International Journal of Engineering & Scientific Research
Vol.12 Issue 03, March 2024
ISSN: 2347-6532 Impact Factor: 8.076
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

# A COMBINATION OF OPTIMIZATION-BASED MACHINE LEARNING AND BLOCKCHAIN MODEL FOR ENHANCING SECURITY AND PRIVACY IN THE MEDICAL SYSTEM

**Ajay Chandra MK**
**Technical ERP Program Manager**

## ABSTRACT

Blockchain technology has emerged in recent years as a cutting-edge method for carrying out operations in an open environment, storing data, building trust, and carrying out transactions. Furthermore, the security and privacy of healthcare data is a major challenge due to third parties and attacks, but the blockchain is one of the most recent revolutions in safe computing without a centralized authority. So, create the Hybrid Ant Lion and Grey Wolf-based Symmetric Key Encryption (HALGW-SKE) model using Blockchain to enhance the security and privacy of medical data. User data is recorded and grouped into blocks according to the blockchain's hash value. As a result, to improve key generation performance, the HALGW is employed to create the optimum key. Additionally, a model called Ensemble Machine Learning with Firefly Optimization (EML-FFO) is designed to identify cloud threats. Additionally, launch attacks in the cloud environment to prove the efficiency of the designed model to identify and detect attacks. The results obtained from the created model are compared to various cutting-edge methods for processing time, accuracy, precision, and decryption and encryption times. The optimized model achieved a 99.23 percent accuracy rate and a reduced encryption time of 0.05 ms.

**KEYWORDS:** Blockchain, Advanced Standard Encryption, Hybrid Optimization, Privacy-Preserving, Healthcare Data, Cloud Security, Machine Learning

## 1. INTRODUCTION

Blockchain-based healthcare provides a sophisticated method of storing medical records, establishing trust for healthcare data integration and exchange, and carrying out medical transactions in a decentralized healthcare setting [1]. Although blockchain technology with a focus on healthcare has garnered the most interest and attention from academia, business, and government [2]. The main goal of information sharing through blockchain implementation in corporate operations and the healthcare sector is privacy and security concerns [3].Within the healthcare industry, patient data and important patient information are created and kept up to date in modified healthcare departments and organizations [4]. The medical professionals failed to get in touch with the vital information that would have allowed them to provide diagnoses, suggestions, treatment decisions, and high-quality care services [5]. In general, the Healthcare Information System (HIS) manages a great deal of complicated data, and to improve HIS, it needs safe, rapid access to the healthcare data [6]. Additionally, a blockchain known as a secure distributed ledger provides a possible means of exchanging medical data along with data exchange, data verification, safe storage, and historical patient records [7].

As a result, blockchain offers a novel method for carrying out operations in an open environment, storing data, building trust, and carrying out transactions [8]. Moreover, one of the most recent developments in decentralized, secure computing is blockchain [9]. By arranging the logs for changing medical records into a hierarchical chain of blocks, the distributed database is a blockchain [10]. Compared to other traditional encryption methods, it provides greater protection.Additionally, blockchain enables new standards in patient data management, insurance claim processing, and medical record management [11, 12]. Two major risks, including information manipulation and leaks, are present in the isolated information found in the medical data [13]. In particular, EHR is crucial when handling discrete data such as medical demand information, inspection symptoms, non-text investigation data, patient fundamental data, and relevant medical records [14]. Additionally, a network of hospitals managed by the organization is housed on the hospital server, which stores private data [15].

A growing interest in using blockchain technology to advance medical services and e-health has emerged [16]. The adoption of blockchain technology also has promising opportunities to streamline healthcare delivery [17]. The patient's health data is then gathered at home using mobile devices, such as smartphones and wearable sensors, and shared in a cloud system [18]. Healthcare professionals' access, review, and provide prompt medical assistance based on the medical records in the interval [19]. Numerous methods have been devised to improve blockchain security and performance, but assaults, low reliability, high error rates, and a lack of confidentiality and privacy remain the key problems [20]. Therefore, create a novel blockchain-based hybrid optimization with the SKE model to secure patient data in the cloud and improve the security and privacy of healthcare data. Create an EML model with FFO optimization to identify threats in the healthcare setting.

Below is a description of the designed model's primary contribution,

- Initially, a Python program is used to gather and train the system with many patient datasets.
- Next, create a cloud-based HALGW-SKE model with the necessary parameters to encrypt data and improve security.
- Utilizing HALGW, generate the best possible SKE key, then encrypt the data with the private key.
- After that, a hash value algorithm is computed to divide the data into blockchain blocks.
- The data is then divided into blocks in the blockchain by calculating the hash value.
- Launch an attack on the developed model to demonstrate its effectiveness.
- The obtained findings are then contrasted with various methods that are currently in use for the following metrics: encryption time, F-measure, processing time, accuracy, precision, decryption time, and recall.

This research study is structured in the following ways. Section 2 covered relevant work based on blockchain security, Section 3 provided a full description of problem statements. Additionally, section 4 provides more detail on the suggested methodology's procedure. Finally, the results and discussion are covered in Section 5, and the established model's conclusion is covered in Section 6.

## 2. RELATED WORKS

For anomaly detection, Mishra et al. [21] created the Hybrid Decision Tree Method (HIDT), which combines blockchain principles and machine learning. With the maximum attack detection accuracy of 99.95 percent for the KD99 dataset, the suggested method (HIDT) forecasts attacks in the lowest period across all datasets. The suggested solution lowers end-to-end delay and routing overhead by quickly identifying rogue nodes. This solution can be used by organizations and governments to increase security and resilience by protecting data from hostile threats.

Based on the utilization of blockchain-enabled Federated Learning, Hamouda et al. [22] introduced a unique privacy-preserving safe framework called PPSS with increased privacy, verification, and accessibility. To protect multi-party processing, the PPSS approach includes Proof-of-Federated Deep-Learning (PoFDL) and a permission blockchain architecture. The findings show that the PPSS architecture has high classification results for detecting industrial IIoT assaults.

To guarantee the security and privacy of sensor-IoT-based infrastructures employing sampled ECS data, Bora et al. [23] suggest privacy-preserving blockchain-based federated learning (PPFchain). FL and cryptographic protocol have been combined in the off-chain fog node to protect privacy. Moreover, offers improved security, increased accuracy, and a comparison of performance with conventional blockchain systems.

Aitizaz et al. [24] present a novel method that combines blockchain technology with homomorphic encryption (HE) algorithms to improve privacy protection in Internet of Things-based healthcare systems. HE protects the secrecy of encrypted material during computation by enabling calculations to be performed on it without the need for decryption. Smart contracts are integrated into the blockchain network by the specified model to establish data-sharing guidelines and control access. These settings give the management a safe and open environment while shielding the data from observation by unauthorized parties.

A blockchain-based lightweight encryption algorithm with federated learning is introduced by Manisha et al. [25] to solve the scalability and trust issues with electronic health data (EHR). The EHR data is fully encrypted during the entire communication with FL and is kept in a decentralized cloud system. To guarantee data privacy between the user and the owner while the contract is being executed, a highly efficient proxy re-encryption method with FL is utilized.

To improve security in the healthcare sector, Ramesh et al. [26] created a blockchain-based data broadcast method that includes a categorization mechanism. The HE system is utilized to guarantee a secure and safe learning environment. The optimal key for the HE method was found using the oppositional-based harmony search (OHS) algorithm. A convolutional neural network is utilized with blockchain technology to securely transfer data to the cloud server and detect the presence of sickness.

