# A Novel Blockchain-Enabled Fuzzy CLSTM Model for Secure and Scalable Heart Disease Prediction in Healthcare

**R. Parthiban[1,*], K. Santhosh Kumar[2]**

[1]Research Scholar, Department of Computer Science and Engineering, Annamalai University, Chidambaram, Tamilnadu, India

[2]Assistant Professor, Department of Information Technology, Annamalai University, Chidambaram, Tamilnadu, India

Emails: parthineyveli@gmail.com; santhosh09539@gmail.com

**Abstract**

The emerging field of healthcare has taken severe measures to safeguard sensitive patient health-related information especially the information taken from the predictive model. In this study, a novel blockchain-based solution is proposed in correlation with the Fuzzy-enhanced CLSTM model (FCLSTM) for storing and transmitting the data securely for heart disease prediction systems by ensuring data integrity, confidentiality, and access control. The proposed model uses a blockchain-based network which is implemented to prevent the tampering or unauthorized access to patients' health-related data. The process begins with techniques that incorporate the predicted heart disease information from the patient's data and is encrypted by using the hashing algorithm. A secure hybrid blockchain-based data management framework (SHB-DMF) is designed for exchanging the patient's health data which enhances scalability and accessibility to the healthcare environment. The system incorporates a SHAES-256 hybrid model for enhancing the data confidentiality and integrity before transmitting to the neural network (FCLSTM). The proposed model uses a smart contract for regulating data access by ensuring the entry of the authorized entities by providing a suitable decrypting mechanism and interacting with the patient's data. The smart contracts can automate the data retrieval workflows by integrating the blockchain seamlessly with the prediction model. The security process is a three-phase process that includes defining the nodes, selecting of consensus mechanism, and establishing the governance structure for facilitating secure operations. The security and load testing ensure resilience to potential cyber threats and the scalability required for handling high transaction volumes of medical data. Deploying the proposed system provides a robust infrastructure that is tamper-resistant thus advancing the reliability of the cardiovascular prediction system.

**Keywords:** Heart Disease Prediction; Blockchain Security; Fuzzy CLSTM; Data Confidentiality; SHAES-256 Encryption; Smart Contracts; Healthcare Scalability

## 1. Introduction

The healthcare system provides a wide range of services including hospitals, and specialty outpatient clinics in association with other types of facilities. When it comes to medical care, administration of treatment is still the most crucial component. It is necessary to give some consideration to it in terms of the common good. To promote and maintain wellness, as well as to prevent and control diseases, it is essential to make certain innovations so that all patients have access to comprehensive and advanced medical care [1]. Maintaining the confidentiality and safety of patient's medical records is an essential component of health data management. This aspect of the process also assists



DOI: https://doi.org/10.54216/FPA.180219
Received: August 22, 2024 Revised: November 26, 2024 Accepted: January 31, 2025

medical professionals in analyzing and integrating patient records in order to arrive at more informed decisions regarding the treatment of patients. At the heart of health records is the collection of sensitive and confidential information pertaining to patients [2].

Sharing medical records by using a wireless device and the support of the individuals who are connected one after the other is enabled by IoMT (Internet of Medical Things). The IoMT is the extension of IoT which facilitates the processing of the data by monitoring the health-related as well as the medical related objectives. Through the use of medical implants, it is possible to restore normal function to biological systems that have been damaged or are absent, to augment those that already exist, or even to completely replace parts of the body that are missing [3]. The implantable medical devices consist of both implantable pills and bioactive implants which the bioactive implants might be used in drug-aiding procedures. Normally, in the medical field, implantable medical devices might get surgically inserted into the body with the intention of being there until the procedure has been completed. The health outcomes can be made better by achieving the different collection modes of the patient's health data. This enables the advanced nomination of the patient profiles including the individual treatment plans with enhanced therapeutic approaches along with stronger relationships between the patients [4]. This will increase the costs associated with healthcare which utilizes a consequence relationship in both the exponential growth of the population along with the newly implemented technology.

The IoMT offers a lot of advantages like enhanced diagnostic accuracy, reduced adverse effects, and cost-effective treatments [5]. By using this technology the application can be combined with the smartphone applications. The patients can send their medical records to the doctors to improve their recognizing capacity in addition to tracking by preventing diseases. The IoT system greatly reduces the need for medical intrusions along with personnel interventions by allowing real-time monitoring of patient's health conditions. IoMT is a healthcare initiative to monitor the effectiveness of cloud-based data collection for patients [6]. For estimating the intensity the cloud server might use the features which help for measuring and storing. The integration, exchange, and transmission of data for processing by multiple devices in the context of IoMT data transfer might give rise to medical security issues, particularly those related to data protection.

In addition to causing problems with compliance and the law, a lack of openness and data protection standards in data use and accessibility brings about these issues. To ensure the safety of data management, a blockchain is utilized for data acquisition in addition to enhanced cloud connectivity [7]. Through the use of smart contracts, the dependability and security of blockchain technology can simultaneously be ensured. Through the utilization of blockchain technology, we can monitor the readings from sensors and prevent the duplication of potentially harmful data. Every piece of information is encrypted, unchangeable, and verifiable by the blockchain. Through the use of replication, blockchain technology guarantees that the identifiers of files are consistent across all of the network nodes [8]. Internet of Things (IoMT) system implementations can be dynamic, defining, authenticating, and securely transferring data when distributed ledger technology is utilized. Because vulnerable patients rely on the knowledge and good intentions of healthcare providers, there is always some degree of risk and uncertainty in the process of ensuring patient safety and providing high-quality care [9].

A better impression of care, increased compliance with treatment plans, decreased anxiety during therapy, and supposedly healthier health facilities linked with higher levels of trust are just some of the benefits that can be gained from this. On the blockchain platform, patients can establish protocols that will subsequently grant specific researchers access to their medical records for a predetermined period. Patients now can automatically record their medical data and connect to other hospitals using the new technology called blockchain [10]. There is a persistent risk of human error as a major safety concern in every industry, but the healthcare industry is particularly vulnerable to this risk. Learning the fundamentals of security awareness training allows healthcare providers to better protect the personal information of their patients and to make decisions based on accurate information with greater confidence [11].

