HP-MDCNN: Privacy Enhanced Blockchain-based Medical Data Security in Healthcare Monitoring System using Hybrid Pooling enabled Convolutional Network

Vishal R. Shinde[1], Akshay Agrawal[2], Sanketi Raut[3],Dr. Rahul Thour[4]

[1,2,3] Ph.D. Scholars, Department of Computer Science & Engineering, Desh Bhagat University, Punjab

[4]Assistant Professor, Department of Computer Science & Engineering, Desh Bhagat University, Punjab

ABSTRACT

The digitization and increased utilization of blockchain in the healthcare industry emphasize numerous benefits however, the vast volume of medical data, diagnostic imaging, and monitoring of patients raised significant concerns. The enormous collection and storage of critical information in the data system rises the exposure to unauthorized access, leakage of data, and insecurity. To overcome these issues, this research presents a permissioned blockchain-based encryption mechanism called the Parallel Triple Data Encryption Standard (P3DES) to enhance privacy through parallel processing of data blocks. The strong security and simultaneous processing led to reduce the encryption and decryption times, ensuring increased protection against cryptographic attacks. The Hyperledger Fabric introduces proof of storage in the blockchain network that enhances privacy and confidentiality, ensuring that only authorized users can access and validate the data. In addition, the Hybrid Pooling-based Modified Deep Convolutional Neural Network (HP-MDCNN) is incorporated to detect the presence of abnormal conditions in patients through health data to ensure timely decisions in order to take faster treatments. The results when experimented on the Heart Attack Analysis & Prediction Dataset for the P3DES showcased superiority with gaining 2.79s of encryption time, 2.19s of decryption time,0.69 of genuine user rate, and 9.90s of responsiveness. Similarly, for detecting abnormalities, the HP-MDCNN achieved 97.43% accuracy, 97.45% sensitivity, and 97.37% specificity, respectively.

Keywords: Health data,Encryption,Hyperledger Fabric,Cloud Storage,Abnormal detectionDeep learning.

I. INTRODUCTION

In today's era, the healthcare industry finds itself on the brink of a significant transformation as the Internet of Things (IoT) revolutionizes the way we gather and exchange data. The integration of IoT devices into healthcare has opened up unprecedented opportunities for monitoring patients' well-being, managing chronic conditions, and optimizing healthcare delivery. However, amid this data-driven evolution, a crucial concern has emerged: the security and privacy of sensitive medical information. Addressing this challenge head-on, a decentralized healthcare blockchain tailored for IoT applications emerges as a promising solution with the potential to reshape the future of healthcare. Healthcare encompasses a wide range of services, spanning from intensive care clinics and emergency care centers to rehabilitation facilities and specialized outpatient services [13]. Healthcare systems provide essential resources to ensure a safe environment for patients, emphasizing disease prevention, control, and overall wellness maintenance [14]. Health data management aids healthcare professionals in incorporating and interpreting medical data to enhance patient care and make informed decisions that elevate the quality of healthcare while safeguarding data confidentiality and privacy. Health records serve as repositories of valuable and confidential patient information. The Internet of Medical Things (IoMT) represents an extension of IoT, specializing in the collection and processing of data for medical and health-related purposes [15]. Patient devices connected to IoT enable secure living, encompassing devices such as wired scales and portable heart monitors. The aggregation of healthcare data holds immense potential, enabling the creation of holistic patient profiles, personalized treatment plans, advancements in medical procedures, strengthened doctor-patient relationships, and ultimately, improved healthcare outcomes [11].

In recent times, several scholars have put forth the idea of integrating Blockchain (BC) technology into healthcare systems. BC is essentially a cryptographically secured, unalterable, and time-stamped public ledger designed for the distributed storage and sharing of data through peer-to-peer communication. Within a BC network, numerous nodes, which are essentially computing machines, are responsible for validating each requested transaction and maintaining records of the verified transactions. Extensive research has confirmed that BC offers a robust solution for security, efficiency, and transparency in various data exchange scenarios [17]. Given its exceptional qualities, BC presents a promising avenue for data exchange and storage in both IoT (Internet of Things) and healthcare systems. Its decentralized nature eliminates the need for patients and hospital management systems to place trust in third parties or centralized data storage authorities, addressing concerns related to single points of failure or attacks. BC's immutability and irreversibility features guarantee that patients' data remains intact and free from malicious tampering [16].

This research strives to improve the privacy of medical data through advanced encryption techniques along with employing modified deeplearning techniques to detect and inform abnormal conditions of health to takesuitable decisions. The decentralized structure of Hyperledger Fabric provides immutability and secure storage of data. The HP-MDCNN makes use of medical data to identify and inform the abnormalities. Moreover, the data is encrypted through P3DES to enhance the integrity, confidentiality, and security of the data. Finally, the data is stored on the Inter-Planetary File System (IPFS) for fast, and reliable accessibility. The primary contributions of the research are summarized as follows.

Parallel Triple Data Encryption Standard (P3DES): Parallel Triple DES built upon the traditional Triple DES processes the data encryption and decryption simultaneously in parallel. This parallel processing leads to advanced encryption and fastens the processing time of the system. P3DES improves the performance by incorporating the core operations of 3DES through encrypting data with three different keys ensuring data integrity and a high level of security.