Using blockchain technology, Chaoyang et al. [27] present an effective privacy-preserving methodology to create a safe mechanism for transferring data between various device nodes. The lightweight barrier secret-sharing technique helps to increase the efficiency and security of medical data sharing. By erasing the semantic meaning of the data, it can preserve privacy. Furthermore, the suggested model's high degree of stability is demonstrated by the transaction processing performance assessments in IoMT.

A blockchain-based privacy-preserving authentication management approach is proposed by Zhaoshun et al. [28]. The protocol employs three-factor authentication and a blockchain. further presents the Chebyshev chaotic map to guarantee user authentication and login security. The proposed technique is secure, according to standard security proof and assessment that makes use of the adversary model and Burrows-Abadi-Needham logic. The suggested protocol may result in higher communication, computing, and storage costs.

Innovative blockchain technology is introduced by Verma et al. [29] to secure health data in the cloud, helping to provide integrity and authenticity for medical information. Develop an enhanced blowfish model that ensures authentication features with the best encryption possible. Additionally, a novel method known as Elephant Herding Optimization with Opposition-Based Learning (EHO-OBL)generates keys in the best possible way. As a result, the suggested technique's key generation time has decreased in value.

## 3. PROBLEM DEFINITION

There is an increased danger of storing medical details in hospitals due to restricted storage capacity in the public medical system. The confidentiality, integrity, and availability of sensitive patient information are threatened by the serious security and privacy issues facing the healthcare system today [30]. Concerns regarding system vulnerabilities put patients at risk of privacy violations and undermine the data integrity of healthcare data. Data privacy, data sharing and storage, authentication, interoperability, data security, and so forth are the most difficult jobs in the health service. The primary concerns are scalability and data access since storing data in a chain signifies the blockchain's specialization [31]. However, due to attacks and unauthorized access that could compromise personal health data, data integrity, security, and privacy are more crucial [32]. Thus, to protect the EHR from outside parties and threats, a unique blockchain-based optimization-based cryptography technique has been devised. Additionally, an optimization model and ensemble machine learning were constructed to identify systemic threats and demonstrate the effectiveness of the methodology.

## 4. PROPOSED METHODOLOGY

Designing a Hybrid Ant Lion and Grey Wolf-based Symmetric Key Encryption (HALGW-SKE) with Blockchain would help to increase the safety and confidentiality of healthcare data, which is the most difficult task in the medical profession. Furthermore, HALGW techniques are used to produce the ideal keys. Furthermore, an ensemble machine learning technique utilizing the optimization technique was created called EML-FFO to recognize and detect cloud-based threats. First, the system and system administrator may access is used to gather and train the patient dataset. Subsequently, initiatesan attack within the developed system to assess the effectiveness of the developed method and demonstrate its efficiency. Figure 1 shows the proposed model's architecture.

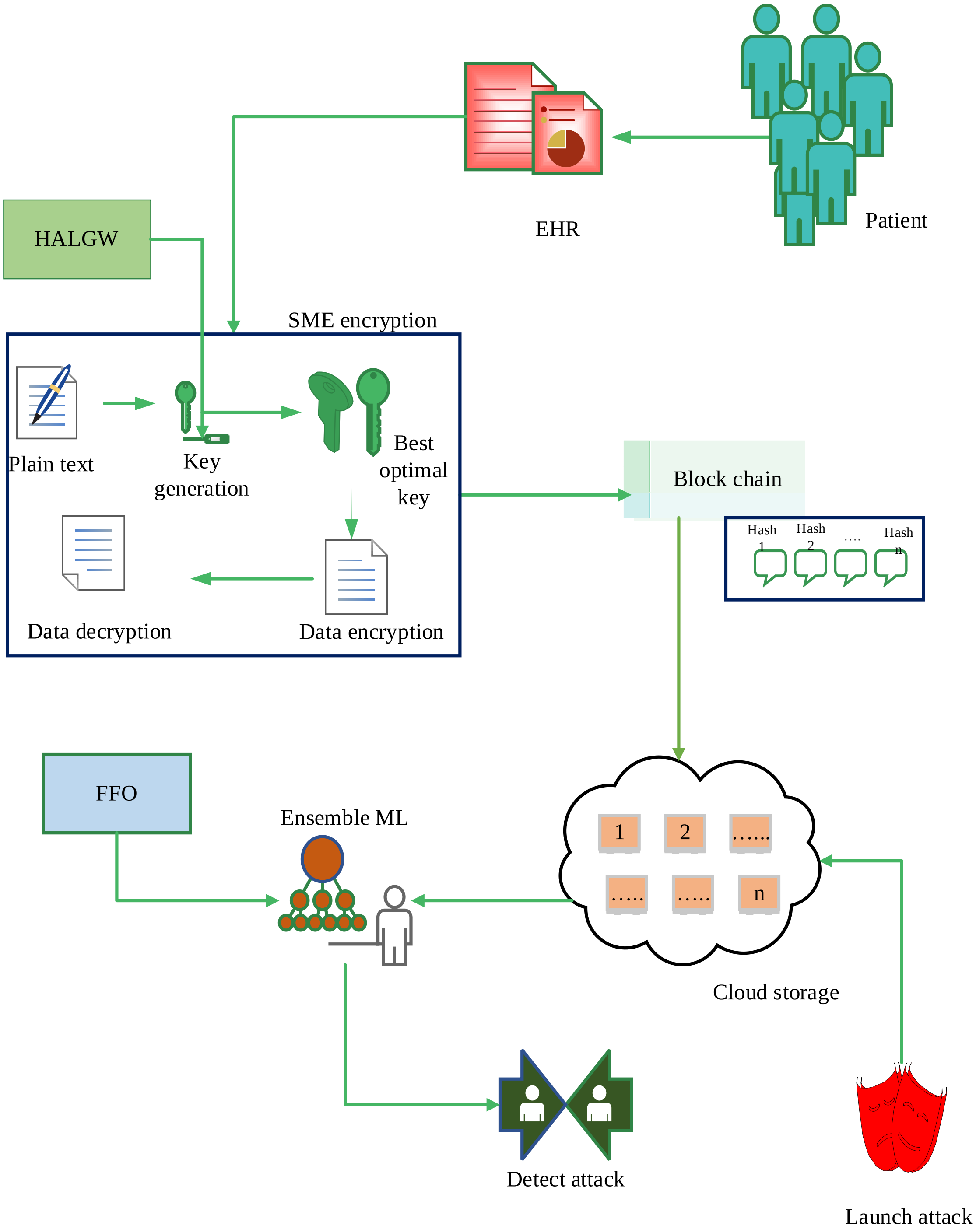

**Fig.1 Proposed methodology**

As a result, the EHR is kept in a cloud database that employs a single public key cryptography method to encrypt and decrypt data using SKE, producing a reliable blockchain solution for the EHR. The best and most optimal keys are generated during the key generation phase utilising HALGW to safeguard the healthcare data. Blockchain blocks are also validated, and every block has a hash function arranged chronologically. Then the hash value is generated using $h_{ash}12 = h_{ash}\left(h_{ash1} + h_{ash2}\right) = h_{ash}\left[\left(T_{x1}.h_{ash}\right) + \left(T_{x2}.h_{ash}\right)\right]$. Additionally, the earlier hash is useful for block validation because it is the hash of the earlier block. The block's creation time is also indicated by the timestamp. The Merkle tree is the architecture used to store a set of data in each block; Nonce is useful for producing hash values at a challenging level. The proposed technique encrypts EHR data and stores it in a cloud database while logging hash values.

### 4.1 HALGW-basedSME

Healthcare data that needs to be encrypted and decrypted using the same key is typically encrypted using the symmetric technique. For hospitals, service providers, and other approved medical institutions to exchange data, key generation is initially more crucial.

