


## RESEARCH ARTICLE

# HECC-ABE: A novel blockchain-based IoT healthcare data storage using hybrid cryptography schemes with key optimization by hybrid meta-heuristic algorithm

Anil Kumar Dubey<sup>1</sup>  Associate Professor | N. Ramanjaneyulu<sup>2</sup> Associate Professor | Mala Saraswat<sup>3</sup> Assistant Professor | G. Brammya<sup>4</sup> Research Associate | Chinnaraj Govindasamy<sup>5</sup> Associate Professor | N. S. Ninu Preetha<sup>4</sup> Research Associate

<sup>1</sup>CSE Department, ABES Engineering College, Ghaziabad, India

<sup>2</sup>Rajeev Gandhi Memorial College of Engineering and Technology, Nandyala, India

<sup>3</sup>School of Computer Science Engineering & Technology, Bennett University, Greater Noida, India

<sup>4</sup>Resbee Info Technologies Private Limited, Thuckalay, India

<sup>5</sup>Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India

## Correspondence

Anil Kumar Dubey, CSE Department, ABES Engineering College, Ghaziabad, India.

Email: [anildudenish@gmail.com](mailto:anildudenish@gmail.com)

## Abstract

The most contemporary development in information technology is the Internet of Things (IoT), which integrates the digital world with the real world. It makes it possible for things and people to communicate via the Internet. Blockchain is one of the popular topics of interest right now, and it can be used in most IoT applications. The blockchain's salient characteristics, like decentralization, data integrity, confidentiality, protection, and openness, are the main reasons for implementing it in healthcare services. Hence, this paper introduces an effective approach for storing IoT-based healthcare data storage in the blockchain. The procedures in this suggested paradigm are as follows: user authentication, user trust verification, and optimal key storage in the blockchain. Wearable sensors are inserted in or adhered to a patient's body and used by IoT networks to gather healthcare data. These details are supplied into the verification structure constructed by adaptive dilated long short term memory with attention network (AD-LSTM-AN). Once the user's authentication is confirmed, then the user's trust level is computed. The same AD-LSTM-AN-based verification structure is used to verify the historical data that has been stored and retrieved by the user, together with their previous transactions, in this phase. The healthcare data are then sent to the hybrid elliptic curve cryptography with attribute-based encryption (HECC-ABE) cryptography schemes for data encryption once the authentication of the person who attempts to store the data is confirmed. An adaptive final position-based golden eagle-Harris hawks optimization (AFP-GEHHO) algorithm is used for optimizing the keys of the encrypted data. The blockchain platform stores the encrypted data of the authorized user with a high level of trust. The same process is done in reverse order whenever a user needs to recover information that is saved in the blockchain to retrieve the initially stored healthcare data. The effectiveness of secure data storage in blockchain is tested through experimental simulations. Throughout the analysis, the designed model achieves 96% in terms of accuracy. Thus, the developed model shows more secure and effective, has less error and reduces the time and memory requirements compared to existing approaches.

## 1 | INTRODUCTION

Transportation, smart cities, and communication are some of the data-driven implications and facilities provided by the growth of IoT.<sup>1</sup> Healthcare platforms are one of the applications of IoT where many sensors are linked and coordinated to establish an IoT<sup>2</sup> system specifically for evaluating healthcare data. The most delicate and data-critical industry is healthcare, which requires constant patient health monitoring via various sensing devices.<sup>3</sup> The technique that uses middleware to gather data from various wearable sensor devices includes healthcare-based IoT.<sup>4</sup> In this way, an internal remote healthcare observation system is established by installing various sensing devices surrounding the patient's facilities. This network detects and transfers information collected by the sensing devices to nearby equipment or websites. Despite its numerous advantages, incorporating IoT into healthcare systems poses several difficulties concerning the safety and confidentiality of the collected data about the patient.

Data regarding the health conditions of a patient mostly contains private and delicate details about the identity of the patient, their health history, and even medical images of their medical examination or scans, which might be compromised or leaked and leads to the life of the patient to danger.<sup>5</sup> Because lots of sensor hubs are always connected in this IoT<sup>6</sup> ecosystem, it is vulnerable to privacy problems, including manipulation of data and espionage.<sup>7</sup> This raises major privacy issues in the healthcare industry since data corruption can lead to incorrect diagnoses, which even leads to the patient's death.<sup>8</sup> This information is possibly transmitted through a system that may not be trustworthy and kept on centralized systems in a healthcare facility, leaving it vulnerable to a number of assaults and leakages.<sup>9</sup> The centralized information storage system leads to a number of problems, including Denial of Service (DoS), hacking of patients' health and personal information, and untrustworthy third-party intervention to store healthcare data.<sup>10</sup> However, conventional strategies for the confidentiality and safety of patient information storage systems are ineffective in healthcare settings because of the intensive memory and computation processes, and the interference of noises in the gathered information reduces the data's usefulness in smart healthcare.<sup>11</sup>

Studies suggested using blockchain in medical facilities to avert these security and confidentiality problems. Blockchain is an open, unchangeable, and time-stamped decentralized platform that uses cryptographical security and peer-to-peer connectivity for saving and transferring information.<sup>12</sup> The blockchain network consists of a number of processing units that verify every demanded transaction and save its details.<sup>13</sup> Blockchain has been proven to offer confidentiality, effectiveness, and openness when implemented in an environment of sharing information.<sup>14</sup> Blockchain is a viable alternative for information sharing and preservation in healthcare IoT because of its exceptional features. Its distributed aspect solves the single-point-of-attack problem by removing the requirement of the patients and the hospital's administration to trust a centralized information storing system.<sup>15</sup> Patients' information cannot be erased or fraudulently altered because of blockchain's irreversibility and immutability characteristics.<sup>16</sup> Additionally, the confidentiality of the patients is maintained by the incognito function, which gives fake names rather than the individuals' actual identity.<sup>17</sup> Despite its many benefits, blockchain faces a number of drawbacks, including adaptability, energy demand, latency, and storage cost in case of a huge network.<sup>18</sup> Using blockchain in IoT programs with numerous devices engaged leads to even greater challenges with regard to the above-mentioned concerns. In an IoT system, enormous amounts of information are transmitted, saved, and processed, which results in significant networking and storage expenses and computational delays. The use of blockchain is not simple, especially in non-delay-resistant healthcare networks with storage and computing resource limitations.<sup>19</sup> Experts have suggested a few strategies for using blockchain in IoT to address these problems. Some of the strategies for securely storing and retrieving medical data in and from the blockchain are developed in this paper.

Some of the main functions that are implemented in this work are given below.

1. To develop a system to securely store medical data in the blockchain using hybrid cryptography schemes together with user authentication and user trust verification to enhance the security of the system further.
2. To implement a hybrid cryptography scheme known as HECC-ABE by combining elliptic curve cryptography (ECC) along with the attribute-based encryption (ABE) scheme in order to encrypt the medical data before storing it in the blockchain and decrypt the medical data after retrieving it from the blockchain.
3. To execute an advanced optimization technique called AFP-GEHHO algorithm for the purpose of optimizing the keys in the HECC-ABE cryptography scheme, hidden neurons in the AD-LSTM-AN, epoch count in AD-LSTM-AN, and steps per epoch in AD-LSTM-AN.
4. To design a novel heuristic-aided classifier called AD-LSTM-AN for user authentication and trust verification of the user before storing the medical data to the blockchain and before retrieving the medical data from the blockchain with parameters optimization by the developed AFP-GEHHO algorithm.

5. To verify and validate the security of the proposed AFP-GEHHO-ADLSTMAN classifier and the AFP-GEHHO-HECC-ABE cryptography schemes by contrasting and comparing them with existing classifiers, algorithms, and cryptography schemes.

The organization of the paper is as follows. In the second portion of the paper, the existing works regarding medical data storage in the blockchain and its advantages and disadvantages are discussed. In the third portion, a secure healthcare IoT data storage in blockchain using hybrid cryptography with keys optimization by hybrid meta-heuristic algorithms is discussed elaborately. In the fourth portion, the user authentication and trust verification for secured healthcare IoT data storage in blockchain with deep learning strategies are developed, and its development process is explained. In the fifth portion, the optimal key-based hybrid cryptography for secure healthcare IoT data storage in blockchain using hybrid meta-heuristic algorithms is given in detail. The sixth portion discusses the results and the analysis that is carried out to verify the security and the performance of the system. And the seventh portion provides the overall summary of the developed work.

## 2 | LITERATURE SURVEY

### 2.1 | Related works

In 2020, Rathee et al.<sup>26</sup> suggested a secure structure for multimedia healthcare data using blockchain by producing hashes for every piece of information in which any modification or adjustment in data or transgression of medicines can be exposed to all the users in the blockchain network. The experimental outcomes were compared and verified with the traditional methods. Because of the utilization of blockchain for security purposes, this model produced an enhanced simulation output of 86% success rate in the dropout ratio of products, wormholes as well as fake attacks, and probabilistic verification.

In 2021, Arul et al.<sup>27</sup> developed adaptive service compliance (BASC) to prevent non-dormant healthcare services for blockchain-based applications. The issues regarding dormancy were overcome by this method. The type of required user assistance was exposed earlier by this suggested compliance. The data was shared with end users using a distributed ledger. Till the requirement of users was fulfilled, the recommended compliance was valid by validating the truthfulness of the transferred information. A back-propagation learning approach was employed for determining the available ledger's accessibility. The results contained affordability verification and verification of background for the integrity of information validation. The subsequent ledger revealed a new perspective on information sharing that was brought on by veracity incapacity. This helped to prevent service postponements, and healthcare services failure, enhanced honesty, and enhanced access to the network at different intervals.

In 2021, Aujla and Jindal<sup>22</sup> proposed a detached ledger strategy. In order to safely send medical information collected by sensing devices to edge hubs, this method used the adjacent edge equipment to build detached blocks in blockchain. The progressive tensor-based technique was used by the edge hubs to transfer and save the information in the cloud. The duplication of the transferred data was reduced as a result of this method. Considering the time for preparing the blocks, the time for producing the header, the elimination of the tensor ratio, and the possibility of error, the findings demonstrated the efficacy of the suggested method.