Hybrid Pooling-based Modified Deep CNN (HP-MDCNN):The HP-MDCNN leverages the strengths of both max and average pooling to capture the subtle features from the complex data, leading to provide better generalization performance. Moreover, the fractional calculus in the HP-MDCNN minimizes overfitting with long-range dependence and enables the model to detect abnormalities and inform the authority to take timely decisions.

2. LITERATURE REVIEW

Patil, S.M. et al. [1] presented a privacy preservation model based on the blockchain (BPPF) to overcome the challenges of vulnerabilities in cyber systems. This approach with the combination of an elliptic curve algorithm with a ring-based signature provides transparency, flexibility, and confidentiality during the situations of cyber-threats. The security mechanisms can result in delayedperformance due to the vast range of working cryptographic techniques. The approach attained a minimized delay of 27s with a blocktime of 2ms.

Lodha, L. et al. [2] designed a security approach integrating the Internet of Medical Things (IoMT) with blockchain (BC-IoMT-SS) to secure medical data and enhance privacy mechanisms. The integration of both techniques led to the effective management of the healthcare data of patients. The outcomes after the simulation process demonstrate a 94% precision ratio which is longer in comparison with other approaches. Though, the larger percentage of outcomes, the model faces scalability issues with limited storage space.

Liu, J. et al. [3] developed an encryption standard that uses mechanisms like inner product search along with multi-keyword search (MK-IPSE) to secure private data with advanced encryption of electronic medical records (EMRs). The federated blockchain with searchable encryption provides resistance to attacks and improved performance. The issues inherited are the scalable and complexities that arise due to the combination of blockchain systems. Despite the issue, the framework showed the required performance in power and storage.

Hu, F. et al. [4] designed an innovative approach called the FL-HMChain that collaborates healthcare and medical data with federated learning (FL). FL-HMChain incorporates the master node as consensus and CNN for validating performance. With an average rate of 4.7% enhancement on Area Under Curve (AUC) over CNN, the model effectively minimizes the leakage of sensitive data. Moreover, the model lacks reliable predictions when applied rather than pathological images.

Alharbi, S.H. et al. [5] introduced IoT IoT-based remote healthcare monitoring system (IoT-RHM) to enhance the level of security mechanism of patient data through a smart contracts technique, that tamper-proofs the data thereby elevating the integrity and privacy. The framework showcases a 97.55% integrity ratio on the evaluation of performance. However, the potential limitations like enlarged resources and heavy consumption of energy remain a constraint.

The approach by Masood, I. et al. [6] involves access-control mechanisms and blockchain integration termed the (BBACM) framework for the management of personal health information (PHI) and physiological parameters of patients (PPPs). The framework configures it as a promising solution for improving the challenges that are prevalent in the context of body sensors and cloud storage systems. However, the framework is not designed specificallyfor emergency management systems which reduces the ongoing trends in healthcare systems.

Izhar, M. et al. [7] introduced a health data management system that includes distributed ledger technology (DLT), along with edge computing. Encryption mechanisms like elliptic curves and edge nodes are integrated to improve the privacy and integrity of healthcare data in the monitoring systems. It also includes machinelearning (ML) methods for the detection of threats. With an accuracy of 99.77%, the model showcases its superiority, yet the challenge of computational overhead is acquired with the utilization of multiple techniques.

The framework introduced by Rastogi, P. et al. [8] enhances the data security of healthcare data through encryption mechanisms like Diffie Hellman Galois–Elliptic-curve cryptography (DHG-ECC), where specific features are optimized by Pearson Correlation Coefficient based Sand Cat Optimization Algorithm (PCC-SCOA). These mechanisms include the IoT-based medical data and encrypts efficiently utilizing the algorithms which replicates prolonged accuracy and security. However, the approach attains a security rate of 96.12%, but the load balancing and challenges of edge networks remain a major issue.

2.1 LIMITATIONS OF EXISTING SYSTEM

The integration of advanced standards of encryption methods to balance the needs of data privacy of patients to enlarge the posture of privacy mechanisms remains a challenging task [1]. Encouraging healthcare providers, IoT device manufacturers, and patients to adopt and understand the benefits of a decentralized blockchain solution results a challenge, as it requires a change in mindset and established practices [3]. Optimizing the resources and consumption of energy along with the delicate consensus mechanisms is lacking peculiarly by the IoT-RHM [5]. The BBACM [6] failed to involve the management of emergency systems. Additionally, the diverse range of scenarios of healthcare poses a significant challenge for expansion. The DHG-ECC [8] suffered from load-balancing strategies and frequent network issues that predominantly disrupt the system and can lead to data loss [8].

2.2 PROBLEM STATEMENT

The rapid growth of healthcare sector with advanced IoT and blockchain system possesses a major boon in research industry, however securing and managing the sensitive data of patients turned as one of the prime challenges. Therefore, to ensure integrity, privacy, and also authenticity for timely and accurate decisions in healthcare, a decentralized blockchain-based healthcare system that integrates an advanced Deep CNN for improved data security is designed in this research.

2.3 OBJECTIVES

To create a decentralized blockchain system for healthcare applications for data security and privacy.

To introduce data verification mechanisms to ensure secure storage and integrity of data.

To improve the model's performance using different techniques, ensuring accurate health-related decisions.