## 2. Related works

Modern healthcare systems face some difficulties in the diagnosis of cardiovascular diseases because of the shortage of suitable approaches. Also, safeguarding the information and transferring the same is difficult due to this non-existence. For enhancing the diagnosis of heart defects, the IoT explores an innovative approach to enhancing the technologies related to healthcare systems. The Congenital Heart Disease Prediction System (CHDPS) is an example of IoT-based technology that is used for identifying and forecasting cardiac issues which includes coronary heart disease [12]. By using these kinds of systems, doctors can keep an eye on the patient's heart-related conditions by



DOI: https://doi.org/10.54216/FPA.180219
Received: August 22, 2024 Revised: November 26, 2024 Accepted: January 31, 2025

enabling effective diagnosis and projections mentioning the state of the individuals. Because of the complexity of the system, there is a need for the introduction of a data security system in advance. Already the user data is more sensitive and it normally contains most of the patient's medical health records and this ensures that the CHDPS is considered to be safer and is dependable for saving the user data [13]. The data authenticity and safety are guaranteed by the implication of the cloud computing technologies with the most effective computational costs. Cloud computing allows doctors to securely have access to patient records and control them whenever they need it [14]. Utilizing its encryption systems, data can be safeguarded against access by illegal users. By using analytics contained in the cloud, providers can also rapidly and safely extract insightful data points.

Furthermore, when providers utilize cloud-based solutions for CHDPS, they can access their services from any device that is capable of functioning with the internet. As a consequence, medical professionals will have less work to do, and there will be increased efficiency and interoperability [15]. It is also possible for providers to easily modify their services to accommodate the ever-evolving requirements of their patients, which is made possible by the scalability that cloud-based solutions provide. By doing so, the costs that are associated with system upgrades or expansions are reduced, and the availability of services is improved. Furthermore, the user-friendly design of cloud-based solutions facilitates the reduction of the time spent on data creation, data administration, and data storage [16]. Although providers are obliged to satisfy CHDPS's security and authentication criteria, using a cloud-based platform can help with data storage and processing safely and effectively. It improves scalability and interoperability as well as allows service providers to access their products from any device. With the help of cloud-based solutions—not only safe but also reasonably affordable—providers can use CHDPS for congenital heart disease prediction and monitoring [17]. One such IoT-based example is the Congenital Heart Disease Prediction System (CHDPS). Long-standing knowledge is clear that this system is successful in reducing the death and suffering related to coronary heart disease. By using data gathered from IoT devices like the body which is mounted equipment and wearable sensors, one can make an accurate prediction of when this fatal disease will show symptoms in an individual [18]. If the data is kept and handled by several cloud providers, the application of CHDPS could be quite prone to security breaches.

A CHDPS cannot operate without strong protocols and robust authentication systems guaranteeing data security. Authorizing user access to their data and verifying their identity can be accomplished with a digital certificate or secure token [19]. Cloud service providers have to create data security policies if they are to ensure the privacy of their consumers' information. Highly recommended is the encryption of data before cloud storage and the digital signature of every leaked data. Using a Cloud Access Security Broker (CASB) is another way CHDPS might improve security. Establishing a Customer Advisory Service Board (CASB) will help to protect the system from a range of hazards, both internal and external, and enable the application of policies [20]. Implementing a firewall protection system for Internet of Things devices helps one to prevent code injection attacks and malevolent hackers. The main focus of the development of a CHDPS should be data protection and authentication.

Virtual firewalls, stringent data policies, and sophisticated authentication systems are all essential components that must be implemented by cloud providers to fetch back the patient’s information [21]. A secure system that will help reduce the suffering caused by coronary heart disease will be created as a result of this in the long run.

IoMT-SAF is one of the recommendations made by the authors regarding such a framework. The wide range of applications that wirelessly transmit private medical data over the cloud is a far exclamation from the concerns regarding the IoMT. The planning, control, tracking, and supervision of protection cannot take place before the calculation has been completed [22]. On the other hand, beginners who are just beginning their journey into the adoption of IoMT may discover that it is challenging to carry out safety assessments that concentrate on locating resilient security practices. It employs a web-based approach to suggest security assessments for the IoMT and to measure the safety and disruptions of IoMT solutions [23]. In addition to adhering to technical and medical standards, the distinctive value of IoMT-SAF lies in its adaptability, scalability, and sophistication, which enable it to provide services to new customers. The task of safeguarding information and knowledge is multifaceted and extremely important, and it is present in every aspect of society. Nevertheless, it is of the utmost importance especially when it comes to matters concerning medicine, where there are dangers to the lives and health of individuals [24]. The MDPAC model that has been suggested provides the security administrator with the authority to delegate different responsibilities, powers, and tasks to different objects and services. The hallmark of the model that has been proposed is communication between the doctor and the patient that is secure, confidential, and efficient. An examination of the management framework for blockchain-enabled medical devices that emphasizes forensics by design was carried out by the authors [25]. The information is delicate and shared with people who have different but complementary



DOI: https://doi.org/10.54216/FPA.180219
Received: August 22, 2024 Revised: November 26, 2024 Accepted: January 31, 2025

concerns about privacy and security, including doctors, patients, hospital staff, and product vendors. A brand new framework known as FGAF has been developed to control who has access to medical records and Internet of Medical Things devices. They have set their primary design goals as the incorporation of forensic design and the guaranteeing of access granularity [26]. The Privacy-Preserving Edge of Things Framework (PPEOTF) is a recommendation made by the authors to ensure the security of the edge of things and smart healthcare surveillance. A significant problem is the management of data in the Cloud of Things, which is being generated by billions of Internet of Things devices that are connected to one another. By mediating communication between on-premises IoT devices and remote servers in the cloud, edge computing provides a potentially useful solution [27]. In light of this, they provided a comprehensive explanation of the theoretical approach by analyzing the biosignal data of a patient in a case study. While guaranteeing rigorous standards of methodology and data protection, the framework expedites research responses and performance [28]. The authors gave a general review of several fields, including healthcare, and current machine learning techniques applied for big data processing.