In 2021, Ersoy et al.<sup>41</sup> presented a MetaRepo approach that helps users securely store digital assets. Especially, the author has developed a new user engine, transaction center, repos models, authenticator engine, and blockchain structure have been for security mechanisms, transaction processing, and user interaction. The MetaRepo is proposed for the testing and evaluation processes. This mechanism is aimed at users who can communicate with diverse metaverse universes and platforms without the need for extra verification and security metrics.

In 2021, Gurfidan et al.<sup>43</sup> developed a blockzincir-based music wallet approach for safe and legal listening of audio files. Here, the audio files chosen from users were transformed into blockchain formation using diverse approaches and algorithms that keep saved into the user's music wallet. The performance comparisons have taken place regarding the length of time on a normal audio player.

In 2021, Mohammad et al.<sup>24</sup> suggested a framework that would allow data owners to specify the accessibility to their sensitive medical data. For the purposes of information transfers and saving policies of accessibilities, BC-health was made up of two distinct chains. By using a clustering strategy, they were able to showcase the issues in blockchain, such as durability, latency, and complexity. The in-depth experiments they have conducted demonstrated

BC-Health's effectiveness concerning processing time and computing time, as well as its resistance to various attacks on security.

In 2021, Sharmila and Jaisankar<sup>25</sup> formulated an edge intelligent agent hybrid hierarchical blockchain framework (EiA-H2B). First, they suggested a highly secure, physically unclonable functions (PUF)-based user authorization method. Second, they suggested a virtual grouping based on high voting. Thirdly, they suggested an attention matrix-based gated recurrent unit (AM-GRU) for generating a scheme for scheduling MAC duty cycle and allocated the time slots for preventing retransmission and packet losses. Fourth, the selection of routing and relay was performed by global optimization based artificial electric field algorithm (AEFA). Finally, they used the human learning assisted state action reward state action (SARSA) algorithm to anticipate warning signals and emergency data. Various tests were carried out on the OMNeT++ simulator, and the working of the recommended EiA-H2B system was verified with respect to consumption of energy, rate of success, the throughput of the network, latency, and rate of packet loss, the time required for processing, and time required for authentication.

In 2022, Bataineh et al.<sup>21</sup> suggested an ethereum blockchain system to deal with the issues raised by the IoT devices' restricted supplies when applying blockchain data mining techniques. The distribution of load within the resources was the main concept taken into consideration for developing this system. Devices with fewer resources were called thin consumers, while those with more resources were called rich customers. Both users could gather information from the blockchain; however, only the rich client could perform the extraction operation. A healthcare structure was also developed that relies on the suggested design. By validating the structure with various well-known IoT-based blockchain designs, the effectiveness of this approach was demonstrated. The acquired findings demonstrated that the suggested blockchain-based IoT structure was suitable for various IoT projects.

In 2022, Demirbaga and Aujla<sup>20</sup> considered the big data environment and developed a flexible computer platform in it. A big data statistics monitoring structure and an associated blockchain-based information storing mechanism were the key features of the suggested design. This method used blockchain technology and big data platforms to evaluate, protect, and allow validated exposure to information from IoT-enabled equipment. The zero-knowledge approach was employed to prevent data interconnections and to ensure that no data was exposed to individuals who were not verified. The outcomes showed how well the approach addressed the difficulties of big data analysis and patient confidentiality.

In 2022, Gürfidan et al.<sup>42</sup> developed the data obtained from the sensors and the transaction records of the devices on a designed IoT network. The IoT network has been utilized to establish by offering internet access services to clients. Additionally, blockchain software using a hyper ledger fabric framework running on the server was realized. This software is configured to convert motion records of devices that are members of the Internet of thing network to be sent to it into a blockchain structure.

In 2022, Zulkifl et al.<sup>23</sup> introduced FBASHI, a system that used blockchain and fuzzy logic to provide verification, accreditation, and judgment service. The suggested method was built on the hyperledger blockchain technology, which offered confidentiality and quick reaction times, making it ideal for healthcare applications. Using fuzzy logic and an optimization method, a behavior-based adaptable, secure strategy for healthcare IoT and blockchain technology was presented. The confidentiality and usefulness of the system were tested by FBASHI. Moreover, a comparative analysis was formed with several other blockchain-based technologies.

## 2.2 | Motivation

The likelihood of a breach increases significantly when several devices are connected, which raises questions about cyber security. While using IoT for healthcare, interoperability across multiple devices is also a challenge. Also, the lack of data standards makes the process of development and implementation challenging. So, blockchain integrated with IoT healthcare is adapted for providing secure data storage and transmission. The features and the challenges of the existing blockchain-secure healthcare IoT models are tabulated in Table 1. MapChain<sup>20</sup> ensures no information is accessible to unauthorized users. But, a mistake once made is unchangeable across the entire network. ERTCA,<sup>21</sup> in addition to using three times less computing time than the hierarchical model, this model assists in spreading the load on the IoT device in a way that it can handle it. This approach, however, cannot be used for other IoT-blockchain integrated networks, nor is it suitable for industries besides healthcare. Edge-blockchain and incremental tensor train decomposition<sup>22</sup> exclude medical management procedures. In-house IoT healthcare data may be sent quickly and effectively to edge devices using this model, which also eliminates the need to prepare block ledgers and headers and prevents security issues during data transmission. The amount of cloud space needed is also reduced by this technique. Yet, this approach does not

**TABLE 1** Features and challenges of existing blockchain in the healthcare IoT model.

Author (citation)	Methodology	Features	Challenges
Demirbaga and Aujla <sup>20</sup>	MapChain	<ul style="list-style-type: none"> <li>It ensures that no information is accessible to unauthorized users.</li> </ul>	<ul style="list-style-type: none"> <li>A mistake once made is unchangeable.</li> </ul>
Bataineh et al. <sup>21</sup>	ERTCA	<ul style="list-style-type: none"> <li>It helps in distributing the load to the IoT device in such a way that it can handle it, and also it takes three times less computational time than the hierarchical model.</li> </ul>	<ul style="list-style-type: none"> <li>This method cannot be implemented for other IoT-blockchain integrated networks, and also it is not applicable for areas other than healthcare.</li> <li>It does not involve the medical management process.</li> </ul>
Aujla and Jindal <sup>22</sup>	Edge-blockchain, incremental tensor train decomposition	<ul style="list-style-type: none"> <li>This method is quick and effective in communicating the in-house IoT healthcare data with the edge devices, and also it eliminates the block ledgers and headers preparation time in addition to preventing security during data communication.</li> <li>This method also decreases the space requirement in the cloud.</li> </ul>	<ul style="list-style-type: none"> <li>This method does not make use of any advanced communication technologies like satellite communication or navigation systems.</li> </ul>
Zulkifl et al. <sup>23</sup>	FBASHI, Hyperledger, fuzzy logic	<ul style="list-style-type: none"> <li>It detects malicious behavior and eliminates several threats against IoT in healthcare.</li> </ul>	<ul style="list-style-type: none"> <li>This method is not applicable in foolproof security.</li> </ul>
Mohammad et al. <sup>24</sup>	IHM, BCHealth	<ul style="list-style-type: none"> <li>It helps to securely share the user data with the medical staff, and also, various nodes are considered as a cluster which enables easy and quick searching and accessing in that cluster.</li> </ul>	<ul style="list-style-type: none"> <li>The management of clusters and optimizing the number of nodes in each cluster, along with optimizing the number of clusters, is a difficult process.</li> <li>The cloud data are not integrated with the system, which results in storage-related issues.</li> </ul>
Sharmila and Jaisankar <sup>25</sup>	EiA-H2B, AM-GRU, AEFA	<ul style="list-style-type: none"> <li>This method is effective and powerful in monitoring health conditions, and also it reduces energy consumption.</li> </ul>	<ul style="list-style-type: none"> <li>This method is not standardized, and it is difficult to interoperate.</li> </ul>
Rathee et al. <sup>26</sup>	VM	<ul style="list-style-type: none"> <li>It is effective in tracing any illegal activity that is happening at any part of the communication network.</li> </ul>	<ul style="list-style-type: none"> <li>This method is expensive and requires a lot of time.</li> </ul>
Arul et al. <sup>27</sup>	BASC	<ul style="list-style-type: none"> <li>It minimizes service failure, delays, and the time required for processing.</li> <li>It enhances access for networks obtained at various intervals</li> </ul>	<ul style="list-style-type: none"> <li>Data mining is highly affected by noise.</li> </ul>

involve any cutting-edge communication technologies. FBASHI, Hyperledger, and fuzzy logic<sup>23</sup> detect malicious behavior and eliminate several threats against IoT in healthcare. But, this method does not apply to foolproof security. IHM and BC-Health,<sup>24</sup> the medical staff may securely access user data because of this method, and as several nodes are grouped together as a cluster, finding and navigating inside that cluster is made simple and rapid. Nevertheless, managing a cluster, and maximizing the number of nodes in each cluster, as well as the number of clusters, is a challenging operation. Moreover, because the Cloud data are not connected to the system, storage-related problems arise. EiA-H2B, AM-GRU, and AEFA<sup>25</sup> are potent and effective in monitoring health status and lowering energy usage. Nevertheless, there are no standards for this method, making it impossible to interoperate. VM<sup>26</sup> is effective in tracing any illegal activity that is happening at any part of the communication network. However, this method is expensive and requires a lot of time. BASC<sup>27</sup> minimizes service failure, delays, and the time required for processing. It also enhances access to networks obtained at various intervals. But, data mining is highly affected by noise.



So, an advanced security system for healthcare IoT for storing information in blockchain is suggested. With the aim of overcoming these challenges, a new hybridized HECC-ABE approach and AFP-GEHHO algorithm is developed for securing the medical data. Here, the parameters in LSTM and attention network are tuned using the AFP-GEHHO algorithm. This performance improvement has been applicable to many real-world applications. Especially the blockchain is used for healthcare in real-time using wearable devices and IoT. Here, for the support of blockchain, the medical data is stored in a secure manner. It helps doctors to track who are high-risk patients, and also, if they need any emergency, the doctors can easily contact them and also provide advice and alert their families and careers. The simulation outcome of the designed method proved that it is statistically significant. The results, like the confusion matrix and ROC curve, proved its efficacy, and also it attains better performance regarding standard performance metrics.