Evaluate the model’s performance using metrics such as accuracy, sensitivity,specificity, Genuine User Rate (GUR), and responsiveness to show its efficiency

3. PROPOSED SYSTEM

The emerging landscape of IoT in the healthcare sector faces more issues in securing the patient secret information and leads to the security vulnerabilities and unauthorized access. Apart from these complications, the scalability of these systems has become a major issue since dealing with large volumes of medical data that often demands enormous processing capabilities and infrastructure. The research aims to encompass MDCNN architecture along with blockchain distributed security to solve the drawbacks relating to data privacy and restrictions on operational performance while enhancing interpretability. In the initial stage, the patient medical information is collected and stored by the medical authority. The organization assigns a specific identifier to the patient as well as the doctor such that the identifier is being generated based on patient details. The authority records the data into the database, which runs on the cloud-based blockchain infrastructure. When the authority or the doctor wants to access the data, the authentication system verifies the authenticity of the user through authentication mechanism. The Hyperledger Fabric-based blockchain serves as a powerful tool, especially in the context of enterprise, where the peers execute and validate the transactions from different blocks and the subsets of them called the endorsing peers execute the transactions.The pre-trained model checks for the abnormalities related to health conditions and warns the particular authority about the conditions, for timely treatments and decisions. The encrypted data is securely stored on the IPFS, which is an advanced storage system that allows users to ensure secured transmission and accessibility. The general workflow of the system is shown in Figure 1.

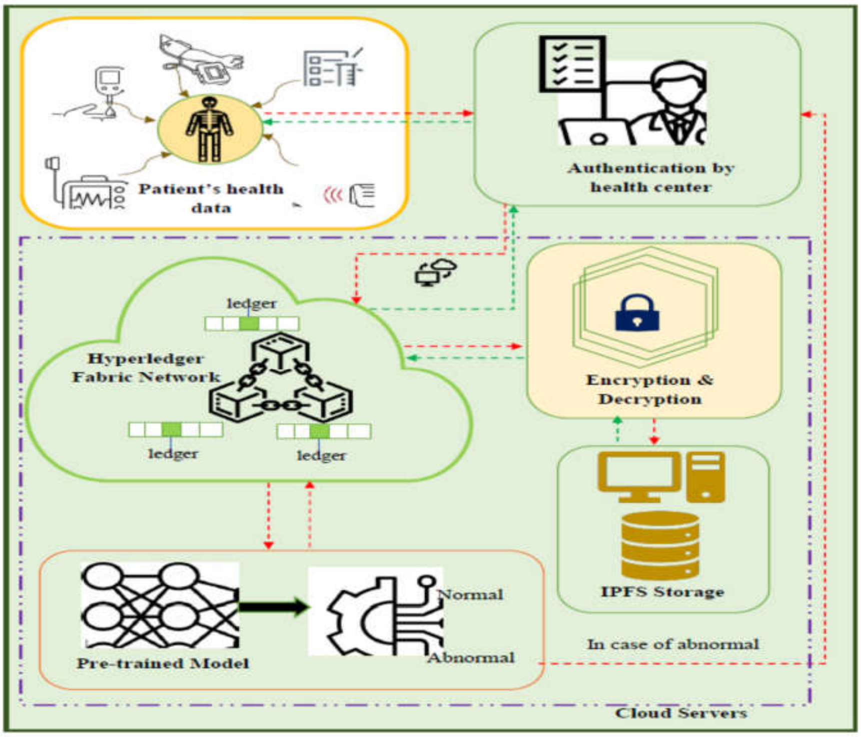

Figure 1. System Model of Block-chain based Healthcare System

4. METHODOLOGY

4.1 BLOCKCHAIN ENABLED HYBRID POOLING-BASED MODIFIED DEEP CONVOLUTIONAL NEURAL NETWORK FOR HEALTHCARE MONITORING SYSTEM

Centralized systems used in healthcare systems for storing health data are distracted by the challenges related to data integrity and authentication.To overcome this, blockchain-based approaches are employed however the systems address the concerns but face difficultyin finding a balance between security, performance, and accessibility. The research designs a priority of establishing a blockchain-based privacy-preserving healthcare system by involving HP-MDCNN along with P3DES to resist the demerits related to data privacy and to take timely decisions. Initially, the organization data like the patient data and pathologist data are gathered. These data are generated through personal identifications and stored on the organization's database which uses the Hyperledger Fabric blockchain network. The network serves as the decentralized architecture that functions through a network of nodescalled the ledgers and provides a higher degree of security.The patient data involves the patient's name, password, ID, the stored blockchain address, and the private key generated at the time of storage. For secure storage and to maintain confidentiality of these data, the patient'sinformation is stored using the signature generated by the Elliptic Curve Digital Signature Algorithm (ECDSA). This signature is further utilized for the accessibility of the specific patient's details by the medical authority. While the owner or the doctor who wants to access the medical datauses the patient's name, password, ID, and the generated signature (hash value). The data stored on the Hyperledger Fabric is forwarded to the HP-MDCNN before encryption and storage on cloud servers. The HP-MDCNN, uses hybrid pooling operations and also includes fractional calculus theory into the model to minimize the risk of overfitting and produce more generalized results. The pre-trained model informs the medical authority if the data reports abnormalities in health data and routesthe way for doctors to take timely decisions for the worse conditions. After this stage the data is encrypted through P3DES, which operates on triple layersof encryption, usingthree different keys. This algorithm securely stores the data making it suitable for healthcare applications where data is enormous. Finally, the encrypted data is secured on the IPFS which stores files and efficiently delivers data. For the accessibility of data, the process is reversed by conversely performing the operations.

