International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(6s) 2026 pp. 259-268
https://doi.org/10.70917/ijcisim-2026-2883
Article

Hybrid Deep Neural Cryptographic Framework for Intelligent Healthcare Monitoring and Secure Medical Data Transmission

Arun Sanjay Dalvi[1], Patlolla Venkat Reddy[2]

[1]School of Engineering and Technology, Sanjivani University, Kopargaon, Maharashtra, India
arundalvi20@gmail.com
[2]School of Engineering and Technology, Sanjivani University, Kopargaon, Maharashtra, India
patlollavenkat83@gmail.com
Corresponding Author: Arun Sanjay Dalvi; arundalvi20@gmail.com

Abstract: The rapid integration of Internet of Medical Things (IoMT) technologies has revolutionized the healthcare sector, enabling real-time patient monitoring, intelligent diagnosis, and seamless data exchange between devices and cloud servers. However, this interconnected ecosystem exposes sensitive medical information to serious privacy and security threats. To address these challenges, this research proposes a Hybrid Deep Neural Cryptographic Framework (HDNCF) for intelligent healthcare monitoring and secure medical data transmission. The proposed HDNCF integrates advanced deep learning and cryptographic methods to ensure both analytical intelligence and end-to-end data confidentiality. In the proposed model, patient data collected from IoMT healthcare monitoring and security undergoes preprocessing for noise removal and normalization. A hybrid deep learning architecture, Deep Convolutional with Stacked Long Short-Term Memory (DCon-Stacked LSTM) networks, combines Deep Convolutional Neural Networks (CNN) for feature extraction, and Stacked LSTMis applied to anomaly detection and disease prediction. To guarantee privacy and security during transmission, the framework employs Rivest–Shamir–Adleman(RSA) that enhances encryption strength while reducing computational complexity. This integration enables lightweight and efficient secure communication suitable for resource-constrained IoMT devices. The experimental evaluation conducted on benchmark healthcare datasets demonstrates that HDNCF overcame these restrictions by obtaining 99.12% accuracy, 97.8% precision, 98.5% recall, and 98.7% F1-score, as well as greatly improved encryption and decryption speeds of 18.0 and 17.6 ms, respectively, to cyberattacks compared to existing models. Overall, the proposed framework establishes a robust foundation for intelligent, secure, and privacy-preserving healthcare ecosystems, fostering trust and efficiency in modern digital healthcare environments.

Keywords: Hybrid Deep Neural Network, Cryptography, IoMT, Secure Data Transmission, Intelligent Healthcare Monitoring, Rivest–Shamir–Adleman (RSA), Deep Learning.

1. Introduction

The Internet of Medical Things (IoMT) has revolutionized the monitoring process in healthcare, posing significant privacy and computational challenges. Traditional machine learning (ML) algorithms had proven ineffective in safe diagnosis. As a result, a model of DL-based cryptography was created to improve accuracy, user-friendliness, and confidentiality of data [1]. IoMT integration of transnational healthcare monitoring had improved disease prevention, yet the cloud-based solution was highly latent and computationally demanding. The original DL algorithms required much processing. Therefore, an edge-enabled DL architecture was designed to guarantee efficient, low-latency, and smart health monitoring [2].Healthcare systems have come to rely more on the IoMT and wearable devices to enhance remote monitoring, but conventional ML models have a high latency and a low level of data security. Consequently, a DNN-based cryptography system was developed to see to it that medical information was handled effectively, precisely, and confidentially [3]. IoMT-based smart healthcare systems were built around blockchain networks to protect the security of data sharing, but the variety of information and insufficient encryption

of data did not contribute to real-time security. In order to overcome the latency, security vulnerabilities, and failure to detect diagnostic errors, a hybrid deep learning (DL)-enhanced cryptography system was developed to provide intelligent and privacy-aware healthcare monitoring [4]. Cloud computing facilitated scalable and affordable services through internet-based storage, yet there were more cyber threats and data compromises that threatened the security of information. A solution to the lack of security andprivacy assurances was to construct a DL-based encryption model that would ensure accurate, reliable, and secure information storage on the cloud [5]. As long as it is on the cloud, it enhances data accessibility and efficiency in addition to causing invasion of privacy in neural network processing.Although the use of the cloud increased accessibility and efficiency of data, it also led to privacy breaches in neural network processing. Consequently, a homomorphism encryption-based neural framework that could offer secure computing along with data confidentiality in the cloud has been developed [6].The many applications of the IoMT in the diagnosis of sleep apnea have been faced with problems. The conventional PSG-based solutions were not scalable and accurate, leading to the application of ingenious, privacy-preserving DL methods [7].Privacy and fragmentation were a problem due to the exponential growth of the IoT healthcare data. The classical cloud-based storage had both trust and access control issues, which triggered blockchain-based structures that combined cryptographic and AI methods to guarantee trusted, decentralized, and transparent sharing of medical data among various healthcare systems [8]. The aim of this research project was to create an intelligent and secure healthcare data management system that utilizes Blockchain and Artificial Intelligence to provide privacy-sensitive data storage, authenticated access, and dependable information sharing about sensitive medical records in IoMT scenarios.

