Soft Computing (2021) 25:12159–12174
https://doi.org/10.1007/s00500-021-05866-3

FOCUS

Cloud- and IoT-based deep learning technique-incorporated secured health monitoring system for dead diseases

Priyan Malarvizhi Kumar[1] · Choong Seon Hong[1] · Gokulnath Chandra Babu[2] · Jeeva Selvaraj[3] · Usha Devi Gandhi[2]

Accepted: 3 May 2021 / Published online: 26 May 2021

Abstract

Internet of Things (IoT)-enabled e-healthcare applications are contributing more to the society for providing healthcare monitoring services efficiently in smart environment. Security of healthcare system is to be considered as an important issue due to the huge volume of users and their secret data availability in this fast internet era and cloud databases. To store the patient's health data securely in the form of electronic version raises the concerns about the patient data privacy and security. Moreover, handling volume of data is also very complex task today with normal classifiers. For this purpose, many deep learning algorithms are available for classifying the huge volume of data successfully. For these all purposes, we propose a new healthcare monitoring system to monitor the disease level by predicting the diseases according to the original data that are collected from the patients who are available in remote places. Moreover, we propose a secured data storage model for storing the patient's data securely in cloud databases. Here, we introduce two new cryptographic algorithms for performing encryption and decryption processes. The experiments have been conducted for evaluating the performance of health monitoring system according to the particular diseases such as heart and diabetic diseases. This work considered the UCI medical dataset and the data collected from patients whose are available remotely through IoT devices. The proposed system is evaluated based on sensitivity, specificity, F-measure and prediction accuracy. The experimental results demonstrate that the proposed system outperforms the existing e-healthcare systems.

Keywords Internet of Things · Deep learning · Machine learning · Encryption · Decryption · Secured storage · Security · Privacy preservation

1 Introduction

The latest technological development is travelling towards the introduction and incorporation of new technologies in the existing data communication technology for ensuring the secured data communication and easy online applications. The new technologies are facilitating the user to secured storage, easy accessibility and to serve the society in the field of healthcare and natural disaster. Now, the Internet of Things (IoT) is playing major roles in the direction of serving people in medical field. IoT is able to connect the people and devices in the fast internet world virtually for exchanging the information. The IoT devices are incorporating into the various online applications specially for collecting data and to create smart homes, e-healthcare, smart transportation and smart cities in this digital world. As of now, the IoT-enabled medical devices and sensors are most useful for developing healthcare applications. e-healthcare is necessary today due to the vast expensive of healthcare and the availability of new diseases in this fast world and urgently needed the transformation of healthcare. Moreover, cloud computing technology and IoT are mutually dependent on each other. This combination has become a valuable platform to monitor the patient's health level whose is remotely available to supply continuous services by providing useful information to the

Communicated by Vicente Garcia Diaz.

✉ Priyan Malarvizhi Kumar
mkpriyan@khu.ac.kr

[1] Department of Computer Science and Engineering, Kyung Hee University, Seoul, Korea

[2] School of Information Technology and Engineering, VIT University, Vellore, India

[3] SRM University, Chennai, India

patients and doctors. This platform is helped for compensating their constraints such as energy, processing cost and storage. Even though, the IoT-based cloud framework is to be enhanced to initiate new services through applications.

The major contributions of this paper are as follows: (1) To introduce a new secured storage algorithm for storing the data securely in cloud database, (2) To propose a new deep learning algorithm for predicting the patient information that is retrieved from remotely available patients through IoT devices, (3) To introduce a new encryption algorithm for encrypting the data safely, (4) To propose a new decryption algorithm for decrypting the data correctly, (5) To introduce new intelligent fuzzy rules for making effective decisions on medical IoT data, (6) To introduce a new formula for ranking the patient's data and a new spatial and temporal constraints were applied on CNN classifier for predicting the patient health condition right now and (7) Conduct the various experiments for evaluating the performance of the proposed health monitoring system.

The remainder of this research article is formulated as below: Sect. 2 summarizes the topics that are available as title of this work such as cloud computing, IoT, medical data, deep learning techniques and secured data storage. The working flow of the proposed works is explained through a common architectural diagram in Sect. 3. Section 4 explained in detail about the proposed secured storage algorithm, data gathering from IoT devices and deep learning algorithms. Section 5 contains the various experimental results and the reason for the performance increment in this work. Section 6 gives proper conclusion for the proposed works in the direction of secured storage, feature selection, data retrieval and prediction or classification along with future works in all directions of this work.

2 Literature survey

Enormous works are available in the literature in the direction of healthcare in the past. Among them, Smith and loff (1999) developed a healthcare system which has data with the consideration of security. Here, the proposed system stores the health records with the concern of data privacy and security. The major objective of their system is not for creating a new idea according to the security perspective of their system. Finally, they have suggested the possible research directions in the area of security in healthcare systems. Chou and Chou (2002) have discussed, the online healthcare portal's, the necessity to develop the healthcare portal, merits, and demerits of the healthcare portal in this fast internet world. Geylani and Turhan (2006) developed a new smart card-based healthcare information system to identify and transmit the healthcare information through distributed and communication protocols that are specially introduced in this work for protecting the secret data. In their system, they have incorporated two newly proposed software modules. Moreover, the patient record also stored in the smart card and it used for authentication in the system on data access activity. In addition, keys were used as encryption key and digital signature key to secure the data and ensured the secured data communication in between the clients and servers through distributed protocol.

The particular legal and rights-oriented issues arising due to the occurrence of cryptographic and the data/user privacy on Indian aspect are analysed by Neha (2009). In her analysis, she has considered the solutions for the questions such as why have to protect the valuable data in network, and how to protect from attackers in network. Moreover, she analysed the way to achieve the speed, cost effectiveness and efficiency. Lu-Chou et al. (2009) developed an approach for preserving the user's privacy and the patient's data security over the local storage space for avoiding any irrelevant situations. According to the HIPAA regulations, approach was developed for protecting, recovering and verifying the patient's identification process on e-health records. End of their analysis, they have proved that their approach is an effective over the process of confirming the data security and data privacies for the patient records by applying a portable storage medium.

Saeed and Ali (2012) presented new protocols for ensuring the data and users privacy preservation for the two neural classifiers such as back propagation and ELM algorithms while partitioning the data in horizontal and vertical manner among various parties. Their protocols preserved the privacy of input data and the newly developed model for upcoming data in learning process. Moreover, the final model is shared with all clients securely who can predict the result for their data. Xiaohui et al. (2012) developed a new authentication scheme and transmission scheme based on two features to safeguard the healthcare data privacy and also protecting in data sharing process in social networks. In health social networks, the users tagged with organized features. Moreover, it enables every user for creating a new feature as proof within the networks and when the features were identified as anonymous. On the other hand in the transmission scheme activates a specific user for encrypting her/his health data into a cipher text that bonded on formulated access policy. In addition, the new policy is defined by a group of target features. Those were fulfilled the policy can decrypt the cipher text. Finally, they have proved that their schemes can resist the different kinds of attacks such as attribute-trace attack, forgery attack, collusion attack by conducting various experiments. Heshan et al. (2016) explored that the challenges and issues in the direction of secured data storage in cloud for the IoT devices. The major applications were analysed with the possible solutions that are already outlined according to the application of homomorphic encryption mechanisms for achieving high data security and the data privacy on cloud environments. The drawbacks of the available models also considered for the analysis and also the systems proposed to achieve high accuracy and efficiency for the encrypted data on cloud environment.

3 System architecture

The overall architecture of the proposed system is shown in Fig. 1. The proposed healthcare monitoring system consists of nine components such as user interface module, decision manager, secured storage model, prediction model, rule manager, rule base, temporal manager, cloud database and IoT devices.