## 3. Proposed Work

Today's healthcare scenario depends on safeguarding the patient's data which is more sensitive. In this study, a novel approach that integrates a blockchain-based framework with a fuzzy-enhanced CLSTM (FCLSTM) model for enhancing heart disease prediction systems by focusing the data security, data integrity, and valid access control has been proposed. The proposed model implements a blockchain-based network for protecting the patient's data against tampering and unauthorized access by mentioning the secure hashing algorithm for encrypting heart disease prediction and other sensitive information. For enabling seamless and scalable data enhancement across various healthcare environments, a Secure Hybrid Blockchain Data Management Framework (SHB-DMF) is proposed in addition to the proposed model as shown in Figure 1.

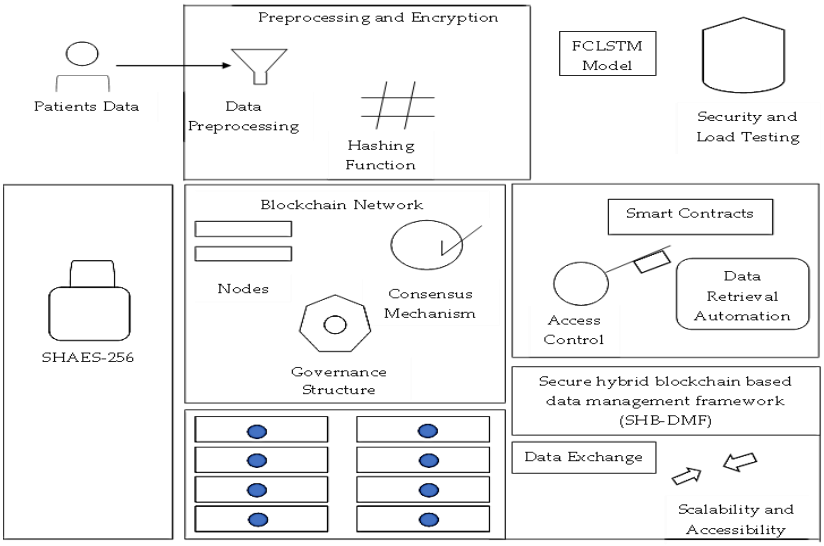


**Figure 1.** Architecture of the proposed healthcare system

The framework implements the SHAES-256-based hybrid model for enhancing data confidentiality and integrity. This is used before sending the data to the FCLSTM model for predictive analysis. The smart contracts might automate the data retrieval process and control access by ensuring the fact that only authorized entities can interact with the patient's data. Here, a three-phase security process is implemented which includes node definition, consensus mechanism selection, and governance structuring. The inclusion of this three-phase security process makes the system optimized for resilience against cyber threats and provides the scalability constraints for using high transaction volumes. This mode of robust system which is tamper resistance will significantly advance the security and reliability of cardiovascular prediction models by ensuring better infrastructure for healthcare applications.

### 3.1. Fuzzy Enhanced CLSTM model (FCLSTM)

The FCLSTM is a hybrid approach designed to improve the predictive performance and interpretability of sequential data models. Here, convolutional neural networks and LSTM are combined to make the prediction to be better. For



DOI: https://doi.org/10.54216/FPA.180219
Received: August 22, 2024 Revised: November 26, 2024 Accepted: January 31, 2025

heart disease prediction, there should be an accurate system that can accommodate all possible needs in the determination of heart diseases. The fuzzy logic is combined with this hybrid model for managing uncertainty-related issues. The convolutional layers are used for handling the spatiotemporal data and LSTMs are used for sequential learning the temporal patterns. Combining both will support the model to capture the spatial and temporal patterns.

Consider the input $X_t$ at time t and the hidden state is represented as $H_{t-1}$ which indicates the previous time stamp. This is mathematically expressed as,

$$f_t = \sigma\left(\Gamma_f * X_t + \psi_f * H_{t-1} + L_f * H_t + b_f\right) \quad (1)$$

where $f_t$ is the output of the function at time step t. The value of the prediction in heart disease is represented in terms of $f_t$. When considering the input and output at time t, the value becomes,

$$i_t = \sigma\left(\Gamma_i * X_t + \psi_i * H_{t-1} + L_i * H_t + b_i\right) \quad (2)$$

$$o_t = \sigma\left(\Gamma_o * X_t + \psi_o * H_{t-1} + L_o * H_t + b_o\right) \quad (3)$$

here σ is the activation function used for fixing the non-linearity of the model. The tanh is considered to be the common activation function used here for enhancing the prediction accuracy. $\left(\Gamma_c, \psi_c, L_c\right)$ are the filters used as layers that enable the convolution function,

$$\hat{C}_t = \tanh\left(\Gamma_c * X_t + \psi_c * H_{t-1} + L_c * H_t + b_c\right) \quad (4)$$

$$C_t = f_t \square C_{t-1} + i_t \square \hat{C}_t \quad (5)$$

$$H_t = o_t \square \tanh(C_t) \quad (6)$$

Then, the bias term is represented as b, $H_t$ is the hidden state used for capturing the temporal and spatial dependencies. The integration of the fuzzy logic might be used for handling the uncertainty and ambiguity in the data. The fuzzy information system is applied to the set of rules for processing the input features related to heart disease risk factors like blood pressure levels and cholesterol levels. This layer will convert the input into the fuzzy values by providing the various degrees of membership which reflect the uncertainty of the input data. The fuzzy rules are typically designed with a form,

IF Input 1 is A AND Input 2 is B THEN Output is C

By which the Input 1 and Input 2 are considered as the patient's health parameters like their age, cholesterol level, blood sugar levels, etc. Then, A and B are considered as fuzzy sets which could be represented in three forms high, medium, and low. The output C is the fuzzy output which leads to the final decision. The health parameters considered for heart disease prediction are shown in Table 1.