The rest of the research was separated: Introduction provides the background and the explanation. Related work examines the literature on the integration of IoMT and HDNCF. Materials and methods outlines the suggested hybrid HDNC model, which encompasses data preprocessing, DLanalysis and RSA. The experimental data werepresented and discussed in result and discussion, and the main findings of the research and future directions were summarized in Conclusion.

2. Related work

The cloud-fog hybrid computing platform used the developed Elliptic Curve-Diffie Hellman EC $(DH)^2$ [9] algorithm to improve data security and efficiency in healthcare situations. Experimental investigation demonstrated high-level encryption performance and reduced operational time; however, higher encryption complexity had an occasional influence on system latency under high-load conditions.Brain tumor diagnostics faced issues such as delayed biopsy and data vulnerability in MIoT [10] systems. Chaotic and Arnold encryption combined with hybrid VGG16-DNNmodels improved MRI image secrecy and classification accuracy, resulting in greater encrypted diagnostic performance while maintaining computing economy.

DL-based brain tumor detection in IoT healthcare used Advanced Encryption Standard with a key length of 128 bits (AES-128) [11]. Password-Based Key Derivation Function 2 (PBKDF) encryption with CNN architectures for secure MRI classification, with 99.92% accuracy and 99.99% AUC. Despite excellent precision, constraints included computational complexity, high resource consumption, and a reliance on huge labeled datasets.Medical images were secured using the Graph Convolutional-Based Twofish Security [12] architecture, which included hash-based dual verification. The model achieved a PSNR of 24.721, a throughput of 71.225 and a 0.002 error, which improved security by 20%, but the memory space and power consumption constraints were not solved.

Instead, a DLmodel with BiLSTM and CNN [13] on a Software-Defined Networking was utilized to enhance safety and productivity in healthcare IoT networks. The model achieved accuracy (99.59%), F1-score (99.53%), latency (3 ms), and energy consumption (55W), but dynamic topologies and redundancy were hard to maintain. The introduction of the IoT [14] in everyday activitieslike fire protection, tracking of items and monitoring of the environmentwas necessitating the need to have safe and efficient image processing. A secure image classification system with DNN and homomorphic encryption was developed. A privacy-protecting image encryption based on blockchain and optimum deep learning (BPPIE-ODL) [15] of secure transfer of IoT healthcare images. The method was able to achieve 0.9551 precision and 0.9813 accuracy using dragonfly-based encryption and SqueezeNet with Nadam optimization, but the high computational complexity and latency made it difficult to scale to large sizes. This was meant to underpin the fact that the IoHT [16] data should be handled in a secure and confidential manner. A federated learning architecture that was lightweight and integrates blockchain smart contracts with differential privacy was created. The test yielded high data security and training proficiency. The disadvantages were lack of scalability and node capacity along with data quality issues that were decentralized.

The block Elliptic Curve Cryptography-Privacy Preserving-Enhanced Sparrow Search Algorithm(ECC-PR-ESSA) [17] hybrid model enhanced IoT device authentication through Whale Optimization Algorithm-Sparrow

Search Algorithm (WOA-SSA) integration to optimize the key parameters, Reducing processing time from (60 ms - 18 ms) while increasing dependability from (25% - 3%) but had scalability and memory issues of 680 b. Cyber-attacks revealed confidential patient data, which was a tremendous obstacle to the security of health data. A CNN-LSTM-based [18] encryption model named NeuroShield with the integration of differential privacy to ensure safe analytics reached an accuracy of 98.73% with the integration of differential privacy. Better protection and interpretability were seen in the analysis; however, processing costs were high and scalability was low. The IoT-based healthcare systems have been faced with privacy issues by sending sensitive data. It was implemented with 98.3% accuracy, 94.2% sensitivity, and 95.9% precision using a BDQNN [19] with the CP-ABPE method, although the communication overhead was 68.1% and there were high encryption-decryption delays. The healthcare IoT data security and efficiency were enhanced utilizing a deep Q-learning neural network with privacy protection (DQ-NNPP) [20]. The system displayed accuracy (93.74%), sensitivity (92%), specificity (92.1%), a communication overhead (67.08%), an encryption time (62.72 ms), and a decryption time (63.72 ms), although it was constrained by energy that prevented scaling.

