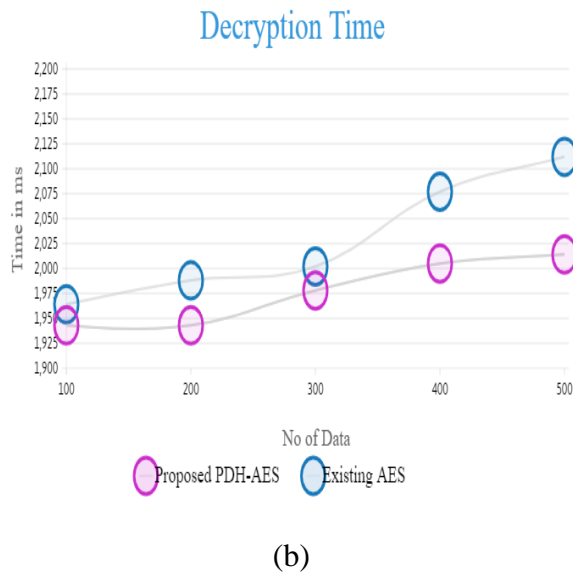### Decryption Time

(b)

Security Level

(c)

Figure 5: Comparison graph for PDH-AES and AES techniques

Figure 5 contrasts the PDH-AES encryption technique's performance with the AES technique concerning (a) E_t, (b) D_t, and (c) S_l. The E_t and D_t varies centred upon the number of data of the IoT device. Totally 500 numbers of data are taken for this comparison. For 100 numbers of data, the PDH-AES takes 2000ms for encrypting the data, but the existing AES gives 2043ms of E_t which is slightly bigger than the PDH-AES method. The same data can be decrypted using the PDH-AES and AES techniques, and these techniques give 1964ms and 1943ms for D_t. Similarly, for 200 nodes, the exiting AES takes 2018 and 1988 for encrypting along with decrypting the data, which is high

when compared to proposed PDH-AES (E_t =2001, and D_t = 1943). When comparing the remaining numbers of data (300, 400, and 500), the proposed PDH-AES takes lesser E_t and D_t than AES. The proposed PDH-AES attains the topmost security (95.87%) than the existing AES (92.54%). So, the PDH-AES method performs well for data transfer in a more secure manner.

C. *Performance analysis of disease prediction system*

Here, the DLMNN classifier's performance for DPS is weighted against the existing artificial neural network (ANN) concerning sensitivity, accuracy, specificity, along with f-measure, which is exhibited in the below figures. The performance measure values are measured in (%), and they are varied centred on the total data. These measures are computed based on '4' values: True positive (tp), false Positive (fp), True Negative (tn), along with False Negative (fn) where, tp is the number of normal classes correctly classified, tn implies the number of normal classes wrongly classified as an abnormal, fp signifies the correctly classified abnormal classes, and tn implies the total abnormal classes incorrectly categorized as a normal. The metrics are evaluated as,

$$S_n = \frac{tp}{tp + fn} \quad (22)$$

$$S_t = \frac{tn}{tn + fp} \quad (23)$$

$$A_y = \frac{tp + tn}{tp + tn + fp + fn} \quad (24)$$

$$F_m = 2.\frac{pr.re}{pr + re} \quad (25)$$

Where S_n, S_t, A_y and F_m indicates the sensitivity, specificity, accuracy, and f-measure metrics. pr and re represent the precision as well as recall that can be computed as