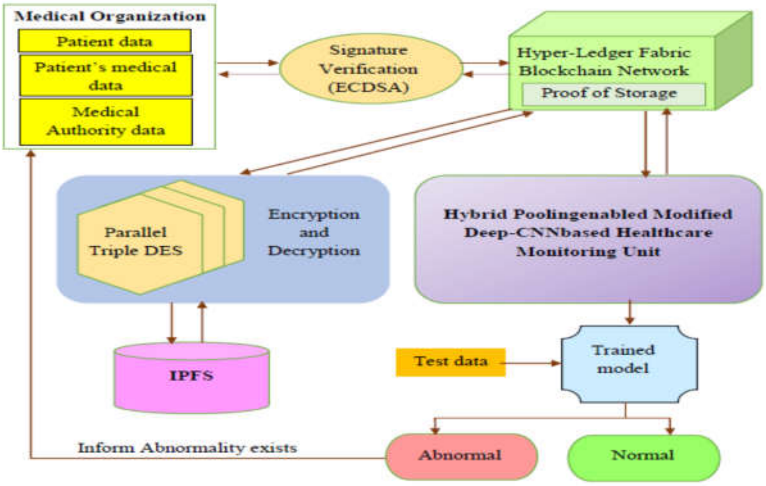
Medical Organization
Patient data
Patient's medical data
Medical Authority data
Signature Verification (ECDSA)
Hyper-Ledger Fabric Blockchain Network
Proof of Storage
Parallel Triple DES
Encryption and Decryption
Hybrid Poolingenabled Modified Deep-CNNbased Healthcare Monitoring Unit
IPFS
Test data
Trained model
Inform Abnormality exists
Abnormal
Normal

Figure 2. Block-diagram representation of model

4.2 ECDSA-BASED SIGNATURE GENERATION AND VERIFICATION

A digital signature is a mechanism used to verify the integrity and authenticity of digital data. The ECDSA algorithm is utilized as the scheme to generate the digital signature. It is an asymmetric cryptographic system that involves the utilization of public keys and private keys. The public key can be shared with the patients while the private key remains secret at the authority end. The ECDSA algorithm [18] functions on the elliptic curve represented as B that is defined on the path N_f, and G is the point with a prime order m in $B(N_f)$, where f denotes the prime number. For the patient p_e, a random number i in the interval $[1,m-1]$ is analyzed for the generation of the public and private key, and $O=i\cdot G$ is computed, where O denotes the public key and i denotes private key of the patient p_e.

Signature generation**:** To digitally sign the message c_e, of the patient, p_e the parameters are considered. The following steps are performed for the generation of signature.

(i)Random number U is initialized along the interval $[1,m-1]$.

(ii) Calculate $UG=n,l$ and $a=n mod\, m$, where n_1,l_1 are the integers between the 0 and $f-1$. The step is reverted to (i) if the value of a_e is 0.

(iii)Calculate $U\, mod\, m$.

(iv) Calculate $b=U\left(H(c)+ia\right)mod\, m$, where H denotes hashed value. The step is reverted to (i) if the value of b_e is zero.

(v) The required digital signature $\{a_e,b_e\}$ is generated for the message c_e.

Signature verification: The generated signature is verified whenever the medical data needs to be accessed. The following steps show the verification process using ECDSA.

(i)The integers $\{a_e,b_e\}$ are verified whether in the $[1,m-1]$ interval or not.

(ii) Calculate, $V=U^{-1}mod\, m$ and $H(c_e)$

(iii) Calculate $j_1=H(c_e)V\, mod\, m$ and $j_2=a_eV\, mod\, m$

(iv) Calculate $j_1G+j_2O=(n_0,l_0)$ and $k=n_0\, mod\, m$

(v)Approve the signature when $k=a_e$

4.3 HYPERLEDGER FABRIC BLOCKCHAIN NETWORK

After the authentication of signatures, the data is forwarded to the cloud servers through Hyperledger fabric network. The Hyperledger Fabric [3] is a permissioned modular blockchain network that operates on smart contracts called the “chain code”. Generally, the network contains the following components clients, Certificate Authority (CA), peers, and ordering nodes. The clients are the users who submit the proposals for the execution of transactions. Peers execute the chaincodesand validate the transaction proposals, and maintain the ledgers of the blockchain. Every peer is not responsible for executing transactions, rather the endorsing peers who are the subset of the majority peers, execute the proposals. The CA is an administrator who issues public, digital, and private certificates and also verifies the identities of the peers when joining the network.Ordering nodes form the order for all the transactions in the network. The workflow of the Hyperledger Fabric in the context of storing patient data can be elaborated as follows.

