Comparative analysis of HP-MDCNN and P3DES algorithm on the Heart Attack Analysis & Prediction Dataset

Vishal R. Shinde[1], Dr. Rahul Thour[2]

[1]Ph.D. Scholar, Department of Computer Science & Engineering, Desh Bhagat University, Punjab
[2]Assistant Professor, Department of Computer Science & Engineering, Desh Bhagat University, Punjab

Abstract:
Unauthorized access, data leaks, and insecurity are increased by the massive collection and storage of vital information in the data system. In order to address these problems, this study proposes the Parallel Triple Data Encryption Standard (P3DES), a permissioned Blockchain based encryption technique that improves privacy by processing data blocks in parallel. Increased protection against cryptographic attacks was ensured by the reduction of encryption and decryption times brought about by the robust security and concurrent processing. Only authorized users can access and validate the data thanks to the Hyperledger Fabric's introduction of proof of storage into the blockchain network, which improves privacy and secrecy. In order to make prompt judgments and administer therapies more quickly, the Hybrid Pooling-based Modified Deep Convolutional Neural Network (HP-MDCNN) is also integrated to identify the existence of aberrant conditions in patients using health data. The experiments on the Heart Attack Analysis & Prediction Dataset demonstrated that the P3DES algorithm performed efficiently for Data security/encryption and for abnormality detection, the HP-MDCNN model showed strong predictive power. [32]

Keywords:
HP-MDCN, P3DES, Hyperledger Fabric Network, Prediction, Analysis.

1. INTRODUCTION

A comparative analysis of the HP-MDCNN and P3DES algorithms on the Heart Attack Analysis & Prediction Dataset reveals that these two approaches serve distinct purposes and their strengths are reflected in different evaluation metrics.

1.1. HP-MDCNN: Focus on Prediction Accuracy

The HP-MDCNN (Hierarchical Parallel Multi-Depth Convolutional Neural Network) is primarily utilized for detecting abnormalities and predicting heart attacks. These results indicate its effectiveness in correctly identifying patients with and without heart disease, making it well-suited for medical diagnostics. [32]

1.2. P3DES: Emphasis on Data Security and Responsiveness

P3DES (Presumably an enhanced DES-based encryption algorithm) focuses on data security for patient records and healthcare environments. It demonstrated efficient cryptographic operations with an encryption time of 2.79s, decryption time of 2.19s, genuine user rate of 0.69, and responsiveness of 9.90s. These metrics suggest that P3DES can secure sensitive health data with relatively low overhead and allow for acceptable responsiveness in a clinical or IoT-based implementation. [32]

2. LITERATURE REVIEW

The relevant research is summarized in the context of privacy preservation in healthcare monitoring systems are explained in this section.

Patil, S.M. et al. [1] proposed a blockchain-based privacy preservation framework (BPPF) that addresses cybersecurity vulnerabilities by combining elliptic curve cryptography with ring-based signatures. This integration enhances transparency, flexibility, and confidentiality under cyber-threat conditions. However, the extensive use of cryptographic techniques may introduce performance delays, with the approach recording a minimized delay of 27 seconds and a block time of 2 milliseconds.

Lodha, L. et al. [2] developed a security model integrating Internet of Medical Things (IoMT) with blockchain technology (BC-IoMT-SS) to secure patient data while strengthening privacy. Simulation results demonstrated a precision ratio of 94%, outperforming comparable methods, though the system faces scalability challenges due to storage constraints

Liu, J. et al. [3] designed an advanced encryption standard utilizing inner product search and multi-keyword search encryption (MK-IPSE) for protecting electronic medical records. Their federated blockchain framework improves resistance against attacks and enhances performance. Nevertheless, the model's scalability and complexity pose challenges due to blockchain integration.

Hu, F. et al. [4] introduced FL-HMChain, a federated learning-based healthcare data management system that incorporates a master consensus node and convolutional neural networks (CNN). The model yields a 4.7% improvement in Area Under Curve (AUC) over standard CNNs and effectively reduces sensitive data leakage. However, its predictive capabilities are limited when applied beyond pathological imaging data.

Alharbi, S.H. et al. [5] proposed an IoT-based remote healthcare monitoring system (IoT-RHM) employing smart contracts to ensure data integrity and privacy. The framework achieved an integrity ratio of 97.55%, though increased resource consumption and energy use remain concerns.

The approach by Masood, I. et al. [6] developed the BBACM framework, which integrates access control mechanisms with blockchain for managing personal health information and physiological parameters. While effective for body sensor and cloud storage contexts, it lacks specific features for emergency management.

Izhar, M. et al. [7] presented a health data management system combining distributed ledger technology (DLT) and edge computing with elliptic curve encryption and machine learning for threat detection. The system achieved an accuracy of 99.77% but faces computational overhead challenges due to combined techniques.

The framework introduced by Rastogi, P. et al. [8] enhances healthcare data security using Diffie-Hellman Galois–Elliptic-curve cryptography (DHG-ECC) optimized via the Pearson Correlation Coefficient based Sand Cat Optimization Algorithm (PCC-SCOA). Their IoT-based framework demonstrates high encryption efficiency and accuracy of 96.12%, though issues related to load balancing and edge network challenges persist.

3. CHALLENGES

The major complications seen from the utilized literature works in relevance with the topic are mentioned in this section.

The integration of advanced encryption standards to balance patient data privacy while expanding privacy-preserving mechanisms remains a complex and challenging task. Despite technical progress, ensuring comprehensive protection without compromising system efficiency continues to be an open problem in healthcare monitoring systems.

Encouraging the adoption of decentralized blockchain solutions by healthcare providers, Internet of Medical Things (IoMT) device manufacturers, and patients presents another significant challenge. This adoption requires a paradigm shift in established mindsets and operating practices, which can slow down the deployment and acceptance of blockchain-based privacy frameworks.

Resource optimization and energy consumption management within healthcare IoT systems are often insufficient. For instance, the IoT-based Remote Healthcare Monitoring (IoT-RHM) system struggles to balance efficient resource utilization with the complexities introduced by consensus mechanisms, indicating a need for more energy-conscious design strategies.

While blockchain-based frameworks such as BBACM show promise in managing personal health information and physiological data from body sensors, they fall short in addressing emergency management scenarios. Moreover, the broad diversity of healthcare applications poses a barrier to the scalability and adaptability of such solutions.

Finally, encryption schemes like Diffie-Hellman Galois–Elliptic-curve Cryptography (DHG-ECC) face technical obstacles regarding load balancing and network disruptions within edge computing environments. These issues can significantly impact system reliability and risk data loss, hampering the overall performance of privacy-preserving healthcare monitoring systems.

3.1. Problem Statement

Accurate prediction of heart disease is critical for timely medical intervention and improved patient outcomes. Traditional diagnostic methods rely heavily on manual analysis of clinical data, which can be time-consuming and prone to error. Advanced deep learning models, such as the Hybrid Pooling-based Modified Deep Convolutional Neural Network (HP-MDCNN), offer promising capabilities in automating and improving the accuracy of heart disease prediction. However, achieving high predictive performance remains challenging due to the complex, high-dimensional nature of medical data and the need to optimize models for clinically relevant metrics such as accuracy, sensitivity, and specificity.

These metrics collectively measure the model's ability to correctly identify both positive cases (patients at risk) and negative cases (healthy individuals), which is essential to minimizing false diagnoses and ensuring reliable clinical decision support. This study addresses the need for a robust predictive framework that maximizes these key metrics, thereby enhancing the diagnostic precision of heart disease prediction systems while reducing misclassification risks.

4. FORMATION OF MEDICAL INFORMATION

4.1. Signature generation and verification process

The Figure 4.1. demonstrates the signature generation and verification process using the ECDSA algorithm.

