RESEARCH PAPER

Blockchain-Enabled Privacy Preservation of Electronic Health Records Using Sha256 and Deep Learning–Optimized Key Generation

[1*]Naveen John J and [2]I. Shatheesh Sam

[1]Department of Computer Science, Nesamony Memorial Christian College, Affiliated to Manonmaniam Sundaranar University, Tirunelveli, India*
[2]Associate Professor in the Department of PG Computer Science, Nesamony Memorial Christian College, Affiliated to Manonmaniam Sundaranar University, Tirunelveli, India
*[*]**Corresponding Author:** naveenjohnj41@gmail.com*

Received: 24th April, 2026; Revised: 20th May 2026; Accepted: 30th June, 2026; Available Online: 10th July, 2026

ABSTRACT
Cloud-assisted smart healthcare (s-healthcare) systems enable an effective approach for storing and managing electronic health records (EHRs), they also have significant security challenges to address, including insider threats and unauthorized data disclosures. To overcome these issues, to proposed a blockchain-based framework for providing privacy preservation to the patient's EHRs through using: SHA256 encryption; secure cloud storage; tamper-resistant delivery of information via blockchain; and controlled decryption. The main innovation of this model is the deep learning–optimized key generation process; utilizing the Augmented Antlion Optimizer (AAO) to generate candidate keys and using a integrated convolutional neural network and deep neural network (CNN-DNN) model to choose the most appropriate key for encryption/decryption purposes enables strong access control and resistance to cryptanalysis. Using various datasets to validate the model and benchmarked against existing algorithms, consistently achieving lower encryption, decryption, and turnaround times while delivering higher restoration efficiency. The results demonstrate the overall feasibility of our proposed framework as a means of securely, reliably, and privately transmitting healthcare data in cloud computing environments.

Keywords: EHR; Privacy Preservation; SHA256 encryption algorithm; hybrid CNN-DNN model; Improved Antlion Optimization.

How to cite this article: John NJ, Sam IS, Blockchain-Enabled Privacy Preservation of Electronic Health Records Using Sha256 and Deep Learning–Optimized Key Generation. Int J Drug Deliv Technol. 2026;16(69s): 1905-1921. DOI: 10.25258/ijddt.16.69s.188
Source of support: Nil.
Conflict of interest: None

1. INTRODUCTION

Electronic Health Records (EHRs) are an electronic storage medium used to collect and share patient data electronically, including the patient's medical records, medicines, allergies, lab outputs, and treatment plans (Adeniyi et al., 2024). When stored in public clouds, EHRs allow for easy access by consumers using technology and offer low-cost multi-user access with efficient controls, but do introduce additional risks to the confidentiality, integrity, and security of EHRs stored in public clouds (Babu et al., 2025). Several cryptographic algorithms have been successfully utilized to secure EHRs in the cloud; however, while satisfactory with external threats, the performance of these algorithms against insider threat attackers (Othman and Getahun 2025). As such, these cryptographic algorithms provide a foundation for securing EHRs in the cloud; the impact of growing reliance on cloud computing for delivering healthcare has introduced significant new obstacles for organizations seeking to provide a scalable, cost-effective, and frictionless experience for providers and patients to utilize when sharing and accessing EHR records (Sabonchi 2025). Moreover, Cloud storage provides a functional view, and raises safety threats and individuals concerns associated with authorization management, information privacy, and revocation control come with using cloud storage (Worapaluk and Fugkeaw 2026).

Although blockchain started with bitcoin transactions, it now shows promise for many other applications, including healthcare. Its decentralized and unchangeable nature makes it an effective solution for improving information security, management, retrieval, communication, and authenticity in healthcare systems (MAITHILI and AMUTHA 2026; Moreau and Sinclair 2024. While blockchain has strong potential to address compliance, security, and privacy issues, its decentralized architecture and consensus mechanisms enhance data integrity and guarantee resistance against unauthorized access and tampering, thus allowing healthcare organizations to build tamper-resistant data repositories and simplify regulatory compliance to achieve robust data protection (Vidhya et al., 2024). Blockchain technology holds significant promise to make medical care services more secure and trustworthy. It employs cryptographic authentication and access control in a distributed, scalable, and secure manner (Masood et al., 2024). Overall, healthcare record systems

**Author for Correspondence: naveenjohnj41@gmail.com*

integrate cryptographic methods like RSA (Senthilkumar et al., 2025), AES (Selvi and Sakthivel 2025), ECC, and SHA-3 (Talukder and Sarker 2025) to safeguard the data protection as well as secrecy of medical records(Haddad et al., 2024). The SHA-256 is a cryptographic method offers more safer, optimized, and high-capacity data handling(Jafer and Abbood).

While blockchain set a strong foundation for healthcare security, its role and effectiveness should be enhanced by another form of AI, deep learning (DL), which is capable of looking for complex patterns and drawing warranted conclusions from massive healthcare data (Kiruthikadevi et al., 2024). While access control and confidentiality issues remain, and medical records in the cloud are compromised by insiders threatening the security and privacy of healthcare information, conventional cryptographic algorithms form the basis of securing healthcare data (Afrihyia et al., 2025; Das et al., 2024). To tackle these security and privacy issues, we propose a hybrid framework that combines blockchain with SHA-256 encryption, CNN-DNN deep learning models, and Adaptive Arithmetic Optimization (AAO). Blockchain ensures decentralized, tamper-proof storage and clear access control, which removes the risks of insider manipulation. SHA-256 provides strong cryptographic protection for sensitive healthcare records, keeping them safe from unauthorized access. The CNN-DNN model improves anomaly detection by learning complex access patterns, which helps identify insider threats and suspicious behaviors more effectively. Finally, AAO enhances key management and computational efficiency, allowing for scalability and interoperability across different healthcare settings. The major key results of that study are:

- We introduce a novel integration of blockchain with SHA-256 encryption, ensuring decentralized, tamper-proof storage and robust cryptographic protection for Electronic Health Records (EHRs).
- By incorporating CNN-DNN models, our method enables intelligent anomaly detection and insider threat mitigation by examining of complicated access patterns in medical records.
- The use of Adaptive Arithmetic Optimization (AAO) enhances scalability and efficiency by optimizing key management and computational processes, making the framework suitable for large-scale healthcare environments.
- The state of healthcare cybersecurity by offering a lightweight yet powerful solution that overcomes the limitations of conventional cryptographic algorithms and existing blockchain-only framework.

This study is organization in the following manner. Section 2 offers an in-depth examination of related work research, emphasizing existing methods and their weaknesses. Section 3 describes the suggested framework in detail, outlining its framework and main elements. Section 4 discusses the performance outcomes, providing analysis as well as analysis of the results. Lastly, Section 5 finalizes discussion through final observations as well as avenues to further study.

2. LITERATURE SURVEY

Reoukadji et al., 2026 introduced a conbined high-dimensional quantum key distribution (HD-QKD) model to safe healthcare records transfer over IoMT, EHR, and SMG domains. This model uses a single central cloud-based Electronic Health Record (EHR) host to manage keys with additional security coming from edge quantum security gateways. It employs qudit encoding to enhance resilience against noise and improve information rates per photon. The edge-centric design ensures minimal delay protection in defence of quantum-based attacks while remaining compatible with leveraging current optical infrastructure via wavelength division multiplexing.

Ali et al., 2025 suggested a framework called "Blockchain-enabled Federated Learning, to improve the safety of EHR execution. The model utilizes non-disclosing proofs for user identity verification, homomorphic processing to ensure computational processes, and collaborative study for decentralized framework learning on an Internet of Things (IoT) Devices to lower health data privacy risks while maintaining the utility of the data itself. Blockchain ensures integrity and transparency through a tamper-proof ledger of EHR transactions. Evaluations show enhanced privacy, minimized processing burden, and improved performance, making BFL a effective strategy for safeguarded, privacy-aware intelligent healthcare platforms.

Ashwini and Puneeth et al., 2026 proposed a Lightweight Elliptic Curve Cryptography Proxy Re-Encryption (LWECC-PRE) model designed to facilitate decentralized and secure sharing of EHR across Ethereum and Hyperledger Fabric blockchains. This system includes a hybrid elliptic curve proxy re-encryption (HEC-PRE) for controlling access, Encryption Protection by ECIES, and verifying integrity and authentication using ECDSA data integrity checks, while leveraging IPFS for peer-to-peer storage. Smart contracts regulate asynchronous data exchange and re-encryption across blockchain networks. Experimental results show reduced computational overhead, improved interoperability, and strong privacy preservation, providing a protected and patient-focused framework for medical information sharing.

In 2024, Abidi et al. introduced a crossover-based multilayer perceptron for the detection of assaults against patient medical records. The gathered data are cleaned and input into the neural network, which promptly alerts healthcare professionals when an attack is detected to prevent data leakage. Additionally, both artificially generated and real-world samples were used to evaluate and compare CMLP's performance by several metrics, the CMLP demonstrated superiority over previous attempts, resulting in better detection ability and reliability to secure healthcare data.