The health data of remotely available patients is to be collected through IoT devices. The data collection agent collects the necessary data from IoT devices and it stored in cloud database. The user interface module is used to collect the necessary data from cloud database which is available freely at a public cloud environment. The collected data is to be sent to the decision manager for the further process. The decision manager sends the data to the secured storage module. The secured storage module consists of three components such as encryption phase, decryption phase and key generation phase. Here, the encryption phase performs encryption process by applying the newly proposed encryption algorithm called RSA-enabled encryption algorithm, the decryption phase performs decryption process by applying the newly proposed encryption algorithm called RSA-enabled decryption algorithm and the key generation process is applied for performing encryption and decryption processes through the proposed key generation algorithm called efficient key generation algorithm. The input data is encrypted and stored into the cloud database. Based on the user request the stored data will be

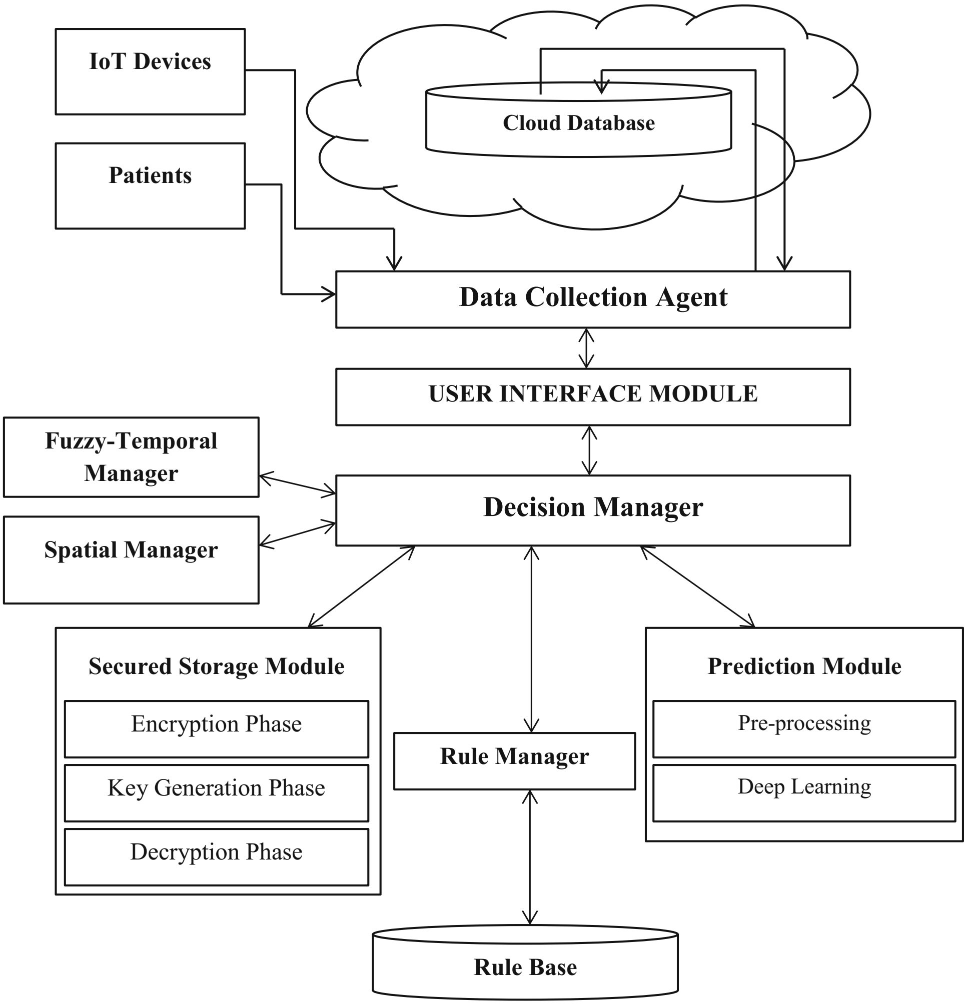


Fig. 1 Overall system architecture

retrieved from cloud database with the help of user interface module by decision manager.

The requested data is sent to the prediction module for predicting the data to know the disease level of the input patient data. The prediction module contains a newly proposed deep learning approach called fuzzy-temporal convolutional neural network (FTCNN) for predicting the disease level. This module uses the temporal manager for confirming the time and also applies spatial manager for confirming the location of the patient data. Moreover, the rule manager is responsible for formulating and finalizing the fuzzy rules and transfers it to the rule base. The rule base contains the necessary fuzzy rules that are useful for predicting the disease level. The decision manager will supply the necessary instruction to the rule manager for formulating the fuzzy rules. The decision manager makes decision over the data according to the recommendation of prediction module. The prediction result as disease level is to be transferred into the respective physicians and patients. Both physicians and patients can get information regarding the disease level from this healthcare monitoring system.

4 Proposed work

The proposed healthcare monitoring system consists of three major components such as data gathering through IoT devices, secured storage model and disease prediction model. These all models have been discussed in detail in this section. First, the data are gathering from remotely available patients. Second, the collected data are stored in cloud database securely by applying the proposed secured storage model. Third, the collected data can be retrieved from cloud database and predicts the disease level of each patient in this work.

4.1 Data gathering from patients through IoT devices

The patient data can be collected from remotely available patients using necessary IoT devices for the various diseases such as cancer, heart and diabetic diseases. The various kinds of IoT devices that are incorporated the suitable sensors used for collecting the symptoms of cancer, diabetic and heart diseases including the glucose level, heart beat rate, ECG values, etc. The important features have been collected and stored as separate record for all the patients with patient identification number. The collected data will be forwarded into the cloud database securely through data collection module, user interface module, decision manager with the help of secured storage module. The data is collected by data collection agent and forward it to user interface module. The user interface module selects the necessary features and sent to the decision manager for securing the collected data. The decision manager sends the pre-processed data to the secured storage module for performing encryption and decryption process and it is stored into the cloud database.

4.2 Secured storage model

This section explains in detail about the newly proposed secured storage model. The proposed secured storage model consists of two newly proposed key generation algorithms, a two-stage encryption algorithm and a two-stage decryption algorithm for storing the medical data and patient data. First, newly proposed key generation algorithms called elliptic curve-based key generation algorithm (ECKGA) is discussed. Generally, the key generation algorithm consists of three steps as follows:

4.3 Key generation

Input: Cloud User Code/any 4-bit value, p.

Output: Generated Keys.

Step 1: Read cloud user code as a 4-bit value.

Step 2: Split the cloud user ID into two 2-bit values as a, b, respectively.

Step 3: Choose random prime number p to fix the size of the GF_p.

Generally, the key generation process reads the cloud user id/ patient id as a 4-bit value. After that, the 4 value is split it into 2-bit values as a and b, respectively. Then, select a random prime number as ‘p’ to finalize the size of the Galois Field (GF). Next, the first stage of encryption process is done by applying the proposed elliptic curve-based key generation algorithm (ECKGA) as below:

4.4 Elliptic curve-based key generation algorithm

Input: The value of $a, b \in N,$ Prime number p.

Output: Generated Public key P_A and P_B.

Step 1: The value of a, b are applied in the elliptic curve equation $E_p(a,b)$.

Step 2: Generate points on the curve $E_p(a,b)$.

Step 3: Choose any random point as a Generator G.

Step 4: Choose private keys n_A as a senders private key and n_B as a user private key.

Step 5: Compute the public keys P_A and P_B by using Diffie–Hellman key exchange method,

$P_A = G \text{ x } n_A$.

$P_B = G \text{ x } n_B$.

Step 6: Generated keys n_A, n_B, P_A and P_B.

The newly proposed ECKGA generates two public keys such as P_A and P_B by using the prime number p in the form of a and b values. The input values a and b are applied and passed as parameters to the elliptic curve equation. Then, generate the points for the input values using elliptic curve. Identify any one of the point as a generator 'G' and selects the private keys n_A as a senders private key and n_B as a user private key. Then, find the public keys P_A and P_B by applying Diffie–Hellman key exchange method that uses the standard formulas. Finally, generate the keys n_A, n_B, P_A and P_B for performing encryption and decryption processes.

Moreover, two more keys are also to generate by using the newly proposed RSA-based Key Generation Algorithm (RSAKGA). The steps of the proposed RSA-based Key Generation Algorithm (RSAKGA) are as follows:

4.5 RSA algorithm-based key generation

Input: Generated Point (q,r).

Output: Generated Keys e, d

Step 1: Choose any large random point from the $E_p(a,b)$ generated points and assign the value of q, r, respectively.

Step 2: Compute the value of $n = q$ x r

Step 3: Compute $\Phi = (q-1)$ x $(r-1)$.

Step 4: Generate public key e with the condition of $gcd(\Phi,e) = 1$ and $e > 1$.

Step 5: Compute private key d by using the value of e and applied the modulus function.

$d \equiv e^{-1} \bmod \Phi$.

Step 6: Generated keys e, d.

In this, RSAKGA used the generated points q and r as input values and it generates the keys e and d as output. First, it selects any large random point from the elliptic curve points $E_p(a,b)$ and assign the value of q, r, respectively. Second, it calculates the value of n by multiplying the values q and r. Third, calculate the Φ value as a result of multiplying the values $(q-1)$ and $(r-1)$. Fourth, generate public key 'e' which is equal to 1 of greatest common divisor of the Φ and e and the e value must be greater than 1. Fifth, find the private key 'd' by applying the value of e and applied the modulus function $d \equiv e^{-1} \bmod \Phi$. Finally, it generates the keys e and d.

The encryption process is also done by using the proposed ECC-based two-stage encryption algorithm (ECC-TSEA). The steps of the newly proposed ECC-TSEA are as below:

4.6 Elliptic curve cryptography-based two-stage encryption algorithm (ECC-TSEA)

Input: Original Text, n_A, P_B, e

Output: Encrypted Cipher Text C_E.

Step 1: Get Original Text T_x.