Transactioncreation: The doctor is a participant in the network who has a digital certificate from the CA requests for the transaction. The CA after validating, transfers the proposal of the transaction to the peers.
Transaction Endorsement: The peers execute the transactions, by checking the authenticity and deliver a message as approved or unapproved, that is forwarded to the client.
Submit to Ordering nodes: The outcome from the endorsement is forwarded to the ordering service. The ordering nodes or the peers responsible for ordering include the transaction details into the particular block and forward them to the peer nodes available in the network.
Updating ledger: With the receiving of the block, the peer nodes of the specific organization update their local ledgers with the received block to commit the new transactions. Figure 4. illustrates the storage service offered by the Hyperledger fabric-based blockchain network.
Proof of Storage: Peers are also responsible for hosting the ledgers and chaincodes, due to blockchain networks generally need consistent copies of data and smart contracts. These smart contracts run on specific mechanisms, where the concept of data storage is attained through the ledger's immutability and using hashes of the medical data. The Hyperledger Fabric [20]is decentralized and stores records that are immutable and the use of storing the actual data is stored separately from the blockchain ledger while the ledger stores only the hashes of the actual data. These two principles known as the Proof of Storage ensure data integrity by verifying storage.

4.4 HYBRID POOLING ENABLED MODIFIED DEEP CNN

The data stored in the blockchainis made available to the healthcare monitoring unit. The unit is trainedusing the model to detect the abnormalities of health conditions through medical data, the HP-MDCNN employs datasets [30] and [31]. The dataset can be mathematically represented as,

$$E=\left\{x_{u,v}\right\},1\le u\le P,1\le v\le Q$$

where E denotes the datasets, $x_{u,v}$ denotes the v^{th} attribute for the u^{th} sample, P implies the total number of samples,and Q implies the total attributes present in the u^{th} sample.For each sample, the output labels are assigned and can be denoted as $y_u\in[0,1]$.

$$y_u=\begin{cases}0, Normal\\1, Abnormal\end{cases}$$

The following data samples are forwarded for cleaning, normalizing, and removing unwanted values. Then, the data are transferred to the proposed HP-MDCNN to recognize the inherent patterns. The data with dimension $[N\times 13\times 1\times 1]$ is processed with the proposed modelthat extract complicated and high-level features. The model employs multiple convolutional layers that produce a hierarchical level of feature extraction. The ReLU is used as activation to include non-linearity, tackle vanishing gradients, and fasten the process. After processing through these layers, hybrid pooling is used which involves incorporating mixed pooling integrating the max pooling and average pooling that indulges priority-based features and smoothing process to preserve the essential details. This hybrid pooling approach minimizes the overfitting issues with a reduction of dimension $[N \times 7 \times 1 \times 32]$. Similarly, the process is repeated for four more cycles to efficiently train and improve the performance. During the first cycle, the dimension is reduced to$[N \times 4 \times 1 \times 64]$, then in the second cycle to $[N \times 2 \times 1 \times 128]$, and subsequent cycles as $[N \times 2 \times 1 \times 64]$,and $[N \times 1 \times 1 \times 32]$. Additionally, the fractional calculus theory [21] is introduced in the model that is applied before the flattened layer and dense layers to enhance learning capacity. Fractional calculus theory is an extended version of ordinary calculus that involves differentiation and integration of functions to fractional orders. The Riemann-Liouville (RL) based fractional derivative is employed for determining the fractional order using the repetition of integration and differentiation. Consider as the analyticfunction$h(x)$, inthe domain$[0,x]$, that is divided into equal grids for the step size of e .The RL fractional derivative of order gamma λ of a function $h(x)$ is represented as,

$$C^{\lambda}h(x) = \frac{1}{\Gamma(-\lambda)}\int_{0}^{x}(x-r)^{-\lambda-1}h(r)\,drx,r$$

where $\Gamma(\cdot)$ denotes the gamma function, $h(r)$denotes the function to be differentiated, and x,r denotes the real variables that determine the input data x along the time r.The generalized form of integration repeated along the interval $[0,x]$.The function λ acts as a normalizing entity, which generalizes the factorial function to fractional orders. The fractional derivatives include the memory effect which means that the state depends not only on the present but also analyses the entire history. This mechanism allows the HP-MDCNN to capture intricate details of irregular health data. The MDCNN produces the output with fractional derivatives as

$$d_A = \sigma\left(W * C^{\lambda}x + Y\right)$$

The HP-MDCNN produces an output of $[N \times 2]$as normal and abnormal and the model notifies the doctor by alerts to provide insights for immediate actions. Moreover, the model's error rate is minimized using the loss function as described in equation (6). The learning rates are tuned effectively using the Adam optimizer to improve response times of alerts through momentum and adaptive learning of complex patterns of medical data.

4.5 PARALLEL TRIPLE DES FOR ENCRYPTION AND DECRYPTION

P3DES is an extensive encryption standard that is built upon the standard DES algorithm executing parallelly three times across each block of data to enhance the security. Due to the small key size of 56 bits, the DES[22] is vulnerable to brute-force attacks. To overcome this, the P3DES was introduced that operates 3DES executions simultaneously using the same plaintext and different keys to generate the cipher text. The cipher text obtained after concatenationis of 192-bit ciphertext form, which makes itimpossible for the attackers to access the data. Consider a plaintext of 64bits$p_t$as inputwhich executes on triple DES operations using keys g_1, g_2 and g_3 of 64bits.