**Table 1:** Description of Health Parameters considered for Cardiovascular Disease Prediction

| **Feature** | **Value** |
|---|---|
| Age | 55 |
| Sex | Male (1) |
| Chest Pain Type | Typical Angina (1) |
| Resting Blood Pressure | 130 mmHg |
| Cholesterol | 250 mg/dl |



DOI: https://doi.org/10.54216/FPA.180219
Received: August 22, 2024 Revised: November 26, 2024 Accepted: January 31, 2025

| | |
|---|---|
| Fasting Blood Sugar | >120 mg/dl (1) |
| Resting ECG | Normal (0) |
| Maximum Heart Rate Achieved | 150 bpm |
| Exercise-Induced Angina | Yes (1) |
| ST Depression Induced by Exercise | 2.0 mm |
| Slope of the Peak Exercise ST Segment | Flat (1) |
| Number of Major Vessels Colored by Fluoroscopy | 1 |
| Thallium Stress Test Result | Normal (3) |
| Heart Disease | Yes (1) |

Table 1 provides the values taken for some common factors that are taken for the prediction of heart diseases. The features taken into consideration are the obtained values from the medical tests. These values might be used for training a machine learning model for identifying the patterns that are associated with heart diseases. The patient's data is analyzed against this model, there is a possibility for assessing the overall risk in the development of heart disease. The FCLSTM integrates the fuzzy reasoning into the LSTM state update process by adjusting the cell state $C_t$ and the hidden state $H_t$ with the relevant fuzzy outputs for reflecting back the uncertainty in the overall predictions. The hybrid model is updated with the predicted parameters and is mathematically expressed as,

$$\widehat{C}_t = \tanh\left(\Gamma_c * X_t + \psi_c * H_{t-1} + L_c * H_t + F_{is}(X_t, R) + b_c\right) \quad (7)$$

where $F_{is}(X_t,R)$ is represented as the output of the fuzzy inference system which is based on the input $X_t$ and the rule set R by which it adjusts to the cell input $C_t$. At last, the FCLSTM is subjected to the dense layer along with a sigmoid function which depends on the various types of prediction specifically the binary class and multiclass predictions. The predicted heart disease value is obtained as a probability score which is mentioned as,

$$\Upsilon_j = \sigma\left(W_o H_t + b_o\right) \quad (8)$$

where $W_y$ is the weight matrix for the output layer and $H_t$ is the hidden state taken after including all the parameters related to the cardiovascular disease predicted value. Then, the activation function is represented as σ which yields the status indicating the presence of the heart disease.

### 3.2. Secure Hybrid Blockchain-Based Data Management Framework (SHB-DMF)

The SHB-DMF module is designed to enhance the data security and efficiency in association with the scalability for ensuring the proper utilization of the healthcare data especially for the prediction of heart diseases. Here, in this framework, a hybrid blockchain approach is combined with cryptographic techniques for ensuring secure transmission and storage. The hybrid blockchain network is split into two parts namely private and public blockchains. The private blockchain will manage the more sensitive patient data with restricted access by ensuring the authorization of the entities given by the doctors and patients since they can access it. Then, the public blockchain manages the healthcare information in addition to the metadata by providing transparency in association with the scalability of the existing non-sensitive data. The system uses a consensus mechanism to validate transactions and maintain blockchain security without the computational intensity of Proof of Work. The architecture of the proposed SHB-DMF is illustrated below in Figure 2.



DOI: https://doi.org/10.54216/FPA.180219
Received: August 22, 2024 Revised: November 26, 2024 Accepted: January 31, 2025

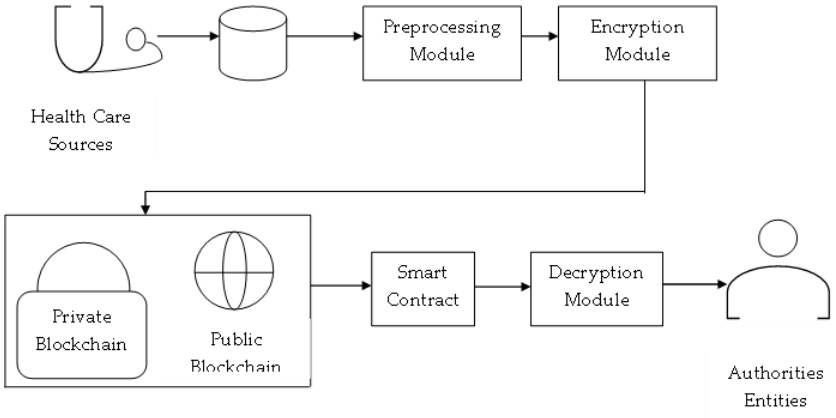


**Figure 2.** Architecture of Secure Hybrid Blockchain-Based Data Management Framework (SHB-DMF)

The SHB-DMF architecture integrates hybrid blockchain technology with data input, encryption, and predictive analysis modules. The process begins with a data collection mechanism from various healthcare sources. After preprocessing, it is then fed to the SHAES-256 algorithm to ensure data security before transmitting. The encrypted data is then stored on a hybrid blockchain by combining a private blockchain for sensitive data and a public blockchain for metadata. Smart contracts within the blockchain will manage access control and automate the data retrieval process by logging each interaction ethically.

### 3.3. SHAES-256 hybrid model

The **Hybrid Secure Hash Algorithm and Advanced Encryption Standard (SHAES-256)** is a combined cryptographic model that integrates SHA-256 (a hashing algorithm) and AES-256 (an encryption algorithm) to provide robust data security. This hybrid approach leverages the strengths of both algorithms, SHA-256's data integrity verification and AES-256's data confidentiality. SHAES-256 is ideal for sensitive healthcare applications where data integrity, confidentiality, and resistance to tampering are critical. The workflow architecture of the SHAES-256 algorithm is shown in Figure 3.