### 3 | SECURE HEALTHCARE IOT DATA STORAGE IN BLOCKCHAIN USING HYBRID CRYPTOGRAPHY WITH KEYS OPTIMIZATION BY HYBRID META-HEURISTIC ALGORITHMS

#### 3.1 | Data storage model in blockchain

A blockchain is a decentralized distributed ledger technology in which any changes or modifications done in it can be known by the entire users connected to the block. The storage of data in the blockchain is not much expensive, and it is more secure than any other means of the storage system. Hence, blockchain is chosen as the source of storage platform in our developed system. The decentralized blockchain network encrypts the data before transmitting it within various interconnected blocks, which makes it difficult for hackers to modify or steal the data from the blockchain. The computation time is very low, and also it can be useful for many in-house applications. So, it is more effective in storing medical data in the blockchain network. However, there is a chance that the individual who accesses the data in the blockchain might not be authorized. Hence a user authentication and trust verification of the user is done in this paper before storing it in the blockchain. The pictorial representation of the data storage model in blockchain is shown in Figure 1.

#### 3.2 | Developed model and its description

##### 3.2.1 | First level of authenticated user verification

The medical data about the patient is gathered using IoT-aided<sup>45</sup> methods. Medical professionals are treated as authorized users. At first, the user (doctor) data and their iris images are collected. The gathered iris images are given as input to the

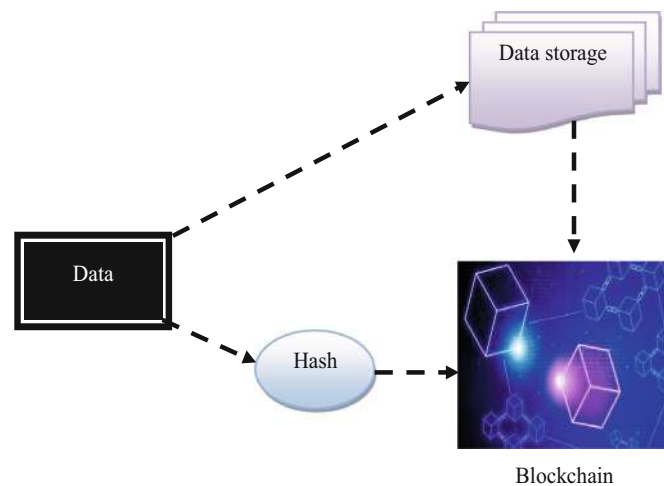


FIGURE 1 Pictorial representation of the data storage model in blockchain.

implemented AD-LSTM-AN model for verification of the user. If the person is authorized, then the AD-LSTM-AN gives output as an authorized user who can further access the blockchain network for storing and retrieving the medical data. The performance of the AD-LSTM-AN model is enhanced by tuning the hyperparameters like the hidden neuron count, the epoch count, and the steps per epoch of the network with the assistance of the suggested AFP-GEHHO algorithm. If the output of the AD-LSTM-AN is an unauthorized user, then the user is revoked from the entire network without further operation. This makes the first level of verification. Only the authentication of the authorized user alone cannot allow the authorized user to store or retrieve medical data.

### 3.2.2 | Second level of user verification

A second stage of user verification is carried out in which the user's trust is verified. The data about the user who needs to access the medical data is given to the same AD-LSTM-AN network. The network analyzes the previous transactions and the user's history in the secure storage system. The same AFP-GEHHO algorithm is used to optimize the parameters, such as the epochs, hidden neurons, and the steps per epoch of the AD-LSTM-AN trust verification system. If the trust level of the authorized user is high, then the user can access the medical data. If the trust level of the authorized user is low, then they are revoked from the system. Once the authentication and trust verification of the user is implemented successfully, the authorized and trustworthy user is allowed to store the medical data in the Blockchain.<sup>46</sup>

### 3.2.3 | Methodology

The medical data is initially subjected to data encryption by the recommended HECC-ABE cryptography scheme, in which the medical data is initially encrypted by the ECC cryptography method, and then the encrypted data from the ECC cryptography scheme is given as input to the ABE cryptography scheme for further encryption so that the security level of the data can be enhanced. The keys generated from the HECC-ABE scheme are tuned using the generated AFP-GEHHO algorithm to minimize the processing time and the complexity of the process. The encrypted medical data from the ABE scheme is finally provided to be stored in the blockchain. The blockchain is considered as the backbone of this work. It is a cryptographic function that is utilized to encrypt the data. In our research work, blockchain is introduced for the high production of medical data. We know that blockchain technology is popular for its application in Bitcoin cryptocurrency, which helps to maintain integrity and transaction of data. The data structure of the blockchain has modeled linearly sequenced blocks. Each block contains cryptographic hashes corresponding to the prior and current blocks. Conversely, the chaining strategy ensures the integrity of this secured data structure. If a user needs to retrieve the stored medical data from the blockchain, again, the authentication and the trust of the user are verified by the same AD-LSTM-AN network. If the user is authorized and trustworthy, then the stored medical data can be recovered by the user. The encrypted data from the blockchain is given to the HECC-ABE cryptography scheme. Here, the encrypted data is initially decrypted by the ABE cryptography scheme, and then it is provided to the ECC cryptography scheme for further decryption. The decrypted data from the ECC cryptography technique is the original medical data that is retrieved from the blockchain. Thus secure storage and access to medical data are possible by implementing this network. The implemented secure healthcare IoT data storage model in blockchain is depicted in Figure 2.

## 4 | USER AUTHENTICATION AND TRUST VERIFICATION FOR SECURED HEALTHCARE IOT DATA STORAGE IN BLOCKCHAIN WITH DEEP LEARNING STRATEGIES

### 4.1 | User biometric information

For performing authentication of the user, the iris image of the authorized individuals is collected. The iris images of the authorized user are collected using infrared cameras or by retinal scanning method and are stored in the database of the hospital along with the details of the doctors. The iris images are encoded into digital templates using the unique iris patterns of the individual. The identification of the individual by their iris image is determined using statistical algorithms. This digital template containing the binary format of the iris image is stored in the hospital database for future use.

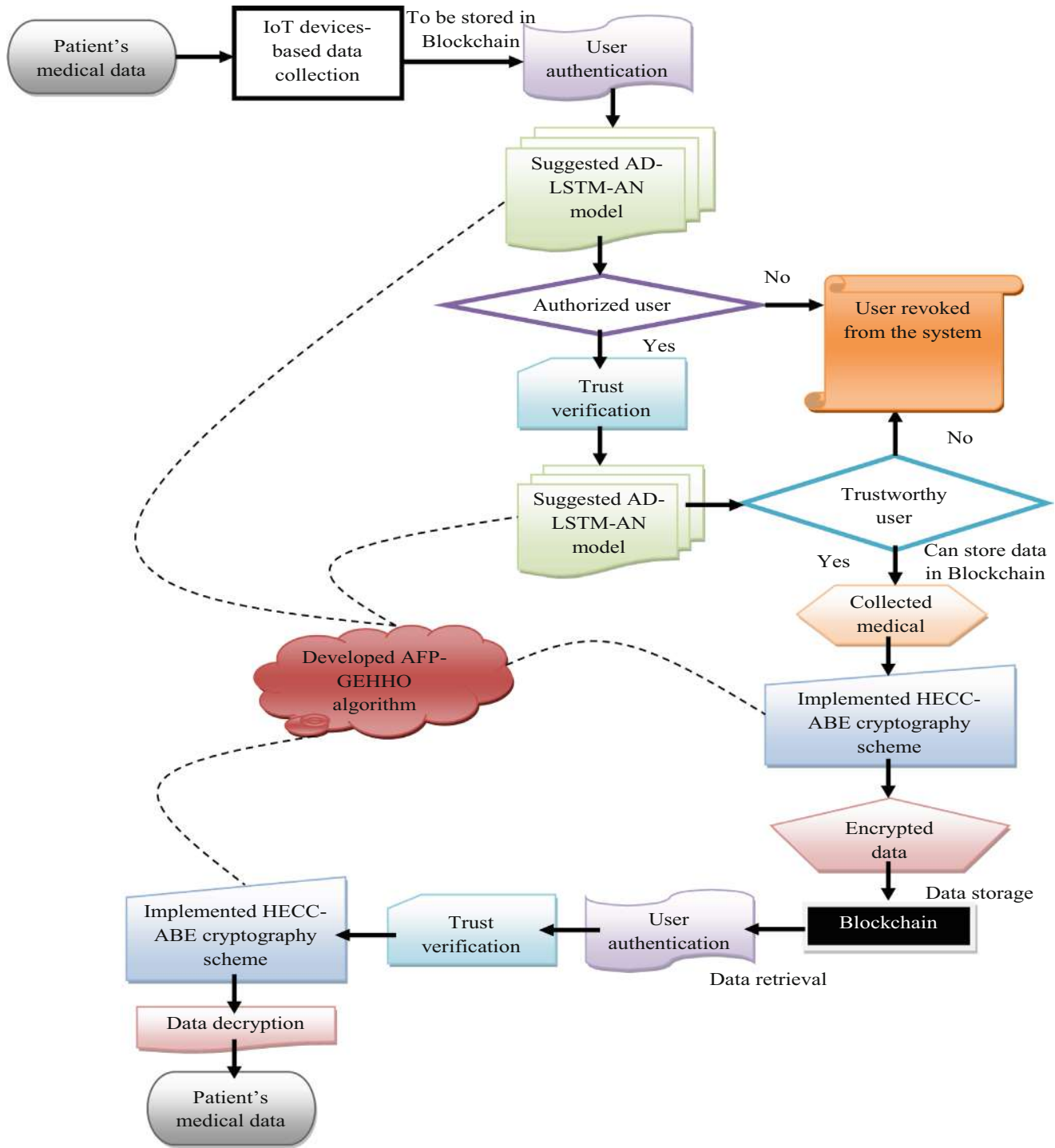


FIGURE 2 Illustration of the implemented secure IoT healthcare data storage model in blockchain.

From the database of the hospital, the iris image of the authorized user is collected for performing user authentication. The obtained iris images of the authorized individuals are represented by  $II_{kj}^{UA}$ .

#### 4.1.1 | User transaction and historical data

All the previous transactions done by the user and their historical data are gathered. These data are collected from the hospital databases. The collected previous transactions and the user history data are represented by  $HD_{kw}^{TV}$ .