3. Materials and methods

Hybrid Deep Neural Cryptographic Framework (HDNCF)

The HDNCF framework integrated IoMT data gathering, data preprocessing, DL, and cryptographic security. Median filtering and Min-Max normalization enhanced data quality and training stability. CNN and stacked LSTM models extracted spatial-temporal features for accurate diagnosis, while RSA encryption secured healthcare data. Optimization minimized encryption error and improved protection accuracy, achieving reliable, privacy-preserved transmission in the HDNCF framework in Figure 1.

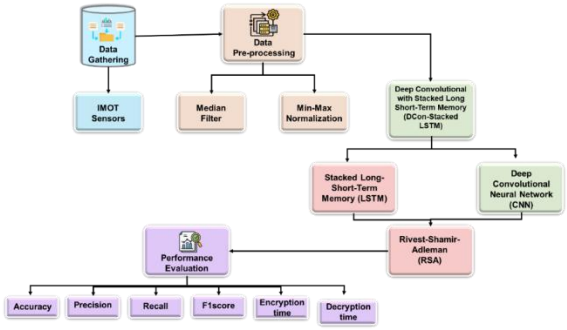

Figure 1 Hybrid Deep Neural Cryptographic Framework.

Data gathering

The IoMT Healthcare Monitoring and Security Dataset, Kaggle https://www.kaggle.com/datasets/zyan1999/iomt-healthcare-monitoring-and-security-dataset, included 2,500 simulated patient records that reflected real-world Internet of Medical Things environments. It includes physiological measurements, medical history, and treatment information, include heart rate, blood pressure, glucose levels, and oxygen saturation. Each entry included contextual information as well as a target Health Status (Healthy, At Risk, or Critical) for healthcare analytics and predictive modeling applications.

Data preprocessing

Preprocessing involved using a median filter to eliminate random impulse noise from IoMT sensor data while keeping critical medical properties for accurate HDNCF analysis. Following that, Min-Max normalization scaled the input data between 0 and 1, resulting in a more balanced value distribution, increased training stability, and higher classification accuracy in the DLmodel.

Median filter: A median filter was used in preprocessing to reduce random impulse noise from IoMT sensor data. By replacing each pixel value with the median of its surroundings, it significantly decreased noise while keeping key medical information for reliable DLHDNCF analysis in Equation (1).

$$g'(a,b) = \underset{(q,r)\in T_{ab}}{median} \{f(q,r)\} \quad (1)$$

Where g' was the filtered image, $g'(a,b)$was the filtered pixel value at position (a,b)after applying the median filter. The $f(q,r)$returns the original pixel values in the vicinity of(a,b). T_{ab}refers to the region of neighboring pixels around the point(a,b), and the medianwas the middle value when all pixel values in T_{ab}were sorted in order.

Min-max normalization: Min-max normalization was used for scale the input data within a specified range, producing a balanced value distribution between the original and processed data. This improved the model's training stability and accuracy for classification in HDNCF in Equation (2).

$$Z_{new} = \frac{Z-\min(Z)}{\max(Z)-\min(Z)} \quad (2)$$

Where Z denotes the original data value before normalization, $\min(Z)$ represents the dataset's lowest value,$\max(Z)$ represents the highest value in the dataset, and Z_{new}represents the normalized value obtained after scaling from 0 to 1.

Deep Convolutional with Stacked Long Short-Term Memory (DCon-SLSTM) networks for the HDNC framework

The HDNC framework used CNN and stacked LSTM architectures to extract spatial-temporal data, which improved diagnostic accuracy and disease predictions.

Deep Convolutional Neural Networks (CNN): The Convolutional Neural Network (CNN) architecture was utilized extract important geographic features input medical data. It processed the input was CNN, pooling, and fully connected layers, resulting in efficient feature transformation and accurate classification, which were critical for improving diagnostic accuracy in the HDNC framework shown in Figure 2.

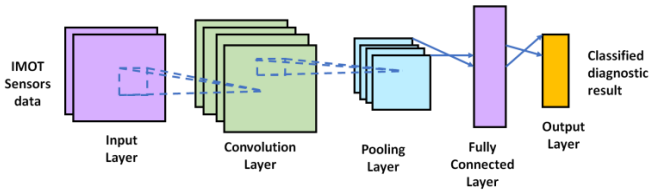

Figure 2 Deep Convolutional Neural Networks (CNN) for the HDNC framework

The convolution layer was used to extract essential spatial information from the input data via convolution kernels. It performed convolution operations between the input matrix and smaller kernels, allowing for fast feature mapping and improving the accuracy of the suggested intelligent HDNC framework in Equation (3).

$$T_{j,i}^{out} = e_{con}\left(\sum_{w=0}^{o}\sum_{z=0}^{o} x_{w,z}\, t_{j+w,i+z}^{in} + a\right) \quad (3)$$

Where$T_{j,i}^{out}$ is the output feature map at (j,i) after convolution, $e_{con}(.)$is the non-linear activation function used after convolution to introduce non-linearity, $x_{w,z}$ are kernel (filter) weights that move over the input matrix.$t_{j+w,i+z}^{in}$Enter the feature value at position$(j+w, i+z)$, and a bias is added to each convolutional output. $o$was kernel size that determines the field of acceptance for HDNCF, which identifies the specific feature extraction.