**Key generation phase:**It contains $K_{MK}$ primary key used to produce the session key. Update the HALGW model during this phase to produce the best possible key $K_g$ and improve key generation performance.

- **Hybrid ant lion and grey wolf model for best key generation**

The ALO approach [33] is used to model the interactions with ant lions and ants in a trap. To assist them become more adept at handling these encounters, ants are required to traverse the search area, and antlions are allowed to hunt and set traps. The ALO program simulates the interactions between caged ants and ant lions. A random walk is chosen to replicate the unpredictable behavior of ants during their food quest, as indicated by equation (1).

$$\vec{X}(t) = \left[0, C_s\left(2\vec{r}\left(t_1\right)-1\right), C_s\left(2\vec{r}\left(t_2\right)-1\right), \ldots\ldots C_s\left(2\vec{r}\left(t_n\right)-1\right)\right] \qquad (2)$$

Let, $C_s$ is considered as cumulative sum, and random walk $\vec{r}\left(t\right)$ is calculated using eqn. (2).

$$\vec{r}(t)=\left\{\begin{matrix}1 & if\vec{r}and>0.5\\ 0 & \vec{r}and\le 0.5\end{matrix}\right\} \qquad (3)$$

The location of the antlions is stored using equation (3).

$$\vec{L}(al)=\begin{bmatrix} al_{1,1} & al_{1,2} & .... & al_{1,f} \\ al_{2,1} & al_{2,2} & .... & al_{2,f} \\ . & . & . & . \\ al_{n,1} & al_{n,2} & ... & al_{n,f} \end{bmatrix} \qquad (4)$$

An equation. (2) is used to modify the ant locations. The equation. (5) is used to normalize the random walks to keep them within the area of the search.

$$\vec{X}_i^{\,t}=\frac{\left(\vec{X}_i^{\,t}-\vec{Z}_i\right)\times\left(\vec{E}_i-\vec{C}_i^{\,t}\right)}{\left(\vec{E}_i^{\,t}-\vec{Z}_i\right)}+\vec{C}_i \qquad (5)$$

Ants' random migration is impacted by ant lion traps. Equations (6) and (7) are utilized to capture the pits of ant lions.

$$\vec{C}_i^{\,t}=al_j^t+\vec{C}^t \qquad (6)$$

$$\vec{E}_i^{\,t}=al_j^t+\vec{E}^t \qquad (7)$$

The $\vec{C}$ and $\vec{E}$ create a hypersphere around a chosen ant lion, with the ants moving randomly within it.

During the key process selection, the following equations were supplied to replicate the social hierarchy of grey wolves [34]. The target location vector $L$, and the next position $g(i+1)$ are measured using eqn. (8) and (9).

$$L=\left|V\,\square\,g_{vt}(i)-g_v(i)\right| \qquad (8)$$

$$g(i+1)=g_{vt}(i)-U\,\square\,L \qquad (9)$$

Let $g_{vt}$ is denoted as target position vector, $i$ is considered as current iteration, $g_v$ is denoted as UAV position vector, $\square$ is denoted as an operator for multiplication of elements by elements, $U$ and $V$ are represented as coefficient vectors. Next, utilize Eqn. (10) to find a new position to simulate group behavior in the search space.

$$g\left(i+1\right)=\frac{\left(g_{v1}+g_{v2}+g_{v3}\right)}{3} \qquad (10)$$

Let, $g_{v1}$, $g_{v2}$, and $g_{v3}$ are the best three corresponding positions $\alpha,\beta,\delta$.

Tomaximize the chance of catching a new ant, if the ant has a higher level of work function than the selected ant lion, it will move on to the pursued ant's most recent site. To identify the best ideal key, the ALO's GW hunting behavior is updated during this step in the ALO prey-catching phase. Equation. (11) determines the fusion of GW hunting behavior in ALO.

$$\vec{F}_s=\left\{\begin{array}{ll} al_i^t & iff\left(al_i^t\right)>f\left(al_j^t\right) \\ g\left(i+1\right) & iff\left(g\left(i+1\right)\right)\leq f\left(g\left(i+1\right)\right) \end{array}\right\}_i^t \qquad (11)$$

Let, $al_i^t$ is denoted as the new position of the AL, $g\left(i+1\right)$ is denoted as the updated new position of GW. Using these two updated positions, the developed model selects the best optimal key using eqn. (12)

$$K_g=\vec{F}_s+\frac{K_{MK}}{S_{ky}}\left(h_{ash1}+h_{ash2}\right)B_1B_2 \qquad (12)$$

Let, $\vec{F}_s$ is denoted as the fitness of antlion, $S_{ky}$ is represented as a session key, $B_1$ and $B_2$ are considered as a bilinear pairing. Moreover, generated keys define the healthcare data using attributes $A_{0,}A_{1,}A_{2,}.....A_n$. Furthermore, session key generation is selecting the random numbers $rn0, rn1, rn2........rn(n), A_n \in S_{ky}$ for the main key $K_{MK}$.

**Hash value generation:**The generated key selects the hash by calculating the hash value $h_{ash}12=h_{ash}\left(h_{ash1}+h_{ash2}\right)=h_{ash}\left[\left(T_{x1}.h_{ash}\right)+\left(T_{x2}.h_{ash}\right)\right]$. Based on the hash value patient selects two random numbers as $\theta$ and $\mu$ from $K_{MK}$. Then the patient calculates the key proportional value which is obtained by Eqn. (13)

$$SK_g=\left(G=D^{(\theta+\mu)/\alpha} \bmod B_1\,B_2\right) \qquad (13)$$

Lastly, give patients and medical organizations access to the secured key for patient information. A session key $S_{ky}$ is generated so that the same key may be used to both encrypt and decrypt data. Thus, the session key is equivalent to the $xy = x(yB) = xyB$ likewise $yX = y(xB) = xyB$. Thus, this devised technique was used by doctors, system administrators, staff, and patients to share the key via a secure network. Figure 2 depicts the designed model's process.