Sharma and Shambharkar 2025 proposed the SA-GBO-ODBN framework, a blockchain-enabled DL framework to ensure protected healthcare information handling and diagnostics. The framework combines hyper ledger fabric for secure, tamper-proof data storing and optimised, efficient important creation with secure records sharing capabilities through the use of SHA-256 and elliptic curve cryptography (ECC). ECC keys are optimized using the Self-Adaptive Gradient-Based Optimizer (SA-GBO) to enhance security. Key features comprise urgent alert messaging, identity and access control, and administrative data updates. For diagnostics, the model applies an Optimized Deep Belief Network (ODBN) to detect epilepsy from continuous EEG recordings.

Alruwaill et al., 2025 presented a hChain 4.0, a permission blockchain architecture that enables protected and extensible governance of health data. The model utilizes Advanced Encryption Standard (AES) for increased security of stored data and partially homomorphic encryption (PHE) for secure computations over encrypted data. The framework also supports the sharing of health data between anonymized users through the use of pseudonyms and provides fine-grained permission through the use of Attribute-Based Access Control (ABAC) across multiple organizations. Experimental evaluations confirm its scalability, cost-effectiveness, and validated security, positioning hChain 4.0 as a reliable solution for secure EHR exchange.

Albakri and Alqahtani 2023 improved an IoMT-based blockchain-enabled smart healthcare system using encryption with an optimal deep learning (BSHS-EODL) model. This model allows the transmission of medical images to be done using an encrypted mode of transport, along with the diagnosis of diseases that would typically occur in an IoMT environment via the collection and classification of data, and the secure transmission of data. The key generation is achieved using the Dingo Optimization Algorithm (DOA), while the actual analysis is conducted on the SqueezeNet, with Bayesian Optimization (BO) for change the parameters and through the use of a Voting Extreme Learning Machine (VELM).

Kokila et al 2024 introduced a DKS-CWH algorithm, which utilizes both dual kernel support vector machines (DKS) and a Crossover Wild Horse Optimization Algorithm (CWHO). Using gray resample medical scans acquired from the clinical MNIST record collection (58,954 total), the categorization and attribute identification process was done within the cloud infrastructure leveraging the DKS-CWH method. The DKS hyperparameter optimization utilized CWHO as an optimisation algorithm. The DKS hyperparameter optimization utilized CWHO as an optimisation algorithm.

Selvaraj et al 2025 developed an Adaptive Feature-Centric Polynomial (AFCP) information protection framework information protection framework designed to enforce privacy across diverse types of electronic health records (EHRs). The scheme classifies EHR features by importance and applies dynamic polynomial-based encryption with feature-specific keys, ensuring fine-grained security. Blockchain integration strengthens confidentiality, while the Healthy Trust Access Restriction mechanism prevents unauthorized entry.

Ramachandraiah et al., 2023 proposed a blockchain-built upon IoT healthcare architecture enhanced with DL and biomimetic algorithms. The system provides secure data storage and user authentication using blockchain technology. Optimal feature selection is obtained using a modified Jellyfish Search Optimization (JSO) procedure. medical condition forecasting is accomplished using a Deep Convolutional Gated Recurrent Unit (DCGRU) architecture that integrates both CNN and GRU architectures together to perform robust analysis. Security is further enhanced using the Twofish encryption algorithm. Table 1 presents the comparative evaluation of existing healthcare information protection models.

Table 1: Comparative overview of recent healthcare security frameworks

Author & Year	Year	Aim	Method	Advantages	Limitations
Reoukadji et al [18]	2026	Secure medical data transmission via HD-QKD	Qudit encoding, edge quantum gateways, fiber-based QKD	Quantum-resilient, noise-resistant, high photon efficiency	Requires quantum infrastructure; limited real-world deployment
Ali et al [19]	2025	Privacy-aware EHR workflows	Blockchain-driven Federated Learning, ZKP, Homomorphic Encryption	Decentralized training, strong privacy, tamper-proof ledger	High computational overhead; scalability challenges
Ashwini and Puneeth et al [20]	2026	Distributed EHR exchange	LWECC-PRE, ECIES, ECDSA, IPFS, smart contracts	Strong privacy, interoperability, reduced overhead	Complex integration across Ethereum & Hyperledger; latency issues

Abidi et al [21]	2024	Detect adversarial attacks on medical records	Crossover-based MLP	High detection accuracy, real-time alerts	Focused only on attack detection, not full EHR security
Sharma and Shambharkar [22]	2025	Secure medical data + epilepsy diagnosis	SA-GBO-ODBN, Hyperledger, ECC, SHA-256	Tamper-proof storage, optimized keys, accurate diagnosis	Application-specific (EEG/epilepsy); limited generalization
Alruwaill et al [23]	2025	Scalable health data management	hChain 4.0, AES, PHE, ABAC	Scalability, fine-grained access, anonymization	Permissioned blockchain limits openness; encryption overhead
Albakri and Alqahtani [24]	2023	IoMT-based secure healthcare	BSHS-EODL, DOA, SqueezeNet, VELM	Secure image transmission, high diagnostic accuracy	Focused on IoMT imaging; less emphasis on EHR privacy
Kokila et al [25]	2024	Medical image classification	DKS-CWH, WHO optimization	Robust classification accuracy	Limited to image datasets; not full EHR security
Selvaraj et al [26]	2025	Feature-centric EHR privacy	AFCP, polynomial encryption, blockchain	Fine-grained encryption, strong access restriction	Polynomial complexity; limited scalability
Ramachandraiah et al [27]	2023	Secure IoT healthcare + prediction	Blockchain, JSO, DCGRU, Twofish	Secure storage, robust prediction	Dataset-specific; throughput constraints

2.1. Research Gap

Most existing healthcare security frameworks rely on quantum infrastructures, federated learning, elliptic curve cryptography, or specialized deep learning models, but they often face challenges such as high computational overhead, limited scalability, complex integration, or application-specific focus. Quantum-based solutions demand advanced infrastructure not yet practical for widespread adoption, federated learning introduces heavy resource requirements across heterogeneous IoT devices, and elliptic curve or proxy re-encryption systems struggle with latency and interoperability. Deep learning approaches are frequently tailored to specific datasets or diseases, while IoMT and imaging-focused models emphasize diagnostic accuracy but neglect secure EHR transmission. Polynomial encryption schemes, though fine-grained, add computational complexity that limits scalability. This leaves a clear gap for a lightweight, scalable, and generalizable framework that ensures privacy-preserving EHR storage and transmission with efficient encryption and intelligent key optimization. The proposed SHA256 + blockchain + CNN-DNN with Augmented Antlion Optimizer model directly addresses this gap by combining practical cryptography, tamper-proof blockchain transmission, and optimized deep learning–based key management to deliver secure, efficient, and broadly applicable healthcare data protection.

3. PROPOSED METHODOLOGY

The model discussed performs as a secure data transfer system through the flow of data from the EHR through 4 phases: Encryption of the EHR data, cloud-based encrypted EHR data, transmission of EHR data across the blockchain, and decryption of EHR data when it is received. EHR data is first encrypted on the sending side of the EHR data using the SHA256 algorithm and encrypted with a private key (generated using the Augmented Antlion Optimizer – AAO) with one private key being chosen as the optimal key by using an optimal hybrid model consisting of CNN-DNN for the optimal key recovery from the protected EHR information maintained on cloud servers. This optimal key ensures robust encryption before the information is maintained on cloud servers. During communication, encrypted data was transmitted securely through blockchain blocks, guaranteeing tamper-proof delivery. At the receiver side, decryption is performed using SHA256 with the same optimal key derived from the AAO+CNN-DNN model, enabling accurate recovery of the original data. This integrated design ensures low-latency, privacy-preserving, and secure transmission of healthcare records between patients and doctors across distributed environments.