Stacked Long Short-Term Memory (SLSTM) for HDNC framework: LSTM solved vanishing gradient and long-term dependency difficulties using gated mechanisms, which the HDNC frameworkimproved sequential learning, anomaly detection, and disease prediction accuracy in IoMT healthcare data processing in Equation (4).

$$e_s = \sigma(X_e w_s + V_e g_{s-1} + a_e) \quad (4)$$

Where $e_s$is the es output of the forget gate, indicating how much past information should be retained,$\sigma(\ldots)$is a sigmoid activation function that restricts values to 0 and 1 for controlled information flow.X_e is the current input feature vector from IoMT sensor data,w_s is the weight matrices defining input and recurrent transformations,$V_e g_{s-1}$ is the previous hidden state preserving temporal context, and a_e is the bias term adjusting the gate's sensitivity.

The gating technique in LSTM contributed to the HDNCF goal by effectively resolving long-term dependency difficulties in IoMT data. The sigmoid and $tanh$based input, forget, and output gates preserved sequential

memory, as indicated in Equations (5-8), improving illness prediction accuracy and stability inside the hybrid deep neural network architecture.

$$j_s = \sigma(X_j w_s + V_j g_{s-1} + a_j) \quad (5)$$

Where j_s is the input gate activation that controls how much new information to add to the cell state, X_j is the current input feature vector, $V_j g_{s-1}$is the previous hidden state enabling temporal dependency, and a_j is the bias term to regulate gate responsiveness.

$$d_s = e_s d_{s-1} + j_s tanh(V_d w_s + V_d g_{s-1} + a_d) \quad (6)$$

Where d_s was updated cell state that captures long-term dependencies, e_s was forget gate output that determines retained information from the previous state, and $d_{s-1}$was previous cell state, $j_s tanh(.)$was candidate memory content scaled by the input gate, $a_d$was bias parameter for state update regulation, $V_d$was weight matrix that connects the prior concealed state to the current candidate cell state, and$g_{s-1}$was hidden state from the preceding time step in the LSTM sequence.

$$p_s = \sigma(X_p w_s + V_p g_{s-1} + a_o) \quad (7)$$

Where $p_s$was activation output at step s, $X_p$was input vector or feature representation from IoMT medical data, $w_s$was weight matrix corresponding to the current state, $V_p g_{s-1}$ was contribution from the previous state, allowing temporal dependency modelling, and a_o was bias term controlling activation sensitivity.

$$g_s = p_s tanh(d_s) \quad (8)$$

Where g_s was gradient strength magnitude after convolutional transformation, p_s was proportional input signal strength, d_s was activation response of the system, and $tanh(d_s)$was nonlinear transformation applied to capture subtle variations in feature deviation.

The Stacked LSTM network enhanced the HDNCF because it learned multi-level temporal relationships on IoMT sensor data. Recurrent layers and Adam optimization brought about a deeper layer of neural networks to optimize the accuracy, the detection of anomalies and prediction of diseases, providing steady healthcare monitoring within the HDNCF.

Rivest-Shamir-Adleman (RSA)Encryption for HDNCF Data Transmission

The use of RSA cryptography secured the transmission of medical data since information was encrypted by means of optimized public and private keys. In order to increase the protection, the HDNC design reduced the error with the original and encrypted data in order to improve encryption accuracy andguarantee reliable and privacy-assured communication in the intelligent healthcare monitoring system in Equation (9).

$$CP = pi^{es}(modmd) \quad (9)$$

Where CP is the ciphertext, Plaintext $pi$is the initial message or information that would be encrypted, and $es$is the exponent of the public key that would be utilized in the encryption. Poor modulus $(md)$was product of two numbers that were prime numbers. The modulus operation $(mod\ md)$ constrains the result of the encryption to a certain range of numbers.