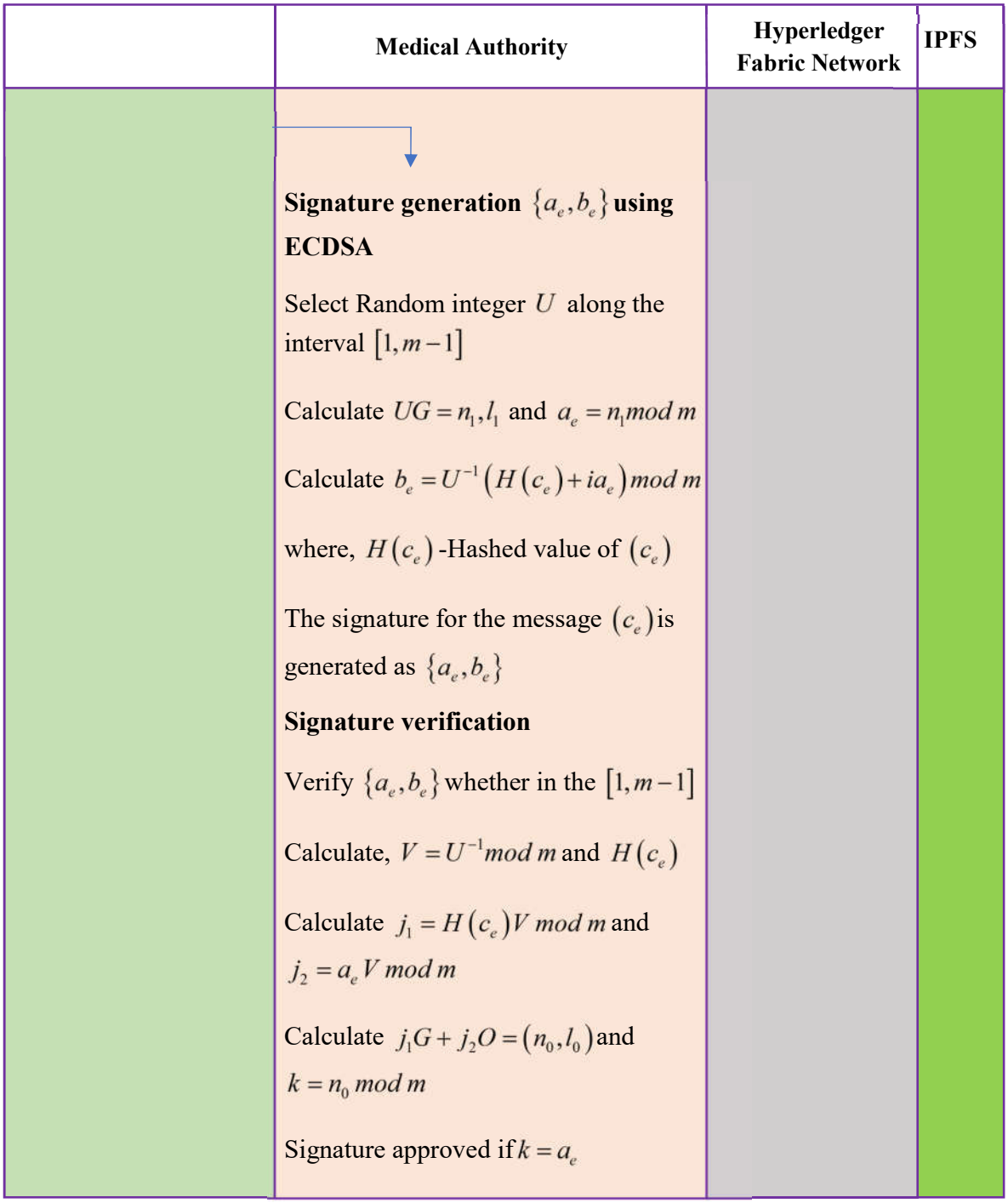


Figure 4.1. ECDSA based Signature generation and verification

4.2 Hyperledger Fabric Blockchain Network

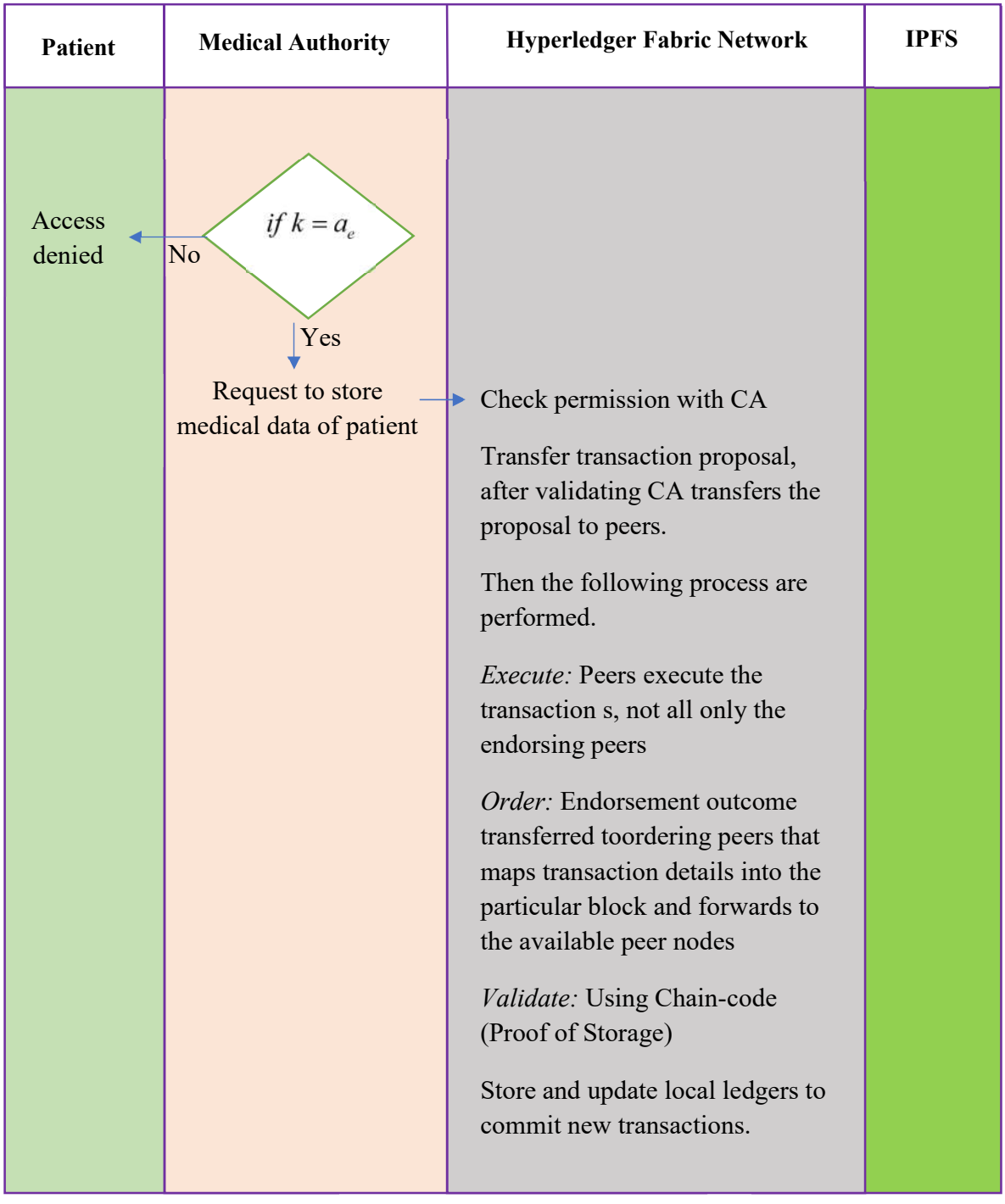


Figure 4.2. Hyperledger-based blockchain network for storing and accessing data

4.3. Hybrid Pooling enabled Modified Deep CNN

The architectural structure of the HP-MDCNN is illustrated in Figure 4.3.