## 4.2 | LSTM network

The robust performance of the LSTM<sup>28</sup> in solving time series-related problems, problems regarding biomedical applications, and language problems made it popular to solve problems regarding long dependencies. The ability of the LSTM to solve problems with long-term dependency is very high. The LSTM comprises a forget gate, various memory blocks with a memory cell in it, a gate for providing input, and a gate for giving out the output. The memory block of the LSTM helps it in retaining information for a very long period of time. All three gates, namely the output, input, and forget gates, contain an activation function to speed up the process. The LSTM is fed with an input of sequence  $q = q_1, q_2, \dots, q_D$  to map the output  $r$  through a hidden layer  $E_V$  from an activation function of recursive nature.

$$f(E_{V-1}, q_V) \quad (1)$$

In Equation (1), the term  $V$  indicates the period required to execute the entire steps. An entropy function is used to minimize the loss function. This cross-entropy function is given by Equation (2).

$$X(q, r) = -\frac{1}{D} \sum_{w \in D} q_w \log r_w \quad (2)$$

The weights in the LSTM are amended with the help of a memory gate that is responsible for determining the data that has to be forgotten or recovered back at each moment of the step. The hidden state is determined using the output and cell state as given in Equation (3).

$$E_V = ot_V \tanh(ca_V) \quad (3)$$

In Equation (3), the term  $ot$  denotes the output gate, and the term  $ca$  denotes the cell state. The output is obtained from the output gate  $ot$ . The mathematical representation of the output gate is given by Equation (4).

$$ot_V = \sigma(wi_{qot}q_{(V)} + wi_{Eot}E_{(V-1)} + wi_{caot}ca_{(V-1)} + biot) \quad (4)$$

The term  $wi$  in Equation (4) denotes the weight,  $bi$  denotes the threshold, and the term  $\sigma$  denotes the activation function (sigmoid). The cell state is given by Equation (5).

$$ca_V = ft_{(V)}ca_{(V-1)} + it_{(V)} \tanh(wi_{qca}q_{(V)} + wi_{Eca}E_{(V-1)} + bica) \quad (5)$$

The amount of information has to be added in every time period that is determined using the input gate  $it$ .

$$it_V = \sigma(wi_{qit}q_{(V)} + wi_{Eit}E_{(V-1)} + wi_{cait}ca_{(V-1)} + biit) \quad (6)$$

The data that need not be recovered back is determined using the forget gate  $ft$ .

$$ft_V = \sigma(wi_{qft}q_{(V)} + wi_{Eft}E_{(V-1)} + wi_{caft}ca_{(V-1)} + bift) \quad (7)$$

Even if the nominal LSTM is good in solving the problems with long-term dependency, there still persist some issues. The addition of certain input functions alters the LSTM's cell state. The execution of the backpropagation procedure and the addition of the  $ca_V$  derivation with respect to  $ca_{(V-1)}$  have resulted in the reduction of the data that is transferred between the layers of the LSTM framework. The basic architecture of the LSTM network is shown in Figure 3.

## 4.3 | User authentication model with developed AD-LSTM-AN

The biometric information (iris image)  $II_{kj}^{UA}$  about the user is provided to the AD-LSTM-AN model for user authentication. The dilated LSTM<sup>29</sup> differs from the general LSTM structure by the presence of dilated skip connections of recurrent layers. In ADLSTM-AN, exponentially rising dilations are provided to the skip connections of recurrent layers. Better

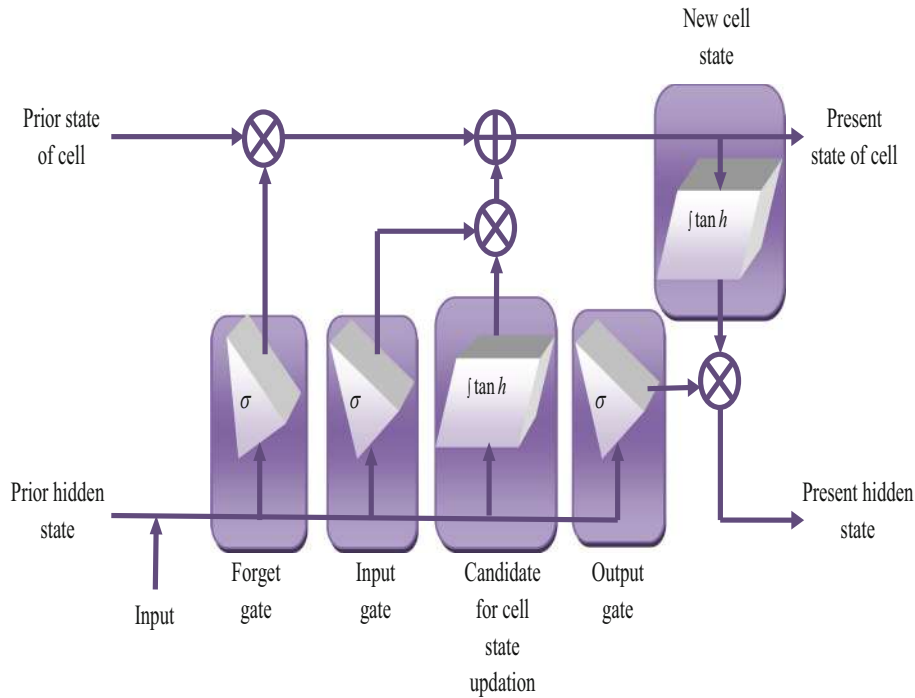


FIGURE 3 The basic architecture of LSTM.

learning of the input sequence and their complicated and temporal dependency of data on various layers are provided to the LSTM with the help of these dilated skip connections. The LSTM may solve the problem regarding long-term learning dependency with the help of its memory state. However, it cannot determine the information that is highly crucial than other information in the given data to perform the present task. This issue can be resolved by incorporating an embedded layer and an attention mechanism in the dilated LSTM structure. With the help of the embedding matrix, the input data is embedded into a matrix. This embedding matrix is then given as the input to the dilation layers of the dilated LSTM. The most vital aspect of the dilated LSTM model is the presence of dilated skip connections that are recurrent in nature. The dilated skip connection is given by Equation (8).

$$ca_V^{(ee)} = FF\left(q_V^{ee}, ca_{V-sl^{ee-1}}^{ee}\right) \quad (8)$$

In Equation (8), the term  $ee$  indicates the layer,  $sl$  denotes the length of the skip, and  $FF(\bullet)$  indicates the cell in the LSTM model. The dilation layer or the skip length is given by Equation (9).

$$sl^{ee} = gg^{(ee-1)}, ee = 1, 2, \dots, hh \quad (9)$$

In order to prioritize the importance of the viable data that is needed to perform the present task from the complete set of information, the attention mechanism is indulged in the LSTM model. The attention<sup>30</sup> is simply a source assignment mechanism that provides more computation sources to the most viable data, thus reducing the computation burden. The increased number of parameters may enhance the expressing capability of characteristics but also leads to the overloading of the data. The loss of data due to the long input data is eliminated, and the unnecessary information from the provided data is removed with the assistance of the attention mechanism, which provides more weight to the data that is more important and the least weight to the unnecessary information. The overall accuracy and efficiency of the LSTM framework are enhanced by including the attention mechanism. The inner cell structure of the LSTM is provided with the attention mechanism for producing enhanced results. The attention mechanism helps attain a better LSTM model, prevents the results that are developed in between, learns the results that are obtained selectively, and provides the output by providing weights to the intermediate results. The attention mechanism also aids in the parallel execution of data, thus eliminating the dependency of the output on the output from the prior step. At first, the distribution of attention to

all the input data is determined, which is followed by the determination of the weighted average of the input data. The attention for all the given inputs is determined using Equation (10).

$$E_V = \text{lay}(q_{(V)}, E_{(V-1)}) \quad (10)$$

In Equation (10), the term *lay* denotes the layers of the LSTM model. The weighted average is computed using Equation (11).

$$ag = \sum_{aa=1}^{bb} \mu_{aa} E_{aa} \quad (11)$$

In Equation (11), the term  $\mu$  denotes the weight ratio among two hidden layers. The value of  $\mu$  is computed as in Equation (12).

$$\mu_{aa} = \frac{\exp\left(F\left(E_V, \overline{E}_F\right)\right)}{\sum_{dd}^{bb} \exp\left(F\left(E_V, \overline{E}_F\right)\right)} \quad (12)$$

In Equation (12), the term  $F$  denotes the method of computing the weight, which is given by  $F\left(E_V, \overline{E}_F\right) = E_V, \overline{E}_F$ . If the user is an authorized person, then Ad-LSTM-AN gives classified output as an authorized user, or else, the user is considered unauthorized. Only the authorized person can store and retrieve the medical data to and from the blockchain. The user authentication is done by storing and retrieving the medical data to the blockchain. The parameters in the AD-LSTM-AN network for user authentication are optimized using the suggested AFP-GEHHO algorithm. The parameters like the hidden neuron count, the epochs, and the steps per epoch are tuned using the developed AFP-GEHHO algorithm to maximize the precision, accuracy, NPV, and minimizing the FPR of the user authentication system.

$$oc1 = \arg \min_{\{hu_{ls}^{UA}, eh_{lw}^{UA}, sp_{la}^{UA}\}} \left( \frac{1}{acuy + prcn + nepr} + fapo \right) \quad (13)$$

The term *oc1* in Equation (13) denotes the objective function of the user authentication model,  $hu_{ls}^{UA}$  denotes the optimized hidden neuron count in the range [5,255],  $eh_{lw}^{UA}$  denotes the optimized epoch count in the range [5, 50], and  $sp_{la}^{UA}$  denotes the optimized number of steps per epoch, which is in the range [50,250]. The optimization of these parameters helps in achieving maximum precision, accuracy, and NPV and minimum FPR, respectively. The negative predictive value (NPV) can be computed using the formula provided in Equation (14).

$$nepr = \frac{AF}{BO + AF} \quad (14)$$

In Equation (14), the term AF indicates the true negative value, and the term BO indicates the false positive value. The precision *prcn* is evaluated using the below-provided Equation (15).