$$pr = \frac{tp}{tp + fp} \quad (26)$$

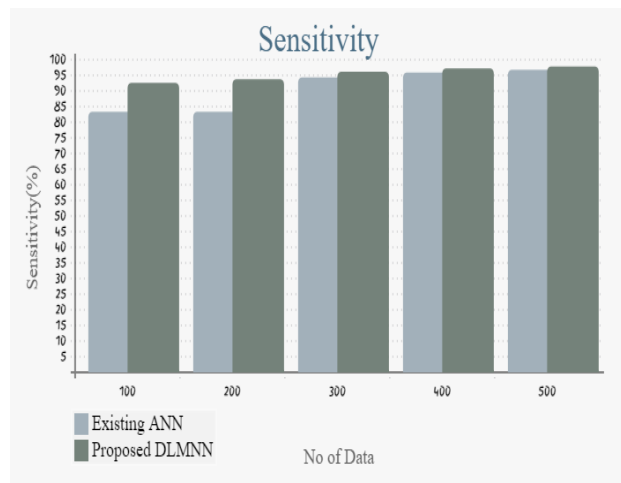$$re = \frac{tp}{tp + fn} \quad (27)$$

Figure 6: Sensitivity comparison of the proposed and existing techniques

Figure 6 compares the DLMNN's performance with ANN concerning sensitivity. 100 to 500 data are considered for this comparison, and the sensitivity is measured for each set of data. For both 100 and 200 data, the existing ANN gives a sensitivity of 83.3333 whereas the proposed DLMNN gives a sensitivity of 92.5925 and 93.75. Here, the DLMM attains the topmost sensitivity. Similarly, when comparing the outcomes of existing ANN and proposed DLMNN for the remaining set of data, such as (300, 400, and 500), the DLMNN gives the highest sensitivity measure that shows the excellent performance rendered by the proposed classifier.
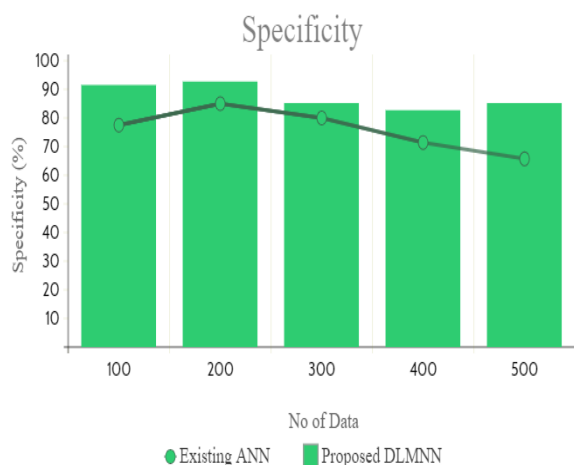

Figure 7: Specificity comparison of the proposed and existing techniques

Figure 7 depicts the specificity values attained by the DLMNN and ANN. For 100 and 200 numbers of data, the existing ANN gives 77.5 and 85 specificity whereas the DLMNN gives 91.3043 and 92.5, which is above the ANN. Similarly, for the remaining data, such as (300 to 500), the DLMNN gives the topmost specificity measure. So, from the

comparison, it is perceived that the DLMNN classifier acquires greater performance concerning the specificity measure.

Figure 8: Accuracy comparison of the proposed and existing techniques

Figure 8 exhibits the accuracy performance graph for the proposed and exiting techniques, which is computed for total 500 data. For 100 nodes, the existing ANN achieves the average accuracy of 81 but the proposed DLMNN acquires the topmost accuracy of 92. The accuracy percentage gradually increases when the number of nodes increases. When considering the highest number of nodes (500), the accuracy of DLMNN is 96.8 but the ANN gives 94.6. The ANN also gives better values for all nodes, but when comparing with the proposed DLMNN, the ANN gets the lowest performance. So, from this comparison, it is known that the proposed DLMNN achieves the highest accuracy for predicting the heart condition of the patient when contrasted with ANN.
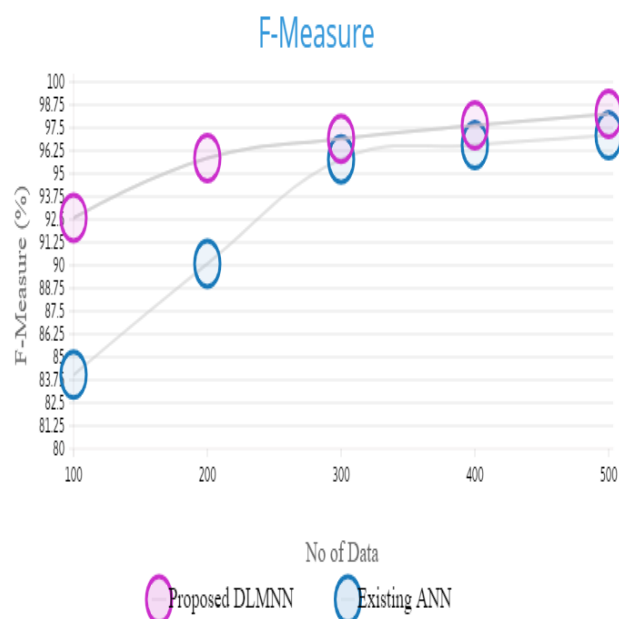
Figure 9: Performance comparison of DLMNN with ANN