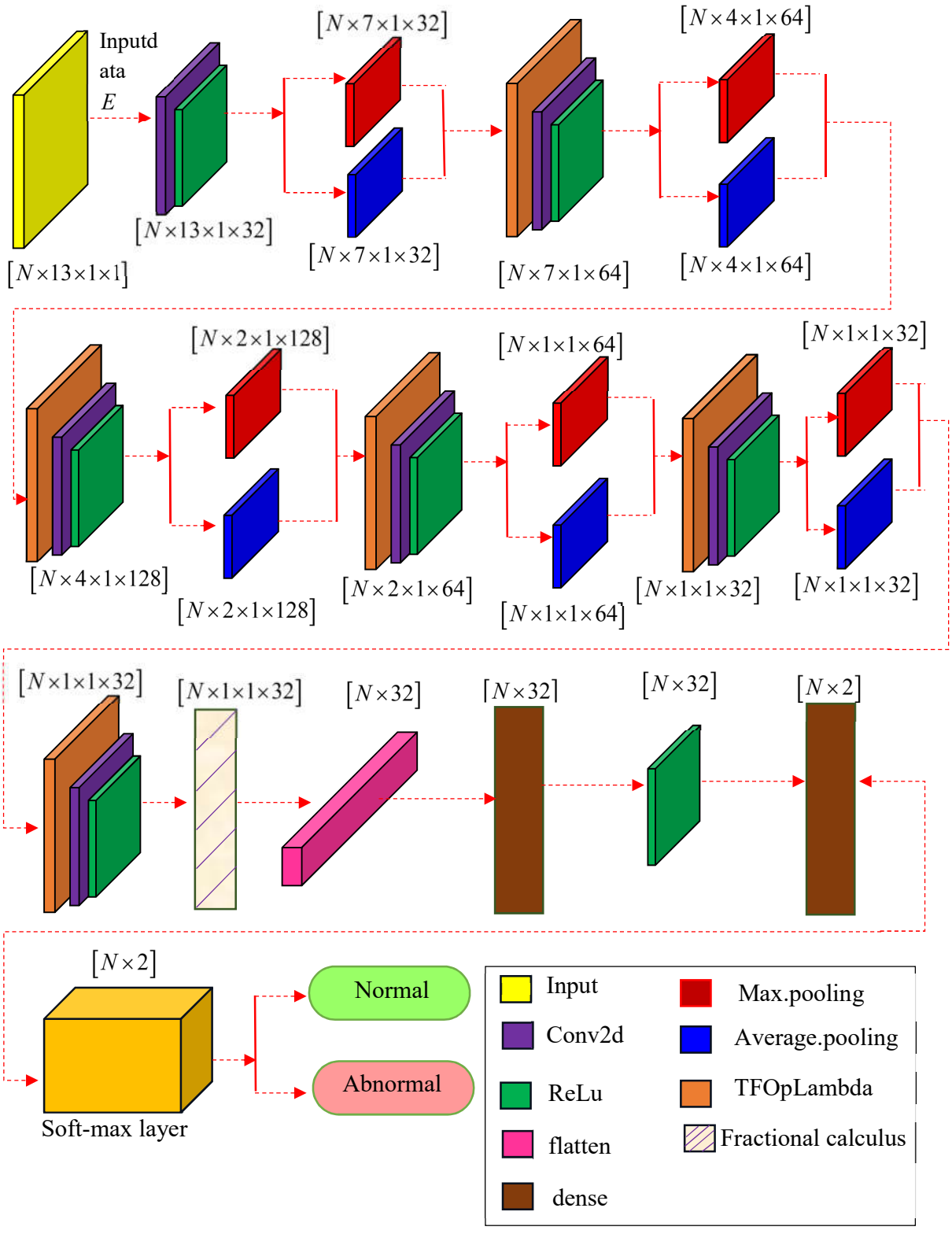


Figure 4.3. Architecture diagram of the HP-MDCNN

4.4. Storage of encrypted data

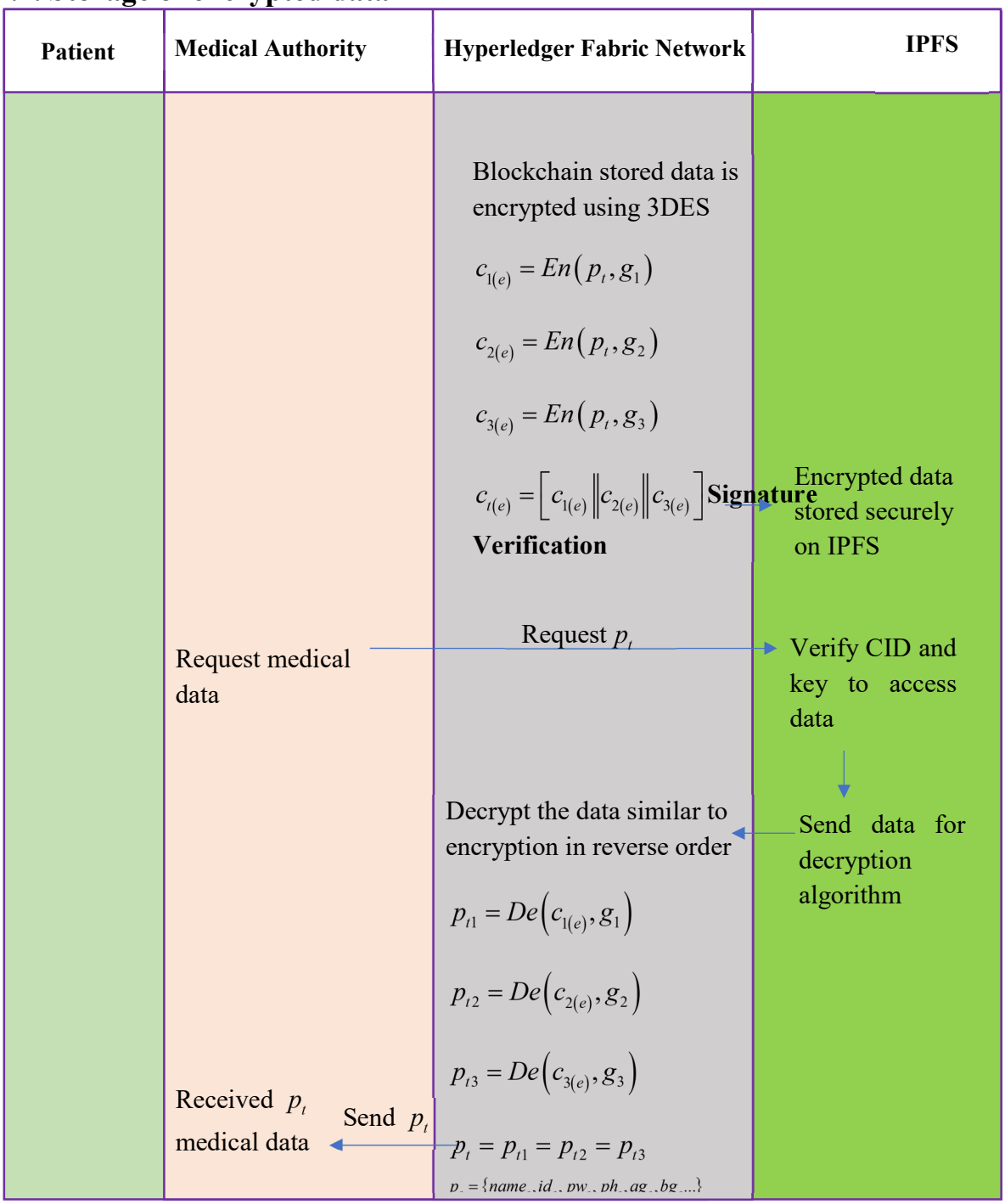


Figure 4.4. P3DES based Encryption and Decryption process and Storage

Encrypted data can be securely stored on IPFS to ensure both confidentiality and decentralized access. The encrypted data is then split into smaller chunks and distributed across the IPFS [19] network using a Content Identifier (CID), which serves as a unique reference for retrieval. Given that IPFS operates on a peer-to-peer (P2P) framework, the encrypted data is distributed across numerous nodes, providing redundancy and ensuring availability. To access the encrypted

information, both the CID and the encryption key are required. When a user requests the data, IPFS retrieves the encrypted segments, reassembles them, and the data is decrypted locally using the provided key. This approach improves data privacy and security by leveraging the decentralized architecture of IPFS, which ensures fast and dependable access while protecting against vulnerabilities associated with single points of failure. The use of encryption guarantees that, even if data is intercepted or accessed by unauthorized parties, it remains secure and unreadable without the correct decryption key.