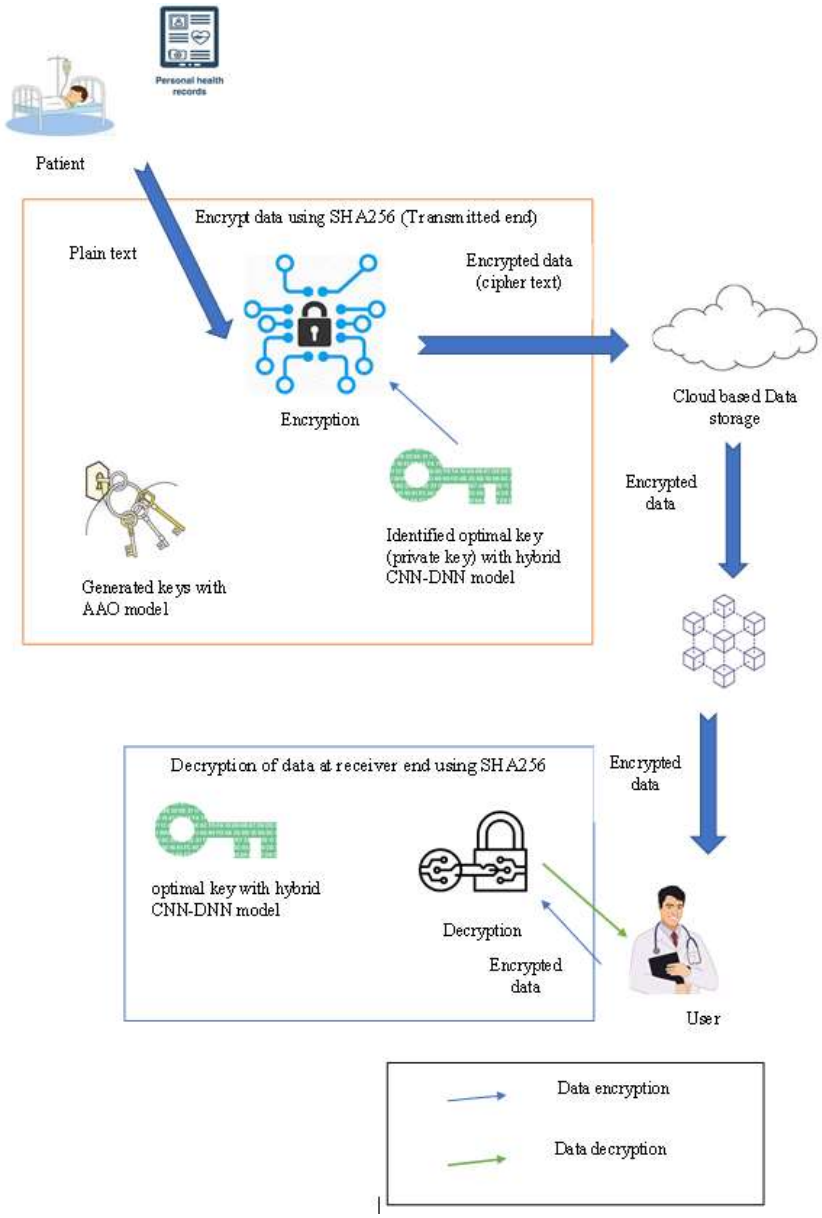

Figure 1: Architecture of the presented work

3.1 System Model

In this section, the presented framework was described. The overall information flow and the architectural modules will be outlined initially. Figure 1 depicts the overall architecture of the presented framework .

3.1.1 System Architecture

The suggested framework includes five major elements (a) data owner (sender-patient), (b) (c) encryption of data, (c) cloud, (d) blockchain, (e) user (doctor)

(a) Data Owner: A EHR Data owner (DO) is a individual or entity that possesses EHR data as well as requests access to or storage of such data. Data Owner (DO) has complete control on his or her EHR information. The DO must establish an access control policy for his or her EHR data, and the DO has the discretion to grant or deny certain access permissions to others. As a result, DO must create the metadata and re encryption keys for his or her PHR. Additionally, DO can give select people permission to upload more EHR data on DO's behalf, and DO can change who has access to the newly added EHR data.

(b) Encryption of Data: In our model, to maintain secrecy, the real EHR records of DO is secured through SHA256 based encryption process. To strengthen confidentiality within the encryption process, the efficient public key (produced through AAO+CNN-DNN) is generated. In fact, the SHA256 based encryption is undergone on EHR. The private key for encryption will be generated using AAO

model. Among the generated arbitrary private keys, the optimal one k_{opt_key} will be selected using the new hybrid optimization model (CNN-DNN). Thus, a highly secured encrypted EHR (cipher-text) is acquired, and it is stored onto the cloud. From the cloud, these encrypted HER's will be communicated to the receiver via the blocks of the blockchain. On the private blockchain, the EHR's metadata will be kept in order to offer search and tamper resistance functionalities.

(c) Cloud Storage: The real encrypted EHR data is kept in cloud storage (CS). CS is regarded as a semi-trusted server as well. Therefore, the blockchain has been implied for data transmission.

(d) Blockchain based data transmission: The encrypted EHR are transmitted via the blocks of the blockchain.

(e) User: The user (U) is a subject who wants access to EHR data of DO. Clinical professionals (like physicians and nurses), health insurance providers, as well as caretakers were some examples of typical U members. The decryption process takes place here. To prevent the unauthorized access over EHR's, the decryption will be accomplished, if and only if the participant employs the identical efficient key k_{opt_key} (generated using AAO+CNN-DNN model). Thus, a secured data communication takes place in the healthcare environment.

3.1.2 Blockchain Mechanism

Blockchain is a securely shared, decentralised data ledger. A limited number of parties can share data using blockchain technology. It has the ability to communicate and gather transactional data from various sources. Data can be separated into enjoyable connected pieces, connected together through specific references represented as encrypted hash values, and its integrity can be guaranteed by a unified repository of knowledge. This removes records replication as well as increases information protection. Blockchain is a better method for connecting distributed databases using peer-to-peer technology. Without any centralised assistance, it protects data.

Figure 2 illustrates how the structure resembles a linked list. The components listed below make up each block.

- Header
- Timestamp
- Previous Hash
- Hash
- Transaction Data

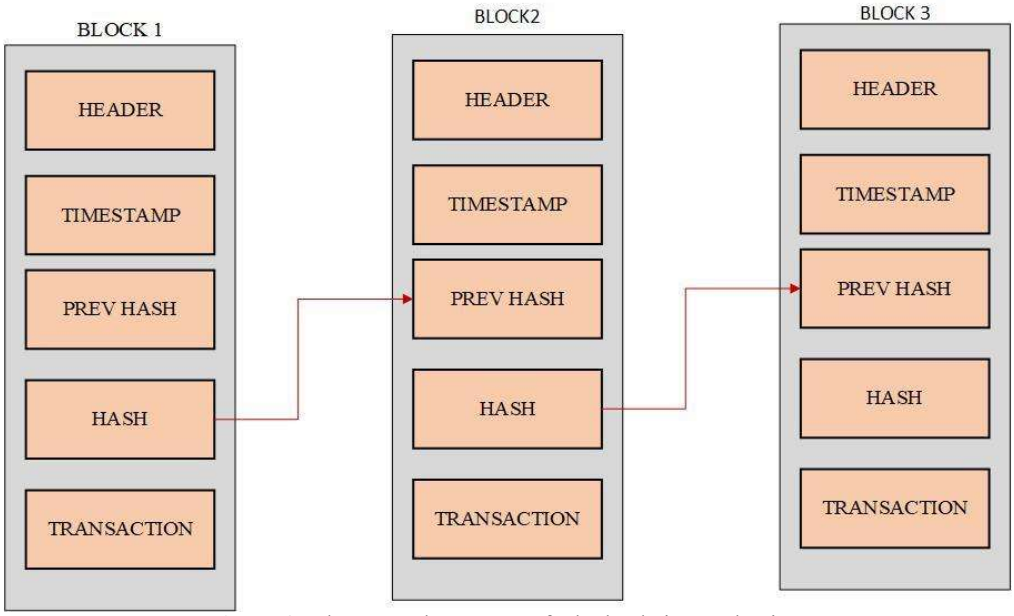

Figure 2: The general structure of Block Chain Mechanism

Block is a spreadsheet-like application. A blockchain is made up of numerous blocks. Blockchain functions like a distributed ledger since the ledger is dispersed over the network within the prevailing neighboring nodes. Each node has a copy of the Blockchain. After a predetermined number of generated transactions, the Block creates a new block. Every ten minutes, it is updated. After the register has been updated, no additional modifications are possible. Therefore, any attacks on the same are impossible. New data can, however, be contributed. Every computer register is updated simultaneously. There is no antecedent to the genesis block, which presents the first stage of the blockchain procedure. The node was a piece of hardware in a blockchain network. They are dispersed throughout the network and perform a variety of functions. An exchange has two primary keys. wallet, which consists

only of an address and a private key that can be any key set and is referred to as a secret key. The transaction message is signed with the private key when the choice is made to transmit money to anyone. The message is disseminated throughout the network. After that, the message is examined by the network of nodes to see if the transaction it includes is legitimate. After verifying the accuracy of the information, the block placement is completed. The data entered into the blockchain does not alter and remains unchanged. Because of the mechanism used, blockchain is incredibly secure. Every hash function in the blockchain serves the purpose of encryption for the blockchain's processing. It is difficult to breach the set hash value's length.