$$c_{1(e)} = En(p_t, g_1)$$

$$c_{2(e)} = En(p_t, g_2)$$

$$c_{3(e)} = En(p_t, g_3)$$

$$c_{t(e)} = \left[c_{1(e)} \| c_{2(e)} \| c_{3(e)}\right]$$

where, $c_{1(e)}, c_{2(e)}, c_{3(e)}$ denotes the three cipher text for the e^{th} patient. $c_{t(e)}$ denotes the generated cipher text after concatenation which is 192 bits long and En denotes the encryption process. The encrypted output is thus stored in the IPFS cloud storage. Similarly, for decryption, the process is reversed. The same keys are used and decrypted each block in parallel.

$$p_{t1} = De\left(c_{1(e)}, g_1\right)$$

$$p_{t2} = De\left(c_{2(e)}, g_2\right)$$

$$p_{t3} = De\left(c_{3(e)}, g_3\right)$$

where De denotes the decryption operation. Since the same keys are used for decryption, the output should match to produce the plaintext.

$$p_t = p_{t1} = p_{t2} = p_{t3}$$

The attained plaintext also serves as the notation for the integrity check to determine whether the data is similar to what has been stored.The DES involves performing similar operations to encrypt and decrypt to enhance the security and reduce the tampering of data. The general operations performed for encryption and decryption in the standalone DES can be described as follows.

4.5.1 CORE OPERATIONS OF P3DES

As the P3DES is built upon the functions of DES [23]algorithm, the core operations are similar as it works on the Fiestel structure undertaking 16 rounds with different keys used for every round. DES performs subsequent functions for each round to encrypt the data. DES uses a fixed 64-bit length of plaintext and key as input. The core operations of the DES are described below.

a) Initial permutation:The first step in DES is the initial permutation, where the plaintext is rearranged using a permutation table.

b) 16 rounds of Fiestel function: The DES algorithm performs a total of 16 rounds to generate the cipher text. These rounds operate on the Fiestel structure that converts block ciphers into two halves as left half of 32 bits and the right half of 32 bits.
i) Key Transformation:The transformation produces a set of different keys using the provided 64-bit key. For every round 8bits are discarded and 48bits are used, thus for every 56-bit key a different 48-bit subkey is generated by transforming the circular shift operations.
ii) Expansion/permutation: The right half of 32 bits is expanded to 48 bits through an expansion table. It increases the dependency of the key because of interchanging the bits. The right-half key is XORed with the round key.
iii) Substitution/Choice (S-box): The S-box permutation divides the 48 bits into 8 blocks each of 6 bits which utilizes substitution using S-box and further reducing it to 4 bits. The 32-bit results create confusion and non-linearity through this operation.
iv) Permutation: The 32-bit values are permuted according to the permutation table.
v) XOR and Swap: The permuted output is XORed with the left half value acquired from the previous round.

c) Final Permutation: After performing the above operations for 16 rounds, the left and right halves values are combined and the final permutation is applied using the inverse of the initial permutation table. The final bits are rearranged to generate the output as 64 bits. Figure 3. demonstrates the core operations carried out for one DES operation in the P3DES.

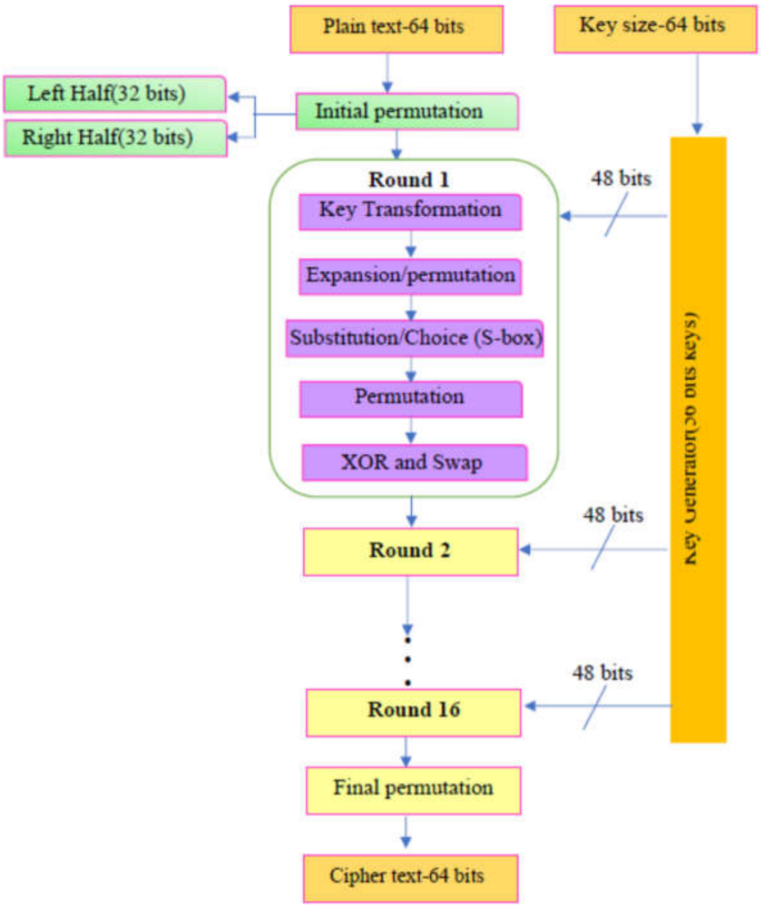

Figure 3. Core Operations of P3DES Encryption Algorithm

4.5.2 ENCRYPTION PROCESS OF P3DES

Generating Key: The three keys are generated using the key generator that creates unique keys.