5. RESULTS

5.1. Experimental Setup

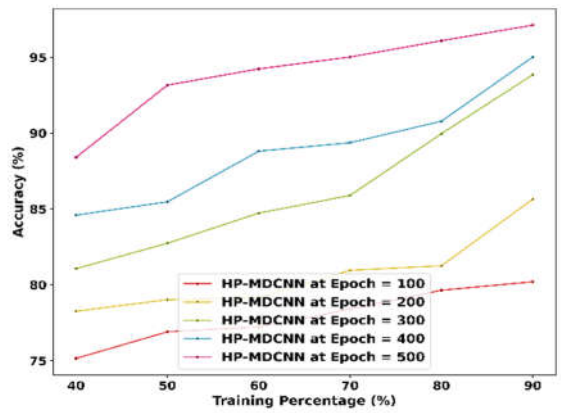
The research is carried out using the PyCharm IDE library of the Python language implemented on Windows 11 containing storage of 16GB RAM and 128GB ROM.

5.2. Dataset Description

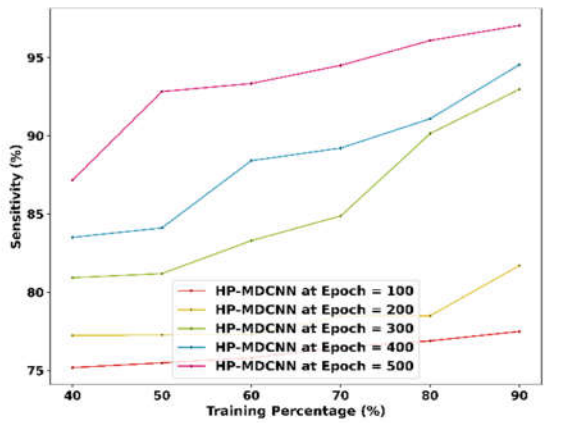
The Heart Disease Prediction dataset [30] includes 270 case studies of heart diseases with 13 important constraints of cardiac variables that showcaseage, sex, blood pressure levels, type of chest pain, cholesterol level, electrocardiogram (ECG) measurements, angina symptoms, and total measure of vessels determining coronary arteries. The dataset provides a standard to measure the risks involved in the disease earlier which can lead to the effects of cardiac arrest or heart failure. The Heart Attack Analysis & Prediction Dataset [31] presents the diverse range of attributes as the same used to determine the severe conditions of occurring stroke and cardiac problems and assist the pathologist by its root cause. The dataset provides a helpful standard for prediction of heart attack occurrence and minimizing the risk on-time helping professionals to develop preventive measures.

5.3. Performance Analysis of HP-MDCNN on Heart Disease Prediction Dataset

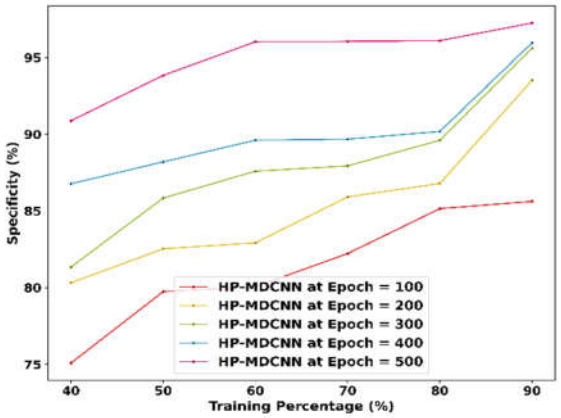
The performance of the HP-MDCNN along different training percentagesis shown in Figure 5.3. The highest value of 97.12% obtained by HP-MDCNN for the accuracy metric is along the epoch 500 for the training percentage of 90%. Similarly, the HP-MDCNN achieved a sensitivity of 97.05% at a training percent of 90%. The specificity is measured along different epochs where the HP-MDCNN achieved a peak specificity of 97.26%. The training value showcases that the model is trained with 90% while the rest of the 10% is used for validating the model. This approach increases the chances of identifying abnormalities present in the medical data.



Accuracy



Sensitivity

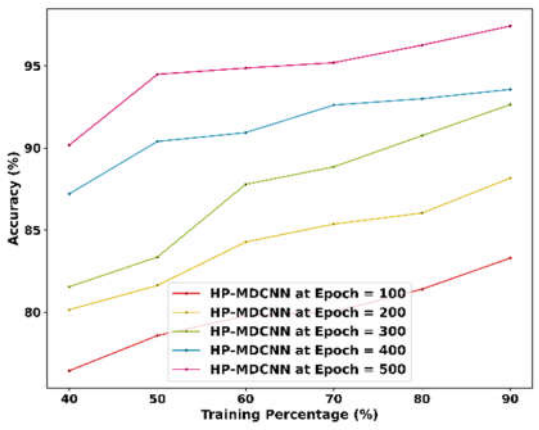


Specificity

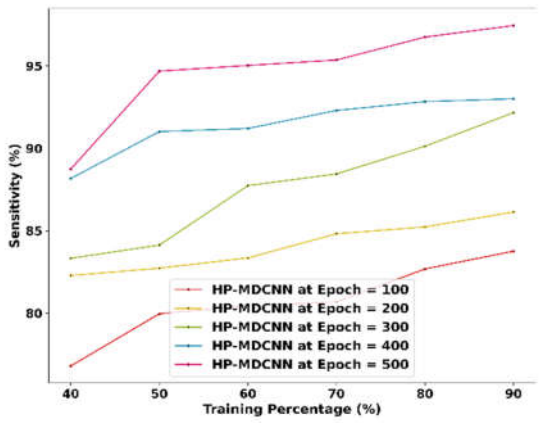
Figure 5.3. Evaluation of performance using Heart Disease Prediction dataset

5.4. Performance Analysis of HP-MDCNN on Heart Attack Analysis & Prediction Dataset

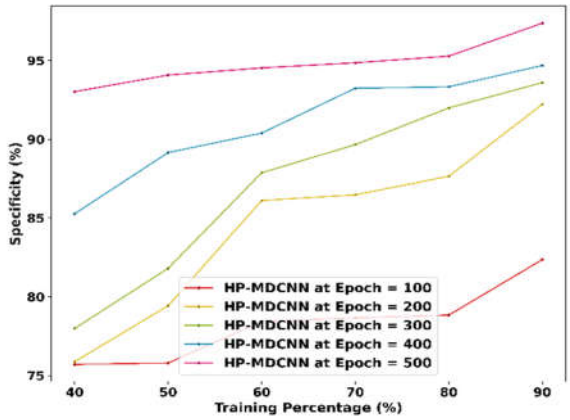
Figure 5.4. illustrates the performance obtained by the HP-MDCNN along different epochs and training percentages. The highest values attained by the metrics are at the training percentage of 90%. For the 90% of training with an epoch count of 500, the accuracy obtained by HP-MDCNN is 97.43%. Similarly, for the sensitivity, the model attained 97.45% at 90% of training at epoch 500. For the same training percentage, the HP-MDCNN gains a 97.37% of specificity. The graph showcases that with the increase in epochs, the performance of the HP-MDCNN also increases. This shows the capability of the model to learn and identify abnormalities.