$$prcn = \frac{BL}{BL + BO} \quad (15)$$

In Equation (15), the term BL indicates the true positive value. The false positive rate (FPR) *fapo* is computed as provided in Equation (16)

$$fapo = \frac{BO}{AH + BO} \quad (16)$$

In Equation (16), the term AH indicates the false negative value. The accuracy *acur* is determined using Equation (17)

$$acur = \frac{BL + AF}{BL + BO + AF + AH} \quad (17)$$

#### 4.4 | User trust verification model with developed AD-LSTM-AN

The user history details and the previous transactions done by the user  $HD_{kw}^{TV}$  are given as input to the AD-LSTM-AN model for trust verification. If the person is trustworthy, the proposed AD-LSTM-AN model will produce a high output. If the person is not trustworthy, then a low value is given as the output by the AD-LSTM-AN. Only a trustworthy person can store or retrieve medical data in the blockchain. The trust of the person is verified while storing and retrieving the medical data from the blockchain. The parameters in the AD-LSTM-AN network for user trust verification are tuned using the implemented AFP-GEHHO algorithm. The optimized parameters are the hidden neuron count, the epochs, and the steps per epoch. This optimization helps in minimizing the MSE of the system.

$$oc2 = \arg \min_{\{hu_{uv}^{TV}, eh_{ux}^{TV}, sp_{ud}^{TV}\}} (mse) \quad (18)$$

The term  $oc2$  in Equation (18) denotes the objective function of the user trust verification model,  $hu_{uv}^{TV}$  denotes the optimized hidden neuron count in the range [5,255],  $eh_{ux}^{TV}$  denotes the optimized epoch count in the range [5, 50], and  $sp_{ud}^{TV}$  denotes the optimized number of steps per epoch, which is in the range [50,250]. The optimization of these parameters helps in achieving the minimum value of mean square error (MSE). The MSE is computed using the formula provided in Equation (19).

$$mse = \frac{\sum (rea - pre)^2}{no} \quad (19)$$

In Equation (19), the term  $rea$  denotes the real value,  $no$  denotes the total number of observations, and  $pre$  denotes the predicted value.

## 5 | OPTIMAL KEY-BASED HYBRID CRYPTOGRAPHY FOR SECURE HEALTHCARE IOT DATA STORAGE IN BLOCKCHAIN USING HYBRID META-HEURISTIC ALGORITHMS

### 5.1 | ECC

The medical data  $MD_{sx}^{pat}$  that has to be stored is first given to the ECC algorithm for encryption. The ECC<sup>44,45</sup> has found its application in low-computation gadgets like IoT and wireless sensor networks (WSN). The popularity of the ECC cryptography scheme in IoT platforms is due to its reduced overheads on computations and reduced key sizes for similar cryptographic level hardness. The effectiveness of the ECC is much better than the other cryptography schemes as the size of the keys generated by it is small. The distinct logarithmic form of the elliptic curves in the fields of finite dimensions serves as the basis for the ECC cryptography algorithm. The ECC algorithm facilitates the transfer of keys between various parties, and also it aids in a secure way of communication among different parties. The ECC also helps to sign information so that its truthfulness is preserved and it is protected from manipulation. The procedure of the ECC cryptography scheme is provided below. The main procedures that are being carried out in the ECC cryptography scheme are point addition, point doubling, and scalar multiplication. Let  $AA$  be an elliptic curve in the field  $BB$ , which is given by the Weierstrass formula as given below in Equation (20).

$$nn^2 = mm^3 + iimm + jj \quad (20)$$

In Equation (20), the term  $ii$  represents a number. The elliptic curve  $DD$  is formed by joining  $AA$  with  $BB$  for performing point addition. Assume two points  $AA(ii_1, jj_1)$  and  $BB(ii_2, jj_2)$ . A line is generated, as shown in Equation (21).

$$jj = llii + kk \quad (21)$$

Let a single variable equation be generated as shown in Equations (22) to (25).

$$(llmm^2 + kk)^2 = ii^3 + mmii + jj \quad (22)$$

$$l^2ii^2 + kk^2 + 2llii = ii^3 + mmii + nn \quad (23)$$

$$ii^3 - l^2ii^2 + mmii = 2llii + kk^2 - nn \quad (24)$$

$$ii^3 - l^2ii^2 + (ii - 2llkk)ii + nn - kk^2 = 0 \quad (25)$$

The roots of the above-provided polynomial are obtained by using Equation (26).

$$AA \cdot BB = (ii_3, ii_3) \quad (26)$$

The elliptic point addition is given in Equation (27)

$$AA + BB = (ii_3, -ii_3) \quad (27)$$

The line's slope is computed as in Equation (28).

$$ll = \frac{(jj_3 - jj_1)}{(ii_3 - ii_1)} \quad (28)$$

The roots are added as in Equation (29).

$$ii_1 + ii_2 + ii_3 = ll^2 \quad (29)$$

The term  $ii_3$  is obtained as in Equation (30).

$$ii_3 = ll^2 - ii_1 - ii_2 \quad (30)$$

The term  $jj_3$  is calculated using Equation (31).

$$jj_3 = jj_1 + ll(ii_3 - ii_1) \quad (31)$$

The reflection point of  $jj$  is evaluated as Equation (32)

$$jj_3 = -(jj_1 + ll(ii_3 - ii_1)) \quad (32)$$

The equality of  $AA$  and  $BB$  is provided point doubling. By derivating  $jj$  in line Equation (20) concerning  $ii$ , the single slope point is obtained as in Equation (33).

$$2jj \frac{\partial jj}{\partial ii} = 3ii^2 + mm \quad (33)$$

$$\frac{\partial jj}{\partial ii} = \frac{3ii^2 + mm}{2jj} \quad (34)$$

Point doubling is shown in Equations (35) and (36).

$$ii_3 = ll^2 - 2ii_1 \quad (35)$$

$$jj_3 = -(jj_1 + ll(ii_3 - ii_1)) \quad (36)$$



Another important procedure in ECC is scalar multiplication, where  $oo$  is multiplied with  $ooAA$  and some other point. The value of  $ooAA$  is determined using Equation (37), so that  $oo_{pp} \in EE\{0, 1\}$  is obtained as given in Equation (38).

$$oo = \sum_{oo=0}^{qq-1} oo_{pp} 2^{pp} \quad (37)$$

$$oo = 2 \times [(2oo_{qq-1}AA + oo_{qq-2}AA) + \dots + oo_0AA] \quad (38)$$

Two keys are generated by the ECC employs as it is an asymmetric cryptography method. Two keys, private and public, are there in the ECC algorithm. The user has to secure the private key provided to them. A generation point of key  $rr$  and an elliptic curve equation are developed between users 1 and 2. Let us consider  $ss$  and  $tt$  be the private keys for users 1 and 2. Then, public keys are calculated using Equations (39) and (40).

$$ss = pr_1 \cdot rr \quad (39)$$

$$tt = pr_2 \cdot rr \quad (40)$$

An arbitrary key is chosen as the private key. Incorrect selection of these private keys may lead the public keys to infinite values. The encrypted medical data from the ECC is denoted as  $ED_{es}^{ECC}$ .

## 5.2 | ABE

The encrypted medical data  $ED_{es}^{ECC}$  is given to the ABE cryptography scheme for further encryption. Unlike conventional cryptography schemes, the cipher texts are not required to be encrypted for a single user in the ABE scheme.<sup>32</sup> The ciphertext and the private keys of the user are linked by a certain rule or attribute in the ABE cryptography scheme. If the ciphertext and the private key of the user are matched, then the user can be able to decrypt the data from the blockchain. Let  $W$  a set of attributes be associated with the private keys of the user. If the user needs to decrypt the data, the  $X$  attribute of  $W$  has to be matched with the private keys and the ciphertext of the user for further decryption.

## 5.3 | Implemented HECC-ABE-based data encryption with optimal key

The medical data  $MD_{sx}^{pat}$  that has to be stored in the blockchain is primarily encrypted before storing it in the blockchain. Once the authentication and trust of the user who wants to save the medical data in the blockchain are verified and claimed to be authorized, then the medical data that needs to be stored is encrypted to enhance the security of the information. The data that has to be stored  $MD_{sx}^{pat}$  is given to the HECC-ABE cryptography method. At first, the medical data is encrypted by the ECC cryptography scheme. The encrypted data from the ECC scheme is  $ED_{es}^{ECC}$ . The encrypted data  $ED_{es}^{ECC}$  is then given to the ABE cryptography scheme for the second encryption stage. The encrypted medical data from the ABE cryptography scheme is  $ED_{ep}^{ABE}$ . The keys of both the ECC and the ABE cryptography schemes in the binary format are optimized using the recommended AFP-GEHHO algorithm. The optimization of the keys is carried out to minimize the processing time and minimize the memory requirement. The objective function of the key optimization in the HECC-ABE cryptography scheme using the AFP-GEHHO algorithm is mathematically represented in Equation (41).

$$oc3 = \arg \min_{\{keys_{pf}^{HECC-ABE}\}} (time + memory) \quad (41)$$

The term  $oc3$  in Equation (41) denotes the objective function,  $keys_{pf}^{HECC-ABE}$  denotes the optimized keys,  $time$  denotes the processing time, and  $memory$  denotes the computational memory requirements. Finally, the encrypted data  $ED_{ep}^{ABE}$  is stored in the blockchain. The diagrammatic illustration of the key optimization in the HECC-ABE cryptography scheme by the implemented AFP-GEHHO algorithm is given in Figure 4.

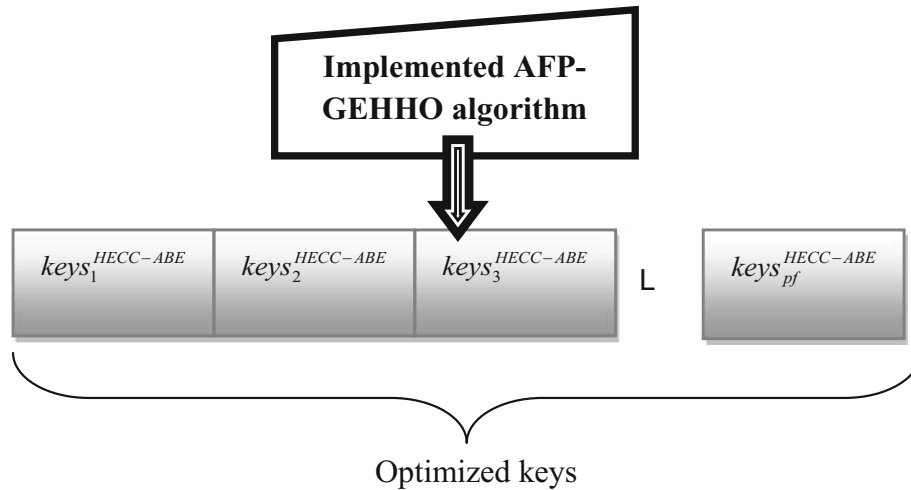


FIGURE 4 Solution diagram of the implemented AFP-GEHHO-HECC-ABE cryptography scheme.