The immutability of blockchain is its most well-known attribute. Immutable is based on a distinct "blocks chains" ledger, where blocks holding transactions are continuously added at the end of the chain in chronological sequence. You must renew all the blocks that come after a block in order to change the data within it. Making the revision of a large number of blocks prohibitively expensive is one of the key functions of consensus algorithms. For instance, only 51% of the computational power is required in proof-of-work blockchain networks (like Bitcoin and Ethereum) to rebuild all blocks with corrupted data. This kind of practical architecture is dependable for data on the blockchain even though participants are not interested in using a lot of processing power to destroy data. In general, it may be said that the blockchain ledger's transaction data has not been "updated" and that the only way for it to be "fixed" is by accepting new transactions. Because corrections leave a trail, blockchains cannot be changed. Tampering is the act of changing something or making it false [13].

The suggested solution incorporates SHA256 encryption and decryption together with an improved hash algorithm.

3.1.3 SHA 256-based hashing

MAC hashing employs the SHA 256 procedure. The number in the hash function's name matches to the bit length of the digest it produces. In this instance, SHA-256 is used to generate the hashing function for the cloud's mechanism for controlling unauthorized access. The SHA-256 hash algorithm is illustrated in Figure 3. A total of eight registers were used to evaluate SHA-256. The registers' starting score is defined as 8×32 bits. Updation of the registers as $X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8$ from $P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8$ is done using the following equations

$$P_1 = \Sigma_0(X_1) + f_{v1}(X_1, X_2, X_3) + \Sigma_1(X_5) + f_{v2}(P_5, P_6, P_7) + X_8 + K_j + M_j \quad (1)$$

$$P_2 = X_1 \quad (2)$$

$$P_3 = X_2 \quad (3)$$

$$P_4 = X_3 \quad (4)$$

$$P_5 = X_4 + \Sigma_1(P_5) + f_{v2}(P_5, P_6, P_7) + X_8 + K_j + M_j \quad (5)$$

$$P_6 = X_5; \quad (6)$$

$$P_7 = X_6; \quad (7)$$

$$P_8 = X_7; \quad (8)$$

f_{S1} and f_{S0} are the two boolean function variables depicted as

$$f_{S1}(d, e, f) = (d \Lambda b) \oplus (\neg d \wedge f) \quad (9)$$

$$f_{S0}(d, e, f) = (d \Lambda e) \oplus (e \Lambda f) \oplus (f \Lambda d) \quad (10)$$

$£_0$ and $£_1$ are represented as

$$£_0(a) = ROT\ K^2(d) \oplus ROT\ K^{13}(d) \oplus ROTK^{22}(d)$$

$$£_1(a) = ROT\ K^6(d) \oplus ROT\ K^{11}(d) \oplus ROTK^{25}(d) \quad (11)$$

The SHA 256 round functions use32-bit word K_j from the message and M_j, $ROT\ K^n$ is the 32-bit right rotation of n bits notation, SHR^n is a 32-bit n bits shift rotation notation of 16 words of 12 bits each is indicated with 64 rounds and signified by a 512-bit hash function.

The calculation of K_j words are performed by the message words $m_0, m_1, m_2, \ldots \ldots m_{15}$, as given

$$K_j = \{m_i \quad for\ 0 \le i \le 15\ \Omega_1(m_{i-2}) + m_{i-7} + \Omega_0(m_{i-15}) + m_{i-16} \quad for\ 16 \le i \le 63 \quad (12)$$

$\Omega_0$and Ω_1 are derived from the equations below

$$\Omega_0(d) = ROT\ K^7(d) \oplus ROT\ K^{18}(d) \oplus SHK^3(d) \quad (13)$$

$$\Omega_1(d) = ROT\ K^{17}(d) \oplus ROT\ K^{19}(d) \oplus SHK^{10}(d) \quad (14)$$

The outcomes hash value for the 256-bit message blocks are derived by linking the register contents after the final iteration of the hashing procedure. This method is used to hash the message authentication code. A overall symbol of the SHA 256 hash algorithm is illustrated in Figure 3.

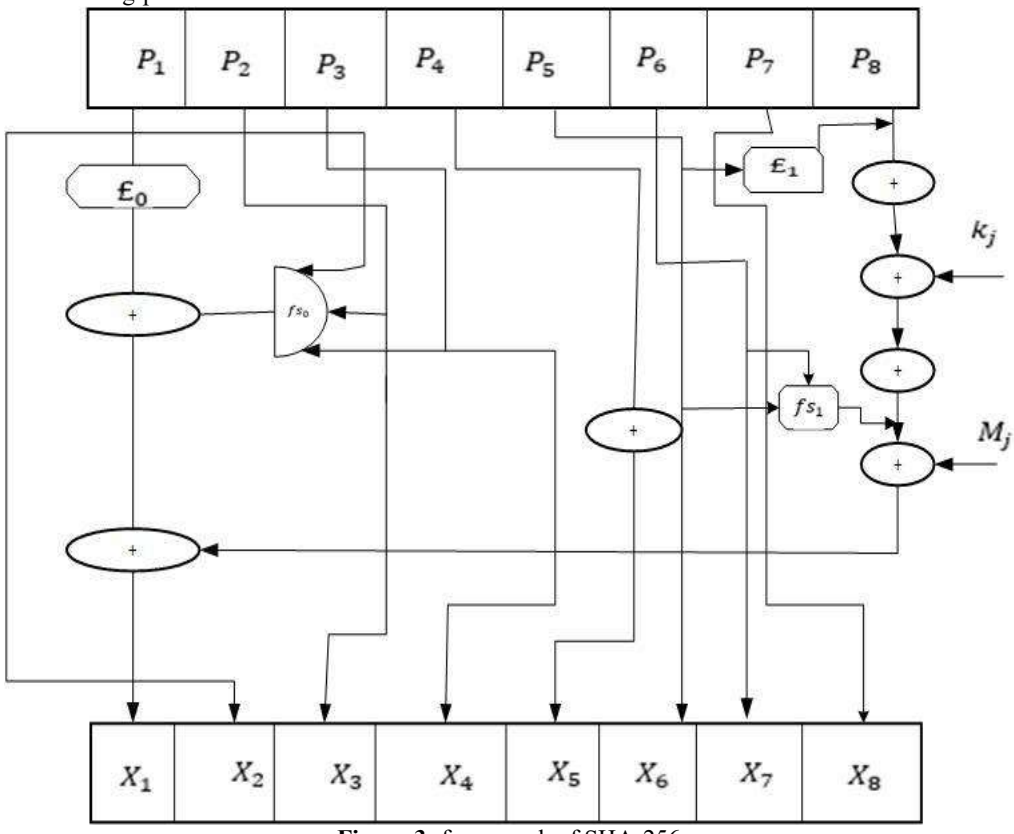

Figure 3: framework of SHA-256

Attackers have a difficult time accessing the data since the hash value, once saved in the blockchain, cannot be modified after storage. Additionally, the use of the SHA256 Hash function for encryption of the Patient Health Records (PHR) and the Key generation process using logistic Map procedure after Ant Lion Optimization

$$X_{n+1} = bX_n\,(1 - X_n\,)$$

Here, the control parameter b is with range $0 < b \leq 4, X_0$ is the value at the start, result system X_n and the range is $0 < X_n < 1$. The following process is involved in the key generation process.

$$X_0 = \frac{\sum_{I=1}^{K} \sum_{J=1}^{L} Q(i,j)}{K \times L \times 255}$$

The values K and L represent the simple image's number o f rows and columns.

- The logistic map in (eq.5) is iterated $L_0 + KL$ times, and the firstL_0 elements are skipped to attain a new Z

Algorithm enhance the protection of the records shared to safe Cloud.

3.1.4 Key generation using Optimized logistic Map

The key applied in the hashing process is derived using a logistic map. Its definition is given by

(15)

- The formula below determines the logistic map's initial value, which depends on the plain image P.

(16)

sequence with KL size. Determine the key using the equation given below.

$$Key(i) = mod(floor(z(i0 \times 10^{14}, 256), i = 1\ KL \qquad (17)$$

- The generated logistic maps are optimized using AAO model, to generate the keys with better security.

$$k_{key} = AAO \rightarrow Key(i))\ ;\ i = 1\ KL$$

Using the above approach, best arbitrary keys can be generated for the encryption and decryption process.

3.1.5 AAO Model

In this research key, the arbitrary keys are generated using AAO model. This AAO framework is an enhanced form of the baseline model ALO model. An Improvement programme called ALO bases its operations on how ant lions naturally hunt. This system picks experts at random and utilises an erratic walk. In this case, traps are deployed for exploitation. It employs pursuing techniques, such as the selection at random of specialists, the construction of traps, the capturing of ants in a snare, the capture of the prey, and the rebuilding of the traps.