The mathematical expression of the optimization objective of minimizing the error between original and encrypted data and maximizing protection accuracy was expressed in Equation (10) and, therefore, met the HDNCF objective of increasing secure healthcare data transmission by optimized RSA encryption integration.

$$Fn_1 = \underset{\{\rho U_b, md\}}{argmin}\,(Err) \quad (10)$$

Where Fn_1 denotes the optimized function or output with the best encryption parameters, $argmin$ refers to the process of determining the parameter values that minimize a particular function. The ρU_brepresents the public key parameter,md represents the public modulus of the RSA encryption,$and\ Err$ indicates the overall encoding error between the original and encrypted data.

The error was defined by Equation (11), and it was the difference between the original data and encrypted data, RSA public keys, to create the minimal error in encryption in the HDNCF framework.

$$Err = \sum_{jb=1}^{JB} \left| DT_{jb} - CP_{jb} \right| \quad (11)$$

Where Err represents the total encryption error, DT_{jb} denotes the original medical data before encryption. CP_{jb} denotes the encrypted data after encryption, JB denotes the total number of data samples evaluated. $\left| DT_{jb} - CP_{jb} \right|$ calculates the absolute difference between each original data point and its encrypted output, $and\ \Sigma$ aggregates absolute differences across all data samples.

4. Result and Discussion

The HDNCF framework performed better than previous ones, achieving higher accuracy, precision, recall, and F1-score at a significantly reduced encryption and decryption time, which shows better efficiency, security and reliability of IoMT-based healthcare communication systems.

Experimental setup

The experimental configuration includes Python 3.10 with Windows 11 on an Intel Core i7 processor, 16 GB of memory, and NVIDIA GeForce RTX graphic card. Models are trained on TensorFlow, features are extracted on NumPy, Pandas, Scikit-learn and Matplotlib to test the encryption-decryption and visualize the HDNCF framework to evaluate its performance and compare it with existing models.

HDNCF for Secure Healthcare Data Transmission research outcomes

The waterfall graphic 3D diagram indicated the pattern of wave intensity at the oxygen saturation and heart rate dimensions. Figure 3 illustrates the dynamics of the temporal features gathered by the LSTM layers that facilitate the analysis of the sequential pattern of health to the HDNCF architecture.

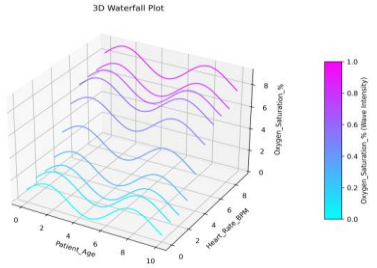

Figure 3 3D waterfall plotsof wave intensity patternsfor the HDNCF framework.

The bubble plot visualized the patient's heart rate and age, along with the body temperature. Figure 4 depicts HDNCF's increased multi-parameter analysis goal of determining the critical relationships between temperature ranges of 36-39 degrees Celsius and cardiac patterns.

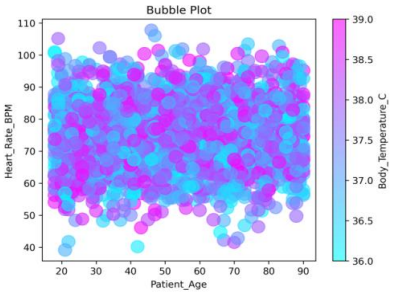

Figure 4 Bubble plot of multi-dimensional relationships with body temperature for HDNCF framework.

The area plot of stacked areas displayed changes in time of 5 vital parameters in 18 samples. Figure 5 showed the success of HDNCF in pre-processing data, which was used to achieve the Stacked LSTM goal to predict the sequential health trends.

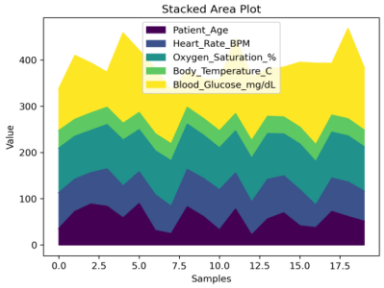

Figure 5 Stacked area plot of health parametersfor the HDNCF framework.

The joint plot used marginal histograms to analyze patterns in the distribution of age and heart rate between70 and 85 BPM across ages. It validated the importance of features for the CNN extraction layer, as shown in Figure 6, which depicts essential biomarker connections required for secure, intelligent diagnosis in the HDNCF framework.

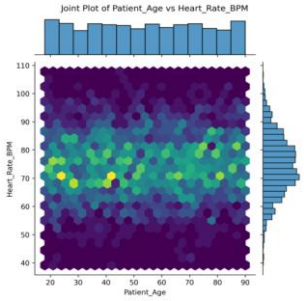

Figure 6 Joint plot of age-heart rate distribution patterns for HDNCF framework.

The 3D scatter plot depicted the correlations between patient age, heart rate, and oxygen saturation. It had a distribution of features to train HDNCF, and Figure 7 showed that it made possible pattern recognition, which is essential to prediction of the disease and anomaly detection in the HDNCF scheme.