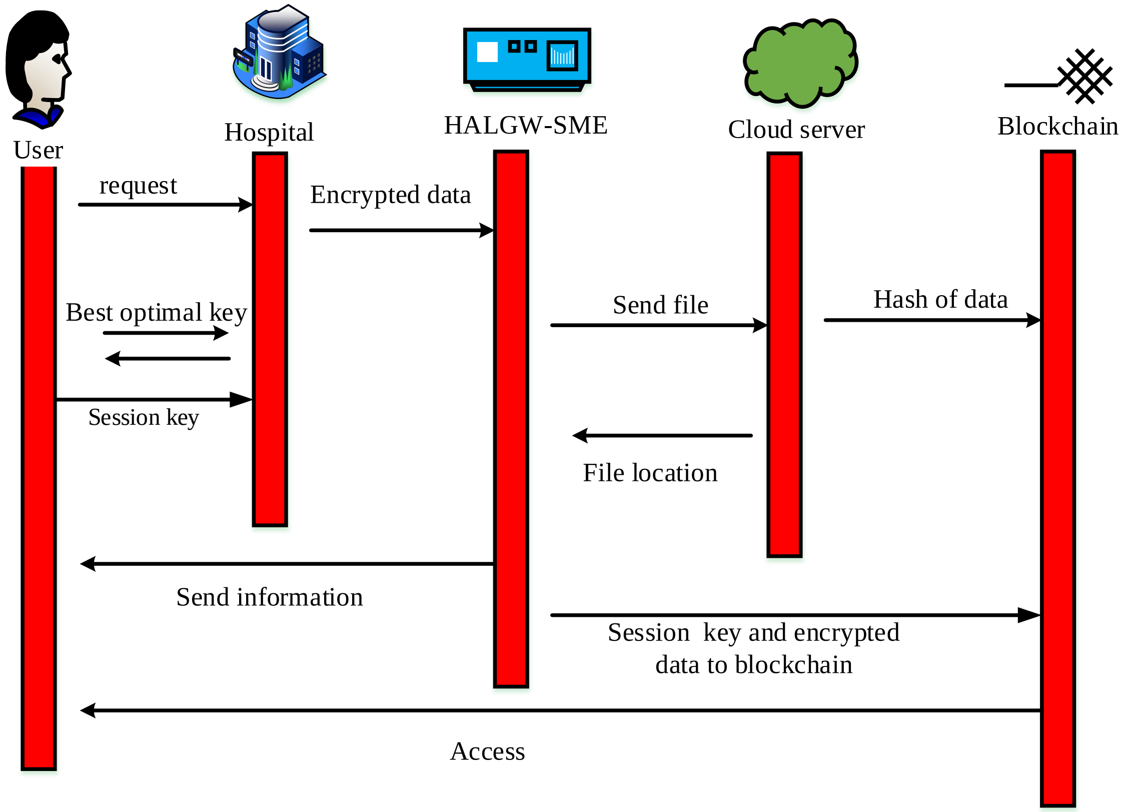

**Fig.2 Process of the designed HALGW-SKEmodel**

The hash function of the cryptographic technique takes in the data and outputs a fixed output of arbitrary size. The hash function $h_{ash}$ is also useful for message authentication and other types of authentications. In general, it is difficult to pinpoint the original messages using the hash value. Thus, Eqn. (14) is used to obtain the hash function.

$$h_{ash}(x) = h_{ash}(y) \quad (14)$$

Let, $x$ and $y$ are the two different messages. The data encryption of the healthcare data to the patients based on the attributes also the patient creates the appropriate pair of private keys to access the patient details $[Q_s(t)]$. Then the generated details are encrypted $g_k(s)$ and the description of the patient information is signed by a private key $Q_s(t)$. Afterward, patient information is utilized on the blockchain.

**Encryption:**Moreover, the designed model generates a random key $S^i_{sk}$ for processing encryption which encrypts the data and transfersit to the patient $P_{at}$. Then the encryption is obtained using Eqn. (15)

$$g_k(s)=S_{ky},Q_s(t)=S^i_{sk},\left(K_g=P_{at}\right)_{i\in S_{ky}}=P(t)\rightarrow c(t) \qquad (15)$$

Let, $P(t)$ is denoted as input data and $c(t)$ is considered as cipher text. Additionally, patient data are encrypted via random cloud locations using the private key $Q_s(t)$. Furthermore, modifications to the original data result in a hash value that is unable to guarantee the updated medical data.

**Blockchain:**Subsequently, the encrypted data is sent to the blockchain, where medical records are indexed chronologically. As a result, every block has a hash, and the contents are unchangeable. As a result, the healthcare patient receives the encrypted health data safely, which generates the session key $S_{ky}$. Additionally, if a patient is registered with the hospital, this enables the data to be kept in the blockchain and provides a file ID based on the IDs stored. Equations (16) and (17) provide the hash ID generated by the EHR in terms of

$$P_a\left(ID,S_{ky,}Address,\ folder,access\right) \qquad (16)$$

$$store\left(ID,S_{ky,}EHR\right)=hash\_ID \qquad (17)$$

The encrypted data is stored under, file address, folder address, and hash ID. Moreover, the patient encrypts and uploads the healthcare data of EHR to the cloud database which generates the session key and uploads the data into cloud storage. For the decryption process, the designed model verifies the session key, whether it is matched to the session key means to grant access to the patient and decrypt the data. Finally, the developed model secures medical data information or data and attains low processing time, encryption time, and decryption time.

### 4.2 Atack detection using ensemble ML and FFO

A cloud-based attack is launched to demonstrate the effectiveness of the built model, and the attack is identified through the use of EML and the FFO model. Three machine learning techniques—naïve Bayes, random decision trees, and simple logistic regression—were employed in the model's development. Ultimately, the approach of majority voting is employed to identify threats by analysing the output of each classifier. To improve the created model's prediction results, the FFO optimization is used in this phase.

#### 4.2.1 Simple Logistic Regression Model

One prominent option for modeling binary classifications is the LR classification method [35]. It is believed for this approach that a correlation between the input features equals the likelihood function of one of the two output categories. A full version of the logistic equation for the classification model is detailed in Eqn. (18).

$$L_r = \ln\left(\frac{W_i}{1-W_i}\right) \tag{18}$$

$W$ is the likelihood that an attack will occur $i$.

#### 4.2.2 Random Decision Tree

One of the well-liked supervised ML algorithms for the graphical illustration of every possible answer is the random decision tree [36]. The decisions are easily interpreted and are predicated on certain conditions. It recognizes and selects the important characteristics that aid in classification. It only chooses characteristics that yield the most information gain ($I_g$). $I_g$ is defined as eqn. (19).

$$I_g = e(pn) - Avge(chn) \tag{19}$$

Let, $pn$ is denoted as the parent node, and v is considered as the child node. The Entropy ($e$) is defined as eqn. (20).

$$e = \sum_i -p_i(\log_2 p_i) \tag{20}$$

$p_i$ is shown as the class's likelihood $i$.

### 4.2.3 Naïve Bayes Classification

The Naïve Bayes classification technique is usually recognized for its efficiency and ease of use. The Naïve Bayes classification system [37] is quick to construct and produces predictions quickly. A statistical classifier, Naïve Bayes calculates feature probabilities according to the target class. It assumes that the presence of one attribute does not affect the presence of the others. Naïve Bayes can perform much better though it relies on other attributes because it doesn't need precise probability estimations as long as the maximum probability is assigned to the right class. The foundation of it is the Bayes theorem, which asserts that Eqn. (21).

$$p(x/y)=\frac{p(y/x)\,p(x)}{p(y)} \tag{21}$$

Let, $p(x/y)$, and $p(y/x)$ are the contingent likelihoods that an attack will occur $x$ given that attack $y$ is true and vice versa.Moreover, $p(x)$ is denoted as prior probability, $p(y)$ is denoted as posterior probability, $p(y/x)$ is considered as a proposition, and $p(x/y)$ is represented as the possibility of classification.

### 4.2.4Majority voting

Voting by majority is a common method in ensemble categorization. Another name for it is plurality voting [38]. The method suggested a majority-based vote system to enhance the classification results following the application of the three previously stated classification algorithms. For every test case, these model classification values are computed, and the final output is anticipated using the results of the majority. In majority voting, each classifier's plurality vote using eqn. (22) is used to anticipate the target class attack.

$$z=\mathrm{mod}\,e\left\{L_r, I_g, p(x/y)\right\} \tag{22}$$

Update the FFO during the majority voting phase to efficiently identify and detect any attacks that may be present in the system through the use of firefly flashing behavior. The presented model uses the trend toward attractive firefly performance to identify optimal categorization outcomes.

**FFO:** The FFO is a heuristic approach [39] that draws inspiration from the bioluminescent transmission phenomena and the flashing behavior of fireflies. Since they are unisexual, fireflies will be drawn to one another irrespective of gender. The brightness of a firefly determines its attractiveness; a firefly with lower brightness will be drawn to one with higher brightness. But as the two fireflies got farther apart, the appeal diminished. The fireflies will fly at random if their brightness levels are the same. By chance stroll and firefly fascination, new solutions are generated.