Initial Permutation: The plaintext of size 64-bit is allowed for the initial permutation operation.

Encryption using three rounds: The plaintext is encrypted three times in parallel using the different keys to create layers of encryption. A single DES operation is applied three times in parallel.

Final Permutation: After performing three levels of encryption, the final permutation is applied to generate the ciphertext of 192 bits.

4.5.3 DECRYPTION PROCESS OF P3DES

The decryption operation is performed using the same process in the reverse order, with feeding ciphertext and the same keys as input to generate the output as the plaintext of 64 bits where each block producesthe outcome of plaintext which is similar to each other.

5. RESULTS AND DISCUSSION

The following section delivers the outcomes of the HP-MDCNN and the P3DES demonstrating their performance.

5.1 PERFORMANCE METRICS

Accuracy: Measures the overall correctness of the classification model.

$$Accuracy = \frac{Z_R + Z_S}{Z_R + Z_S + L_R + L_S}$$

Here Z_R, Z_S denotes the correctly identified positive cases and L_R, L_S denotes the incorrectly identified positive and negative cases.

Sensitivity: Determines the percent of identified positive cases by the model.

$$Sensitivity = \frac{Z_R}{Z_R + L_S}$$

Specificity: Determines the percent of identified negative cases by the model.

$$Specificity = \frac{Z_S}{Z_S + L_R}$$

Encryption Time: Total time required for the encryption algorithm to encrypt the data.

Decryption Time: Total time required for the encryption algorithm to encrypt the data.

Genuine User Rate: Determines the percentage of genuine users authenticated by the system.

Responsiveness: The time taken by the system to process the requests. A lower value indicates the greater response of the system.

5.2 COMPARATIVE DISCUSSION

The emergent services in healthcare emphasize the need for advanced monitoring systems. However, traditional methods employed for the work faced enlightened limitations. The TinyML [4] performs well with the combination of ML models but is vulnerable to network attacks that limit its adaptability. The Ensem-HAR [25] delivers excellent results but the possible misclassification occurs between the human activities. CNN [26] model resulted in higher costs and an inability to handle huge data which is inherited in health organizations. The UNET [27] model detects the brain barriers effectively, but while interpretation, it lacks generalization and the implementation in the clinical setting remains a major challenge. Similarly, the models like CNN-LSTM [28], and 1D-CNN-BiLSTM [29] suffered from performance and scalability issues due to the limited availability of datasets. However, the MDCNN by incorporating mixed pooling increases the generalization capability along with the enhanced performance. The fractional calculus allows the model to learn complex features thereby providing valuable insights into the abnormal conditions of health and allowing the pathologists for early treatments. Table 1. illustrates the comparative discussion of the HP-MDCNN on both datasets.

Table 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**

Table 2. demonstrates the comparative discussion table of the P3DES on comparing with existing methods. The secured storage and access of medical data are inhabited by factors like diminished privacy, vulnerabilities by attackers, and so on. Several block-chain-based systems were incorporated earlier to tackle these issues however the BC-IoMT-SS [2] implemented based on IoMT faces a challenge in the context of balancing the encryption standards that leads to reduced performance. Moreover, the MK-IPSE [3] lacks scalability due to the integration of different decentralized architectures. The BBACM [6] framework involves blockchain to improve its diversity against health data management but failed to address the emergency management services EEDAM [7] due to its combination of ML models improved the standardized healthcare management however, the substantial computational requirements remain a major constraint to be addressed. The DHGECC [8] employed diverse techniques that hindered the system with load alongside led to data loss. The P3DES with the combination of traditional 3DES efficiently handles these issues. P3DES encrypted data provides more security by generating prolonged ciphering and parallel execution of operations making it a robust security mechanism with less computational needs.

Table 2. 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**
		Responsivenss (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**

6. CONCLUSION

The research proposes an encryption mechanism, P3DES to protect the privacy and effective accessibility of the health data. The P3DES inherits the benefits from 3DES and processes encryption in parallel, which minimizes time and faster responsiveness of the system. It also retains the strong core operations of the original 3DES, for encryption ensuring a high level of data security. Moreover, the HP-MDCNN is incorporated to determine the critical conditions from health data for early diagnosis. Hybrid pooling allows to capture of dominant and essential features of complex medical data leading to better generalization and enhanced performance. Moreover, the fractional calculus in the MDCNN introduces memory and long-range dependency which helps in more precise identification of abnormalities.The HP-MDCNN when tested on Heart Attack Analysis & Prediction Dataset, attained accuracy of 97.43%, sensitivity of 97.45%, and specificity of 97.37% at 90% training percentage. For the encryption mechanisms, the P3DES showed impressive results by achieving an encryption time of 2.79s, decryption time of 2.19s, genuine user rate of 0.69, and responsiveness of 9.90s respectively. The future direction of research would concentrate on designing the hybrid optimization algorithm for key generation in encryption mechanism.

REFERENCES

[1] S.M. Patil, B.S Dakhare, S.M. Satre, and S.D. Pawar, “Blockchain-based privacy preservation framework for preventing cyberattacks in smart healthcare big data management systems,” Multimedia Tools and Applications, pp.1-20, 2024.