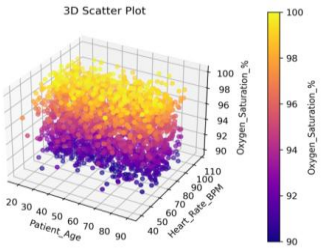

Figure 7 3D scatter plot of patient age, heart rate, and oxygen saturationfor HDNCF framework.

The ISO surface contour plot was used to show the level of intensity in (-1.92 +1.92) in age (20-90 years) and heart rate (40-110 BPM) dimensions. The critical decision boundaries in the detection of abnormalities in health are presented in Figure 8 and this enables the Stacked LSTM to identify abnormal health trends within the safe HDNCF framework.

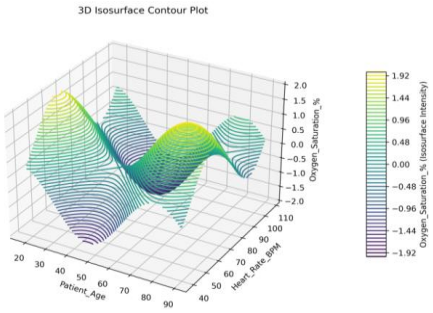

Figure 8 ISOsurface contour plot of intensity levels for the HDNCF framework

The ellipsoid plot depicted normalized feature space bounds for three critical parameters, includingoxygen saturation ranging from -6 to +6. It demonstrated data preparation effectiveness for DCon-Stacked LSTM training, and Figure 9 (a) displays the appropriate feature scaling needed for intelligent illness prediction within the HDNCF framework. The hyperboloid plot revealed complex, non-linear connections between patient age, heart rate, and oxygen saturation(-10 to +10 intensity). It proved the need for DLin HDNCF; Figure 9 (b) depicts the intricate patterns that require an advanced CNN-LSTM architecture for the HDNCF framework.

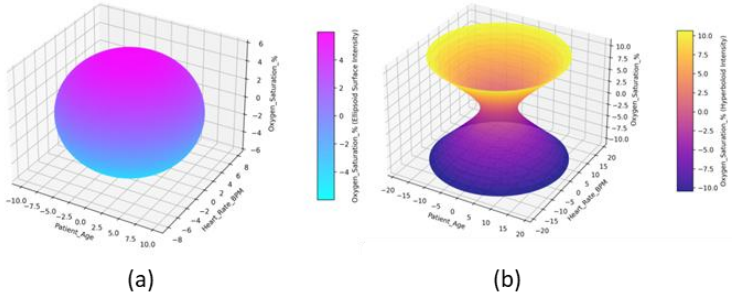

Figure 9 For HDNCF frameworks (a) Ellipsoid plot of three vital parameters, (b) Hyperboloid plot of complex non-linear relationships

Performance analysis

Accuracy refers to the overall correctness of the model in classifying healthcare data and disease patterns. Higher **precision** indicates that the test is effective in correctly identifying healthy individuals without falsely alarming them of being diseased. **Recall** assesses the system's capacity to recognize all applicable medical conditions. **F1-score** provides a balanced evaluation of a model's performance. **Encryption time** measures the rate at which data is processed before being transferred. **Decryption time** measures how fast the encrypted medical data can be accessed for analysis.

The HDNCF is targeted to improve the safety and effectiveness of IoT healthcare communication. The suggested HDNCF was compared with the previous approaches, i.e. NeuroShield CNN-LSTM [18], BDQnn-AS [19] and DQ-NNPP [20]. As demonstrated in Table 1, HDNCF performed better in terms of accuracy(99.12%), precision(97.8%),recall (98.5%), and F1-score (98.7%), which decreased encryption and decryption times to 17.6 ms and 18.0 ms, each of which is better than the existing methods. The accuracy and recall were demonstrated in Figure 10 (a-b), whichshow the encryption and decryption time.

Table 1 Performance evolution for the HDNC framework

Methods	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1score (%)**	**Encryption time (ms)**	**Decryption time (ms)**
NeuroShield CNN-LSTM model [18]	98.73	96.2	97.89	98.2	-	-
BDQNN-AS [19]	98.3	-	94.2	-	59.4	60.2
DQ-NNPP [20]	93.74	-	92	-	58.72	62.72
HDNCF [proposed]	99.12	97.8	98.5	98.7	18.0	17.6