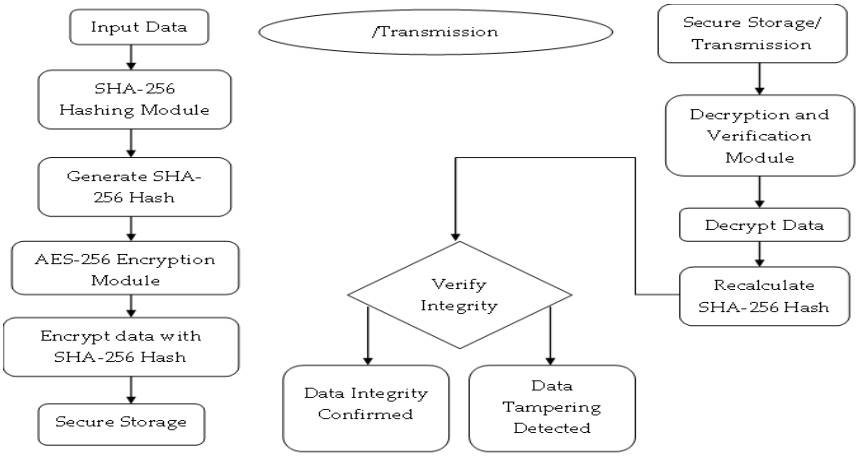


**Figure 3.** Workflow Architecture of the SHAES-256 Algorithm

The input data is hashed using SHA-256 to generate a unique fixed-length 256-bit hash which acts as a digital fingerprint. The original data which is combined with the SHA-256 hash might get encrypted by using AES-256 along with a secure key to ensure the data confidentiality and security during each transmission and storage. After the data retrieval process, the encrypted data is decrypted and the SHA-256 hash of the decrypted data is recalculated to verify that no tampering has occurred.

The input data such as the patient information is initially hashed by using SHA-256 for generating the unique digital fingerprint. This is mathematically expressed as,



DOI: https://doi.org/10.54216/FPA.180219
Received: August 22, 2024 Revised: November 26, 2024 Accepted: January 31, 2025

$$H=SHA\text{-}256(D) \quad (9)$$

where H is the hash output and D is the original data that is to be hashed. The obtained hash value is then combined with the original data and is encrypted by using AES-256 along with a secure key. The data D is then encrypted using the AES-256 algorithm. The encryption key K is used to encrypt both the original data and its SHA-256 hash, forming the ciphertext C. This is expressed as,

$$C=AES\text{-}256(D,K) \quad (10)$$

The AES-256 algorithm applies to multiple rounds with the mathematical procedure of permutation and substitution on data D by using secure key K for retrieving the data it is to be decrypted and recalculated. This is expressed as,

$$H' = SHA\text{-}256(D_{\text{decrypted}}) \Rightarrow H' = H \quad (11)$$

where H′ is the recalculated hash. If H′≠H, this indicates tampering or data corruption. The SHAES-256 algorithm combines SHA-256 and AES encryption and is expressed as,

$$C=AES(SHA\text{-}256(P),K) \quad (12)$$

where P is the plain text which is the patient's data and K is the encryption key. SHA-256(P) produces a unique value representing the hash outcome of the data. Then, the AES(K) will encrypt this hash with AES and thus generate the cipher text C. The smart contract $S_c$ is deployed to regulate data access,

$$S_c: \text{If } (U \in A) \rightarrow \text{Grant Access} \quad (13)$$

where U is the access for user requisition and A is the set of unauthorized users and the smart contract grants access when U is in A. The blockchain system validates data integrity by periodically checking stored hashes against recalculated values which is represented as,

$$Verify: H(P) = SHA-256(P) \quad (14)$$

where H(P) is the stored hash value and this will indicate the data tampering process when there occurs any deviation in it. When considering the private blockchain-based sensitive data a lighter consensus mechanism is used,

$$Consensus: Authority\ Nodes = N \quad (15)$$

where n is considered as the set of authorized validators that reduce the computational load while maintaining the overall security.

**4. Results and Discussion**

The dataset used for the experimentation is taken from the Kaggle database. In this section, the findings of the proposed SHB-DMF for heart disease prediction after implementation are presented. The obtained results are analyzed in order to demonstrate the effectiveness of SHB-DMF, which addresses the need for security and efficiency in handling the patient's health data management. Combining a fuzzy-enhanced CLSTM model with blockchain technology ensures data integrity, confidentiality, and accessibility which is critical in managing the patient's sensitive information. The testing will focus on the evaluation of the model's accuracy prediction which could be taken in favor of analyzing the resilience against cyber threats. The key performance metrics used for the analysis include accuracy, latency, and encryption efficacy. This is obtained to validate the effectiveness of the proposed model. In addition to this, the efficiency of the smart contract is analyzed and the potential of the system is reviewed for improving the reliability and scalability of the model. The obtained experimentation results highlight the importance of predictive performance and data security.

Initially, the performance of the FCLSTM model is analyzed for the prediction of heart disease. The metrics used for the evaluation include accuracy, sensitivity, specificity, and F1-score. This proposed model reaches better accuracy proving that the heart disease prediction capability is more effective and reliable. The identification of the positive and negative cases is analyzed from the sensitivity and specificity results and is illustrated in Table 2.



DOI: https://doi.org/10.54216/FPA.180219
Received: August 22, 2024 Revised: November 26, 2024 Accepted: January 31, 2025

**Table 2:** Heart Disease Models' Performance

| **Model** | **Accuracy (%)** | **Sensitivity (%)** | **Specificity (%)** | **F1-Score** |
|---|---|---|---|---|
| FCLSTM | 96.4 | 95.2 | 97.1 | 0.95 |
| Traditional CNN | 88.2 | 87 | 89.3 | 0.87 |
| SVM | 85 | 83.9 | 85.8 | 0.86 |
| Logistic Regression | 82.8 | 81.2 | 84.3 | 0.84 |
| Random Forest | 86.6 | 85.45 | 87.55 | 0.87 |
| RNN | 85.5 | 84.1 | 86.8 | 0.86 |

The comparison is made with the traditional models like CNN and SVM. The analysis proves that the FCLSTM shows better performance in all the considered metrics. This shows the robustness of the model in heart disease prediction and its accuracy in prediction performance as shown in Figure 4.