## 5.4 | Proposed AFP-GEHHO

With the aim of optimizing the hidden neurons of AD-LSTM-AN, steps per epoch in AD-LSTM-AN, epochs of AD-LSTM-AN, keys in binary format for ECC, and the keys in binary format for ABE, the recommended AFP-GEHHO algorithm is utilized. The GEO algorithm is utilized because of its balancing between the exploitation and exploration stages. The HHO algorithm is implemented because of its accurate and efficient local searching mechanism, even with fewer parameters. However, the solution provided by these two algorithms is not satisfactory. Hence, the AFP-GEHHO algorithm is developed to obtain the best results. Using an adaptive concept, the location of the variable is optimized. The key contribution of the recommended AFP-GEHHO algorithm is given in Equation (42).

$$Loc = Loc_{old} + \frac{\alpha(loc1, loc2)}{\tau(loc1, loc2)} \quad (42)$$

The term  $Loc$  in Equation (42) denotes the amended location,  $\alpha$  denotes the variance,  $\tau$  denotes the standard deviation,  $loc1$  denotes the upgraded location using the GEO algorithm given by Equation (47),  $loc2$  denotes the upgraded location using the HHO algorithm determined in Equation (62), and  $Loc_{old}$  denotes the old position. Once the upgraded locations from the GEO and HHO algorithms are obtained, the final location is amended using Equation (42).

### 5.4.1 | GEO

The GEO algorithm<sup>33,34</sup> is introduced by keeping the intelligent hunting behavior of the golden eagle, which adjusts its velocity of the spiral path on foraging. The golden eagle has a greater affinity for wandering around and monitoring its prey before it attacks the selected prey. The wandering ability and the affinity for attacking make the golden eagle get the optimal prey faster within a predefined search area. The wandering and attacking behavior of the golden eagle has certain special characteristics. They are as follows:

1. The golden eagle adopts a circular path when wandering and monitoring the prey.
2. The prey is always on either the left or right side of the eagle as it moves in a circular motion.
3. They search in neighboring area for other better options of prey.
4. The golden eagle's memory has all the details about the location of the best food in it and neighboring areas.
5. The golden eagle has more affinity to wandering and hunting.
6. When it attacks prey, the motion of the golden eagle is linear.
7. They perform either wandering or hunting in all the stages of the flight.

### 5.4.2 | Circular motion

The golden eagle retains the memory of all the locations it has visited before those that have optimal prey in it. The affinity of the golden eagle for simultaneous wandering and hunting of its food is more to determine the best food. In each iteration, the  $B$  golden eagle arbitrarily selects the prey of other golden eagles  $b$ . The golden eagle  $B$  encircles the best prey spotted by the other golden eagle  $b$ . The ability of the golden eagle to wander to the best location in its memory should also be taken into consideration in the GEO algorithm. Therefore,  $b \in \{1, 2, \dots, q\}$ , in which the term  $q$  denotes the golden eagle population.

### 5.4.3 | Selection of the prey

In order to perform hunting and to perform wandering in a circular path, the golden eagle has to choose a prey in all the iterations. Also, the golden eagle selects prey from the targets determined by other golden eagles in its population as well. The chosen prey decides the wandering and hunting vectors of the golden eagle. In the end, the golden eagle verifies if there is any better location available or not. If a better location is available, then the golden eagle moves towards the new location and selects prey there.

### 5.4.4 | Hunting

The entire hunting process begins from the current position of the golden eagle and ends at the location of the chosen prey. The formula to determine the hunting vector is provided by Equation (16).

$$\vec{g}_B = \vec{e}_b^* - \vec{e}_B \quad (43)$$

The term  $\vec{e}_B$  in Equation (43) indicates the present location of  $B$ ,  $\vec{g}_B$  indicates the hunt vector, and  $\vec{e}_b^*$  indicates the optimal location of the prey chosen  $b$ .

### 5.4.5 | Cruise

The vector of the cruise is tangential to the circular path and is  $90^\circ$  to the hunting vector. The linear velocity at which the golden eagle attacks the prey is given by this vector. The destination of the cruise vector is determined by Equation (44).

$$n_s = \frac{o - \sum_{h,h \neq s} k_h}{k_s} \quad (44)$$

The term  $k_s$  in Equation (44) indicates the dimensional space,  $k_h \in \vec{g}_B$  in which  $\vec{g}_B = [k_1, k_2, \dots, k_m]$ , and  $o$  indicates the hyperplane which is given by  $o = \vec{w} \cdot \vec{y} = \sum_{B=1}^m x_h z_h$  where  $\vec{w} = [x_1, x_2, \dots, x_m]$  indicates nominal vector, and  $\vec{y} = [z_1, z_2, \dots, z_u]$  indicates the arbitrary hyperplane. The vector for the cruise is given as provided in Equation (45).

$$\vec{n}_0 = \left( C_1 = G, C_2 = G, \dots, C_w = \frac{o - \sum_{h,h \neq s} k_h}{k_s}, \dots, C_m = G \right) \quad (45)$$

In Equation (45), the term  $G$  denotes an arbitrary parameter.

#### 5.4.6 | Location transition

The hunt and cruise vector determines the golden eagle's updated location. The step vector is given by Equation (46).

$$\Delta v_B = \vec{H}_1 z_k \frac{\vec{g}_B}{\|\vec{g}_B\|} + \vec{H}_2 z_C \frac{\vec{n}_B}{\|\vec{n}_B\|} \quad (46)$$

The terms  $\|\vec{g}_B\|$  and  $\|\vec{n}_B\|$  in Equation (46) indicate the Euclidean distance between the hunting and cruise vectors,  $\vec{H}_1$  and  $\vec{H}_2$  indicates vectors of random values in the limit  $[0,1]$ ,  $z_k$  and  $z_C$  indicates the coefficient of hunting and cruise, respectively. The upgraded location of the golden eagle is provided by the formula given in Equation (47).

$$v^{u+1} = v^u + \Delta v_B^u \quad (47)$$

When the fitness of the current location of the golden eagle is good enough than the prior location, then the golden eagle upgrades its memory on the updated location.

#### 5.4.7 | Shift from exploring to exploit

The transition from exploration to exploitation stages is determined using the coefficient of hunting and cruising. The coefficient of hunting is determined using Equation (48).

$$z_k = z_k^0 + \frac{u}{u_{\max}} [z_k^{u_{\max}} - z_k^0] \quad (48)$$

The coefficient of the cruise is obtained by implementing Equation (49).

$$z_C = z_C^0 + \frac{u}{u_{\max}} [z_C^{u_{\max}} - z_C^0] \quad (49)$$

In Equations (48) and (49), the term  $u_{\max}$  denotes maximum iteration  $z_k^0$  and  $z_C^0$  denotes the hunt and cruise coefficient's initial values, respectively.

#### 5.4.8 | HHO

The hunting behavior of the Harris hawks serves as the motivation for the HHO algorithm.<sup>35,36</sup> The Harris hawks are intelligent beings that try to capture their prey from every direction so that the prey cannot get escaped. The attacking style of the Harris hawks varies from prey to prey. The HHO algorithm is a slope and population-based optimization technique. The searching for prey, unannounced attack, and the attacking style are all the steps that are considered in the HHO algorithm.

#### 5.4.9 | Parameters initialization

The entire parameters, the Harris hawks population, the fitness function, and the lookup regions are initially initialized.

#### 5.4.10 | Inspection stage

Consider that every resting place technique is given the same amount of opportunities  $j$  in the investigation stage. The location of its prey and its co-members while hunting determines the resting place of the Harris hawk when  $j < \frac{4}{8}$ .

Or else, an arbitrary location is chosen by the Harris hawk as the resting place. In the inspection stage, the location of the Harris hawk is upgraded as provided in Equation (50).

$$a(c+1) = \begin{cases} a_p(c) - a_d(c) - g_3(A + g_4(l - A)) & j < \frac{4}{8} \\ a_R(c) - g_1|a_R(c) - 2g_2a(c)| & j \geq \frac{4}{8} \end{cases} \quad (50)$$

In Equation (50)  $a_p(c)$  denotes the location at which the prey of the Harris hawk is present,  $a(c+1)$  indicates the next location of the Harris hawk,  $c$  denotes the iteration,  $a(c)$  indicates the Harris hawk's current location,  $g_1, g_2, g_3, g_4$ , and  $j$  are arbitrary parameters in the limit  $(0, 1)$  in which the scaling parameter  $g_3$  enhances the arbitrary nature of the arbitrary parameter  $g_4$ ,  $a_d(c)$  denotes the Harris hawk population's average location,  $A$  denotes the lower boundary of the lookup space,  $a_R(c)$  denotes the arbitrary Harris hawk that is chosen randomly, and  $l$  denotes the higher boundary of the lookup space. The value of  $g_4$  is maintained very much closer to 1. The Harris hawk population's mean location is determined using Equation (51).

$$a_d(c) = \frac{1}{i} \sum_{l=1}^i a_l(c) \quad (51)$$

The term  $i$  in Equation (51) represents the population of the Harris hawk in the swarm. Any Harris hawk can be found in the location within the limits  $(A, l)$  of the lookup area.

#### 5.4.11 | Switch from investigation to utilizing stage

The energy of the prey that tries to escape from the Harris hawk is a decreasing factor. This decreasing prey's energy is given by Equation (52).

$$J = 2J_0 \left( 1 - \frac{c}{c_{\max}} \right) \quad (52)$$

In Equation (52), the term  $J$  indicates the energy that is escaped from the prey,  $c_{\max}$  indicates the maximum count of iteration, and  $K_0 \in (-1, 1)$  indicates the energy available in the prey initially, and it changes randomly at every iteration. The initial amount of energy available in the prey is given by Equation (53).

$$J_0 = 2g_5 - 1 \quad (53)$$

The term  $g_5 \in (0, 1)$  in Equation (53) indicates an arbitrary parameter. The investigation stage is carried out if the value of  $|J| \geq 1$ , and utilizing stage is carried out if the value of  $|J| < 1$ .