Step 2: Convert it into ASCII value A_v.

Stage 1: ECC-based encryption

Input: A_v, n_A, P_B

Output: First Stage of Encrypted Text $F_{E(x,y)}$.

Step 1: Compute $H = n_A$ x P_B.

Step 2: Generate F_E by applying the value of A_v and H in the formula of $F_E = A_v + H$.

Step 3: Encrypted Text $F_{E(x,y)}$.

Stage 2: RSA-based encryption

Input: $F_{E(x,y)}$, e, n

Output: Second Stage of Encrypted Text $E_{(x,y)}$.

Step 1: Apply the value F_{Ex}, e in the formula of $C_x = F_{Ex}^{e} \bmod n$

Step 2: Apply the value F_{Ey}, e in the formula of $C_y = F_{Ey}^{e} \bmod n$.

Step 3: Encrypted Text $E_{(x,y)} = (C_x,C_y)$.

Step 3: Convert $E(x,y)$ into *HEX Decimal* value E_{CH}.

The proposed elliptic curve cryptography-based two-stage encryption algorithm (ECC-TSEA) takes original text and keys as input and it produces a cipher text as an output. Here, first reads original text T_x and it converts into ASCII value A_v; then, applies two stages of encryption processes by using elliptic curve cryptography-based encryption and RSA-based encryption. In stage 1, the ASCII values of original text along with the keys n_A and P_B are considered as input and it produces the first stage encrypted text. Here, calculates H value by multiplying the values of n_A and P_B that are received along with cipher text. Then, it generates the F_E by using the values A_v and H as $F_E = A_v + H$. Finally, the encrypted text $F_{E(x,y)}$ is received as output in this work. Second stage of encryption process is started with the encrypted text of first stage encryption process. Here, the encrypted text along with the values of e and n is provided as input and received the encrypted text $E_{(x,y)}$. First, apply the value of F_{Ex},and e over the formula $C_x = F_{Ex}^{e} \bmod n$. Second, apply the values of F_{Ey},and e on $C_y = F_{Ey}^{e} \bmod n$. Finally, the encrypted text $E_{(x,y)}$ is received and it equalized into (C_x,C_y). Finally, it converts the encrypted text $E(x,y)$ into *HEX Decimal* value E_{CH}.

The decryption process is also done by using the proposed ECC and RSA-based Double Decryption Algorithm (ECRS-DDA). The steps of the newly proposed ECRS-DDA are as below:

4.7 Elliptic curve cryptography and RSA-based double decryption algorithm (ECRS-DDA)

Input: Encrypted Cipher Text E_{CH}, n_B, P_A, d.

Output: Decrypted Original Text.

Step 1: Convert *HEX Decimal* value E_{CH} to Decimal value $D_{(x,y)}$.

Stage 1: RSA-based decryption

Input: $D_{(x,y)}$, d.

Output: First Stage of Decrypted Text $F_{D(x,y)}$.

Step 1: Apply the value D_x, d in the formula of $B_x = D_x^d$ *mod n.*

Step 2: Apply the value D_y, d in the formula of $B_y = D_y^d$ *mod n.*

Step 3: Decrypted Text $F_{D(x,y)} = (B_x, B_y)$.

Stage 2: ECC-based decryption

Input: Decrypted Text $F_{D(x,y)}$, n_B, P_A.

Output: Original Decrypted Text A_v.

Step 1: Compute $I = n_B$ x P_A.

Step 2: Generate A_v by applying the value of I in the formula of $A_v = F_{D(x,y)} - I$.

Step 3: Generated $A_v = F_{Dx}$ or $A_v = F_{Dy}$.

Step 2: Convert the Generated ASCII value A_v into T_x.

Step 3: Decrypted Original Text T_x.

The newly proposed elliptic curve cryptography and RSA-based double decryption algorithm (ECRS-DDA) consider the encrypted cipher text E_{CH} as input along with public keys n_B, P_A and d, and produce the decrypted original text as output. First, it converts the *HEX Decimal* value from E_{CH} to Decimal value $D_{(x,y)}$. In stage 1 of the decryption process in this algorithm considered $D_{(x,y)}$, d as input and produce a decrypted text $F_{D(x,y)}$ as output. First, apply the value of D_x and d over the formula of $B_x = D_x^d$ *mod n*. Next, use the values of D_y and d in the formula of $B_y = D_y^d$ *mod n*. Then, the decrypted text is received by assigning the values (B_x, B_y) into $F_{D(x,y)}$ for getting output. In stage 2, the ECC-based decryption starts with the decrypted text $F_{D(x,y)}$, n_B, P_A as input and the original text A_v as output. Here, calculate the I value by multiplying the values of n_B and P_A. It generates the value of A_v by using the value of I on the equation $A_v = F_{D(x,y)}–I$. Then, generate the ASCII value A_v for the decrypted texts F_{Dx} and F_{Dy}. Finally, it converts the generated ASCII value A_v into the original text T_x.

5 Mathematical proof

In this work, the patient/cloud user ID will be any 4-bit value 1124 and the prime number p is *17* as input and to be generated the keys that are useful for securing the data by applying encryption and decryption processes. The input user ID 1124 is to be split as a = 11 and b = 24. Then, choose random prime number $p = 17$ to fix the size of the GF_{17}.

Elliptic Curve Key Generation: The value of $a = 11$, $b = 24 \in N$, Prime number p = 17 are considered as input. First, the value of $a= 11$, $b = 24$ are applied in the elliptic curve equation $E_{17}(11,24)$ .It generate the following points for the curve $E_{17}(11,24)$.

Points are: (1,6) (1,11) (3,4) (3,13) (4,8) (4,9) (7,6) (7,11) (9,6) (9,11) (13,1) (13,16) (14,7) (14,10)

Now, choose any random point as a Generator $G = (3,4)$ and also select the private keys $n_A = (7,6)$ as a senders private key and $n_B = (9,11)$ as a user private key. Calculate the public keys P_A and P_B by using Diffie–Hellman key exchange method,

$P_A = G$ x $n_A = (3,4)$ x $(7,6) = (21,24)$ $\therefore$ $P_A = (21,24)$.

$P_B = G$ x $n_B = (3,4)$ x $(9,11) = (27,44)$ $\therefore$ $P_B = (27,44)$.

The generated keys are as below:

$n_A = (7,6)$, $n_B = (9,11)$, $P_A = (21,24)$ and $P_B = (27,44)$.

RSA Algorithm Key Generation: Select any large random point from the $E_p(a,b)$ generated points and assign the value of $q = 13$, $r = 16$, respectively. Calculate the value of n as below: $n = q$ x $r = 13 \times 16 = 208$. Calculate the Φ value as below:

$\Phi = (q\text{-}1)$ x $(r\text{-}1)$.

$= (13–1)$ x $(16–1)$.

$= 12 \times 15$.

$= 180$.

Generate public key e with the condition of $gcd\ (\Phi,e) = 1$ and $e > 1$.

gcd (Φ,e) = gcd (180,11) = 1

$\therefore$ $e = 11$.

Compute private key d by using the value of e and applied the modulus function $d \equiv e^{-1} mod\ \Phi$.

$d \equiv e^{-1} \bmod \Phi$

$11 \times 131 \equiv 1 \bmod 180$

$\therefore d = 131$.

Generated keys are $e = 11$, $d = 131$.

Encryption Phase: The original text ‘G’, $n_A = (7,6)$, $P_B = (27,44)$, $e = 11$. First, get original text G is assigned to T_x. Convert it into ASCII value $A_v = 71$.

ECC-based Encryption: The input ASCII value is 71, curve point is (7,6) and the keys (27, 44) are considered in this work.

A_v = 71, n_A = (7,6), P_B = (27,44).

Compute $H = [n_A \text{ x } P_B] mod\ p = [(7,6) \text{ x } (27,44)]\ mod\ 17$.

H = (189,264) mod 17

∴ $H = (2,9)$

Generate F_E by applying the value of A_v and H in the formula of $F_E = A_v + H$.

$F_E = A_v + H$ = 71 + (2,9)

∴ F_E =(73,80)

Encrypted Text $F_{E(x,y)} = (73,80)$.

RSA-based encryption:

$F_{E(x,y)}$ = (73,80), e = 11, n = 208.

Apply the value $F_{Ex} = 73,\ e = 11$ and $n = 208$ in the formula of $C_x = {F_{Ex}}^e\ mod\ n$.

$C_x = {F_{Ex}}^e$ mod n = 73^{11}mod 208 = 57

∴ C_x = 57

Apply the value $F_{Ey} = 80_,\ e = 11\ and\ n = 208$ in the formula of $C_y = {F_{Ey}}^e\ mod\ n$.

$C_y = {F_{Ey}}^e$ mod n = 80^{11}mod 208 = 176

∴ C_y = 176

Encrypted Text $E_{(x,y)} = (C_x,C_y) = (57,176)_.$

Convert $E(x,y) = (57,176)$ into *HEX Decimal* value $E_{CH} = (39,B0)$.