Figure 9 illustrates the DLMNN's performance with ANN concerning f-measure. For 100 numbers of data, the DLMNN gives 92.5925 for f-measure, which is higher than the existing ANN's f-measure (84.0336). For 500 numbers of data, DLMNN gives 98.2532 for f-measure, but the ANN technique is 97.0873. For the remaining 200, 300, as well as 400 numbers of data, ANN gives the lowest performance when weighed against DLMNN. So, from the comparison of all measures, the sensitivity, specificity, f-measure, along with accuracy, it is stated that the DLMNN classifier provides better results for predicting HD contrasted with the ANN.

V. CONCLUSION

Here, a technique to detect HD is proposed using the DLMNN classifier. The experiment's outcomes are evaluated for proposed and existent methods. Three comparisons have been made for the proposed methods utilized in DC, data transfer, and disease prediction. The proposed MHA utilized in DC gives the highest values of CR and takes lesser time for DC. The PDH-AES technique utilized in secure data transfer achieves the best results, which offer the highest level of security (95.87%), and the lowest time aimed at encryption along with decryption. Finally, the DLMNN aimed at disease prediction provides the highest level of sensitivity, accuracy, specificity, together with f-measure in disease prediction. Using this IoT-centred DLMNN classifier, the HD of the patient can be identified more accurately. If the heart condition of the patient is identified as abnormal, then further treatment will be rendered to the patient immediately by the doctor.

REFERENCES

1. Praveen Kumar Gupta, Bodhaswar T. Maharaj, and Reza Malekian, "A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres", Multimedia Tools and Applications, vol. 76, no. 18, pp. 18489-18512, 2017.

2. Prabal Verma, Sandeep K. Sood, and SheetalKalra, "Cloud-centric IoT based student healthcare monitoring framework", Journal of Ambient Intelligence and Humanized Computing, vol 9, no. 5, pp. 1293-1309, 2018.

3. MuraliSubramaniyam, Deep Singh, Se Jin Park, SeoungEun Kim, Dong Joon Kim, Jung Nam Im, Kyung-Sun Lee, and Seung Nam Min, "IoT based wake-up stroke prediction-Recent trends and directions", In IOP Conference Series: Materials Science and Engineering, IOP Publishing, vol. 402, no. 1, pp. 012045, 2018.

4. TaherehSaheb, and Leila Izadi, "Paradigm of IoT big data analytics in healthcare industry: A review of scientific literature and mapping of research trends", Telematics and Informatics, 2019.

5. Kwok Tai Chui, Ryan Wen Liu, Miltiadis D. Lytras, and Mingbo Zhao, "Big data and IoT solution for patient behaviour monitoring", Behaviour& Information Technology, pp. 1-10, 2019.

6. Jagadeeswari, V., Subramaniyaswamy V., Logesh R., and Vijayakumar V., "A study on medical internet of things and big data in personalized healthcare system", Health information science and systems, vol. 6, no. 1, pp. 14, 2018.

7. Ganesan, M., and Sivakumar N., "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), IEEE, pp. 1-5, 2019.

8. PriyanMalarvizhi Kumar, and Usha Devi Gandhi, "A novel three-tier Internet of Things architecture with machine learning algorithm for early detection of heart diseases", Computers & Electrical Engineering, vol. 65, pp. 222-235, 2018.

9. AshviniKamble, and SonaliBhutad, "IOT based patient health monitoring system with nested cloud security", In 4th International Conference on Computing Communication and Automation (ICCCA), IEEE, pp. 1-5, 2018.

10. Ani, R., Krishna S., Anju N., Sona Aslam M., and Deepa O. S., "Iot based patient monitoring and diagnostic prediction tool using ensemble classifier", In International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE, pp. 1588-1593, 2017.

11. AmjadFayoumi, and Khalid BinSalman, "Effective Remote Monitoring System for Heart Disease Patients", In IEEE 20th Conference on Business Informatics (CBI), IEEE, vol. 2, pp. 114-121, 2018.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3007561, IEEE Access

IEEE Access

Author Name: Preparation of Papers for IEEE Access (February 2017)

12. FatmaPatlarAkbulut, and Aydin Akan, "A smart wearable system for short-term cardiovascular risk assessment with emotional dynamics", Measurement, vol. 128, pp. 237-246, 2018.