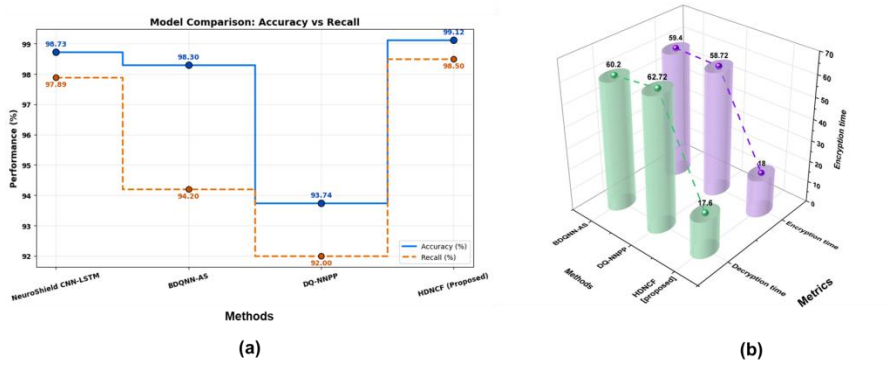

Figure 10 Performance evolutions forHDNC framework of (a) Accuracy and Recall, and (b) Encryption and Decryption times.

5. Discussion

The HDNCF framework was dedicated to the improvement of data security and computing performance in the IoT-basedhealthcare systems. The NeuroShield CNN-LSTM [18] model was extremely analytical and requiredreal-time secure communication optimization. The privacy was enhanced by the BDQNN-AS approach [19]conservation but introduced extra latency at data processing as a result of complex encryptionprocesses. The DQ-NNPP [20] model was able to do anomaly detection but at lower accuracy when used in dynamiccommunication loads. To improve end-to-end encryption and, at the same time, minimize lightweight computational operations, the proposed HDNCF method used hierarchical deep neural cryptography to achieve shorter reduced delays in data transmission and higher data integrity. Nonetheless, possible limitations were the longer sequencing time to configure the initial model and the dependence on the parameter optimization to achieve the best possible encryption-decryption time, and the ability to provide medical data sharing in a secure, scalable, and energy-saving manner in most IoT healthcare applications.The main advantage of the framework was the enhanced reliability of the communication, the fast reaction to the encryption-decryption requests, and the stability of the approach to provide the medical information sharing in the most secure, effective, and energy-efficient manner across most IoT healthcare contexts.

6. Conclusion

The HDNCF system has been able to improve safe medical data transfer and intelligent health surveillance within the domain of IoMT. It also included deep convolutional and stacked LSTM systems in order to offer the correct anomaly detection and disease, and RSA encryption prediction, which ensures that sensitive patient information, is safeguarded during communication. Its diagnostic reliability and encryption-decryption efficiency with a low latency (18.0 ms and 17.6 ms) were better, and the framework has accuracy (99.12%), a precision (97.8%), a recall (98.5%), and an F1-score (98.7%). The hybrid architecture provided the appropriate tradeoff between analytical intelligence and privacy safeguards in ensuring quality and dependable communications in health care. The objective of the suggested structure was to come up with an optimized and privacy-enabling solution capable of processing intricate healthcare data in a safe and efficient manner on dynamic IoMT systems. The outcomes of the experiment proved the ability of the experiment to resist data breaches and to introduce computational delays but at the same time made the experiment scalable to real-life applications. There were prospects to research future adaptive cryptographic optimization, lightweight encryption key control and blockchain-aided authentication schemes to add yet more trust, interoperability, and resilience to large-scale intelligent healthcare ecosystems.

References

1. Ahmad, S., Khan, S., AlAjmi, M.F., Dutta, A.K., Dang, L.M. and Joshi, G.P., 2022. Deep learning enabled disease diagnosis for secure internet of medical things. Computers, Materials & Continua, 73(1). 10.32604/cmc.2022.025760
2. Pustokhina, I.V., Pustokhin, D.A., Gupta, D., Khanna, A., Shankar, K. and Nguyen, G.N., 2020. An effective training scheme for deep neural network in edge computing enabled Internet of medical things (IoMT) systems. IEEE Access, 8, pp.107112-107123. 10.1109/ACCESS.2020.3000322
3. Yadav, R., Pradeepa, P., Srinivasan, S., Rajora, C.S. and Rajalakshmi, R., 2024. A novel healthcare framework for ambient assisted living using the internet of medical things (IOMT) and deep neural network. Measurement: Sensors, 33, p.101111.https://doi.org/10.1016/j.measen.2024.101111