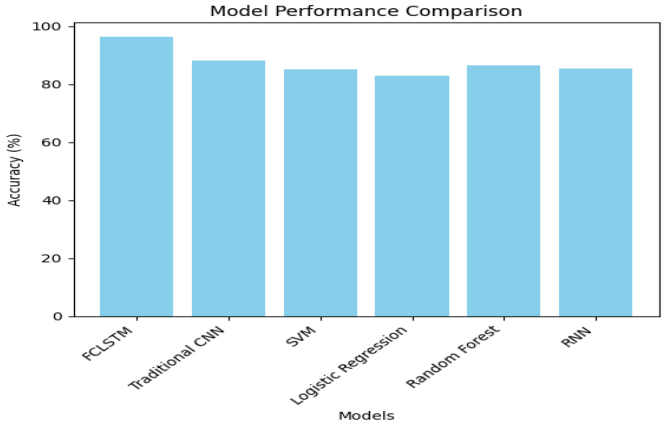


**Figure 4.** Accuracy of heart disease prediction

The FCLSTM provides a better accuracy of about 96.4% which outperforms the other traditional models. When including the SHAES-256 algorithm in association with the blockchain network will enhance security and confidentiality. The performance of this inclusion is evaluated using parameters like data integrity, tampering resistance, and the efficiency of access control. The experimental results prove that the SHAES-256 algorithm influences effectively the prevention of unauthorized access without any breaches during the testing process as shown in Table 3.

**Table 3:** Blockchain Integrity and Confidentiality Measures

| **Security and Confidentiality Measure** | **Metric** | **Result** |
|---|---|---|
| **Data Integrity** | Breach Incidence Rate | 0 breaches |
| **Confidentiality** | Unauthorized Access Attempts | 0 attempts |
| **Encryption Time** | Average Encryption Time (ms) | 21.34 ms |



DOI: https://doi.org/10.54216/FPA.180219
Received: August 22, 2024 Revised: November 26, 2024 Accepted: January 31, 2025

| | | |
|---|---|---|
| **Decryption Time** | Average Decryption Time (ms) | 17.56 ms |
| **Access Control via Smart Contracts** | Authorization Compliance Rate | 100% compliance |
| **Access Control** | Average Access Log Response Time | 13.4 ms |
| **Tamper Resistance** | Verified Data Integrity Checks | 100% tamper-free |

Table 3 illustrates that the SHAES-256 encryption algorithm effectively maintains confidentiality with minimal latency and smart contracts that provide robust access control by ensuring the unauthorized handling of the patient's data. The encryption time and the decryption time were measured by confirming the model's suitability for real-time healthcare applications. The smart contract for secure access control in a blockchain-based healthcare system is shown in Table 4.

**Table 4:** Proposed Smart contract for blockchain-based network

| **Smart Contract Component** | **Description** |
|---|---|
| **Contract Name** | *PatientDataAccess* |
| **Purpose** | Regulate access to patient health data, ensuring only authorized entities can view or modify data. |
| **Variables** | - *owner*-Address of the contract owner |
| | - *authorizedUsers*- Mapping of addresses with access permissions |
| **Events** | - *AccessGranted(address user)*- Logs when access is granted |
| | - *DataAccessed(address user, uint timestamp)*- Logs each access with a timestamp |
| **Functions** | - *addAuthorizedUser(address user)*- Adds a new authorized user to *authorizedUsers* |
| | - *revokeAccess(address user)*-Revokes access from an existing user |
| **Data Access Function** | *function viewData() public returns (data)*- Checks if *msg.sender* is in *authorizedUsers*; if true, grants access and emits *DataAccessed* event |
| **Encryption Handling** | *function encryptData(data) internal returns (encryptedData)*- Encrypts patient data using SHAES-256 before storage |
| **Decryption Handling** | *function decryptData(encryptedData) internal returns (data)*- Decrypts data when accessed by authorized users |
| **Access Control Logic** | - Verifies *msg.sender* authorization before granting access |
| | - Automatically logs each access event and updates *accessLog* |
| **Guard Functions** | - *onlyOwner()*- Modifier that allows only the owner to execute specific functions. |



DOI: https://doi.org/10.54216/FPA.180219
Received: August 22, 2024 Revised: November 26, 2024 Accepted: January 31, 2025

The smart contract developed has proved to be robust in its functionalities for regulating the access control with proper access logs provides 100% authorization compliance and the authorized interactions might consume faster response times. This experimentation result proves that the proposed blockchain-based model is better at providing confidentiality and data integrity for maintaining more sensitive data. Then, the testing is conducted at various transaction volumes to ensure scalability and load testing in the blockchain-based data management system. This shows that the system is sustainable to low latency and faster transaction speeds ensuring better scalability. The capacity for handling the increase in the loaded data shows reliable performance as shown in Table 5.

**Table 5**: Scalability and Load Testing of the blockchain system

| **Load Level** | **Transaction Volume (per second)** | **Average Transaction Speed (ms)** | **Average Latency (ms)** | **Average Data Retrieval Time (ms)** |
|---|---|---|---|---|
| Low Load | 350 | 22 | 12 | 29 |
| Medium Load | 750 | 24 | 15 | 32 |
| High Load | 1250 | 27 | 19 | 35 |
| Very High Load | 2250 | 30 | 27 | 42 |

The results shown in Table 5 indicate the effectiveness of blockchain in ensuring scalability when handling high transaction loads with minimum delays with decent transaction and retrieval times. In this instance, the increase in the transaction loads, and response time might rise slightly but within the acceptable range showing that the proposed framework is much more suitable for the healthcare environment when the real-time massive dataset is considered. The variation in the transaction speed, latency, and processing time in association with the transaction volume is shown in Figure 5.

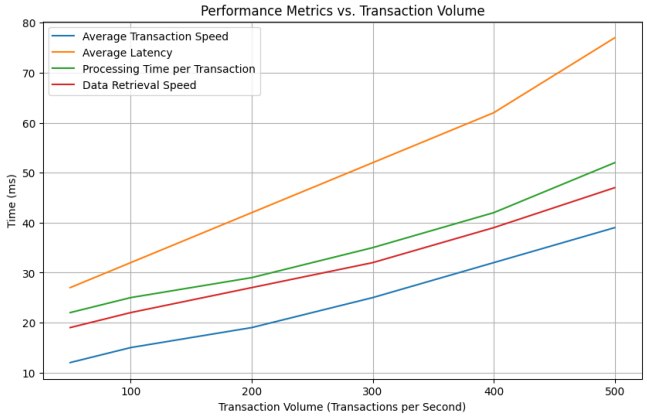


**Figure 5.** Scalability and Load Testing Results (Performance metrics vs Transaction Volume)

If there is an increase in the patient's record, the system will manage more effectively and hence it will support the real-time increase in medical needs. The Cybersecurity resilience testing will demonstrate the system's robust defense against common cyber threats. The various performance variations predicted for different attacks are shown in Table 6.