The brightness of its attractiveness, $K$ of the firefly $i$ inside the firefly $j$ is determined by how brilliant the firefly $i$ and the distance $k_{ij}$ between the fireflies $i$ and $j$ as in Eqn. (23)

$$K(x)=\frac{K_s}{x^2} \qquad (23)$$

The firefly brightness $i$, is connected to the goal function $f(p_i)$ using $k_i$ is equivalent to the firefly solution $i$.

A firefly's brightness $K$ is selected to display the most current location of its fitness value $f(p)$ as in Eqn. (24).

$$K_i = f(p_i) \qquad (24)$$

Each firefly has a unique appeal rating, and the brighter one attracts and moves the less elegant one $\vartheta$. However, the value of appearance $\vartheta$ depends on how far apart the fireflies are from one another.The firefly's attraction function is determined by Equation (25).

$$\vartheta(x)=\vartheta_o e^{-\alpha x^2} \qquad (25)$$

where $\vartheta_o$ is denoted as the firefly attractiveness value at $k=0$ and $\alpha$ is considered as the light absorption coefficient of the medium.

The firefly's movements $i$ at position $k_i$ shiftto a firefly that is more luminous $j$ at position $k_j$ byeqn. (26).

$$p_i\left(t+1\right)=p_i\left(t\right)+\vartheta_o e^{-\alpha x^2}\left(p_i-p_j\right)+\alpha\sigma_i,\vartheta_o=0 \qquad (26)$$

where $\vartheta_o e^{-\alpha x^2}\left(p_i-p_j\right)$is owing to the firefly's attraction $p_j$and $\alpha\sigma_i$is considered asa randomization parameter;if $\vartheta_o=0$then it appears to be just a basic, random movement.The new firefly position's attractiveness is compared to the previous one by the algorithm. The firefly is relocated to the new location if it yields a higher attraction rating; if not, it stays in its existing location. The FA's termination criterion is based on either a predetermined fitness value or an arbitrary predetermined number of iterations.

Using Equation, the brightest firefly travels at random (27).

$$p_i\left(t+1\right)=p_i\left(t\right)+\alpha\sigma_i \qquad (27)$$

Lastly, use eqn. (23) to adjust the brightest firefly's random movement during the majority voting phase torecognize and detect attacks.

$$z=\text{mod}\,e\left\{L_r,I_g,p\left(x/y\right)*p_i\left(t+1\right)\right\} \qquad (28)$$

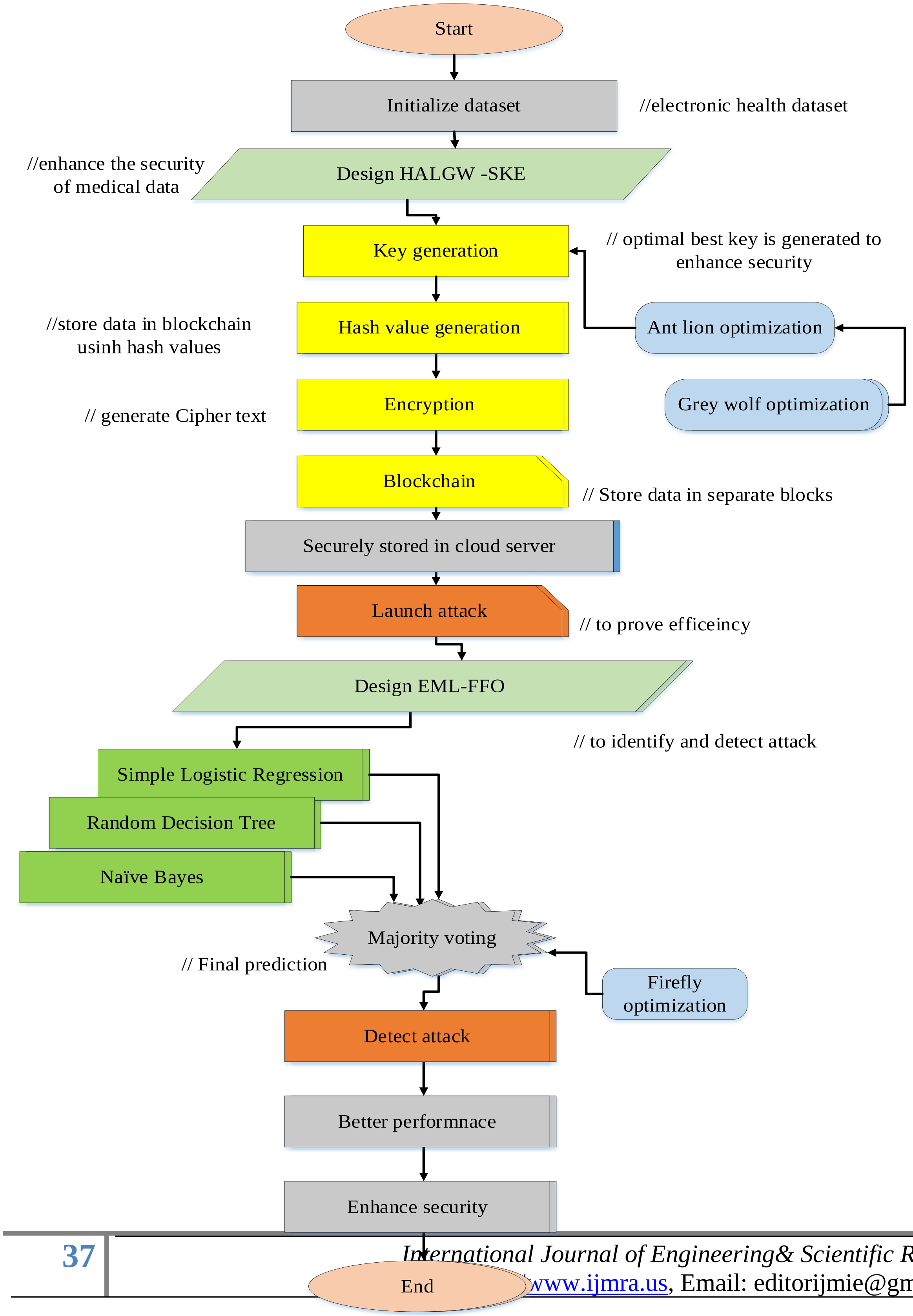
Start
Initialize dataset
//electronic health dataset
//enhance the security of medical data
Design HALGW -SKE
Key generation
// optimal best key is generated to enhance security
//store data in blockchain usinh hash values
Hash value generation
Ant lion optimization
Encryption
// generate Cipher text
Grey wolf optimization
Blockchain
// Store data in separate blocks
Securely stored in cloud server
Launch attack
// to prove efficeincy
Design EML-FFO
// to identify and detect attack
Simple Logistic Regression
Random Decision Tree
Naïve Bayes
Majority voting
// Final prediction
Firefly optimization
Detect attack
Better performnace
Enhance security
End

**Fig.3 Flowchart of the developed model process**

The created EML-FFO model uses majority voting and FFO behavior to efficiently identify the assaults that are present in the system. Furthermore, it is capable of recognizing and detecting assaults within the cloud environment. This method is aimed at protecting medical data on the cloud and improving people's lives at the same time. The flowchart representation of the developed model process is shown in fig.3.

## 5. RESULTS AND DISCUSSIONS

The suggested HALGW-SKE scheme is first implemented in a Python tool, and the effectiveness of the generated model is evaluated in comparison to other existing methods in terms of processing, decryption, and encryption times. The newly proposed solution uses blockchain technology to encrypt and secure data, and it employs the EML-FFO model to detect attacks and protect the data from unauthorized access. To confirm the efficacy of the proposed scheme, a subsequent score of the planned model is validated using other existing models.