Accuracy



Sensitivity



Specificity

Figure 5.4. Evaluation of performance using Heart Attack Analysis & Prediction Dataset

5.5 Comparative methods

The efficient monitoring of health data to identify abnormalities, using HP-MDCNN utilizes methods like Convolutional Neural Network(CNN)[26], Tiny Machine Learning (TinyML)[24], UNET[27], Ensemble-Human Activity Recognition System (Ensem-HAR)[25], Convolutional Neural Network with Long Short-Term Memory network (CNN-LSTM[28], and the one-dimensional convolutional neural network with Bidirectional Long Short-Term Memory network (1D-CNN-BiLSTM)[29] for the comparison.

The encryption mechanism P3DES is compared with established encryption standards like BC-IoMT-SS [2], MK-IPSE [3], BBACM [6], EEDAM [7], and the DHGECC[8] to determine the superiority in ensuring security.

5.5.1 Comparative analysis of HP-MDCNN with Heart Disease Prediction dataset

The comparative evaluation is performed separately for model and encryption mechanisms. The HP-MDCNN is evaluated against strategies like CNN, TinyML, UNET, Ensem-HAR, CNN-LSTM, ID-CNN-BiLSTM, and DCNN whereas for encryption the established approaches such as BC-IoMT-SS, MK-IPSE, BBACM, EEDAM, and the DHGECC are compared. The comparison of the HP-MDCNN with existing methods using Heart Disease Prediction is demonstrated in Figure 5.5.1. For 90% of training, the accuracy attained by HP-MDCNN is 97.12% which surpasses other models with margins of 3.24% with CNN, 4.78% with TinyML, 9.99% with UNET, 5.95% with Ensem-HAR, 12.10% with CNN-LSTM, 4.76% with 1D-CNN-BiLSTM, and 1.72% with DCNN. For sensitivity metric, the HP-MDCNN achieved a sensitivity rate of 97.05%, which is higher than CNN by 3.25%, TinyML by 3.26%, UNET by 13.51%, Ensem-HAR by 4.96%, CNN-LSTM by 13.95%, 1D-CNN-BiLSTM by 4.01%, and DCNN by 1.43%. Similarly, for the specificity, the proposed model gained a specificity of 97.26% which is more effective than 3.22% with CNN, 7.81% with TinyML, 2.95% with UNET, 7.92 with Ensem-HAR, 8.40% with CNN-LSTM, 6.25% with1D-CNN-BiLSTM, and 2.29% with DCNN, respectively.

Table 5.5.1. Comparative discussion table of the HP-DCNN

			CNN	TinyML	UNET	Ensem-HAR	CNN-LSTM	ID-CNN-BiLSTM	DCNN	**HP-MDCNN**
Heart Disease Prediction dataset	Training Percentage= 90%	Accuracy (%)	93.98	92.48	87.42	91.34	85.37	92.50	95.45	**97.12**
		Sensitivity (%)	93.90	93.89	83.94	92.24	83.51	93.16	95.67	**97.05**
		Specificity (%)	94.13	89.66	94.38	89.55	89.09	91.17	95.03	**97.26**
Heart Attack Analysis & Prediction Dataset	Training Percentage= 90%	Accuracy (%)	93.56	92.83	89.15	91.45	91.21	88.99	95.08	**97.43**
		Sensitivity (%)	94.51	93.26	89.77	89.98	91.92	89.93	95.24	**97.45**
		Specificity (%)	91.66	91.98	87.92	94.40	89.79	87.11	94.76	**97.37**

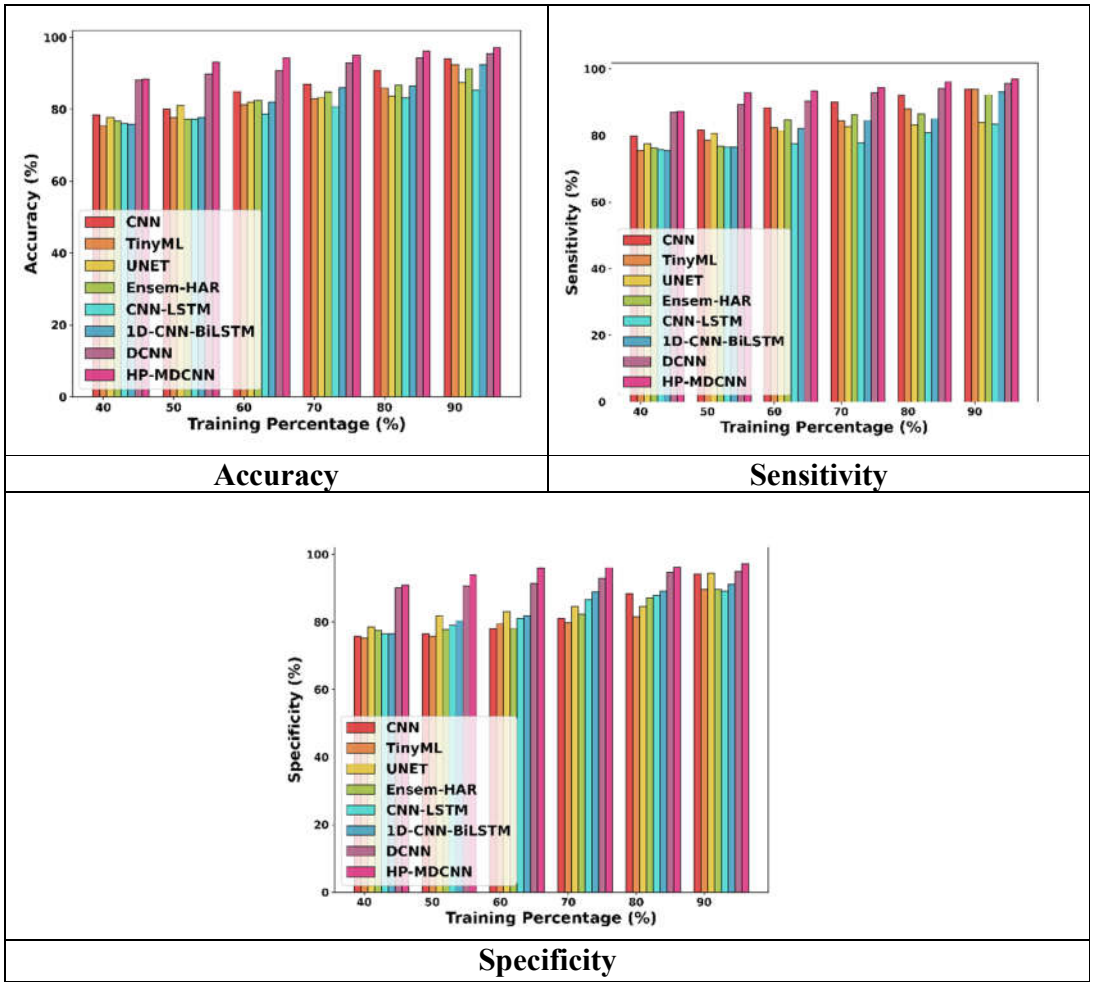


Figure 5.5.1. Comparison of HP-MDCNN using Heart Disease Prediction dataset

5.5.2 Comparative Analysis of HP-MDCNN with Heart Attack Analysis & Prediction Dataset

Figure 5.5.2. depicts the comparative analysis of the HP-MDCNN with established methods using the Heart Attack Analysis & Prediction Dataset. The HP-MDCNN at 90% training percent, achieved an accuracy rate of 97.43% which is higher compared to other methods demonstrating a difference range of 3.97% with CNN, 4.71% with TinyML, 8.49% with UNET, 6.13% with Ensem-HAR, 6.38% with CNN-LSTM, 8.66% with 1D-CNN-BiLSTM and 2.41% with DCNN. For the sensitivity, the HP-MDCNN achieved a rate of 97.45% surpassing CNN, TinyML, UNET, Ensem-HAR, CNN-LSTM, 1D-CNN-BiLSTM, and DCNN with percentages of 5.86%, 5.53%, 9.71%, 3.05%, 7.78%, 10.54%, and 2.68% respectively. The specificity gained by the HP-MDCNN with a training percentage of 90% is 97.37%, which is far better than other methods with margins of 5.86% with CNN, 5.53% with TinyML, 9.71% with UNET, 3.05% with Ensem-HAR, 7.78% with CNN-LSTM, 10.54% with 1D-CNN-BiLSTM and 2.68% with DCNN correspondingly.