- **Arbitrary walk of the ants:** Antlion traps have an impact on the various random routes that ants take throughout the search region, and antlions can construct apertures that are suitable for their fitness.

$$Key(i) = \{\beta_{key1}, \beta_{key}\ , \beta_{key3,} \dots \dots \beta_{keyn}\} \quad (18)$$

- **Fitness:** The measure of chaos in a grayscale image is called entropy. The surface of the info image is represented by a precise randomness indication. The best cryptographic image is chosen, and this image is then sent to the target. This image has the highest noteworthy entropy and lowest correlation coefficient.

An ant lion, which is the most fit ant lion, can catch every ant in the initial class and during every iteration process. The arbitrary walk's scope is adaptively decreased to proliferate down ants in the direction of ant lions.

$$Fitness\ Value = MaxValue(Entropy) \quad (19)$$

$$Entropy = \sum_{i=0}^{2G-1} \quad Prob_i\ log(\frac{1}{Prob_i}) \quad (20)$$

Here, G depicts the grey stage count as well as $Prob_i$ was the probability of grey stage data i

Those who are not chosen as elites each generation during the fitness computation process do not exhibit any interest in reproducing, even though the algorithm may provide superior results overall as a result of their contact with the elites.

- **New ant lion (keys) updating:** By employing traps, ant lions can follow them and get substantially more muscular. To replicate these interactions, ants must ascend above the interest space. The conditions below illustrate the Random Walk of the Ant Lions

$$Key(i) = \{0, S\big(2f(k_1 - 1)\big), S\big(2f(k_2 - 1)\big) \dots \dots \dots \dots S\big(2f(k_n - 1)\big)\} \quad (21)$$

$$f(k) = \{1\ if\ rand \geq 0.5\ 0\ if\ rand\ \leq 0.5 \quad (22)$$

Here S is the cumulative Sum, K is the Iterations maximum count and $f(k)$ a stochastic function. However, it is not possible to use the a forementioned condition to merely update ant locations. To keep the arbitrary paths within the search space, the Min-Max Normalization procedure is used. As per the proposed AAO model, the S position is given by,

$$S_c = S_{cm} + N(0,1) \times (S_{cn} - S_{cm}) + S_{cn} \quad (23)$$

Here the values S_{cn} and S_{cm} indicate the limits at the maximum and minimum levels on the c^{th} and d^{th} dimensions. $N(0,1)$ Depicts a random value in [0,1]. In the proposed model, S_{cn} and S_{cm} are newly adopted to avoid the solution from being stuck into the local optima. To ensure random walks remain within the search space, they are standardized applying the Z-score Normalization (proposed).

$$K(pos) = \frac{K(pos)_i^t - Mean\ (K(pos))}{SD}$$

Here, $K(pos)_i^t$ is the position of key and $Mean\ (K(pos)$ represents the mean of the generated keys as well as SD denotes the standard deviation of the generated keys.

The fitness value computation corresponding to each of the Fs positions is gained by the choice variable values substitution in a function, and the computed values are maintained in an array as follows

- **Antlion building traps:** A better chance of collecting ants is a sign of improved fitness. Here, the chosen antlion and the first-class ant lion lead the random walk of ants, and as a result, the relocation of a particular ant seems to be typical of each of the erratic walks.

$$N_{\ elite}, Key(i) = \frac{A_t(k) + A_E(k)}{2} \quad (24)$$

here $A_t(k)$ an arbitrary walk around N_{sel} ant lion $A_E(k)$ is the arbitrary walk around the elite antlion $N_{\ elite}$ and k_{key} is the generated best keys.

- **Ants catching and rebuilding pits:** The Ant Lion captures the ant and then updates its location with the ant's location as detailed below when the key's (ant's) fitness estimation is more (max) than the Ant Lion's fitness.

$$K(b\_pos)_i^t = K(pos)_i^t;\ if\ f(K(pos)_i^t) < (K(b\_pos)_i^t) \quad (25)$$

This method is produced by adding up all fitness values and ordering them from lowest to maximum fitness. The generated best arbitrary keys are pointed as k_{key}.

$$k_{key} = K(b\_pos)_i^t \quad (26)$$

Since the top ant lions are the fittest, it should be able to influence the growth of numerous ants over the course of iterations. The first n lines were then changed to reflect the appropriate positioning of the ant lions and their fitness at that time. From the generated arbitrary keys k_{key}, the optimal one is selected using the hybrid CNN-DNN model.

3.1.6 Hybrid CNN-DNN-based Optimal Key Generation

CNN**:** Convolution neural network (CNN), a deep learning approach, is utilised in the suggested system. Pooling layers, a fully regulated layer, an output layer, and convolutional layers make up its structure. The image input offset is subjected to a convolution process by the convolution filters. A training technique for optimising weights is gradient descent. The mapping the structures obtained from the convolution layer for the feature set is carried out by a Rectified Linear unit (ReLu). Gradients are normalised using the Batch Normalization Layer (BNL), which is added between the Rectified Linear Unit and the Convolution Layer. The feature maps are condensed while retaining the most important information from the photos thanks to the pooling layer. Performance of the fully linked layer is reliant on the cost function being reduced and weight updates being reversed. The fully connected layer's parameters are tuned and learned via stochastic gradient descent training. The hyperparameters supplied have a significant impact on how well CNN performs (Regularization, Momentum, Learning rate, and Epochs). The batch size, height, breadth, and depth characteristics of the image make up the 4-dimensional form of the input data. The image's batch dimension is shown in the first dimension, while its height, width, and depth are shown in the extra three. In RGB images, the depth equals 3, while in greyscale images, it equals 1. The depth represents the image's colour channels. The size of the input batch is constant, but the image's depth, width, and height vary depending on the size of the kernel, filter, and padding that are employed.

From the input vector A, a feature map R is produced. Convolution is carried out by employing a filter or kernel "M.".

$$R(i,j) = \sum_p \quad \sum_q \quad B(i-p, i-q).M(p,q) \quad (27)$$

The best CNN structure is one that uses 5-size 64 kernels in a 1-dimensional CNN layer. A causal padding function and a Rectified Linear Unit (ReLU) transfer purpose are also included, with one stride remaining the default. The Deep Neural Network is once more fed the CNN's output as an input. The next section of this study describes the capabilities of DNN.

The implementation of a Deep Neural Network (DNN) includes initial-training and fine-tuning stages, as shown in figure 4. The base framework and standard direct propagation framework known as the deep belief network (DBN), which is working at the beginning of the training phase, have various hidden layers, also referred to as numerous layers, where the primary layer gives input that goes through the final layer. It enables the covert components that give the system conviction to deliver the essential initiations. Additionally, designers employed the restricted Boltzmann machine (RBM) to fix the model's flaws. The RBM, a subset of the Markov random field, contains two layers stochastic hidden units and stochastic identifiable units. During initialization, the input units are assigned to the input vector.

$$R\ (v,w) = -\sum_{j=1}^{j} \quad \sum_{k=1}^{k} \quad R_{jk} v_k w_k - \sum_{j=1}^{j} \quad \beta_j \Upsilon_j - \sum_{k=1}^{k} \quad \Upsilon_k w_k \quad (28)$$

R_{jk} depicts the interaction within the v_k and the hidden unit w_k β, γ depicts the bias norm; The visible and hidden units count are depicted by *J*, *K*. It is possible to use an RBM's impartial value $(v_k, w_k)_{data}$ to locate any hidden units that may be present.

$$\sigma(v_k{=}1|w) = \alpha\ (\sum_{j=1}^{l} \quad R_{jk} v_k + \beta_k) \quad (29)$$

Unbiased samples are v_k, w_k. The random steepest ascent in log probability of the Learning dataset is implemented at the validation stage by extending the visible and hidden units, the path is defined

$$OpR_{jk}\Theta(v_k, w_k)_{data} - (v_k, w_k)_{reconstruction} \quad (30)$$

During the training phase, an RBM is organised and adopts the form of a layered architecture. The habits of the RBM layers are implemented by setting the current weights and biases. The tuning stage is grounded on the core principles back-propagation (BP) approach. The data collection may be classified applying the DNN's standard layer. Similar to this, the hidden layers are assigned for the DNN and N key attributes are used as the data. The final Training sets ideal weight phases using systematic data gathering, with BP starting weight gained during the initial phase.