### 5.1 Performance Assessment for HALGW-SKE model

Python is used to implement the developed HALGW-SKE paradigm. Acquired performance measurements are also verified concerning accuracy, processing time, precision, encryption time, decryption time, etc. Thus, the achieved performance is validated with other prevailing methods such asHIDT [21], PoFDL [22], EHO-OBL [29], and HE-OHS [26].

### 5.1.1 Encryption Time (ET)

ET is defined as the amount of time required by the designed system to convert plain text into ciphertext. It is employed in the computation of the encryption technique. The effectiveness of the established approach and the rate of encryption is also shown by the encryption time.

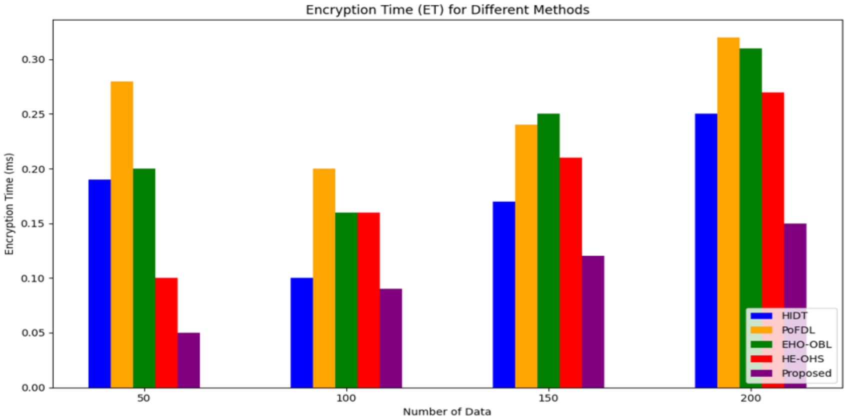

**Fig.4 Comparison of encryption time**

Additionally, the created technique's encryption time of 0.05 ms was achieved by utilizing 50 data points, and the obtained findings are contrasted with those of other current approaches, including HIDT, PoFDL, EHO-OBL, and HE-OHS. Additionally, utilizing 50 data, the HIDT model achieves 0.19s, PoFDL achieves 0.28s, EHO-OBL achieves 0.2s, and the HE-OHS model gains 0.1ms. The created framework achieves reduced ET when compared to other strategies; the ET comparison is displayed in Figure 4.

### 5.1.2 Decryption Time (DT)

DT is often determined by measuring the amount of time needed to decrypt a text and then extract the plain text from the decrypted text. Moreover, one of the methods used to translate encrypted data is decryption, which is the reverse of encryption. The processing time comparison is displayed in Figure 5.

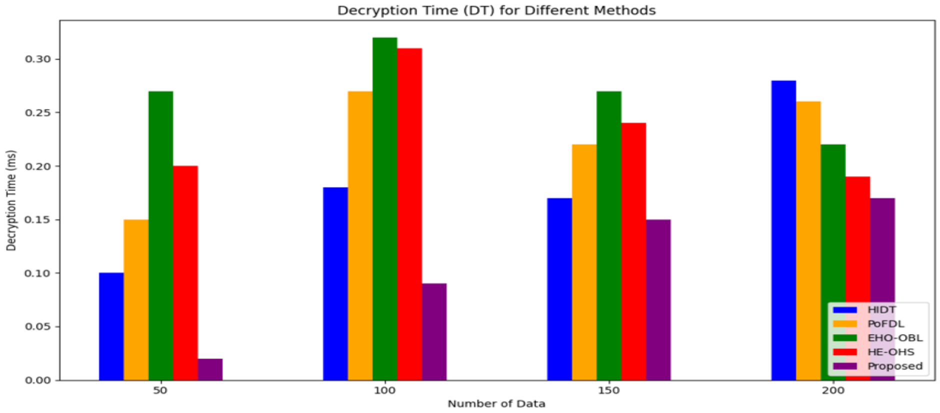

**Fig.5 Comparison of decryption time**

Additionally, the created technique's DT of 0.02 ms was achieved by utilizing 50 data points, and the obtained findings are contrasted with those of other current approaches, including HIDT, PoFDL, EHO-OBL, and HE-OHS. Additionally, utilizing 50 data, the HIDT model achieves 0.1s, PoFDL achieves 0.15s, EHO-OBL achieves 0.27s, and the HE-OHS model gains 0.2ms. The created framework achieves reduced DT when compared to other strategies.

### 5.1.3 Processing time

The time elapsed between a patient's request for healthcare data and when that data is accessed at a specific point in time is known as the processing time. Additionally, the overall amount of time spent collecting and storing patient data. The total time spent on the blockchain during the entire procedure is used to compute the processing time.

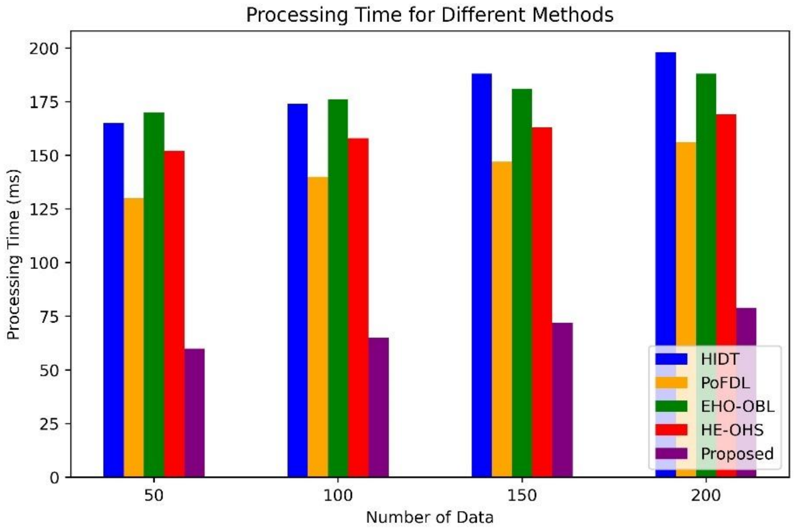

**Fig.6 Comparison of processing time**

Additionally, the proposed technique's processing time reached 60 ms for 50 data points, and the obtained results are contrasted with those of other currently in use approaches including HIDT, PoFDL, EHO-OBL, and HE-OHS. Additionally, utilizing 50 data, HIDT achieved 165 ms, PoFDL 130 ms, EHO-OBL 170 ms, and HE-OHS 152 ms. The created framework achieves a lower processing time when compared to previous methodologies; the processing time comparison is displayed in Figure 6.

### 5.1.4 Accuracy

The ability of a system to accurately detect and categorize attacks while reducing false prediction results is referred to as accuracy.Accuracy is 'the extent to which the outcome of a measurement adheres to the accurate value. It basically means the proximity of a test to its desired value.

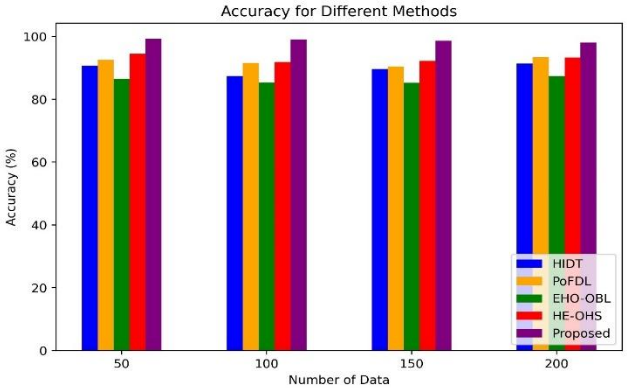

**Fig.7 Comparison of accuracy**

Additionally, employing 50 data, the proposed technique's accuracy reached 99.23%, and the findings are compared to those of other existing approaches like HIDT, PoFDL, EHO-OBL, and HE-OHS. Additionally, utilizing 50 data, HIDT achieved 90.63 percent, PoFDL attained 92.54 percent, EHO-OBL attained 86.53 percent, and HE-OHS attained 94.44 percent. The created framework achieves excellent accuracy when compared to previous methodologies; the accuracy comparison is displayed in Figure 7.