Decryption Phase: The Encrypted Cipher Text is E_{CH-} = (39,B0) along with keys n_B, P_A and d as input and the decrypted original text is received as output.

Convert *HEX Decimal* value $E_{CH} = (39,B0)$ to Decimal value $D_{(x,y)} = (57,176)$.

RSA-based decryption:

$D_{(x,y)}$ = (57,176), d = 131, n = 208.

First Stage of Decrypted Text $F_{D(x,y)}$.

Apply the value $D_x = 57,\ d = 131$ in the formula of $B_x = {D_x}^d\ mod\ n$.

$B_x = {D_x}^d\ mod\ n$ = 57^{131} mod 208 = 73

Apply the value $D_y = 176,\ d = 131$ in the formula of $B_y = {D_y}^d\ mod\ n$.

$B_y = {D_y}^d\ mod\ n$ = 176^{131} mod 208 = 80

Decrypted Text $F_{D(x,y)} = (B_x,\ B_y) = (73,80)$.

$F_{D(x,y)}$ = (73,80)

ECC-based Decryption: The Decrypted Text $F_{D(x,y)-} = (73,80),\ n_B = (9,11),\ P_A = (21,24)$ and will be received as original decrypted text A_v.

Compute $I = (n_B \text{ x } P_A)\ mod\ p = [(9,11) \text{ x } (21,24)]\ mod\ 17$.

I = (189,264) mod 17 = (2,9)

∴ I =(2,9)

Generate A_v by applying the value of $I = (2,9)$ in the formula of $A_v = F_{D(x,y)} - I$.

$A_v = F_{D(x,y)} - I$ = (73,80) – (2,9)

∴ A_v = (71,71)

Generated $A_v = F_{Dx}$ or $A_v = F_{Dy}$.

∴ $A_v = 71$

Convert the Generated ASCII value $A_v = 71$ into $T_x = G$.

Decrypted Original Text $T_x = G$.

Finally, the decryption algorithm is produced the original text ‘G’.

5.1 Disease prediction model

This section describes in detail about the proposed multichannel spatio-temporal convolutional neural network (MCST-CNN)-based disease prediction model for predicting the disease level according to the collected patient data and the standard benchmark datasets that are available for research like UCI Repository Machine Learning Dataset. The proposed prediction model consists of two major modules. First, symptoms based severity analysis using deep learning approach according to the patient's feedback in the form of text and estimate the sentiment scores over the individual disease for finding the severity level. Second, this model considered the severity rating features with the respective user ratings for comparing the severity-based rating and display the stage of the disease for the particular data. The following subsections are discussing more about these two stages in the proposed disease prediction model.

5.1.1 Severity-based Prediction

Severity terms are typically finalized based on the available values of most important features that are contained in the dataset and patient information. The aim of this model is to extract the disease severity and calculate the patient polarity values of the extracted disease severity. For achieving that, this work proposes a MCST-CNN architecture specifically for the severity extraction process and also used a Latent Dirichlet Allocation (LDA) method for grouping the created severity level. The proposed MCST-CNN is an enhanced version of the standard CNN architecture. The proposed model consists of four CNN channels according to the severity levels such as abnormal, medium, low and normal. Generally, all the feature in the dataset is checked with the value of low dimensional vector by a lookup layer transformation leading to a matrix $X \in R^{n \times k}$. For the severity level embedding channel, the major aim of this process is to provide better and accurate severity level according to the severity. According to Jebbara (2016), this work applies a severity analyser that is encoded as a 45-dimensional vector. This can formally be given as $wt_z \in R^{n \times 45}$.

5.1.1.1 Convolution layer The major role of convolutional layer is to fetch the more relevant attributes from the medical dataset, medical report and physicians report. It generates valuable attributes by applying two kinds of filters with different sizes for the features and severity level embedding process. Let assume that $wt_x \in R^{h\times k}$ is a filter where 'h' represents the filter height for the matrix x of the specific embedding process channel. Usually, the attributes were identified by using Eq. (1) for the specific time duration and space:

$$CH_i\langle t1, t2, sp\rangle = ATT(wt.x_{i+h} + b) \tag{1}$$

where ATT represents a nonlinear function and 'b' relates to a term which is bias. Obtain the relevant attribute map given in Eq. (2):

$$CH_x\langle t1, t2, sp\rangle = \left[CH_1^x, CH_2^x, \ldots.., CH_{n-h+1}^x\right] \tag{2}$$

where $t1$ indicates the starting time and $t2$ represents the ending time and with $CH_x \in R^{n-h+1}$ for the specific place and time duration. For severity merging process and attribute embedding process in embedding channel, use the various filters $wt_z \in R^{h\times 1}$ and identify an attribute map like given in Eq. (3).

$$CH_z\langle t1, t2, sp\rangle = \left[CH_1^z, CH_2^z, \ldots.., CH_{n-h+1}^z\right]. \tag{3}$$

For the $CH_z \in R^{n-h+1}$. Generally, apply the filter and to create various filters for generating different meanings and attributes, respectively.

5.1.1.2 Pooling layer The pooling operation has been used for capturing the maximum features of the input values. Generally, it is presented as given in Eq. (4).

$$C\,H_x = \mathrm{MAX}(ch_x) and \underset{z}{CH} = \mathrm{MAX}(ch_z). \tag{4}$$

After performing the pooling operation, the last attributes are given by applying the concatenation operation over the semantically meaningful and the attributes by applying a filter. Generally, it is indicated as $CH = \overset{1}{\underset{x}{CH}} \oplus \overset{1}{\underset{z}{CH}}$, where $\oplus$ indicates the concatenation operation. The final attributes can be represented as given in Eq. (5).

$$CH = \overset{1}{\underset{x}{CH}} \oplus \ldots\ldots \oplus \overset{n}{\underset{x}{CH}} \oplus \overset{1}{\underset{z}{CH}} \oplus \ldots\ldots\ldots \oplus \overset{m}{\underset{z}{CH}} \tag{5}$$

where the variables 'n' and 'm' are representing the different filters for the specific meaningful and attributes, respectively.

5.1.1.3 Output layer Generally, the soft-max method is used to generate the resultant attributes. Here, this work is also considered the severity level extraction as a sequence labelling method. Generally, the result is presented as given in Eq. (6):

$$0 < t1, t2, sp > \; = wt.(c \circ rs) + b \tag{6}$$

where O indicates the masking operator and $rs = R^{n+m}$ is a sample drawn from Bernoulli distribution.

5.1.2 Grouping the severity level equivalent patients

This section explains the patient's disease level severity and also related attributes are grouped as clusters that are applied to estimate the severity level-based ratings. The various severity levels-related attributes were identified in the patient record as dataset, even though various severity relevant attributes are referred for the related severity group. Moreover, the severity represented attributes are all depicted the different kinds of severity. Thus, to group the meaningful attributes and map the extracted severity-related attributes into the relevant attributes. For achieving this, it is required to map the extracted severity relevant attributes into the relevant attributes. The standard LDA is used for finding the relevant attributes from standard dataset. The LDA is allowed that the specific levels of severity are from different groups. The space and time are also considered in this LDA method which is enhanced from the work (Blei and Jordan (2003).

5.1.3 Disease severity-based rating process

The relevant features are grouped together that are useful for predicting the disease severity level and also calculated the polarity values of each severity level of a specific disease. Thus, to calculate the severity level for the particular rating matrices $RM^1, RM^2\ldots\ldots RM^K$, according to the work, first, it calculates the polarity scores for each disease severity and it considers the polarity value. In this approach, each disease severity rating is calculated according to the relevant attribute that is grouped with datasets. Here, the available severity level SLA_k in a dataset DS_{ij} and calculate the severity level rating as given in Eq. (7).

$$r_{ijk}\langle t1, t2, sp\rangle = \frac{\sum_{w\in W_k}(DS_{ij})SVL(w)}{\left|W_k(DS_{ij})\right|} \tag{7}$$

where W_k corresponds to the set of words in the review DS_{ij} that is grouped with the severity level a_k and SVL (w) indicates the polarity value of attributes according to the meaning of attributes.