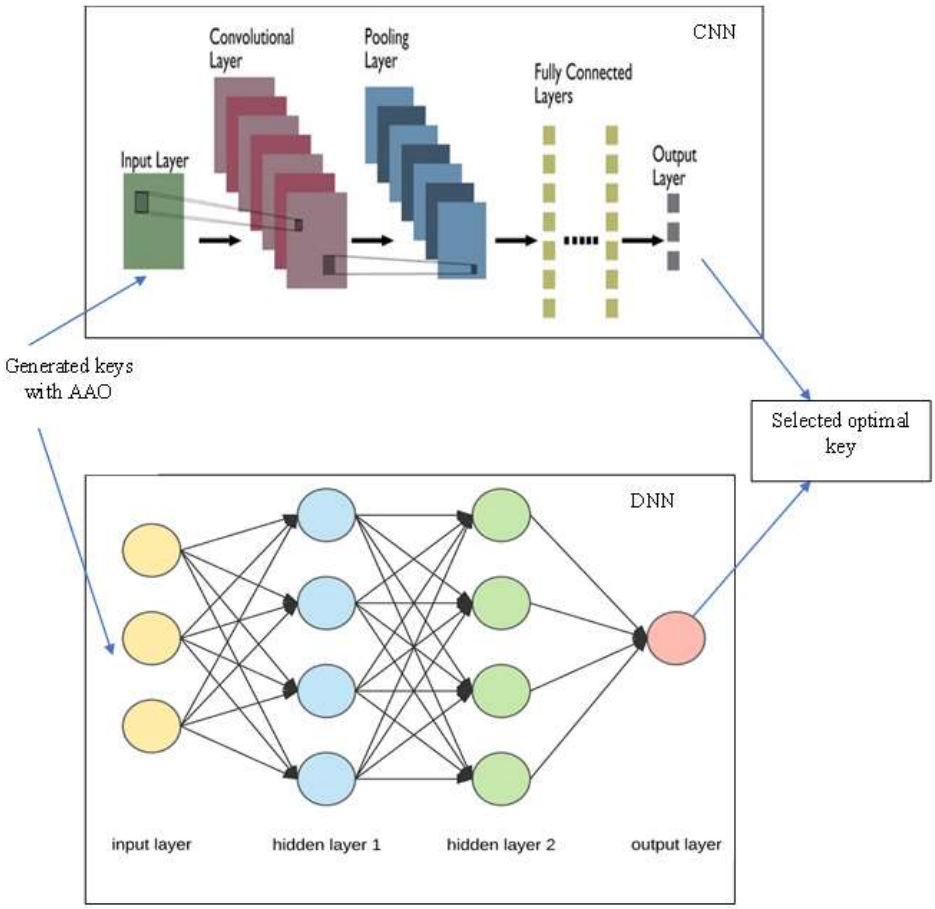

Figure 4: CNN-DNN for optimal key selection

4. RESULTS AND DISCUSSION

The suggested framework was evaluated applying PYTHON for its efficiency in the evaluation indicators like Encryption time, Decryption time, processing cycle time, and recovery effectiveness for three different image records. The presented framework was validated across three distinct databases Database-1 (https //www.kaggle.com/datasets/masoudnickparvar/brain-tumor-mri-dataset), Database-2 (https //www.kaggle.com/datasets/andrewmvd/covid19-ct-scans) and Database-3 (https //www.kaggle.com/code/carlosdg/a-detail-description-of-the-heart-disease-dataset). The system was then compared with existing systems like African Vulture Algorithm (AVA), Particle swarm Optimization (PSO), Sine Cosine Algorithm (SCA), Effective Lightweight Homomorphic Cryptographic Algorithm (ELHCA) (Thabit et al., 2022), simulation of a novel secure quantum key distribution (SQKD) (Sasikumar et al., 2022) and LHES [6]. The assessment was conducted with respect to Encryption time, decryption time, Turnaround time, recovery performance, as well as KPA analysis and CPA evaluation.

4.1 Performance Metrics

- **Encryption Time**

Encryption time: The encryption period is the total duration to convert plaintext into ciphertext.

- **Decryption Time:** The decryption period was the total duration to turn a cipher text into plain text.
- **Turnaround time:** It is the the overall duration between the submission of a data for the execution process in the Python platform used and the return of the complete result to the user after completion.
- **Restoration efficiency:** It is the efficiency of the system to estimate the clean or original image from the corrupt, noisy, or blurred image resulting due to various factors.

4.1.1 Overall Performance Evaluation

The suggested framework is validated for Database-1, database-2 and Database-3. This evaluation is carried out with respect to Encryption time, decryption time, Turnaround time, Restoration efficiency, respectively.

Database-1**:** The suggested framework has achieved the least Encryption Time(s), Decryption Time(s) and Turnaround Time(s), while compared to the existing models. This enhancement results from the choice of the optimal keys with AAO+CNN-DNN model. Furthermore,

the recovery effectiveness of the suggested framework is 0.954218, which is better than AVA=0.893824, PSO=0.943425, SCA=0.876794, ELHCA [26] = 0.82285, LHES [6] = 0.939083. Thus, the proposed model is said to be much sufficient for transmitting MRI images securely.

Database-2**:** Using the proposed model, the CT images were transmitted, and the reliability of the model has been tested. This evaluation is conducted with respect to Encryption Time(s), Decryption Time(s) and Turnaround Time(s). According to the obtained results, the suggested framework has achieved the least Encryption Time(s)= 0.214673, Decryption Time(s)= 0.199637 and Turnaround Time(s)= 0.414311. The arbitrary keys were generated using the AAO model, rather than ransom approach. This boosted the restoration effectiveness of the suggested framework, and therefore the suggested framework has reached the highest restoration efficiency as 94.4%.

Database-3**:** The suggested framework has been evaluated using the bigdata (heart disease database), and the evaluation has been made. Even with bigdata, the proposed model was efficient in securely transmitting data. Moreover, it has also consumed less time for encryption, decryption as well turnaround time. The Encryption Time(s) consumed by the proposed model is 0.219032, which is better than AVA=0.247749, PSO=0.240675, SCA=0.238678, ELHCA=0.227853, SQKD=0.227853 and LHES=0.22451. Furthermore, the suggested framework has additionally achieved the least Decryption Time(s) and Turnaround Time(s). On the other hand, the proposed model has recorded the maximal Restoration Efficiency as 96.3%. Thus, the proposed model is said to be much sufficient for secured data transmission. Table 2-4 is shown below.

Table 2: Analysis of the proposed model's performance using Database-1

Database 1	**AVA**	**PSO**	**SCA**	**ELHCA [26]**	**SQKD [27]**	**LHES [6]**	**Proposed**
Encryption Time(s)	0.238268	0.227	0.245272	0.236291	0.225574	0.223224	0.216842
Decryption Time(s)	0.232551	0.210435	0.218997	0.204132	0.242243	0.20759	0.201654
Turnaround Time(s)	0.470819	0.437435	0.464269	0.440423	0.467817	0.430814	0.418496
Restoration Efficiency	0.893824	0.943425	0.876794	0.82285	0.947258	0.939083	0.954218

Table 3: Analysis of the proposed model's performance using Database-2

Metrics for Image2	**AVA**	**PSO**	**SCA**	**pap1[26]**	**pap2[27]**	**LHES [6]**	**Proposed**
Encryption Time(s)	0.22473	0.233928	0.235886	0.223318	0.242819	0.220042	0.214673
Decryption Time(s)	0.20833	0.202091	0.230225	0.239821	0.216807	0.20463	0.199637
Turnaround Time(s)	0.43306	0.436019	0.466111	0.463139	0.459627	0.424673	0.414311
Restoration Efficiency	0.933991	0.814621	0.884886	0.937785	0.868026	0.925697	0.944676

Table 4: Analysis of the proposed model's performance using Database-3

Metrics for Image3	**AVA**	**PSO**	**SCA**	**pap1[26]**	**pap2[27]**	**LHES [6]**	**Proposed**
Encryption Time(s)	0.247749	0.240675	0.238678	0.227853	0.229293	0.22451	0.219032
Decryption Time(s)	0.221209	0.2349	0.206194	0.24469	0.21256	0.208785	0.203691
Turnaround Time(s)	0.468959	0.475575	0.444872	0.472543	0.441853	0.433295	0.422723
Restoration Efficiency	0.885651	0.902853	0.831161	0.956826	0.952955	0.944492	0.963857

4.2 Analysis on Proposed Model

4.3.1 Encryption Time Analysis

The suggested architecture is evaluated for 3 databases, with respect to encryption time. The obtained results are shown in Figure 5. This evaluation n is done with 70th training information. As per the acquired outcomes, the suggested framework has recorded the minimum encryption time for all the three databases. The encryption time achieved by the suggested framework under database 1 is 0.21s, which is better than AVA=22.8%, PSO=21.7%, SCA= 23.89%, ELHCA=24.89%, SQKD= 23.56% and LHES=24.23%. In suggested framework has also achieved

the least encryption time for database 2 and database 3 also. Thus, the suggested framework is reported to be extremely applicable for secured data transmissions.