### 5.1.5 Precision

One important indicator of a detection system's effectiveness is precision. Precision is a metric used to evaluate a system's accuracy. It counts the percentage of attacks that are correctly recognized among all cases.

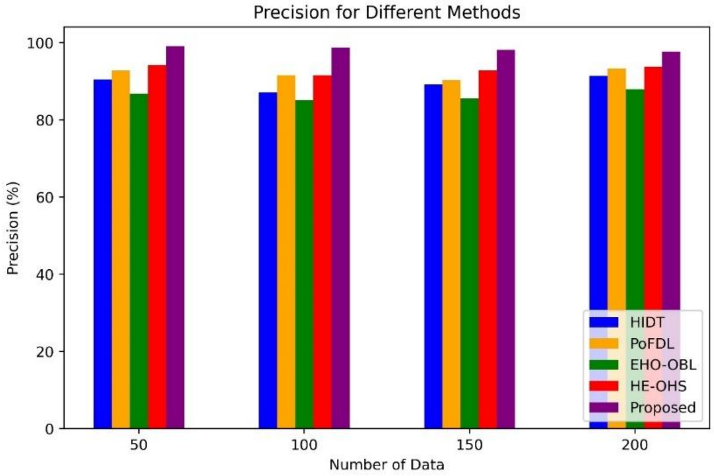

**Fig.8 Comparison of accuracy**

Additionally, employing 50 data, the proposed technique's precision reached 99.11 percent, and the findings are compared to those of other current techniques such as HIDT, PoFDL, EHO-OBL, and HE-OHS. Additionally, utilizing 50 data, HIDT achieved 90.45 percent, PoFDL attained 92.77 percent, EHO-OBL attained 86.78 percent, and HE-OHS attained 94.21 percent. The created framework achieves excellent precision when compared to previous techniques; the precision comparison is displayed in Figure 8.

**Recall**

Recall is an assessment that assesses a system's capacity to accurately recognize all pertinent attack incidents. The ratio of precisely recognized attacks to the total number of missed attacks is used to compute recall.

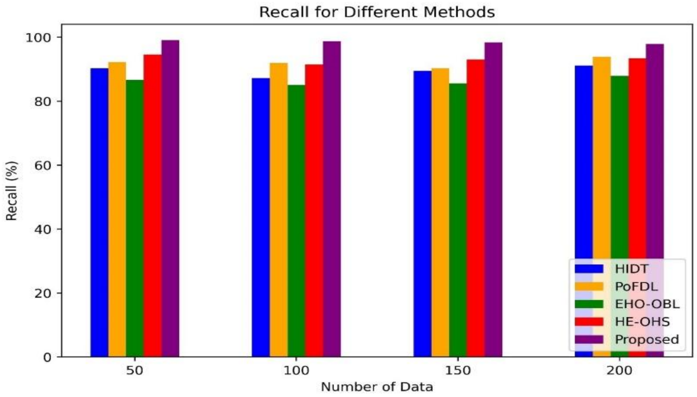

**Fig.9 Comparison of recall**

Additionally, employing 50 data, the created technique's recall rate reached 99.06 percent. The obtained findings are compared to those of other current approaches, including HIDT, PoFDL, EHO-OBL, and HE-OHS. Additionally, utilizing 50 data, HIDT achieved 90.20 percent, PoFDL attained 92.21 percent, EHO-OBL attained 86.65 percent, and HE-OHS attained 94.56 percent. The created framework achieves high recall when compared to previous methodologies; the recall comparison is displayed in Figure 9.

**F-measure**

A machine learning algorithm's effectiveness is assessed using a metric called the F-measure. It yields a single score that incorporates recall and precision.

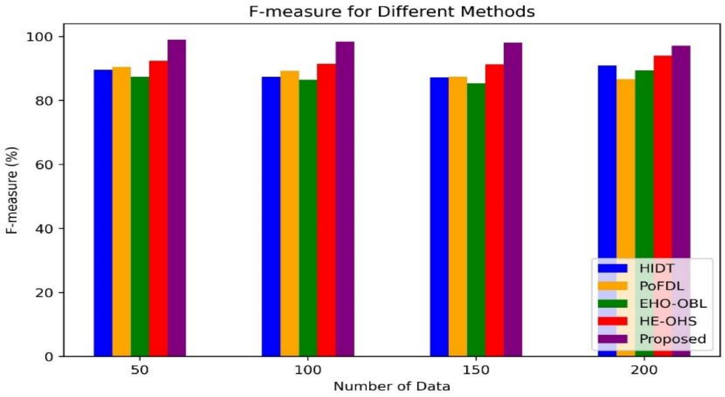

**Fig.10 Comparison of F-measure**

Additionally, the developed technique's F-measure reached 99 percent with 50 data, and the results obtained are compared with those of other current techniques such as HIDT, PoFDL, EHO-OBL, and HE-OHS. Additionally, utilizing 50 data, HIDT achieved 89.56 percent, PoFDL achieved 90.45 percent, EHO-OBL achieved 87.43 percent, and HE-OHS achieved 92.43 percent. The developed framework achieves a high F-measure when compared to previous methodologies; the comparison of F-measures is displayed in Figure 10.

## 6. CONCLUSIONS

This study proposes a blockchain-based HALGW-SKE system to safeguard and secure cloud-based medical data. Additionally, the EML-FFO framework was created by recognizing and detecting cloud-based threats. Here, the developed technique makes use of optimization, ML, and encryption techniques. Additionally, the best optimum key is chosen using a hybrid ALO and GWO technique to increase security. The hash values are produced to securely store encrypted data in the blockchain. Furthermore, the cloud assault using FFO is identified and predicted by three machine learning classifiers. The suggested method produced superior outcomes. The encryption, decryption, accuracy, F-measure, processing time, precision, recall, and encryption and decryption times of the suggested technique are also compared. As a result, the developed model achieved a high accuracy of 99.23 percent and a reduced processing time of 60 ms. The developed method raises the attack detection rate and strengthens the security and privacy of medical data in this way.

## REFERENCES

1. Wu, H., Dwivedi, A.D. and Srivastava, G., 2021. Security and privacy of patient information in medical systems based on blockchain technology. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 17(2s), pp.1-17.
2. Shah, V., Thakkar, V. and Khang, A., 2023. Electronic health records security and privacy enhancement using blockchain technology. In Data-Centric AI Solutions and Emerging Technologies in the Healthcare Ecosystem (pp. 1-13). CRC Press.
3. Ali, A., Rahim, H.A., Pasha, M.F., Dowsley, R., Masud, M., Ali, J. and Baz, M., 2021. Security, privacy, and reliability in digital healthcare systems using blockchain. Electronics, 10(16), p.2034.
4. Chen, Z., Xu, W., Wang, B. and Yu, H., 2021. A blockchain-based preserving and sharing system for medical data privacy. Future Generation Computer Systems, 124, pp.338-350.
5. Egala, B.S., Pradhan, A.K., Badarla, V. and Mohanty, S.P., 2021. Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet of Things Journal, 8(14), pp.11717-11731.
6. Liu, H., Crespo, R.G. and Martínez, O.S., 2020, July. Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts. In Healthcare (Vol. 8, No. 3, p. 243). MDPI.
7. Zhang, R., Xue, R. and Liu, L., 2021. Security and privacy for healthcare blockchains. IEEE Transactions on Services Computing, 15(6), pp.3668-3686.
8. Zou, R., Lv, X. and Zhao, J., 2021. SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. Information Processing & Management, 58(4), p.102604.
9. Wang, M., Guo, Y., Zhang, C., Wang, C., Huang, H. and Jia, X., 2021. MedShare: A privacy-preserving medical data sharing system by using blockchain. IEEE Transactions on Services Computing.