#### 5.4.12 | Utilizing stage

The possibility of obtaining prey prior to an unannounced attack is considered as  $U$ . On the basis of the value of  $J$  and  $U$ , there are four possible attacks.

##### *Soft beleaguer*

The soft beleaguer is performed by the Harris hawk if  $|J| \geq \frac{1}{2}$  and  $U \geq \frac{1}{2}$ . Now the location of the Harris hawk is upgraded using Equations (54) and (55).

$$a(c+1) = \Delta a(c) - J|La_p(c) - a(c)| \quad (54)$$

$$\Delta a(c) = a_p(c) - a(c) \quad (55)$$



In Equation (54), the term  $L$  indicates the escaping ability of the prey and  $\Delta a(c)$  indicates the distance between the location of the prey and the Harris hawk. The prey's escaping ability  $L$  is determined using Equation (56).

$$L = 2(1 - g_6) \quad (56)$$

In Equation (56), the term  $g_6$  is an arbitrary parameter in the limit (0, 1).

#### *Tough beleaguer*

Tough beleaguer is performed by the Harris hawk if  $|J| < \frac{1}{2}$  and  $U \geq \frac{1}{2}$ . The location of the Harris hawk is upgraded using Equation (57).

$$a(c + 1) = a_p(c) - J|\Delta a(c)| \quad (57)$$

There is no chance for the prey to escape in this phase.

#### *Soft beleaguer with enhancing dives*

The zigzag escaping pattern of the prey is obtained using the Levy Flight. When the prey tries to escape, a swarm of Harris hawk tries to attack the prey quickly and in random ways. This attacking phase of the Harris hawk is done when  $|J| \geq \frac{1}{2}$  and  $U < \frac{1}{2}$ . More agile methods are adapted by the Harris hawk in this phase. The technique adopted by the Harris hawk for soft beleaguer is given by Equation (58).

$$O = a_p(c) - J|La_p(c) - a(c)| \quad (58)$$

Following the Levy Flight, the Harris hawk dives to attack the prey using Equation (59).

$$M = O + P \times f(Q) \quad (59)$$

In Equation (59), the term  $P$  denotes an arbitrary vector of dimension  $1 \times Q$ ,  $f$  denotes the Levy Flight operation, and  $Q$  denotes the overall size of the problem. The Levy Flight is determined using Equation (60).

$$f = 0.01 \frac{\phi \epsilon}{|\iota|^{\frac{1}{\delta}}}; \epsilon = \left( \frac{\chi(1 + \delta) \sin\left(\frac{\pi \delta}{2}\right)}{\chi\left(\frac{1 + \delta}{2}\right) \delta \cdot 2^{\frac{\delta - 1}{2}}} \right)^{\frac{1}{\delta}} \quad (60)$$

In Equation (60), the term  $\delta$  denotes a constant variable whose value is assumed as 1.5 and  $\iota$  and  $\epsilon$  belongs to (0, 1). The Harris hawk's location is upgraded as provided in Equation (61) during the soft beleaguer with enhancing dives stage.

$$a(c + 1) = \begin{cases} M & \text{if } S(M) < S(a(c)) \\ O & \text{if } S(O) < S(a(c)) \end{cases} \quad (61)$$

#### *Tough beleaguer with enhancing dives*

The hard beleaguer with enhancing dives is performed when  $|J| < \frac{1}{2}$  and  $U < \frac{1}{2}$ . The Harris hawk's location is upgraded as provided in Equation (62) during the tough beleaguer with enhancing dives stage.

$$a(c + 1) = \begin{cases} M' & \text{if } S(M') < S(a(c)) \\ O' & \text{if } S(O') < S(a(c)) \end{cases} \quad (62)$$

The value of  $M'$  and  $O'$  is determined using Equations (63) and (64).

$$M' = O' + P \times f(Q) \quad (63)$$

$$O' = a_p(c) - J|La_p(c) - a_d(c)| \quad (64)$$

The pseudocode of the generated AFP-GEHHO algorithm is given in [Algorithm 1](#).

---

**Algorithm 1.** Implemented AFP-GEHHO algorithm
 

---

```

The population of the golden eagle and the Harris hawks are inputted
The parameters of the GEO and HHO algorithm are inputted
The fitness function is determined for the entire golden eagle and Harris hawk population
For ( $t = 1 \rightarrow T$ ).
  For ( $F = 1 \rightarrow F_{\max}$ )
    While (the conditions are not satisfied)
      Perform location updates using the GEO algorithm
      A prey is selected randomly from the memory of the golden eagle population
      The vector of the hunt  $\vec{g}_B$  is determined
      If ( $\vec{g}_B \neq 0$ )
        The vector of the cruise  $\vec{n}_0$  is determined
        The vector of steps  $\Delta v_B$  is determined
        The location of the golden eagle is upgraded using Equation (47)
        The fitness function for the upgraded location is updated
        If ( $oldfit < newfit$ )
          The memory of the golden eagle is updated
        End if
      End if
      Perform location updates using the HHO algorithm
      The decreasing energy of the prey  $J$  is computed
      If  $|J| \geq 1$ 
        The investigation stage is performed
        The location of the Harris hawk has been upgraded
      End if
      If  $|J| < 1$ 
        The utilizing stage is performed
        Soft beleaguer, tough beleaguer, soft beleaguer with enhancing dives, and tough beleaguer with enhancing
        dives are performed
        The new location of the Harris hawks is amended using Equation (62)
      End if
      The location is updated using an adaptive concept as provided in Equation (42)
      The fitness function of the optimum location is determined
      The optimum location is amended
    End while
  End for
End for

```

---

## 6 | RESULTS AND DISCUSSION

### 6.1 | Experimental setup

The deployed data storage model for medical data in blockchain was implemented in the Python paradigm. The security and better performance of the suggested AFP-GEHHO-AD-LSTM-AN user authentication and trust verification model were contrasted with various heuristic algorithms and existing classifiers to verify its performance. The implemented AFP-GEHHO-HECC-ABE cryptography scheme was validated with other cryptography schemes regarding processing time, memory consumption, and expense. Various algorithms like arithmetic optimization algorithm

(AOA)-ADLSTMAN,<sup>37</sup> tree seed algorithm (TSA)-ADLSTMAN,<sup>38</sup> GEO-ADLSTMAN,<sup>33</sup> and HHO-ADLSTMAN,<sup>35</sup> classifiers like recurrent neural network (RNN),<sup>39</sup> visual geometry group (VGG-16),<sup>31</sup> LSTM,<sup>28</sup> and ADLSTM,<sup>29</sup> and cryptography schemes such as ECC,<sup>31</sup> HECC-ABE,<sup>40</sup> ERTCA,<sup>20</sup> and MapChain<sup>21</sup> were utilized for the evaluation of the implemented model. The chromosome length was chosen as 3 and  $2 \times 256$ , the maximum iteration count was taken as 50, and the maximum population was considered as 10.

## 6.2 | Performance measures

The error measures used to validate the developed secured data storage model for healthcare IoT in blockchain are given below.

(a) Root mean square error (RMSE) is evaluated using Equation (65).

$$rms = \sqrt{\frac{\sum_{cv=1}^{fpc} (rea_{cv} - pre_{cv})^2}{fpc}} \quad (65)$$

In Equation (65), the term  $fpc$  denotes the count of the fitted points and  $cv$  denotes the computational value. The type 1 and type 2 metrics used in the analysis of the developed model can be computed by using the formulae provided in [https://en.wikipedia.org/wiki/Sensitivity\\_and\\_specificity](https://en.wikipedia.org/wiki/Sensitivity_and_specificity), and the error measures used in the validation are computed using the formulae provided in [https://en.wikipedia.org/wiki/Mean\\_squared\\_error](https://en.wikipedia.org/wiki/Mean_squared_error) for reference.

## 6.3 | Authentication-based cost function analysis

The cost function analysis of the developed user authentication model is shown in Figure 5. The cost requirement by the developed AFP-GEHMO-ADLSTM-AN model for user authentication is 60%, 33.33%, 75%, and 50% lesser than the AOA-ADLSTM-AN, TSA-ADLSTM-AN, GEO-ADLSTM-AN, and HHO-ADLSTM-AN algorithms respectively at an iteration count of 30.

## 6.4 | Analysis of the developed user authentication model

The classifier-based analysis of the developed user authentication model is given in Figure 6, and the algorithm-based analysis of the developed user authentication model is given in Figure 7. The precision of the developed

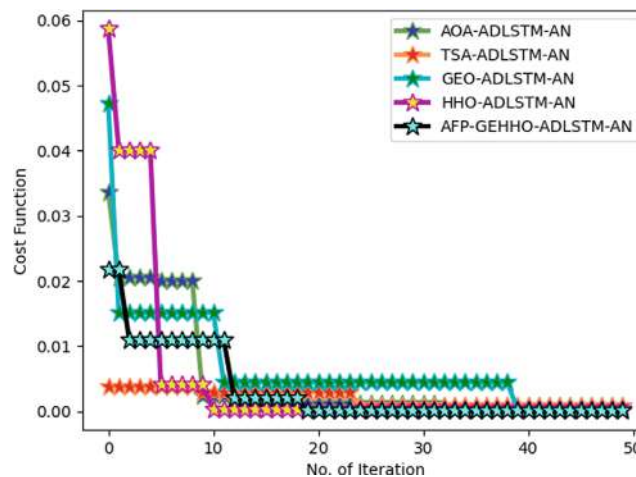


FIGURE 5 Cost function analysis of the developed user authentication model.