13. Aieshwarya. B. Chavan Patil, "An IoT based health care and patient monitoring system to predict medical treatment using data mining techniques: Survey", International Journal of Advanced Research in Computer and Communication Engineering, vol. 6, no. 3, 2017.

14. Chao Li, Xiangpei Hu, and Lili Zhang, "The IoT-based heart disease monitoring system for pervasive healthcare service", Procedia computer science, vol. 112, pp. 2328-2334, 2017.

15. PriyanMalarvizhi Kumar, S. Lokesh, R. Varatharajan, Gokulnath Chandra Babu, and P. Parthasarathy, "Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier", Future Generation Computer Systems, vol. 86, pp. 527-534, 2018.

16. Zafer Al-Makhadmeh, and AmrTolba, "Utilizing IoT wearable medical device for heart disease prediction using higher order Boltzmann model: A classification approach", Measurement, vol. 147, pp. 106815, 2019.

17. PavleenKaur, Ravinder Kumar, and Munish Kumar, "A healthcare monitoring system using random forest and internet of things (IoT)", Multimedia Tools and Applications, pp. 1-12, 2019.

18. Majumder, A. K. M., YosufAmrElSaadany, Roger Young, and Donald R. Ucci, "An energy efficient wearable smart iot system to predict cardiac arrest", Advances in Human-Computer Interaction 2019.

19. Senthilkumar Mohan, ChandrasegarThirumalai, and Gautam Srivastava, "Effective Heart Disease Prediction Using Hybrid Machine Learning Techniques", IEEE Access, vol. 7, pp. 81542-81554, 2019.

20. NashifShadman Md, Md Rakib Raihan, and Mohammad Hasan Imam Rasedul Islam, "Heart disease detection by using machine learning algorithms and a real-time cardiovascular health monitoring system", World Journal of Engineering and Technology, vol. 6, pp. 854-873, 2018.

21. SambitSatpathy, Prakash Mohan, Sanchali Das, and SwapanDebbarma, "A new healthcare diagnosis system using an IoT-based fuzzy classifier with FPGA", The Journal of Supercomputing, pp. 1-13, 2019.

22. YosufElSaadany, AKM Jahangir A. Majumder, and Donald R. Ucci, "A wireless early prediction system of cardiac arrest through IoT",In 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), IEEE, vol. 2, pp. 690-695, 2017.

23. Deevi Radha Rani, and Geethakumari G, "Secure data transmission and detection of anti-forensic attacks in cloud environment using MECC and DLMNN", Computer Communications, vol. 150, pp. 799-810, 2020, 10.1016/j.comcom.2019.11.048.

24. Cuttlefish Optimization Algorithm: https://sites.google.com/site/cuttlefishalgortihm/

25. Deepak Gupta, Arnav Julka, Sanchit Jain, Tushar Aggarwal, Ashish Khanna, N. Arunkumar, and Victor Hugo C. de Albuquerque, "Optimized cuttlefish algorithm for diagnosis of Parkinson's disease", Cognitive systems research, vol. 52, pp. 36-48, 2018, 10.1016/j.cogsys.2018.06.006.

26. Adel Sabry Eesa, and Zeynep Orman, "A new clustering method based on the bio-inspired cuttlefish optimization algorithm", Expert Systems, vol. 37, no. 2, e12478, 2020.

27. Muataz Salam Al Daweri, Salwani Abdullah, and KA Zainol Ariffin, "A migration-based cuttlefish algorithm with short-term memory for optimization problems", IEEE Access, vol. 8, pp. 70270-70292.

Simanta Shekhar Sarmah is an IT Professional having more than 12 years of experience is various industries such as Education, Health care, Hedge Funds, Government etc. He had received his Bachelor of Computer Technology degree from Nagpur University, India and received a master's degree in science from Texas A&M University - Commerce, USA. He has been working as a BI Consultant at National Science Foundation, USA since 2014. He has published several papers in various international journals and his research interest include Blockchain Technology, Internet of Things, Artificial Intelligence, Cloud Computing, Data Security, etc.