5.1.4 Severity-based weight estimation

This section describes in detail about the severity-based weight estimation process for the given input data. This work calculates the weight of attribute, applies a three-dimensional AF, WT which is the right way for capturing the relationship between the attributes, users and the disease severity level. The tensor WT is decomposed as given in Eq. (8).

$$wt \approx \sum\nolimits_{r=1}^{R} x_r^{\circ} y_r^{\circ} z_r \tag{8}$$

where R and the operator $^{\circ}$ denote the number of rank-one components and the vector outer product, respectively, x_r, y_r and z_r are the column vectors in the corresponding factor matrixes X, Y and Z. $I \times R, J \times R$ and $K \times R$ are the sizes of X, Y and Z, respectively. Element-wise, Eq. (8) can be replaced as:

$$\underset{ijk}{wt} = (x_r, y_r, z_r) = \sum\nolimits_{r=1}^{R} x_{ir} \cdot y_{jr} \cdot z_{kr}, \tag{9}$$

where each row x_r, y_r and z_r of these matrices represent the patient, attribute and severity level weight factors. The disease prediction ratings $\underset{ij}{r}$ according to the proposed prediction model for calculating based on severity level ratings and also the weight vector as given in Eq. (10).

$$\underset{ij}{r} = \underset{ij}{\overset{T}{w}} r_{ij} = \sum_{k=1}^{K} \underset{ijk}{w} \cdot r_{ijk}. \tag{10}$$

To calculate the optimized values of X, Y and Z parameters according to the prediction error, the objective function fn is minimized:

$$fn = \frac{1}{2} \sum_{i=1}^{I} \sum_{j=1}^{J} m_{ij} \left(r_{ij} - \hat{r}_{ij} \right)^2. \tag{11}$$

Based on the below limitations:

$$g_{ijk} \equiv -w_{ijk} \leq 0, \tag{12}$$

$$h_{ij} \equiv \sum_{k=1}^{K} I_{ijk}.w_{ijk} - 1 = 0 \tag{13}$$

For all i = 1,…I, j = 1,….,J, and k = 1,2……,K where g_{ijk} and h_{ij} are shorthand's to be applied in the sequel. Following the PHR method (Rockafellar 1973), the constrained objective function ofn is to be converted into the unconstrained objective function as given in Eq. (14):

$$\Phi(t1, t2, sp) = f + \sum_{i=1}^{I} \sum_{j=1}^{J} m_{ij}.v_{ij}.h_{ij} + \frac{\rho}{2} \sum_{i=1}^{I} \sum_{j=1}^{J} m_{ij}.v_{ij}.h_{ij}^2 + \frac{1}{2\rho} \sum\nolimits_{i=1}^{I} \sum\nolimits_{j=1}^{J} \sum\nolimits_{K=1}^{K} I_{ijk} \cdot \{[\max(0, u_{ijk} + \rho g_{ijk})]^2 - u_{ijk}^2\} \tag{14}$$

where v_{ij} and u_{ijk} are the multipliers of the equality-constraints on h_{ij} and inequality constraints g_{ijk}, and ρ is the penalty parameter.

Let $e_{ij} \equiv \widehat{r}_{ij} - r_{ij}$ represent the model prediction error. The partial derivatives of the unconstrained objective functions Φ w.r.t model parameters x_i, y_j, z_k.

Having computed X, Y and Z and hence $\mathcal{WT}$ calculated by applying Eq. (8), now, it can be obtained the weighted severity rating matrix $\overline{R}^k$ as given in Eq. (15).

$$\overline{RT}^k = \mathcal{WT} \oplus RT^k \tag{15}$$

where the matrix $\mathcal{WT}$ represents the weights users gives on the aspects a_k of items, meaning that each entry is estimated by $\widehat{r}_{ijk} = w_{ijk} \times r_{ijk}$.

5.1.5 Overall disease severity level prediction

The overall patient records are to be predicted in the presence of severity ratings in the weighted rating matrix. For achieving that, according to the work, integrate the overall severity rating matrix RT along with weighted attribute rating matrices $\overline{RT}^1, \overline{RT}^2$…… forming a new 33rd orders-tensor $\overline{RT}$ which is factorized by applying the method called CP-WOPT. Assuming that the factor matrices A, B and C are the results from the CPs decompositions of $\overline{R}$, the predicted value of the ratings that user v_i will give for a product P_j can be obtained as:

$$\tilde{r}_{ij} = \hat{r}_{ij1} = \sum_{d=1}^{D} a_{id} b_{jd} c_{1d} \tag{16}$$

where the D is the positive-integer which represents the D-dimension of the tensor. Finally, it predicts the overall disease severity level by applying fuzzy rules. The necessary fuzzy rules have been generated in this work for predicting the disease severity level more accurately for the various standard benchmark datasets including diabetes, heart and cancer disease datasets, the collected patient records from IoT devices and the physician's medical report.

6 Results and discussion

The proposed disease monitoring system has been developed by using Java Programming and Net Beans environment in cloud tool called CloudSim. In this work, the proposed health monitoring system uses the standard dataset called University of California, Irvine (UCI) Machine Learning Repository that consists of datasets related to the diseases such as heart, diabetic and cancer diseases. The health monitoring system is contributing more in society for knowing the disease severity level easily and it is useful for safeguarding them from dead diseases. This section describes the various medical datasets such as heart, diabetic and cancer datasets used in this work, performance metrics used for evaluating the proposed health monitoring system and the experimental results.

6.1 Medical datasets

The UCI Machine Learning Repository datasets are widely used for research by various researchers in this world. The major dead disease benchmark datasets are discussed in detail in this subsection. The heart disease dataset is explained first. Then, the diabetic dataset has been explained with the detail of number of features available and finally the cancer dataset is explained with the necessary information.

A. *Cleveland heart disease database*

The Cleveland heart disease database is used as a heart disease dataset to predict the heart disease and also applied by the various data analysis researchers. Majority of the researchers conducted various experiments with different sizes of dataset for evaluating their algorithms. Currently, the available dataset contains 14 attributes of the 76 attributes which are present in the finalized database. Specifically, the data analyser uses Cleveland heart disease database for their disease analysis and also confirms their own real medical dataset originality through s their healthcare applications. The symptoms of the disease on a person are mentioned in the 'goal' field with integer value between 0 and 4. Here, 0 means the person is normal and not affected by the heart disease and 4 represents the person affected by the heart disease. The used heart disease dataset contains the patient identification number, age of the person, gender of the person, CP level of the person, trestbps level, chol value, fbs rate, restecg value, thalach rate, exang value, oldpeak rate, slope value, ca value, thal and num values of the person.

B. *Diabetic dataset*

The benchmark dataset applied in this health monitoring system has been taken and considered from the standard UCI Repository. This dataset contains two different classes such as Type1 and Type2 diabetes with eight features such as number of times pregnant, plasma glucose concentration in 2 h in an oral glucose tolerance test, diastolic blood pressure (mm Hg), triceps skin-fold thickness (mm), 2 h serum insulin (mu U/ml), body mass index (weight in kg/(height in m)^2), diabetes pedigree function and age (years). This dataset contains 768 instances totally with the above mentioned fields. This dataset has been prepared with adults who are greater than 21 years old. This dataset considered plasma glucose concentration, diastolic blood pressure, triceps skin-fold thickness, insulin value and body mass index for analysing the patient disease severity level. Moreover, the benchmark dataset is concentrated over the snapshot values of features and also considered the spatial and temporal values are considered for creating the real medical dataset that are collected from patients in remote places through IoT devices. In addition, MCST-CNN and fuzzy rules were applied for predicting the disease and the level.

6.1.1 C. WDBC dataset

The Wisconsin Diagnostic Breast Cancer data (WDBC) is a standard dataset which is benchmark and applied as input value for evaluating the newly developed health monitoring system. The newly developed health monitoring system applies three kinds of datasets including WDBC dataset. Here, the standard WDBC dataset consists of text as data values in the form of different files and it also stored the patient's records.

6.2 Performance evaluation metrics

The performance evaluation metrics of the proposed model is presented as two subsections namely secured storage and disease prediction with different evaluation parameters.

6.2.1 Secured storage

The secured storage part of this proposed disease prediction system is evaluated by using the evaluation metrics such as key generation time (KGT), encryption time (ET) and the decryption time (DT). Moreover, the relevant formulae for calculating the different time are given in Eqs. (17), (18) and (19).

$$\mathrm{KGT} = \mathrm{ITT} + \mathrm{ET} \tag{17}$$

where ITT indicates the Information Transferring Time and ET represents the encryption time. Here, the ET is calculated is the amount of time taken by the data to encrypt the original data as an encrypted data.

$$\mathrm{ET} = \mathrm{ENDT} - \mathrm{STARTT} \tag{18}$$

where ENDT indicates the end time and STARTT represents the starting time of encryption process. Here, the DT is calculated is the amount of time taken by the data user to decrypt the encrypted data that is mentioned in milliseconds and it is calculated by applying Eq. (19).

$$\mathrm{DT} = \mathrm{ENDT} - \mathrm{STARTT}. \tag{19}$$

6.2.2 Disease prediction

The disease level prediction process can be done in this work by using the formulas for measuring the precision value, recall value and F-measure value. First, the precision value is measured based on the presence of disease symptoms by applying the formula given in Eq. (20). Here, this work uses True Positive (TP) which has symptom of disease and predicted correctly, and the False Positive (FP) that has not symptom but predicted as disease affected. Next, the recall value is calculated according to the number of records predicted successfully as disease affected by applying the formula given in Eq. (21). Here, the False Negative (FN) represents the record which is wrongly predicted as disease affected. Finally, the F-measure value is calculated using the formula given in Eq. (22) according to the fraction of value between Eqs. (20) and (21) that are representing the Precision and Recall values.

$$\text{Precision} = \frac{TP}{TP + FP} \tag{20}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{21}$$

$$F - \text{Measure} = \frac{\left(1 + \beta^2\right) * \text{Precision} * \text{Recall}}{\beta * (\text{Precision} + \text{Recall})} \tag{22}$$

$$\text{Prediction Accuracy} = \frac{\text{No. of records correctly predicted}}{\text{Total no. of records considered}} \tag{23}$$

The prediction accuracy is computed by applying Eq. (23) as a formula and it finalizes the overall performance of the proposed MCST-CNN classifier and the health monitoring system.