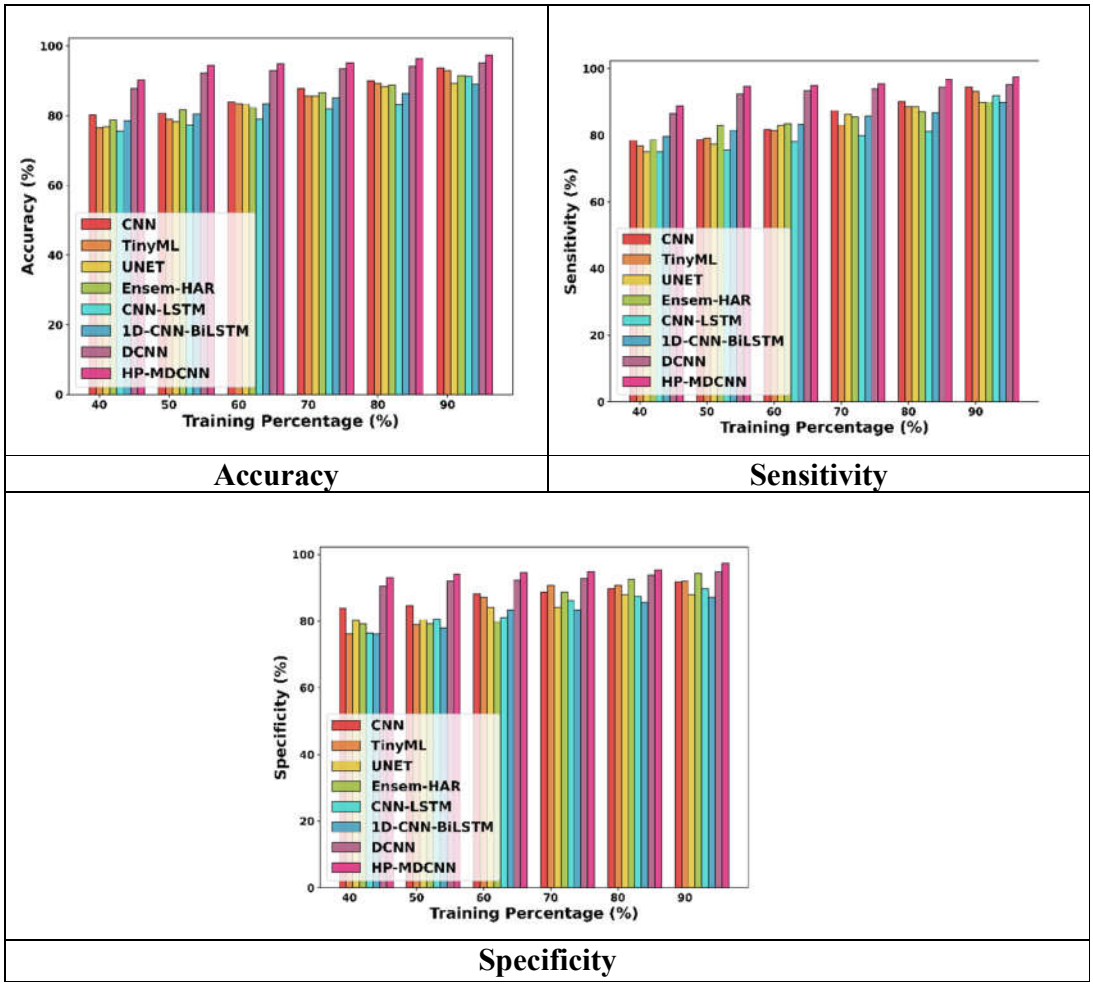


Figure 5.5.2. Comparison of HP-MDCNN using Heart Attack Analysis & Prediction Dataset

5.5.3 Comparison of P3DES with varying users using Heart Disease Prediction dataset

The comparative analysis of the P3DES against other methods with varying the 50,100, 150, 200, and 250 users are illustrated in Figure 5.5.3. For the 250 users, the P3DES required 2.38s which is lower than BC-IoMT-SS with a margin of 0.77s, MK-IPSE with 0.67s, BBACM with 0.60s, EEDAM with 0.41s, and the DHGECC with 0.22s. For the decryption, the P3DES needs 2.16s, which is far better than BC-IoMT-SS with a difference of 0.67s, MK-IPSE with 0.60s, BBACM with 0.52s, EEDAM with 0.46s, and the DHGECC with 0.46s. For genuine user rate, the P3DES for 250 users, gained 0.62 authenticated percent of users, whereas BC-IoMT-SS, MK-IPSE, BBACM, EEDAM, and the DHGECC authenticates 0.52, 0.53, 0.57, 0.59, and 0.60. For responsiveness, P3DES showed a lower rate of 9.79s which is lower than other models with a margin of BC-IoMT-SS by 1.86s, MK-IPSE by 0.89s, BBACM by 0.74s, EEDAM by 0.19s, and DHGECC by 0.07s respectively.

Table 5.5.3. Comparative discussion table of the P3DES

			BC-IoMT-SS	MK-IPSE	BBACM	EEDAM	DHGECC	P3DES
Heart Disease Prediction dataset	Number of Users = 250	Encryption time(s)	3.15	3.05	2.98	2.79	2.60	**2.38**
		Decryption time (s)	2.83	2.76	2.68	2.62	2.62	**2.16**
		Genuine User Rate	0.52	0.53	0.57	0.59	0.60	**0.62**
		Responsiveness (s)	11.65	10.68	10.53	9.98	9.86	**9.79**
Heart Attack Analysis & Prediction Dataset	Number of Users =250	Encryption time(s)	3.19	3.19	3.13	2.92	2.81	**2.79**
		Decryption time (s)	3.10	2.96	2.86	2.82	2.35	**2.12**
		Genuine User Rate	0.50	0.52	0.54	0.56	0.57	**0.69**
		Responsiveness (s)	11.15	10.32	10.24	10.24	9.94	**9.90**