10. Sharma, P., Borah, M.D. and Namasudra, S., 2021. Improving security of medical big data by using Blockchain technology. Computers & Electrical Engineering, 96, p.107529.
11. Wang, B. and Li, Z., 2021. Healthchain: A privacy protection system for medical data based on blockchain. Future Internet, 13(10), p.247.
12. Wu, G., Wang, S., Ning, Z. and Zhu, B., 2021. Privacy-preserved electronic medical record exchanging and sharing: A blockchain-based smart healthcare system. IEEE Journal of Biomedical and Health Informatics, 26(5), pp.1917-1927.
13. Zhang, G., Yang, Z. and Liu, W., 2022. Blockchain-based privacy preserving e-health system for healthcare data in cloud. Computer Networks, 203, p.108586.
14. Alzubi, O.A., Alzubi, J.A., Shankar, K. and Gupta, D., 2021. Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things. Transactions on Emerging Telecommunications Technologies, 32(12), p.e4360.
15. Meisami, S., Beheshti-Atashgah, M. and Aref, M.R., 2021. Using blockchain to achieve decentralized privacy in IoT healthcare. arXiv preprint arXiv:2109.14812.
16. Huang, H., Zhu, P., Xiao, F., Sun, X. and Huang, Q., 2020. A blockchain-based scheme for privacy-preserving and secure sharing of medical data. Computers & Security, 99, p.102010.
17. Zarour, M., Ansari, M.T.J., Alenezi, M., Sarkar, A.K., Faizan, M., Agrawal, A., Kumar, R. and Khan, R.A., 2020. Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records. IEEE Access, 8, pp.157959-157973.
18. Miyachi, K. and Mackey, T.K., 2021. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Information Processing & Management, 58(3), p.102535.
19. Jayabalan, J. and Jeyanthi, N., 2022. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. Journal of Parallel and Distributed Computing, 164, pp.152-167.

20. Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M. and Abid, M., 2021. HealthBlock: A secure blockchain-based healthcare data management system. Computer Networks, 200, p.108500.
21. Mishra, S., 2023. Blockchain and Machine Learning-Based Hybrid IDS to Protect Smart Networks and Preserve Privacy. Electronics, 12(16), p.3524.
22. Hamouda, D., Ferrag, M.A., Benhamida, N. and Seridi, H., 2023. PPSS: A privacy-preserving secure framework using blockchain-enabled federated deep learning for industrial IoTs. Pervasive and Mobile Computing, 88, p.101738.
23. Sezer, B.B., Turkmen, H. and Nuriyev, U., 2023. PPFchain: A novel framework privacy-preserving blockchain-based federated learning method for sensor networks. Internet of Things, 22, p.100781.
24. Ali, A., Al-Rimy, B.A.S., Alsubaei, F.S., Almazroi, A.A. and Almazroi, A.A., 2023. HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. Sensors, 23(15), p.6762.
25. Guduri, M., Chakraborty, C. and Margala, M., 2023. Blockchain-based federated learning technique for privacy preservation and security of smart electronic health records. IEEE Transactions on Consumer Electronics.
26. Vatambeti, R., Krishna, E.P., Karthik, M.G. and Damera, V.K., 2023. Securing the medical data using enhanced privacy preserving based blockchain technology in Internet of Things. Cluster Computing, pp.1-13.
27. Li, C., Dong, M., Xin, X., Li, J., Chen, X.B. and Ota, K., 2023. Efficient privacy-preserving in IoMT with blockchain and lightweight secret sharing. IEEE Internet of Things Journal.
28. Miao, J., Wang, Z., Wu, Z., Ning, X. and Tiwari, P., 2024. A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things. Expert Systems with Applications, 237, p.121329.

29. Verma, G., 2024. Blockchain-based privacy preservation framework for healthcare data in cloud environment. Journal of Experimental & Theoretical Artificial Intelligence, 36(1), pp.147-160.
30. Keshta, I. and Odeh, A., 2021. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), pp.177-183.
31. Song, J., Zhang, P., Alkubati, M., Bao, Y. and Yu, G., 2022. Research advances on blockchain-as-a-service: Architectures, applications and challenges. Digital Communications and Networks, 8(4), pp.466-475.
32. Ahmad, G.I., Singla, J. and Giri, K.J., 2021. Security and Privacy of E-health Data. Multimedia Security: Algorithm Development, Analysis and Applications, pp.199-214.
33. Assiri, A.S., Hussien, A.G. and Amin, M., 2020. Ant lion optimization: variants, hybrids, and applications. IEEE Access, 8, pp.77746-77764.
34. Makhadmeh, S.N., Al-Betar, M.A., Doush, I.A., Awadallah, M.A., Kassaymeh, S., Mirjalili, S. and Zitar, R.A., 2023. Recent advances in Grey Wolf Optimizer, its versions and applications. IEEE Access.
35. Schober, P. and Vetter, T.R., 2021. Logistic regression in medical research. Anesthesia and analgesia, 132(2), p.365.
36. Charbuty, B. and Abdulazeez, A., 2021. Classification based on decision tree algorithm for machine learning. Journal of Applied Science and Technology Trends, 2(01), pp.20-28.
37. Kurniawan, Y.I., Razi, F., Nofiyati, N., Wijayanto, B. and Hidayat, M.L., 2021. Naive Bayes modification for intrusion detection system classification with zero probability. Bulletin of Electrical Engineering and Informatics, 10(5), pp.2751-2758.
38. Bamhdi, A.M., Abrar, I. and Masoodi, F., 2021. An ensemble based approach for effective intrusion detection using majority voting. Telkomnika (Telecommunication Computing Electronics and Control), 19(2), pp.664-671.

39. Wu, J., Wang, Y.G., Burrage, K., Tian, Y.C., Lawson, B. and Ding, Z., 2020. An improved firefly algorithm for global continuous optimization problems. Expert Systems with Applications, 149, p.113340.

**Author Biography**

Ajay Chandra MK( Ajay Chandra Manukondakrupa) is a seasoned professional with a master's degree in computer science and a remarkable career spanning over 24 years in the technology space. His journey through various domains, including Automobile, Pharma, Retail, Banking, and Telecom, has established him as a versatile and accomplished leader. Throughout his career, Ajay has honed his expertise in automation and the implementation of Enterprise Applications and ERP systems, playing a pivotal role in digital transformation projects across industries. His ability to conceptualize and execute comprehensive tech strategies, coupled with a strong aptitude for communication and response management, has been a hallmark of his success. Ajay has held influential positions at renowned organizations, including the World Bank, AbbVie, Ford Motors, Sephora, and currently working as Global Technical Program Manager for a telecommunications and satellite Organization. In these roles, he served as a technical program manager, overseeing cloud computing and SAP S4 HANA implementations. His leadership and technical acumen have contributed significantly to these companies' growth and digital evolution. Ajay Manukonda's career is a testament to his dedication to the ever-evolving world of technology and his profound impact on digital transformation in diverse sectors. His commitment to innovation and excellence continues to drive his career forward, making him a true luminary in the field of technology and enterprise solutions.