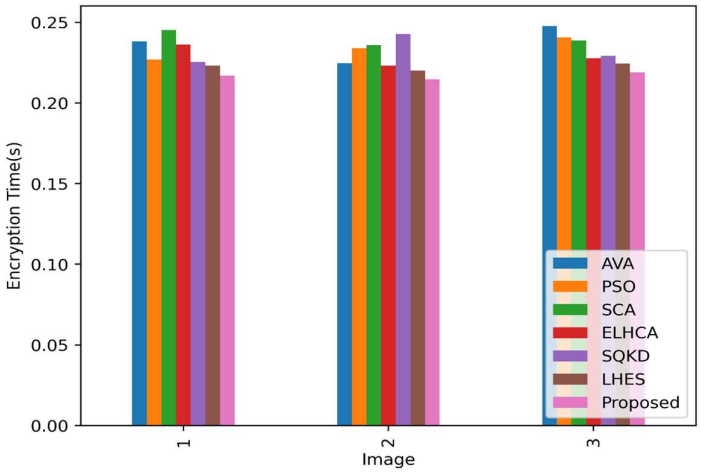

Figure 5: Evaluation of the proposed model's encryption time using 3 databases

4.3.2 Decryption Time Analysis

The Decryption period was analyzed in the graph as shown in Figure 6 where the decryption time values were compared for all three database The graph shows the overall analysis where the proposed system had a lower decryption time value than the existing system proving the proposed model to be more efficient than the others. The decryption time recorded by the proposed model under database 1 is 20.16%, database 2 is 19.9% and database 3 is 20.3%, which is better than the existing models. Thus, the sensitive data will get transferred in a secured manner.

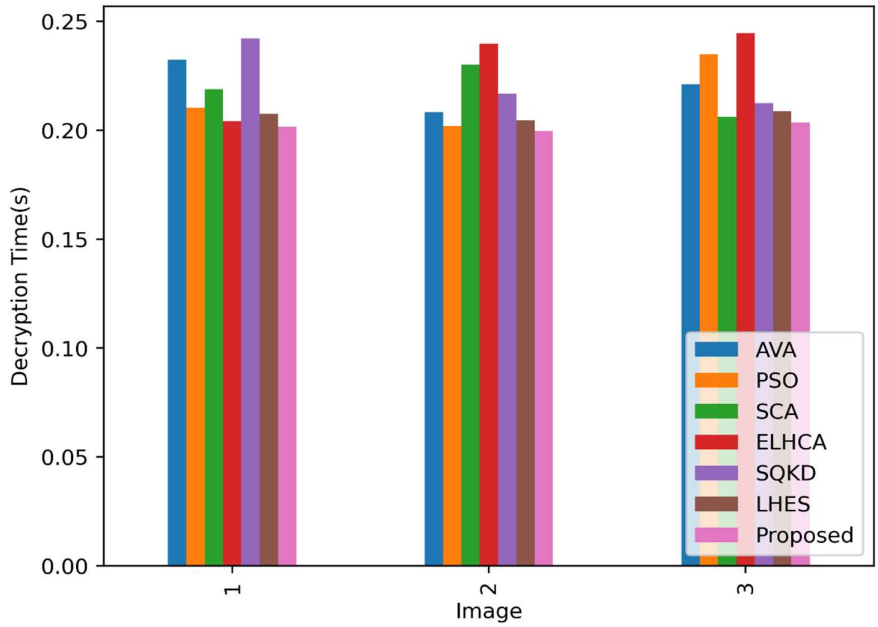

Figure 6: Evaluation of the proposed model's decryption time using 3 databases

4.3.3 Turnaround Time Analysis

The Turn Around time is analyzed in the graph as shown in Figure 7 where the Turnaround time values were compared for all three databases. The graph shows the overall analysis where the proposed system had a lower Turnaround time value than the existing system proving the proposed model to be more efficient than the others. The turnaround time recorded by the proposed model

under database 1 is 44.2%, which is better than existing models like AVA, PSO, SCA, ELHCA, SQKD and LHES by 49.02%, 45.7%, 46.4%, 45.08%, 46.7% and 42.09%, respectively. In addition, the turnaround time recorded by the proposed model under database 2 is 41.3%, which is better than AVA, PSO, SCA, ELHCA, SQKD and LHES by 45.6%, 44.69%, 47.78%, 47.37%, 46.39% and 43.9%, respectively. In addition, the turnaround time recorded by the proposed model under database 3 is 41.2%, which is better than AVA, PSO, SCA, ELHCA, SQKD and LHES by 47.69%, 49.5%, 45.7%, 48.54%, 49.25%, 45.12% and 44.3%, respectively. Thus, the proposed model is highly secure and has better privacy preservation in transmitting medical data in a secured fashion.

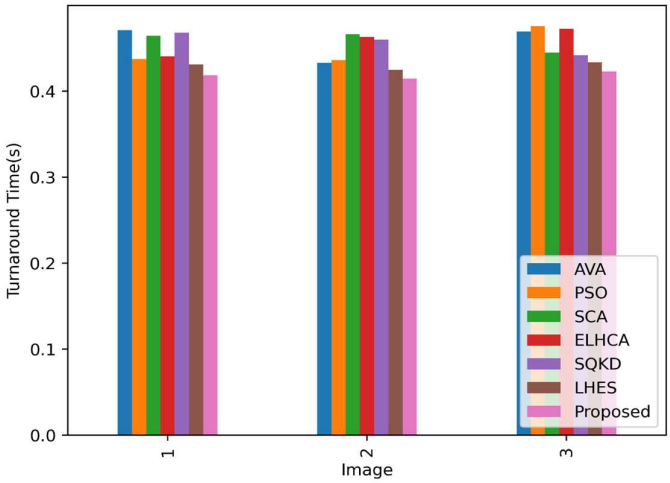

Figure 7: Comparative Analysis of the Proposed Turnaround time of the 3 databases

4.3.4 Restoration Efficiency Analysis

The Restoration Efficiency is analyzed in the graph as shown in Figure 8 where the values for the restoration efficiency were compared for all three images. The graph shows the overall analysis where the proposed system had higher Restoration efficiency than the existing systems, proving the proposed model to be more efficient than the others. The suggested framework has achieved the maximum restoration efficiency as 96.45%, 97.56% and 98.43% for database 1, database 2 and database 3, respectively. Therefore, the proposed model is recognized as highly efficient in transmitting data without any information loss.

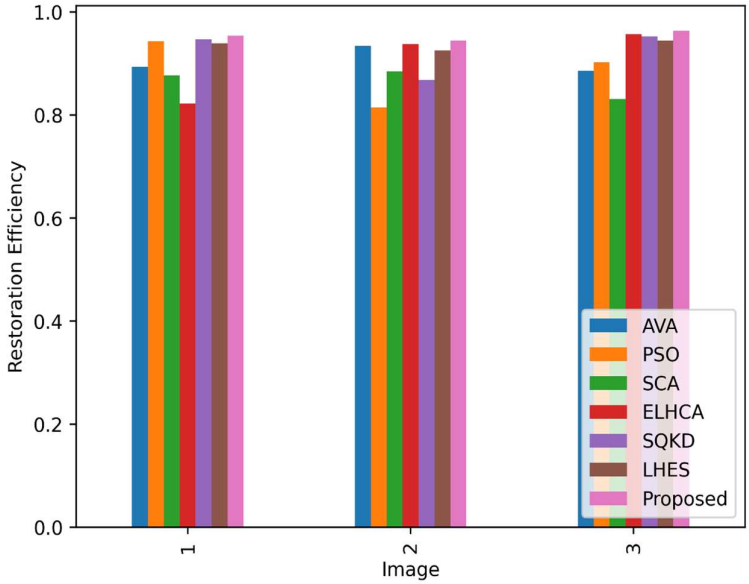

Figure 8: Comparative Analysis of the Proposed Restoration Efficiency of the 3 databases

4.3 KPA and CPA Analysis

A cryptanalysis attack paradigm known as KPA is one in which the adversary possesses knowledge of the plaintext–ciphertext pairs. This section examines how the CPA as well as KPA assault affected the relationship between the source and reconstructed information. Similar to this, relationship between the source and recovered information is examined after the KPA assault. When CPA and KPA attacks occur, there is little connection between the recovered information and the source information. According to the definition of CPA, it is "an attack model for cryptanalysis that assumes. The adversary is able to generate ciphertexts for chosen plaintexts." When the CPA attack is complete, relationship between the source and reconstructed information is examined in this section. Similar to this, analysis of the relationship between the source and reconstructed information is done after the KPA attack. When CPA and KPA attacks occur, there is little connection between the recovered information and the source information . As a result, the proposed algorithm has been successful in protecting cloud data from attacks and has outperformed other algorithms in this regard.