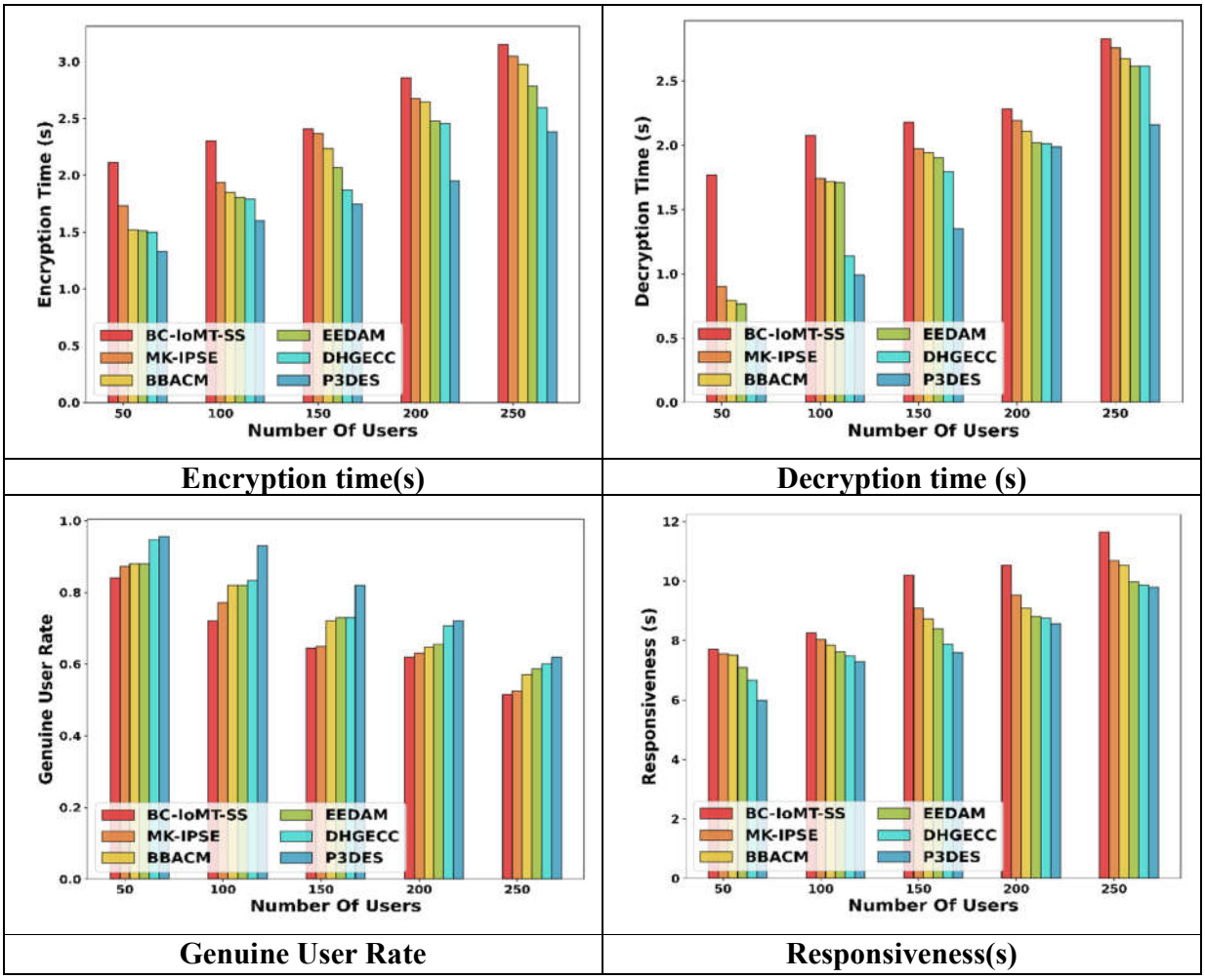


Figure 5.5.3. Comparison of P3DES using Heart Disease Prediction dataset

5.5.4 Comparison of P3DES with varying users using Heart Attack Analysis & Prediction Dataset

The comparison of the P3DES with the Heart Attack Analysis & Prediction Datasetis shown in Figure 5.5.4. The P3DES for the 250 users exhibits an encryption time of 2.79s, which is reduced on comparison with other methods achieving the difference rate of 0.40s over BC-IoMT-SS, 0.40s over MK-IPSE, 0.34s over BBACM, 0.13s over EEDAM, and 0.02s over DHGECC. Similarly, for decryption, the P3DES required 2.12s which is better by 0.98s with BC-IoMT-SS, 0.84s with MK-IPSE, 0.74s with BBACM, 0.70s with EEDAM, and 0.23s with DHGECC. The P3DES attained a genuine user rate of 0.69 surpassing BC-IoMT-SS, MK-IPSE, BBACM, EEDAM, and the DHGECC which acquired 0.50, 0.52, 0.54, 0.56, and 0.57, respectively. For the responsiveness, the P3DES achieved a rate of 9.90s, which is minimized with other techniques acquiring 1.25s of margin with BC-IoMT-SS, 0.42s with MK-IPSE, 0.34s with BBACM, 0.34s with EEDAM, and 0.04s margin with DHGECC respectively.

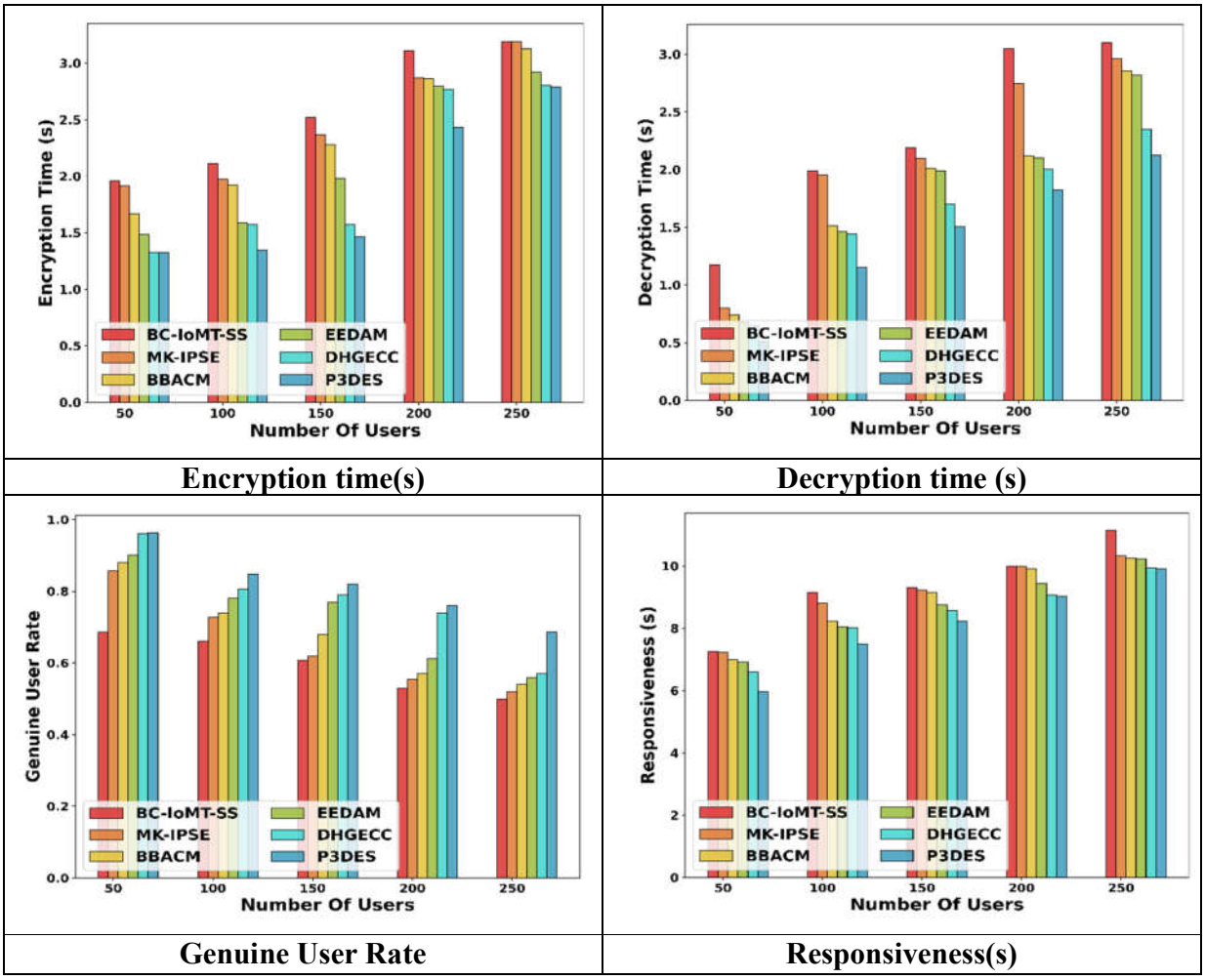


Figure 5.5.4. Comparison of P3DES using Heart Attack Analysis & Prediction Dataset

6. Conclusion:

The proposed research introduces the Parallel Triple Data Encryption Standard (P3DES) as an efficient encryption mechanism to safeguard the privacy and accessibility of healthcare data. P3DES extends the traditional Triple Data Encryption Standard (3DES) by utilizing parallel processing, which significantly reduces encryption time and enhances system responsiveness. This method preserves the robust core encryption functions of 3DES, ensuring a high degree of data security. Complementing this, the Hybrid Pooling-based Modified Deep Convolutional Neural Network (HP-MDCNN) is employed to facilitate early diagnosis by identifying critical health conditions from complex medical datasets. The hybrid pooling technique effectively extracts dominant and essential features to improve generalization and model performance. Furthermore, the incorporation of fractional calculus in the MDCNN architecture introduces memory effects and long-range dependencies, contributing to the precise identification of abnormalities. When evaluated on the Heart Attack Analysis & Prediction Dataset with 90% of the data used for training, the HP-MDCNN achieved an accuracy of 97.43%, sensitivity of 97.45%, and specificity of 97.37%. The P3DES encryption method demonstrated promising performance, with an encryption time of 2.79 seconds, decryption time of 2.19 seconds, a genuine user rate of 0.69, and responsiveness of 9.90 seconds. [32] Future research directions will focus on developing hybrid optimization algorithms to further enhance key generation processes within the encryption mechanism.