6.3 Experimental results

This section presented the experimental results of the proposed model which has two subsections such as secured storage and disease prediction.

6.3.1 Secured storage

The proposed secured storage model is evaluated by using the standard cryptographic evaluation parameters such as encryption time, decryption time and computation time. Figure 2 demonstrates that key generation time analysis of the proposed secured storage model. Here, five different experiments have been conducted with 200, 400, 600, 800 and 1000 cloud users.

From Fig. 2, it can be observed that the proposed secured storage algorithm takes time to generate keys according to the number of users. Here, increase the key generation time according to the number of cloud users.

Figure 3 shows the encryption time analysis for the proposed secured storage algorithm. Here, five different experiments have been conducted with different sizes of data such as 200 kb, 400 kb, 600 kb, 800 kb and 1000 kb for evaluating the performance of the proposed secured storage model.

From Fig. 3, it can be observed that the proposed secured storage model takes time to encrypt the data according to the size of the input data. This is due to the uses of elliptic curve cryptography, two-stage encryption and decryption processes.

Figure 4 shows the encryption time analysis for the proposed secured storage algorithm. Here, five different experiments have been conducted with different sizes of

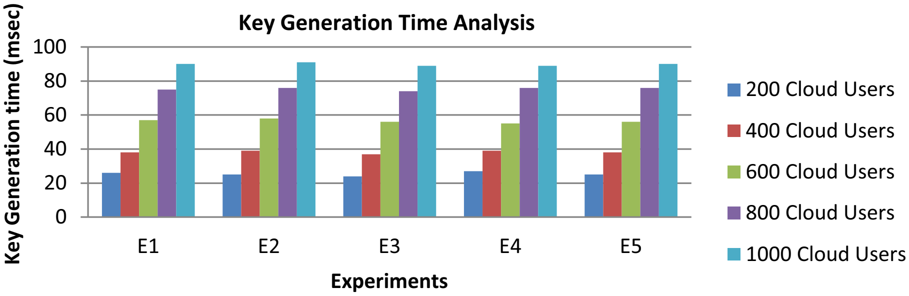


Fig. 2 Key generation time analysis

Fig. 3 Encryption time analysis

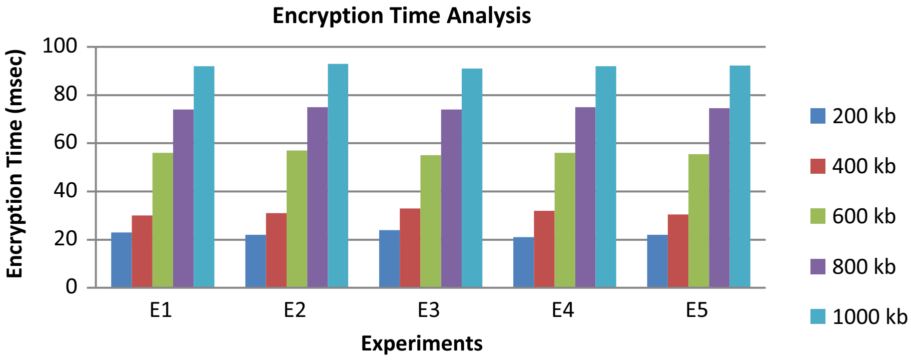


Fig. 4 Decryption time analysis

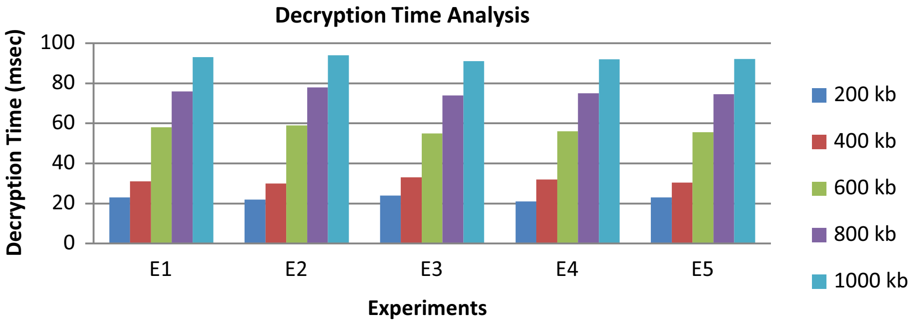


Fig. 5 Computation time analysis for the data size 10 GB

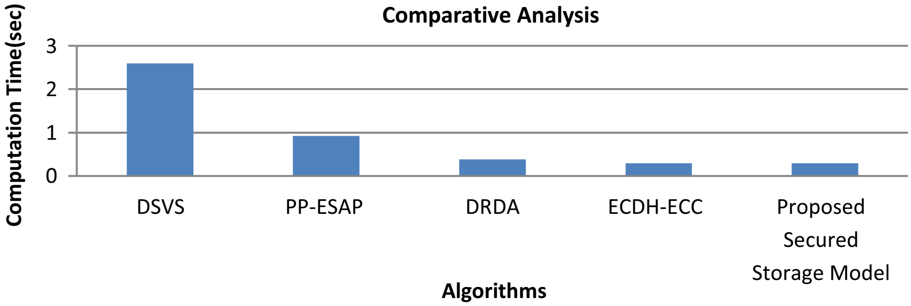
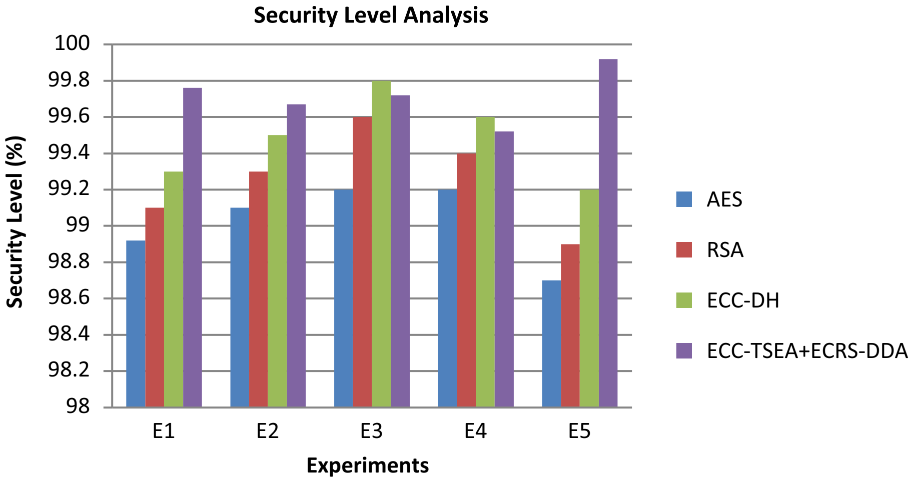


Fig. 6 Security level analysis



data such as 200 kb, 400 kb, 600 kb, 800 kb and 1000 kb for evaluating the performance of the proposed secured storage model.

From Fig. 4, it can be observed that the proposed secured storage algorithm takes time to decrypt the patient data that are collected from the remote patients through IoT devices according to the size of the input data. This is due to the uses of two-stage decryption process.

Figure 5 shows the computational time analysis for the proposed secured storage algorithm. Here, five different works have been considered for conducting experience with the size of input data as 10 GB.

From Fig. 5, it can be observed that the proposed storage algorithm takes less computation time than the existing systems such as DSVS, PP-ESAP, DRDA, ECDH-ECC. This is due to the application of the concept elliptic curve cryptography and processes of encryption and decryption in double the time for performing the 10 GB data.

Figure 6 shows the security level analysis between the proposed ECC-TSEA + ECRS-DDA and the existing secured storage algorithms such as ECC-DH, RSA and AES. Here, we have conducted five experiments for analysing the security levels.

From Fig. 6, it can be observed that the security level of the proposed secured storage model (ECC-TSEA + ECRS-DDA) is better than the existing secured storage algorithms such as AES, RSA and ECC-DH. This is due to the use of two-stage RSA-based encryption and decryption process along with elliptic curve cryptography.