**Table 6:** Cybersecurity Resilience Testing Results

| **Threat Type** | **Resilience** | **Vulnerabilities** |
|---|---|---|
| DDoS Attack | High | Minor |
| Unauthorized Access Attempts | Complete protection | None |



DOI: https://doi.org/10.54216/FPA.180219
Received: August 22, 2024 Revised: November 26, 2024 Accepted: January 31, 2025

| | | |
|---|---|---|
| Data Tampering Attempt | Full integrity | None |
| Phishing Attack Simulation | High | Minor |
| Network Interruption Simulation | 99.98% uptime | Minor |

The simulated DDoS attacks might cause minor delays which will not create any impact on data integrity since the resilience is improved by using rate limiting and load balancing mechanisms. The effectiveness of the SHAES-256 algorithm is enhanced with the tampering of the unauthorized access attempts done by the proposed mechanism. The reliability testing shows about 99.98% effectiveness in ensuring the robustness and security of the system. Figure 6 illustrates the effectiveness of the system performance demonstrated for various security threats indicating the overall reliability of the system.

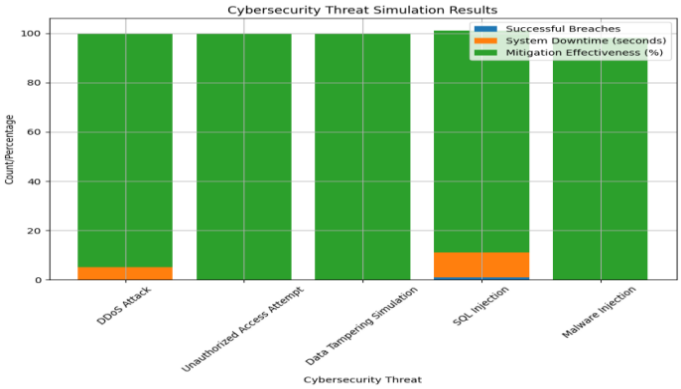


**Figure 6.** Cybersecurity threats vs count of attempts

The model maintained an average uptime of 99.8% with fast response times even during high attacks. The tampering resistance is marked to be 100% and the average response time is about 30 ms. The implication of the hybrid blockchain framework might provide high efficiency in the data retrieval process while combining it with smart contract-based automation. The testing result shows that the data retrieval speed is increased sequentially by reducing the retrieval time by upto 42%. The inclusion of smart contracts will improve the process as shown in Figure 7.

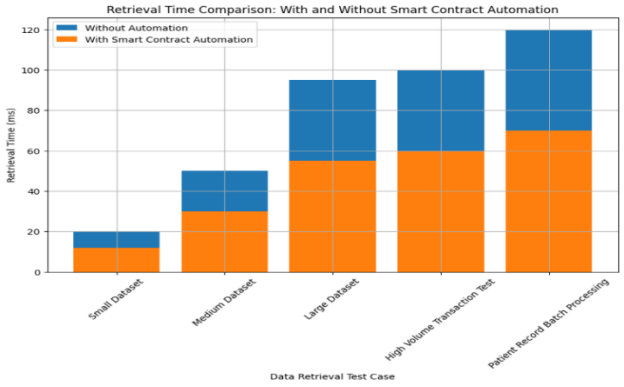


**Figure 7.** Retrieval time comparison: With and Without smart contract Automation

The smart contract might streamline the accessibility and the transaction is made faster without human intervention. The patient records are retrieved for about 55ms with automation and 95ms without automation. The results prove that the proposed framework is better at managing the data with high transaction volume and is effectively suitable in real-time healthcare environments where speed and accuracy are mandatory. When comparing the proposed system with the other systems considering the key performance metrics which is relevant to heart disease prediction and secure data management, the proposed system shows better performance as shown in Table 7.

**Table 7:** Performance Comparison of Proposed model with other models



DOI: https://doi.org/10.54216/FPA.180219
Received: August 22, 2024 Revised: November 26, 2024 Accepted: January 31, 2025

| Metric | Proposed System (Fuzzy-Enhanced CLSTM with Blockchain) | Traditional CNN Model | SVM Model | Logistic Regression |
|---|---|---|---|---|
| **Data Retrieval Speed (ms)** | 14 | 28 | 37 | 38 |
| **Encryption Time (ms)** | 15 (SHAES-256) | Not applicable | Not applicable | Not applicable |
| **Decryption Time (ms)** | 12 (SHAES-256) | Not applicable | Not applicable | Not applicable |
| **Unauthorized Access Attempt Rate** | 0 attempts | Not applicable | Not applicable | Not applicable |
| **System Uptime (%)** | 99.8 | 96 | 97.5 | 94.8 |
| **Tampering Resistance** | 100% tamper-free | Moderate | Moderate | Low |

Table 7 illustrates the advantage of the proposed system in terms of all the available performance metrics for establishing a comprehensive solution for secure and efficient healthcare data management.

## 5. Conclusion

In this study, a complete solution is presented to enhance the security, confidentiality, and accessibility of heart disease prediction systems. By integrating a secure hybrid blockchain-based data management framework (SHB-DMF) with a fuzzy-enhanced CLSTM model (FCLSTM), the system addresses critical challenges in healthcare data management. The SHAES-256 hybrid encryption model ensures that there is a robust data confidentiality and integrity model that is developed for protecting the most sensitive patient data from unauthorized access and tampering. Smart contracts are used to further streamline the secure access control by allowing only authorized entities to interact with patient information, thus automating workflows and ensuring accountability. The proposed system utilizes a three-phase security approach namely node definition, consensus mechanism selection, and governance structure to provide resilience against cyber threats and will support high transaction volumes which is essential for scalable healthcare applications. By delivering a tamper-resistant infrastructure, the proposed framework not only improves heart disease prediction accuracy but also strengthens data protection and operational efficiency by advancing both patient trust and healthcare reliability.

**Funding:** This study received no external funding.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

**[1]** P. Ponikowski *et al.*, "Heart failure: preventing disease and death worldwide," *ESC Heart Fail.*, vol. 1, no. 1, pp. 4–25, 2014.