References

[1]Patil, S.M., Dakhare, B.S., Satre, S.M. and Pawar, S.D., 2024. Blockchain-based privacy preservation framework for preventing cyberattacks in smart healthcare big data management systems. Multimedia Tools and Applications, pp.1-20.
[2] Lodha, L., Baghela, V.S., Bhuvana, J. and Bhatt, R., 2023. A blockchain-based secured system using the Internet of Medical Things (IOMT) network for e-healthcare monitoring. Measurement: sensors, 30, p.100904.
[3] Liu, J., Fan, Y., Sun, R., Liu, L., Wu, C. and Mumtaz, S., 2023. Blockchain-aided privacy-preserving medical data sharing scheme for e-healthcare system. IEEE Internet of Things Journal, 10(24), pp.21377-21388.
[4] Hu, F., Qiu, S., Yang, X., Wu, C., Nunes, M.B. and Chen, H., 2024. Privacy-Preserving Healthcare and Medical Data Collaboration Service System Based on Blockchain and Federated Learning. Computers, Materials & Continua, 80(2).
[5] Alharbi, S.H., Alzahrani, A.M., Syed, T.A. and Alqahtany, S.S., 2024. Integrity and privacy assurance framework for remote healthcare monitoring based on IoT. Computers, 13(7), p.164.
[6] Masood, I., Daud, A., Wang, Y., Banjar, A. and Alharbey, R., 2024. A blockchain-based system for patient data privacy and security. Multimedia Tools and Applications, 83(21), pp.60443-60467.
[7] Izhar, M., Naqvi, S.A.A., Ahmed, A., Abdullah, S., Alturki, N. and Jamel, L., 2023. Enhancing healthcare efficacy through IoT-edge fusion: A novel approach for smart health monitoring and diagnosis. IEEE Access, 11, pp.136456-136467.
[8] Rastogi, P., Singh, D. and Bedi, S.S., 2024. An improved blockchain framework for ORAP verification and data security in healthcare. Journal of Ambient Intelligence and Humanized Computing, 15(6), pp.2853-2868.
[9] Hossein, K.M., Esmaeili, M.E., Dargahi, T., Khonsari, A. and Conti, M., 2021. BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications. Computer Communications, 180, pp.31-47.
[10] Zou, R., Lv, X. and Zhao, J., 2021. SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. Information Processing & Management, 58(4), p.102604.
[11] Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S. and Almansour, F.M., 2024. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Personal and ubiquitous computing, 28(1), pp.59-72.
[12] Dwivedi, A.D., Srivastava, G., Dhar, S. and Singh, R., 2019. A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 19(2), p.326.
[13] Wei, P., Wang, D., Zhao, Y., Tyagi, S.K.S. and Kumar, N., 2020. Blockchain data-based cloud data integrity protection mechanism. Future Generation Computer Systems, 102, pp.902-911.
[14] Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J. and Ni, W., 2020. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security, 88, p.101653.
[15] Aceto, G., Persico, V. and Pescapé, A., 2020. Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. Journal of Industrial Information Integration, 18, p.100129.
[16] Sullivan, C. and Burger, E., 2017. E-residency and blockchain. Computer law & security review, 33(4), pp.470-481.
[17] Puthal, D., Malik, N., Mohanty, S.P., Kougianos, E. and Das, G., 2018. Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. IEEE Consumer Electronics Magazine, 7(4), pp.6-14.
[18] Kaushalya, J. and Sai, R.V., 2020. A survey on efficient and secure implementation of ECDSA against fault attack. Int. J., 8(7), pp.2945-2954.

[19] Ullah, Z., Raza, B., Shah, H., Khan, S. and Waheed, A., 2022. Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment. IEEE access, 10, pp.36978-36994.
[20]HonarPajooh, H., Rashid, M.A., Alam, F. and Demidenko, S., 2022. Experimental performance analysis of a scalable distributed hyperledger fabric for a large-scale IoT testbed. Sensors, 22(13), p.4868.
[21]Liang, Y.S. and Su, W.Y., 2024. A geometric based connection between fractional calculus and fractal functions. Acta Mathematica Sinica, English Series, 40(2), pp.537-567.
[22]Sipayung, L.Y. and Purba, M., 2023. Data security analysis with triple DES cryptographic algorithm. Journal of Intelligent Decision Support System (IDSS), 6(4), pp.285-294.
[23] Malathy, K. and Jaichandran, R., 2024. Secure healthcare data for block chain networking based on Triple Des (TDES) protocol and Ekmc. Engineering Research Express, 6(4), p.045202.
[24]Arthi, R. and Krishnaveni, S., 2024. Optimized Tiny Machine Learning and Explainable AI for Trustable and Energy-Efficient Fog-Enabled Healthcare Decision Support System. International Journal of Computational Intelligence Systems, 17(1), p.229.
[25] Bhattacharya, D., Sharma, D., Kim, W., Ijaz, M.F. and Singh, P.K., 2022. Ensem-HAR: An ensemble deep learning model for smartphone sensor-based human activity recognition for measurement of elderly health monitoring. Biosensors, 12(6), p.393.
[26] Gupta, P., Chouhan, A.V., Wajeed, M.A., Tiwari, S., Bist, A.S. and Puri, S.C., 2023. Prediction of health monitoring with deep learning using edge computing. Measurement: Sensors, 25, p.100604.
[27] Yousaf, F., Iqbal, S., Fatima, N., Kousar, T. and Rahim, M.S.M., 2023. Multi-class disease detection using deep learning and human brain medical imaging. Biomedical Signal Processing and Control, 85, p.104875.
[28] Wang, Y., Wang, H., Li, Z., Zhang, H., Yang, L., Li, J., Tang, Z., Hou, S. and Wang, Q., 2024. Sound as a bell: a deep learning approach for health status classification through speech acoustic biomarkers. Chinese Medicine, 19(1), p.101.
[29] Ayano, Y.M., Schwenker, F., Dufera, B.D., Debelee, T.G. and Ejegu, Y.G., 2024. Interpretable Hybrid Multichannel Deep Learning Model for Heart Disease Classification Using 12-leads ECG Signal. IEEE Access.
[30] Heart Disease Prediction dataset, "https://www.kaggle.com/datasets/thedevastator/predicting-heart-disease-risk-using-clinical-var?select=Heart_Disease_Prediction.csv", accessed on March, 2025.
[31] Heart Attack Analysis & Prediction dataset, "https://www.kaggle.com/datasets/sonialikhan/heart-attack-analysis-and-prediction-dataset?select=heart.csv", accessed on March. 2025.
[32] Shinde, Vishal R., Dr Rahul Thour "HP-MDCNN: Privacy Enhanced Blockchain-based Medical Data Security in Healthcare Monitoring System using Hybrid Pooling enabled Convolutional Network."