[2] L. Lodha, V.S. Baghela, J. Bhuvana, and R. Bhatt, “A blockchain-based secured system using the Internet of Medical Things (IOMT) network for e-healthcare monitoring,” Measurement: sensors, 30, p.100904. 2023.

[3] J. Liu, Y. Fan, R. Sun, L. Liu, C. Wu, and S. Mumtaz, “Blockchain-aided privacy-preserving medical data sharing scheme for e-healthcare system,” IEEE Internet of Things Journal, 10(24), pp.21377-21388. 2023.

[4] F. Hu, S. Qiu, X. Yang, C. Wu, M.B. Nunes, and H. Chen, “Privacy-Preserving Healthcare and Medical Data Collaboration Service System Based on Blockchain and Federated Learning.” Computers, Materials & Continua, 80(2). 2024.

[5] S.H Alharbi, A.M. Alzahrani, T.A. Syed, and S.S. Alqahtany, “Integrity and privacy assurance framework for remote healthcare monitoring based on IoT.” Computers, 13(7), p.164. 2024.

[6] I. Masood, A. Daud, Y. Wang, A. Banjar, and R. Alharbey, “A blockchain-based system for patient data privacy and security.” Multimedia Tools and Applications, 83(21), pp.60443-60467. 2024.

[7] M. Izhar, S.A.A. Naqvi, A. Ahmed, S. Abdullah, N. Alturki, and L. Jamel, “Enhancing healthcare efficacy through IoT-edge fusion: A novel approach for smart health monitoring and diagnosis.” IEEE Access, 11, pp.136456-136467. 2023.

[8] P. Rastogi, D. Singh, and S.S. Bedi, “An improved blockchain framework for ORAP verification and data security in healthcare.” Journal of Ambient Intelligence and Humanized Computing, 15(6), pp.2853-2868. 2024.

[9] K.M. Hossein, M.E. Esmaeili, T. Dargahi, A. Khonsari, and M. Conti, "BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications." Computer Communications, 180, pp.31-47. 2021.

[10] R. Zou, X. Lv, and J. Zhao, "SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system." Information Processing & Management, 58(4), p.102604. 2021.

[11] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F.M.Almansour, "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. 2024.

[12] A.D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT." Sensors, 19(2), p.326. 2019.

[13] P. Wei, D. Wang, Y. Zhao, S.K.S. Tyagi, and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism." Future Generation Computer Systems, 102, pp.902-911. 2020.

[14] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities." Computers & Security, 88, p.101653. 2020.

[15] G.Aceto, V. Persico, and A. Pescapé, I"ndustry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0." Journal of Industrial Information Integration, 18, p.100129. 2020.

[16] C. Sullivan, and E. Burger, "E-residency and blockchain. Computer law & security review," 33(4), pp.470-481. 2017.

[17] D. Puthal, N. Malik, S.P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems." IEEE Consumer Electronics Magazine, 7(4), pp.6-14. 2018.

[18] J. Kaushalya, and R.V. Sai, "A survey on efficient and secure implementation of ECDSA against fault attack." Int. J., 8(7), pp.2945-2954. 2020.

[19] Z. Ullah, B. Raza, H. Shah, S. Khan, and A. Waheed, "Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment." IEEE access, 10, pp.36978-36994. 2022.

[20] H. HonarPajooh, M.A. Rashid, F. Alam, and S. Demidenko, "Experimental performance analysis of a scalable distributed hyperledger fabric for a large-scale IoT testbed." Sensors, 22(13), p.4868. 2022.

[21] Y.S. Liang, and W.Y. Su, "A geometric based connection between fractional calculus and fractal functions." Acta Mathematica Sinica, English Series, 40(2), pp.537-567. 2024.

[22] L.Y. Sipayung, and M. Purba, "Data security analysis with triple DES cryptographic algorithm."Journal of Intelligent Decision Support System (IDSS), 6(4), pp.285-294. 2023.

[23] K. Malathy, and R. Jaichandran, "Secure healthcare data for block chain networking based on Triple Des (TDES) protocol and Ekmc." Engineering Research Express, 6(4), p.045202. 2024.

[24] R. Arthi, and S. Krishnaveni, “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. 2024.

[25] D. Bhattacharya, D. Sharma, W. Kim, M.F. Ijaz, and P.K. Singh, “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. 2022.

[26] P. Gupta, A.V. Chouhan, M.A. Wajeed, S. Tiwari, A.S. Bist, and S.C. Puri, “Prediction of health monitoring with deep learning using edge computing.” Measurement: Sensors, 25, p.100604. 2023.

[27] F. Yousaf, S.Iqbal, N. Fatima, T. Kousar, and M.S.M. Rahim, “Multi-class disease detection using deep learning and human brain medical imaging.” Biomedical Signal Processing and Control, 85, p.104875. 2023.

[28] Y. Wang, H. Wang, Z. Li, H. Zhang, L. Yang, J. Li, Z. Tang, S. Hou, and Q.Wang, “Sound as a bell: a deep learning approach for health status classification through speech acoustic biomarkers.” Chinese Medicine, 19(1), p.101. 2024.

[29] Y.M. Ayano, F. Schwenker, B.D. Dufera, T.G. Debelee, and Y.G. Ejegu, “Interpretable Hybrid Multichannel Deep Learning Model for Heart Disease Classification Using 12-leads ECG Signal.” IEEE Access. 2024.

[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.