**[2]** J. Kulynych and H. T. Greely, "Clinical genomics, big data, and electronic medical records: reconciling patient rights with research when privacy and science collide," *J. Law Biosci.*, vol. 4, no. 1, pp. 94–132, 2017.

**[3]** K. S. Kumar, T. A. Kumar, A. S. Radhamani, and S. Sundaresan, "Blockchain technology: an insight into architecture, use cases, and its application with industrial IoT and big data," in *Blockchain Technology*, CRC Press, 2020, pp. 23–42.

**[4]** C. Castaneda *et al.*, "Clinical decision support systems for improving diagnostic accuracy and achieving precision medicine," *J. Clin. Bioinform.*, vol. 5, pp. 1–16, 2015.

**[5]** Z. Ashfaq *et al.*, "A review of enabling technologies for Internet of Medical Things (IoMT) ecosystem," *Ain Shams Eng. J.*, vol. 13, no. 4, p. 101660, 2022.

**[6]** R. Dwivedi, D. Mehrotra, and S. Chandra, "Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review," *J. Oral Biol. Craniofac. Res.*, vol. 12, no. 2, pp. 302–318, 2022.



DOI: https://doi.org/10.54216/FPA.180219
Received: August 22, 2024 Revised: November 26, 2024 Accepted: January 31, 2025

**[7]** I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," *Neural Comput. Appl.*, pp. 1–16, 2022.
**[8]** P. Ruan, T. T. A. Dinh, D. Loghin, M. Zhang, and G. Chen, *Blockchains: Decentralized and Verifiable Data Systems*, Springer Nature, 2022.
**[9]** C. A. Oster and J. S. Braaten, *High Reliability Organizations: A Healthcare Handbook for Patient Safety & Quality*, Sigma Theta Tau, 2020.
**[10]** U. Chelladurai and S. Pandian, "A novel blockchain based electronic health record automation system for healthcare," *J. Ambient Intell. Humaniz. Comput.*, vol. 13, no. 1, pp. 693–703, 2022.
**[11]** T. Lysaght, H. Y. Lim, V. Xafis, and K. Y. Ngiam, "AI-assisted decision-making in healthcare: the application of an ethics framework for big data in health and research," *Asian Bioeth. Rev.*, vol. 11, pp. 299–314, 2019.
**[12]** P. Szolovits and E. Alsentzer, "Knowledge-based systems in medicine," in *Intelligent Systems in Medicine and Health: The Role of AI*, Cham: Springer, 2022, pp. 75–108.
**[13]** E. H. Shortliffe and M. F. Chiang, "Biomedical data: their acquisition, storage, and use," in *Biomedical Informatics: Computer Applications in Health Care and Biomedicine*, Cham: Springer, 2021, pp. 45–75.
**[14]** A. K. Nair and J. Sahoo, "Internet of Things in smart and intelligent healthcare systems," in *Intelligent Internet of Things for Smart Healthcare Systems*, CRC Press, 2023, pp. 1–19.
**[15]** A. Jaleel *et al.*, "Towards medical data interoperability through collaboration of healthcare devices," *IEEE Access*, vol. 8, pp. 132302–132319, 2020.
**[16]** A. I. Kayode, A. Tella, and S. O. Akande, "Ease-of-use and user-friendliness of cloud computing adoption for web-based services in academic libraries in Kwara State, Nigeria," *Internet Ref. Serv. Q.*, vol. 23, no. 3–4, pp. 89–117, 2020.
**[17]** A. K. Jumani, W. A. Siddique, and A. A. Laghari, "Cloud and machine learning based solutions for healthcare and prevention," in *Image Based Computing for Food and Health Analytics: Requirements, Challenges, Solutions and Practices: IBCFHA*, Cham: Springer, 2023, pp. 163–192.
**[18]** O. S. Saleh, O. Ghazali, and M. E. Rana, "Blockchain based framework for educational certificates verification," *J. Crit. Rev.*, 2020.
**[19]** G. J. Silowash *et al.*, *Common Sense Guide to Mitigating Insider Threats*, 2012.
**[20]** D. Pradhan, M. Behera, and M. Gheisari, "Dynamic data placement strategy with network security issues in distributed cloud environment for medical issues: An overview," *Recent Adv. Comput. Sci. Commun.*, vol. 17, no. 6, pp. 25–38, 2024.
**[21]** P. K. Sadhu *et al.*, "Prospect of internet of medical things: A review on security requirements and solutions," *Sensors*, vol. 22, no. 15, p. 5517, 2022.
**[22]** L. Khan and F. Kabir, "In-depth analysis on secure and privacy-preserving smart care homes based on Internet of Medical Things (IoMT)," in *2024 IEEE Int. Conf. Interdiscip. Approaches Technol. Manage. Soc. Innov. (IATMSI)*, vol. 2, pp. 1–6, 2024.
**[23]** M. Singer, H. Baer, A. Pavlotski, and D. Long, *Introducing Medical Anthropology: A Discipline in Action*, Rowman & Littlefield, 2019.
**[24]** A. H. Ameen, M. A. Mohammed, and A. N. Rashid, "Dimensions of artificial intelligence techniques, blockchain, and cyber security in the Internet of medical things: Opportunities, challenges, and future directions," *J. Intell. Syst.*, vol. 32, no. 1, p. 20220267, 2023.
**[25]** K. T. Putra *et al.*, "A review on the application of Internet of Medical Things in wearable personal health monitoring: A cloud-edge artificial intelligence approach," *IEEE Access*, 2024.
**[26]** O. Ali *et al.*, "A comprehensive review of Internet of Things: Technology stack, middlewares, and fog/edge computing interface," *Sensors*, vol. 22, no. 3, p. 995, 2022.
**[27]** H. S. Mahmood, "Conducting in-depth analysis of AI, IoT, web technology, cloud computing, and enterprise systems integration for enhancing data security and governance to promote sustainable business practices," *J. Inf. Technol. Inform.*, vol. 3, no. 2, 2024.



DOI: https://doi.org/10.54216/FPA.180219
Received: August 22, 2024 Revised: November 26, 2024 Accepted: January 31, 2025