4. Albakri, A. and Alqahtani, Y.M., 2023. Internet of medical things with a blockchain-assisted smart healthcare system using metaheuristics with a deep learning model. Applied Sciences, 13(10), p.6108. https://doi.org/10.3390/app13106108
5. Priya, A. and Saradha, S., 2021. Implementation of hybrid cryptographic schemes in a cloud environment for enhanced medical data security. International Journal of Nonlinear Analysis and Applications, 12(2), pp.1785-1800.http://dx.doi.org/10.22075/ijnaa.2021.5316
6. Sana, M.U., Li, Z., Javaid, F., Liaqat, H.B. and Ali, M.U., 2021. Enhanced security in cloud computing using neural network and encryption. IEEE Access, 9, pp.145785-145799.10.1109/ACCESS.2021.3122938
7. Ravikumar G, Venkatachalam K, AlZain MA, Masud M, Abouhawwash M. Neural Cryptography with Fog Computing Network for Health Monitoring Using IoMT. Computer Systems Science & Engineering. 2023 Jan 1; 44(1).DOI: 10.32604/csse.2023.024605
8. Ramachandraiah, K.R.D., Bommagani, N.J. and Jayapal, P.K., 2023. Enhancing healthcare data security in IoT environments using blockchain and DCGRU with Twofish encryption. Inf. Dyn. Appl, 2(4), p.173185.https://doi.org/10.56578/ida020402
9. Devi, B.K., Vijayakumar, V., Suseela, G., Kavin, B.P., Sivaramakrishnan, S. and Rodrigues, J.J., 2022. An improved security framework in health care using hybrid computing. Malaysian Journal of Computer Science, pp.50-61, 1/2022.https://doi.org/10.22452/mjcs.sp2022no1.4
10. Rezk, N.G., Alshathri, S., Sayed, A., Hemdan, E.E.D. and El-Behery, H., 2025. Secure Hybrid Deep Learning for MRI-Based Brain Tumor Detection in Smart Medical IoT Systems. Diagnostics, 15(5), p.639. https://doi.org/10.3390/diagnostics15050639
11. Lata, K., Singh, P., Saini, S. and Cenkeramaddi, L.R., 2024. Deep learning-based brain tumor detection in privacy-preserving smart health care systems. IEEE Access 12, 2024.10.1109/ACCESS.2024.3456599
12. Singh, A., Sharma, V.S., Basheer, S. and Chowdhary, C.L., 2024. A Deep Cryptographic Framework for Securing the Healthcare Network from Penetration. Sensors, 24(21), p.7089.https://doi.org/10.3390/s24217089
13. Babar, M., Tariq, M.U., Ullah, Z., Arif, F., Khan, Z. and Qureshi, B., 2025. An efficient and hybrid deep learning-driven model to enhance security and performance of healthcare internet of things. IEEE Access 13, 2025.10.1109/ACCESS.2025.3536638
14. Hassan, A., Liu, F., Wang, F. and Wang, Y., 2021. Secure image classification with deep neural networks for IoT applications. Journal of Ambient Intelligence and Humanized Computing, 12(8), pp.8319-8337.https://doi.org/10.1007/s12652-020-02565-z
15. Alamgeer, M., Alotaibi, S.S., Al-Otaibi, S., Alturki, N., Hilal, A.M., Motwakel, A., Yaseen, I. and Eldesouki, M.I., 2022. Privacy Preserving Image Encryption with Deep Learning Based IoT Healthcare Applications. Computers, Materials & Continua, 73(1). 10.32604/cmc.2022.028275
16. Rahman, M.A., Hossain, M.S., Islam, M.S., Alrajeh, N.A. and Muhammad, G., 2020. Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. Ieee Access, 8, pp.205071-205087. 10.1109/ACCESS.2020.3037474
17. Corthis, P.B., Ramesh, G.P., García-Torres, M. and Ruíz, R., 2024. Effective identification and authentication of healthcare IoT using fog computing with hybrid cryptographic algorithm. Symmetry, 16(6), p.726. https://doi.org/10.3390/sym16060726
18. Durai, C.R.B., Dhanasekaran, S., Rani, M.J. and Sekharan, S.C., 2025. Integrating advanced neural network architectures with privacy enhanced encryption for secure and intelligent healthcare analytics. Scientific Reports, 15(1), p.30367.https://doi.org/10.1038/s41598-025-92575-8
19. M. Lorate Shiny. (2024). Secure Data Transmission in Healthcare Internet of Things Using Bayesian Deep Q Neural Network with Privacy Preservation Authentication Scheme. International Journal of Intelligent Systems and Applications in Engineering, 12(3), 4057–4066.https://ijisae.org/index.php/IJISAE/article/view/6109
20. Kathamuthu, N.D., Chinnamuthu, A., Iruthayanathan, N., Ramachandran, M. and Gandomi, A.H., 2022. Deep Q-learning-based neural network with privacy preservation method for secure data transmission in internet of things (IoT) healthcare application. Electronics, 11(1), p.157. https://doi.org/10.3390/electronics11010157