6.3.2 Disease prediction

The proposed disease prediction system is evaluated based on the performance of the feature selection algorithm which is proposed and incorporated with this system and the existing CNN classifier that is used for performing the classification process over the different standard benchmark datasets such as Heart, Diabetic and WDBC.

The performance of the newly proposed MCST-CNN is compared with the performance of the existing classifiers in this direction including the standard CNN, TFMM-PSO (Ganapathy et al. 2014), FTCM (Sethukkarasi et al. 2014), ANN, SVM and C4.5 for proving the efficiency of the MCST-CNN in terms of classification accuracy. For this purpose, three different datasets like heart, diabetic and cancer diseases datasets were used for conducting experiments. In addition, full set of featured datasets were used for performing classification. Figure 7 shows the prediction accuracy of the three datasets with different accuracy.

From Fig. 7, the classification accuracy of MCST-CNN is high when it is compared with the standard classification algorithms such as FTCM, TFMM-PSO, ANN, SVM and C4.5. The reason for the classification accuracy enhancement is the application of multichannel concept, spatial, temporal constraints and deep learning approach.

The computational time analysis between the proposed MCST-CNN and the existing FTCM is shown in Table 1. It shows the time taken to perform training and testing processes for the various medical datasets like Heart, Diabetic and WDBC datasets.

From Table 1, it can be observed that the time taken to perform training process and the testing process over the various datasets such as Heart, Diabetic and WDBC in better and optimal than other classifier called FTCM. The proposed MCST-CNN takes less time only for training and testing processes than FTCM classifier on all the datasets.

Figure 8 shows the performance comparative analysis over the diabetic dataset based on the accuracy of proposed MCST-CNN and the domain expert opinions. Here, the different sets of patient records have been considered to perform the comparative analysis on the diabetic dataset. Moreover, the patient records are considered only that are extracted from the UCI machine learning repository.

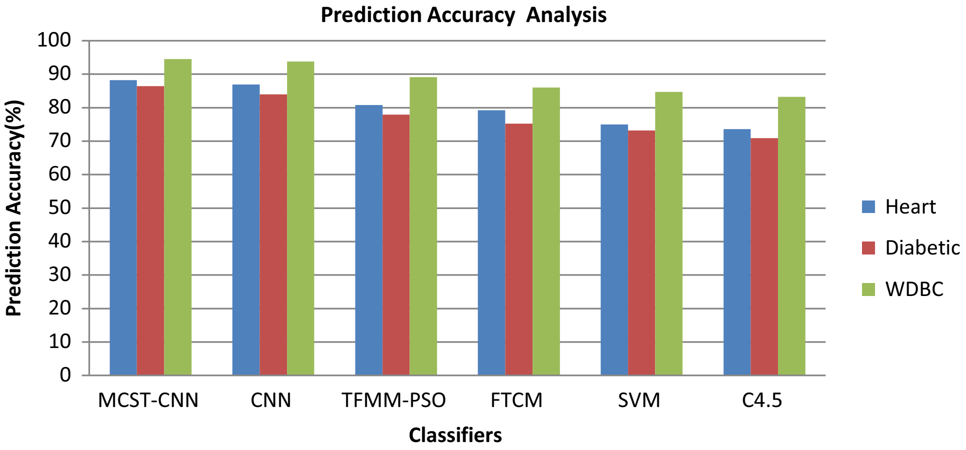


Fig. 7 Prediction accuracy analysis

Table 1 Computational time analysis

Dataset	Time taken (Sec) for MCST-CNN		Time taken (Sec) for FTCM	
	Training	Testing	Training	Testing
Heart	0.38	0.17	0.41	0.21
Diabetic	1.72	0.78	1.82	0.81
WDBC	0.41	0.12	0.45	0.15

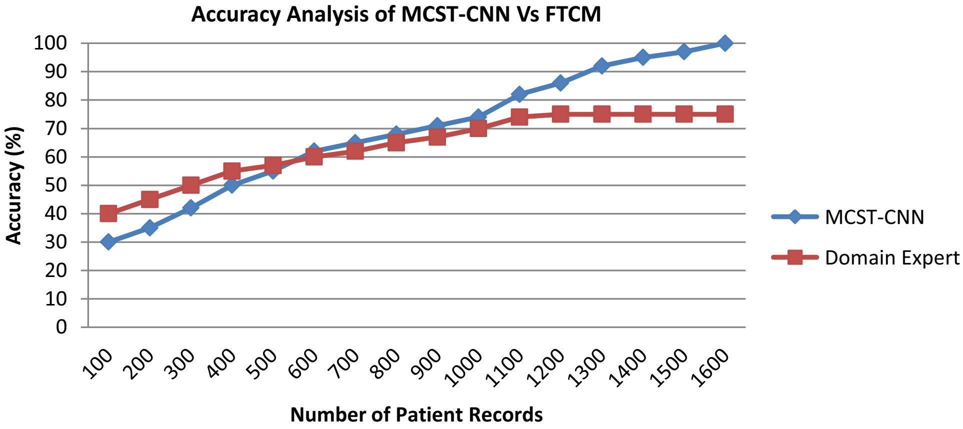


Fig. 8 Accuracy analysis between the MCST-CNN and the domain expert

Table 2 Precision, recall and F-measure analysis

Datasets	Precision (%)	Recall (%)	F-measure (%)
Heart	87.86	98.42	93.79
Diabetic	85.23	99.32	94.17
WDBC	94.79	99.59	94.19

From Fig. 8, it can be seen that the prediction accuracy of the proposed MCST-CNN is better than the prediction accuracy of domain expert. The prediction accuracy over the patient records goes down and stabilized at same percentage of accuracy while increasing the number of patient records from 1000 records. At the same time, the proposed MCST-CNN provides better result than domain expert even the number of records cross the 1000 records. This is because the efficiency of the MCST-CNN provides this result.

Table 2 demonstrates the precision, recall and F-measure values analysis of the proposed MCST-CNN.

From Table 2, the recall values of all the different datasets are high when it is compared with the precision and F-measure values. This is because of the use of spatial and temporal constraints of the dataset in the proposed MCST-CNN.

The fuzzy rules are taken considered to forecast the new patient records that performs based on the spatial constraints, Allen’s interval algebra and the relevant rules. In

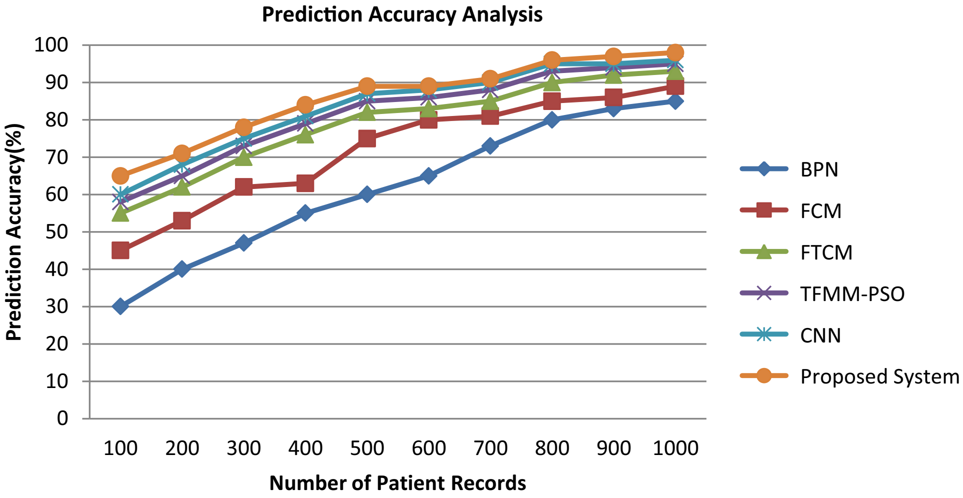


Fig. 9 Comparative analysis based on the prediction accuracy

addition, the patterns that are frequently occurred as identified in the general pattern lists which are taken consider with spatial and temporal features. Moreover, the fuzzy rules have been created with time constraints as features on MCST-CNN to forecast the most useful patterns in the diabetic dataset. Here, the general patterns are compared with the related patient data pattern in this work. If there is a similar pattern occurs based on the temporal relational features, then the activation function is considered for the biological disorder like blood glucose level and the insulin dosage level for the particular patient. Figure 9 shows the comparative analysis based on the prediction accuracy.

From Fig. 9, it is proved that the efficiency of the proposed MCST-CNN is achieved better prediction result than the existing algorithms namely BPN, FCM, FTCM, TFMM-PSO and the standard CNN. The reason for the enhancement is the consideration of spatial and temporal features on the development of fuzzy rules that are applied to make a decision on MCST-CNN.