AVA	0.206467
PSO	0.303501
SCA	0.258171
ELHCA	0.313387
SQKD	0.199795
LHES	0.269967
Proposed	0.192231
AVA	0.368284
PSO	0.323537
SCA	0.338709
ELHCA	0.475829
SQKD	0.326782
LHES	0.332872
Proposed	0.308101

5. CONCLUSION

This study has developed a blockchain-based privacy-preserving Intelligent healthcare framework to safeguard patient privacy and data protection of electronic health records (EHRs). The proposed model integrates four key phases—EHR data encryption, cloud-based encrypted storage, blockchain-enabled transmission, and secure decryption—providing end-to-end protection of sensitive medical data. By employing SHA256 for encryption and decryption, combined with optimized key generation through the Augmented Antlion Optimizer (AAO) and a hybrid CNN-DNN model, the framework achieves robust security with efficient key management. The use of blockchain ensures tamper-proof data transmission, while the deep learning–driven optimization enhances reliability and adaptability. Experimental evaluation in terms of encryption time, decryption time, turnaround time, and restoration efficiency demonstrates the effectiveness of the system. Totally, the suggested framework provides a robust, adaptable, and privacy-focused framework for modern healthcare environments, addressing critical challenges in privacy-preserving EHR management.

Future Work

- Extend the framework to handle multi-modal healthcare data (genomic records, medical imaging, IoT sensor streams).
- Explore post-quantum cryptographic techniques (e.g., lattice-based encryption) for resilience against emerging threats.
- Validate scalability through real-world deployment across multi-hospital networks and integration with healthcare standards (HL7, FHIR).
- Incorporate explainable AI mechanisms to improve transparency and clinician trust in security and diagnostic processes.

DECLARATIONS

Funding

On Behalf of all authors the corresponding author states that they did not receive any funds for this project.

Conflicts of Interest

The authors declare that we have no conflict of interest.

Competing Interests

The authors declare that we have no competing interest.

Data Availability Statement

All the data is collected from the simulation reports of the software and tools used by the authors. Authors are working on implementing the same using real world data with appropriate permissions.

Author's Contributions

Author 1: Naveen John J

He participated in the methodology, Conceptualization, Data collection and writing the study

Author 2: Shatheesh Sam I

He Performed the Analysis the overall concept, writing and editing

Ethics Approval
No ethics approval is required.

Consent to Participate
Not Applicable

Consent for Publication
Not Applicable

REFERENCE

[1] Adeniyi, A.O., Arowoogun, J.O., Chidi, R., Okolo, C.A. and Babawarun, O., 2024. The impact of electronic health records on patient care and outcomes: A comprehensive review. *World Journal of Advanced Research and Reviews*, *21*(2), pp.1446-1455.

[2] Babu, J.A., Patil, S., Parameshachari, B.D., Rinaldi, S., Balmuri, K.R. and Hemalatha, K.L., 2025. Block chain enabled hybrid cryptographic algorithm for security and privacy preservation of electronic health records. *ICT Express*, *11*(5), pp.945-950.

[3] Othman, S.B. and Getahun, M., 2025. Leveraging blockchain and IoMT for secure and interoperable electronic health records. *Scientific Reports*, *15*(1), p.12358.

[4] Sabonchi, A.K.S., 2025. Securing Electronic Health Records with Cryptography and Lion Optimization. *Journal of Cybersecurity (2579-0072)*, *7*(1).

[5] Worapaluk, K. and Fugkeaw, S., 2026. Blockchain-Enabled Privacy-Preserving Access Control for EHRs Sharing With Optimized User and Attribute Revocation. *IET Information Security*, *2026*(1), p.3917525.

[6] MAITHILI, K. and AMUTHA, S., 2026. AN ADAPTIVE HASH DRIVEN ACCESS CONTROL MODEL FOR ENHANCED PATIENT DATA SECURITY IN HEALTHCARE. *Journal of Theoretical and Applied Information Technology*, *104*(1).

[7] Moreau, I. and Sinclair, T., 2024. A Secure Blockchain-Enabled Framework for Healthcare Record Management and Patient Data Protection. *Global Journal of Medical Terminology Research and Informatics*, *2*(4), pp.30-36.\

[8] Vidhya, S., Siva Raja, P.M. and Sumithra, R.P., 2024. Blockchain-Enabled Decentralized Healthcare Data Exchange: Leveraging Novel Encryption Scheme, Smart Contracts, and Ring Signatures for Enhanced Data Security and Patient Privacy. *International Journal of Network Management*, *34*(5), p.e2289.

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

[10] Senthilkumar, M., Kannan, S. and Ravi, V., 2025. Developing an Innovative Medical Image Security Framework Based on Larger Chunk-Adaptive Integrated AES and RSA. *Security and Privacy*, *8*(5), p.e70090.

[11] Selvi, P. and Sakthivel, S., 2025. A hybrid ECC-AES encryption framework for secure and efficient cloud-based data protection. *Scientific Reports*, *15*(1), p.30867.

[12] Talukder, A.S. and Sarker, S.H., 2025. Advanced SHA256-AES Hybrid Algorithm for Enhanced Data Confidentiality and Integrity in Cloud Data Security. *Journal of Computer Science and Technology Studies*, *7*(12), pp.453-466.

[13] Haddad, A., Habaebi, M.H., Elsheikh, E.A., Islam, M.R., Zabidi, S.A. and Suliman, F.E.M., 2024. E2EE enhanced patient-centric blockchain-based system for EHR management. *Plos one*, *19*(4), p.e0301371.

[14] Jafer, A.S. and Abbood, H.N., Secure Data Management via Lightweight Cryptographic Frameworks: A Comparative Study of ChaCha20 for Encryption and SHA-256 for Hashing Secure Using a Big Data.

[15] Kiruthikadevi, K., Sivaraj, R. and Vijayakumar, M., 2024. A blockchain and hybrid deep learning for secure and efficient healthcare data transmission and management. *Tehnički vjesnik*, *31*(6), pp.2140-2145.

[16] Afrihyia, E., Chianumba, E.C., Mustapha, A.Y., Forkuo, A.Y. and Omotayo, O., 2025. Developing privacy-preserving data sharing protocols for healthcare systems using cryptographic and blockchain-based techniques. *International Journal of Advanced Multidisciplinary Research and Studies*, *5*.

[17] Das, P., Singh, M. and Verma, K.K., 2024. Blockchain-enabled deep learning approach to improve healthcare system. *Journal of Multimedia Information System*, *11*(1), pp.9-16.

[18] Reoukadji, D.M., Olivier, M.M., Bokonda, P.L. and Ait Madi, A., 2026. High-Dimensional Quantum Key Distribution for Secure Healthcare Communication Systems: Integrating Internet of Medical Things, Electronic Health Records, and Smart Medical Gate. *Journal of Current Science and Technology*, *16*(1), pp.153-153.

[19] Ali, A.A., Gunavathie, M.A., Srinivasan, V., Aruna, M., Chennappan, R. and Matheena, M., 2025. Securing electronic health records using blockchain-enabled federated learning for IoT-based smart healthcare. *Clinical eHealth*, *8*, pp.125-133.

[20] Ashwini, D.Y. and Puneeth, R.P., 2026. Blockchain-Based Framework for Enhancing Interoperability and Security in EHR Exchange Using Lightweight ECC

Proxy Re-Encryption. *Acta Informatica Pragensia*, *2026*(1), pp.90-108.

[21] Abidi, M., Alkhalefah, H. and Aboudaif, M., 2024. Enhancing healthcare data security and disease detection using crossover-based multilayer perceptron in smart healthcare systems. *Computer Modeling in Engineering & Sciences*, *139*(1), p.977.

[22] Sharma, N. and Shambharkar, P.G., 2025. Towards secure healthcare: SA-GBO-ODBN model utilizing Blockchain and deep learning for data handling and diagnosis. *The Computer Journal*, *68*(10), pp.1386-1423.

[23] Alruwaill, M.N., Mohanty, S.P. and Kougianos, E., 2025. hChain 4.0: A secure and scalable permissioned blockchain for EHR management in smart healthcare. *arXiv preprint arXiv:2505.13861*.

[24] Albakri, A. and Alqahtani, Y.M., 2023. Internet of medical things with a blockchain-assisted smart healthcare system using metaheuristics with a deep learning model. *Applied Sciences*, *13*(10), p.6108.

[25] Kokila, M.S., Fenil, E., Ponnuviji, N.P. and Nirmala, G., 2024. Securing cloud-based medical data: an optimal dual kernal support vector approach for enhanced EHR management. *International Journal of System Assurance Engineering and Management*, *15*(7), pp.3495-3507.

[26] Selvaraj, D., Jasmine, J.J., Ramani, R., Dhinakaran, D. and Prabaharan, G., 2025. AFCP Data Security Model for EHR Data Using Blockchain. *Journal of Cybersecurity & Information Management*, *15*(1).

[27] Ramachandraiah, K.R.D., Bommagani, N.J. and Jayapal, P.K., 2023. Enhancing healthcare data security in IoT environments using blockchain and DCGRU with Twofish encryption. *Inf. Dyn. Appl*, *2*(4), p.173185.