7 Conclusion and future works

A new healthcare monitoring system has been proposed and implemented in this work for monitoring the level of dead diseases such as diabetic and heart diseases. Here, the disease level is predicted by using the by predicting the diseases according to the original data that are collected from the patients who are available in remote places. Moreover, a secured data storage model is also developed and incorporated in this system to store the patient's data securely in cloud databases. In addition, three new algorithms were developed in this work to perform the encryption, decryption and key generation processes on secured storage model. A new deep learning algorithm called MCST-CNN is also developed and incorporated with the proposed healthcare monitoring system for predicting the disease level efficiently in this work. The various experimental results that are obtained from the various experiments conducted in this work proved the efficiency of the proposed healthcare system in terms of prediction accuracy as 99.45% and security level is 99.72% than other healthcare systems.

Compliance with ethical standards

Conflict of interest The author declares that they no conflict ofinterest. The author of this research acknowledges that they are not involved in any financial interest.

References

Ahmad, N (2009) Restrictions on cryptography in India – a case studyof encryption and privacy. Computer Law Security Review 25(2):173–180

Alqahtani F, Al-Makhadmeh Z, Tolba A, Said O (2020) TBM: a trust-based monitoring security scheme to improve the service authentication in the internet of things communications. Comput Commun 150:216–225

Babu GC, Shantharajah SP (2019) Optimal body mass index cutoff point for cardiovascular disease and high blood pressure. Neural Comput Appl 31(5):1585–1594

Belotti M, Božić N, Pujolle G, Secci S (2019) Cedric, Cnam, Paris, France, "A vademecum on blockchain technologies: when, which, and how." IEEE Communications Surveys & Tutorials 21(4):3796–3838

Breast cancer using fuzzy temporal rules", National Academy Science Letters, 42: 227-232 2019

Chou DC, Chou AY (2002) Healthcare information portal: a web technology for the healthcare community. Technol Soc 24(3):317–330

Elias Yaacoub, Khalid Abualsaud, Tamer Khattab, Mohsen Guizani, Ali Chehab, 2019 "Secure mHealth IoT data transfer from the patient to the hospital: a three-tier approach", *IEEE Wireless Communications*, 26(5): 70–76

Francis H (2007) Roger France, Marc Bangels, Etienne De Clercq, "Purposes of health identification cards and role of a secure access platform (Be-Health) in Belgium." Int J Med Informatics 76(2–3):84–88

Ganapathy S, Sethukkarasi R, Yogesh P, Vijayakumar P, Kannan A (2014) An intelligent temporal pattern classification system using fuzzy temporal rules and particle swarm optimization. Sadhana 39(2):283–302

Gautami Tripathi, Mohd Abdul, Ahada Sara Paiva, "S2HS- A blockchain based approach for smart healthcare system", Healthcare, Article No. 100391, 2019

Geylani Kardas E, TurhanTunali, (2006) Design and implementation of a smart card based healthcare information system. Comput Methods Programs Biomed 81(1):66

Huang L-C, Chu H-C, Lien C-Y, Hsiao C-H, Kao T (2009) Privacy preservation and information security protection for patients' portable electronic health records. Comput Biol Med 39(9):743–750

Hussein AF, Arun Kumar N, Burbano-Fernandez M, Ramírez-González G, Abdulhay E, Victor HC, Albuquerque De (2018) An automated remote cloud-based heart rate variability monitoring system. IEEE Access 6:77055–77064

Kanimozhi U, Ganapathy S, Manjula D, Kannan A (2019) An intelligent risk prediction system for breast cancer using fuzzy temporal rules. National Academy Science Letters 42:227–232

Kumar PM, Lokesh S, Varatharajan R, Babu GC, Parthasarathy P (2018) Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier. Futur Gener Comput Syst 86:527–534

Kumarage H, Khalil I, Alabdulatif A, Tari Z, Yi X (2016) Secure data analytics for cloud-integrated internet of things applications. IEEE Cloud Computing 3(2):46–56

Kwabena O-A, Qin Z, Zhuang T, Qin Z (2019) MSCryptoNet: multi-scheme privacy-preserving deep learning in cloud computing. IEEE Access 7:29344–32935

Lake Bu, Mihailo Isakov , Michel A. Kinsy, 2019 "A secure and robust scheme for sharing confidential information in IoT systems", Ad Hoc Networks, 92: 101762.

Li T, Gao C, Jiang L, Pedrycz W, Shen J (2019) Publicly verifiable privacy-preserving aggregation and its application in IoT. J Netw Comput Appl 126:39–44

Liang X, Barua M, Rongxing Lu, Lin X (2012) Xuemin (Sherman) Shen, "HealthShare: Achieving secure and privacy-preserving health information sharing through health social networks." Comput Commun 35(15):1910–1920

Mahmud Hossain SM, Islam R, Ali F, Kwak K-S, Hasan R (2018) An internet of things-based health prescription assistant and its security system design. Futur Gener Comput Syst 82:422–439

Manogaran G, Shakeel PM, Hassanein AS, Kumar PM, Babu GC (2018a) Machine learning approach-based gamma distribution for brain tumor detection and data sample imbalance analysis. IEEE Access 7:12–19

Manogaran G, Varatharajan R, Lopez D, Kumar PM, Sundarasekar R, Thota C (2018b) A new architecture of internet of things and big data ecosystem for secured smart healthcare monitoring and alerting system. Futur Gener Comput Syst 82:375–387

Omnia Abu Waraga, Meriem Bettayeb, Qassim Nasir, Manar Abu Talib, "Design and implementation of automated IoT security testbed", Computers & Security, Vol. 88, Article No. 101648, pp. 1–17, 2020.

O'Donovan P, Gallagher C, Leahy K, O'Sullivan DTJ (2019) A comparison of fog and cloud computing cyber-physical interfaces for Industry 4.0 real-time embedded machine learning engineering applications. Comput Ind 110:12–35

Prabhu B, kavin, S Ganapathy, (2019) A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications. Comput Netw 151:190

Qingchen Zhang, Laurence T. Yang, Zhikui Chen, Peng Li, M. Jamal Deen, (2018). "Privacy-preserving double-projection deep computation model with crowdsourcing on cloud for big data feature learning", *IEEE Internet of Things Journal*, 5: 4, 2896–2903,

Roan Thi Ngan, Mumtaz Ali, Hamido Fujita, Nguyen Long Giang, Gunasekaran Manogaran, MK Priyan, 2019 "A new representation of intuitionistic fuzzy systems and their applications in critical decision making", *IEEE Intelligent Systems*.

Samet S, Miri A (2012) Privacy-preserving back-propagation and extreme learning machine algorithms. Data Knowl Eng 79(80):40–61

Selvi M, Thangaramya K, Saranya MS, Kulothungan K, Ganapathy S, Kannan A (2019) Classification of Medical Dataset Along with Topic Modeling Using LDA. Nanoelectronics, Circuits and Communication Systems, Springer, pp 1–11

Sethukkarasi R, Ganapathy S, Yogesh P, Kannan A (2014) An intelligent neuro fuzzy temporal knowledge representation model for mining temporal patterns. Journal of Intelligent & Fuzzy Systems 26(3):1167–1178

Shangping Wang Xu, Wang YZ (2019) A secure cloud storage framework with access control based on blockchain. IEEE Access 7:112713–112724

Shen M, Ma B, Zhu L, Xiaojiang Du, Ke Xu (2019a) Secure Phrase Search for Intelligent Processing of Encrypted Data in Cloud-Based IoT. IEEE Internet Things J 6(2):1998–2008

Shen M, Tang X, Zhu L, Xiaojiang Du, Guizani M (2019b) Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart Cities. IEEE Internet Things J 6(5):7702–7712

Sivakumar Krishnan, S. Lokesh, M. Ramya Devi, "An efficient Elman neural network classifier with cloud supported internet of things structure for health monitoring system", Computer Networks, Vol. 151, pp. 201–210, 2019.

Smith E, J.H.PE loff, (1999) Security in health-care information systems—current trends. Int J Med Informatics 54(1):39–54

Tuli S, Basumatarya N, SinghGill S, Kahani M, Arya RC, SinghWander G, Buyya R (2020) HealthFog: an ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments. Futur Gener Comput Syst 104:187–200

Vadavalli AK, Subhashini R (2018) ECDH-ECC: A combination of elliptic curve cryptography and diffie hellman based cryptography technique for big data security. Journal of Engineering and Applied Sciences 13(15):6043–6052

Verma P, Sood SK (2018) Cloud-centric IoT based disease diagnosis healthcare framework. Journal of Parallel and Distributed Computing 116:27–38

William Stallings, "Cryptography and network Security: Principles and Practice", Pearson Education/Prentice Hall, 5th Edition.

Zisang Xu, Cheng Xu, Wei Liang, Jianbo Xu, And Haixian Chen, 2019 "A lightweight mutual authentication and key agreement scheme for medical internet of things", 7: 53922–53931

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.