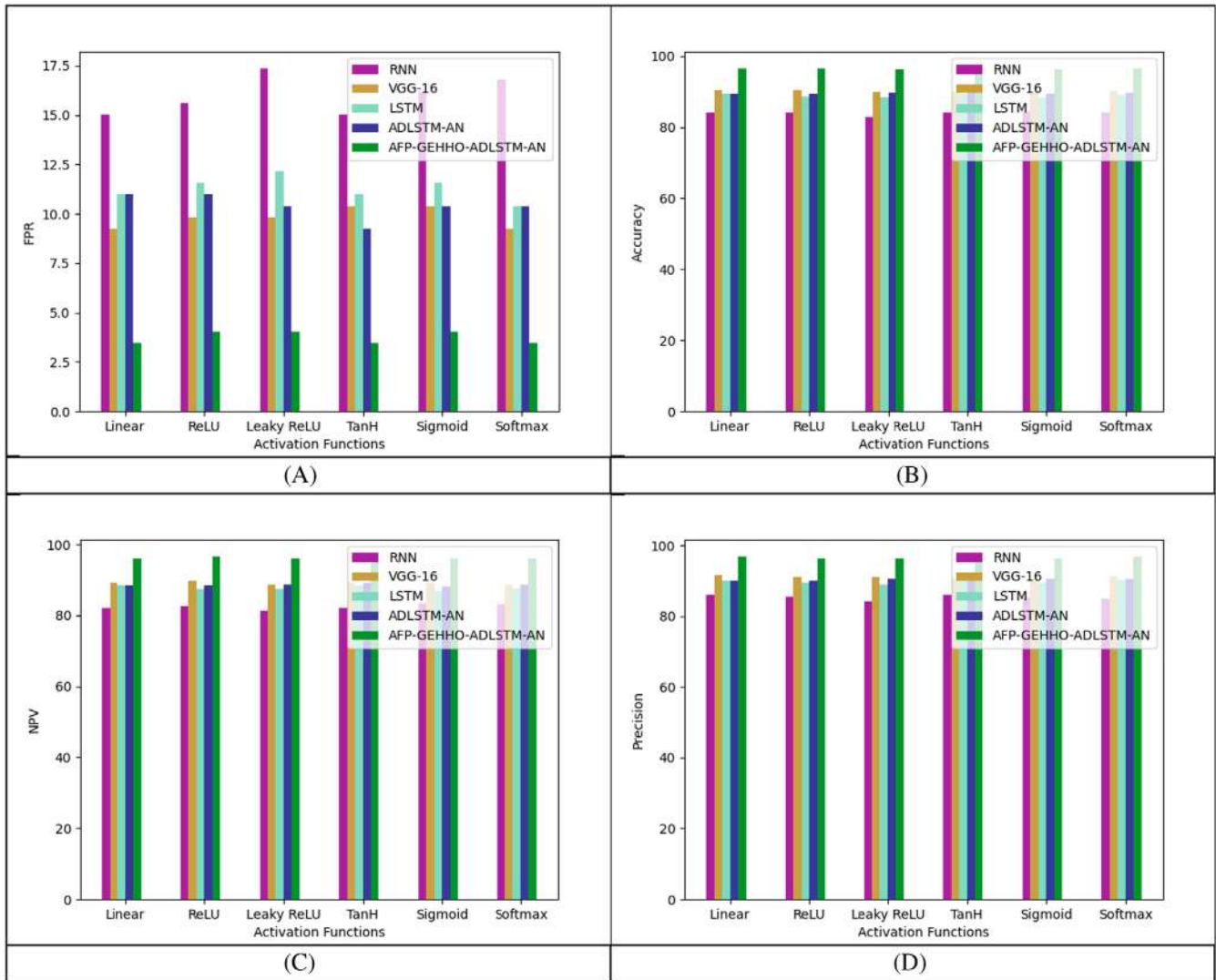


FIGURE 6 Classifier-based analysis of the developed user authentication model in terms of “(A) FPR, (B) Accuracy, (C) NPV, and (D) Precision”.

AFP-GEHHO-ADLSTM-AN model for user authentication is 10.47%, 4.4%, 6.15%, and 5.56% higher than the RNN, VGG-16, LSTM, and ADLSTM-AN classifiers, respectively at ReLU activation function.

## 6.5 | Confusion matrix analysis of the user authentication model

The confusion matrix and the ROC curve of the suggested AFP-GEHHO-ADLSTM-AN model for user authentication are shown in Figures 8 and 9.

## 6.6 | Convergence evaluation of the encryption scheme

The convergence evaluation of the suggested encryption method is shown in Figure 10. The cost requirement by the suggested AFP-GEHHO-HECC-ABE scheme for the encryption of data is 0.74%, 0.99%, and 0.25% lesser than the TSA-HECC-ABE, GEO-HECC-ABE, and HHO-HECC-ABE algorithms respectively and similar to the AOA-HECC-ABE algorithm at a block size of 15 in iteration 20.

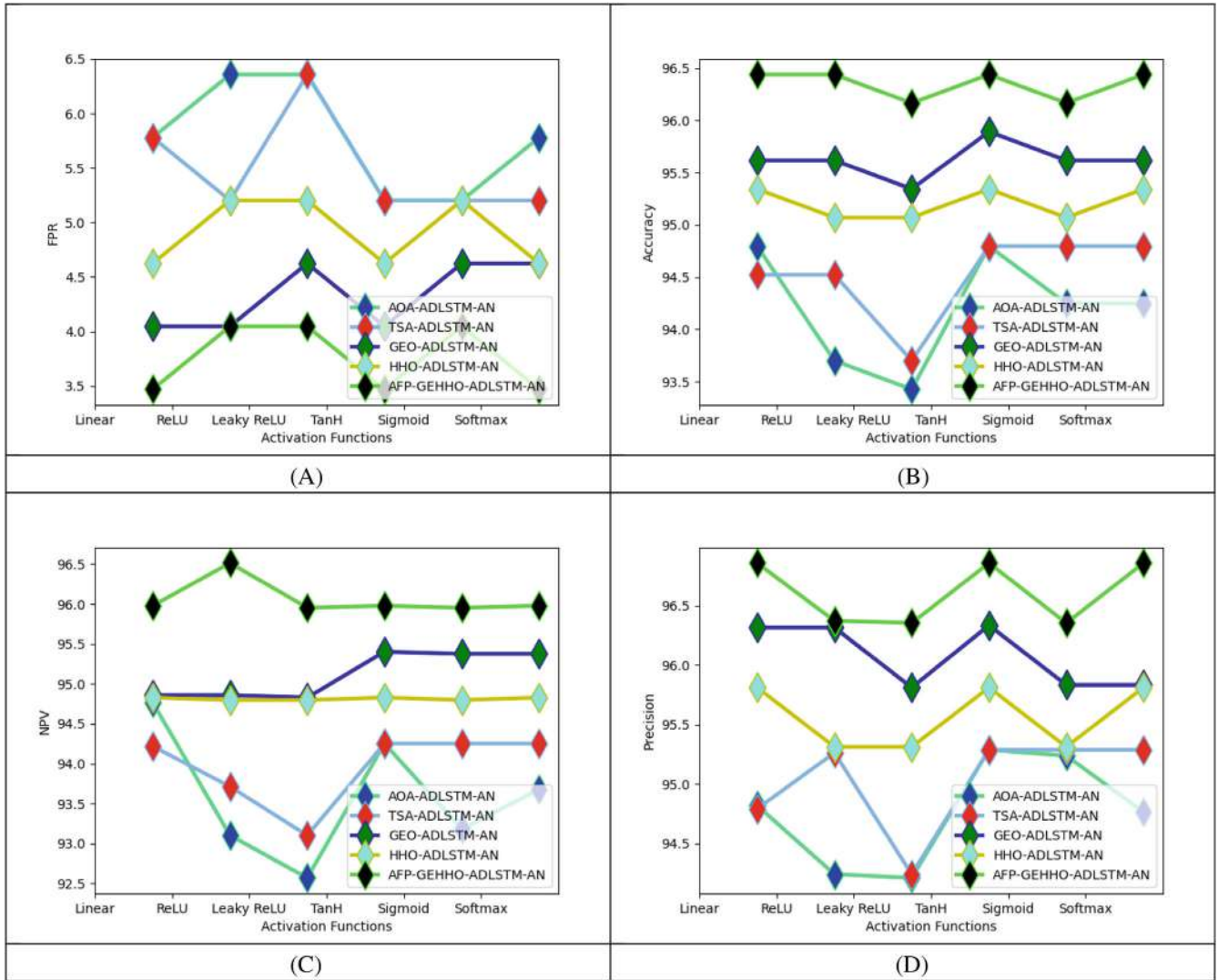


FIGURE 7 Algorithm-based evaluation of the proposed user authentication framework in terms of “(A) FPR, (B) Accuracy, (C) NPV, and (D) Precision”.

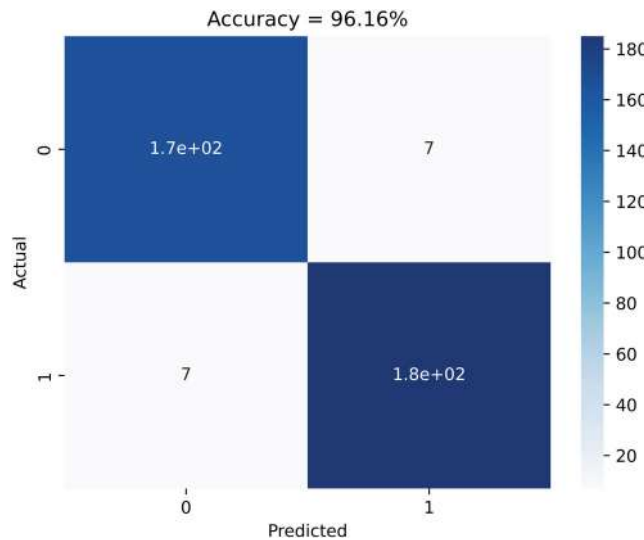


FIGURE 8 Confusion matrix analysis of the user authentication model.



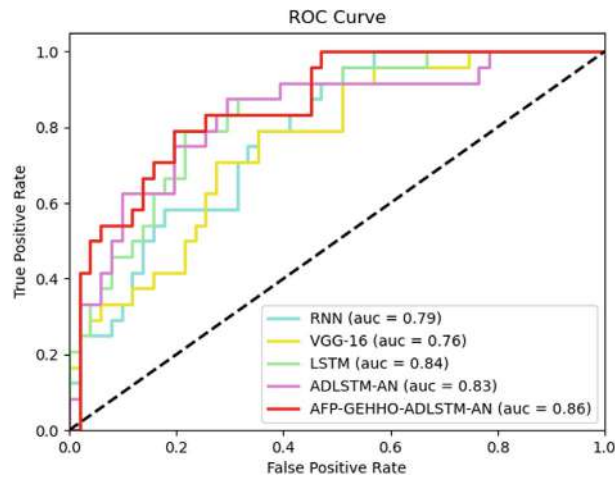


FIGURE 9 ROC examination of the recommended secure framework.

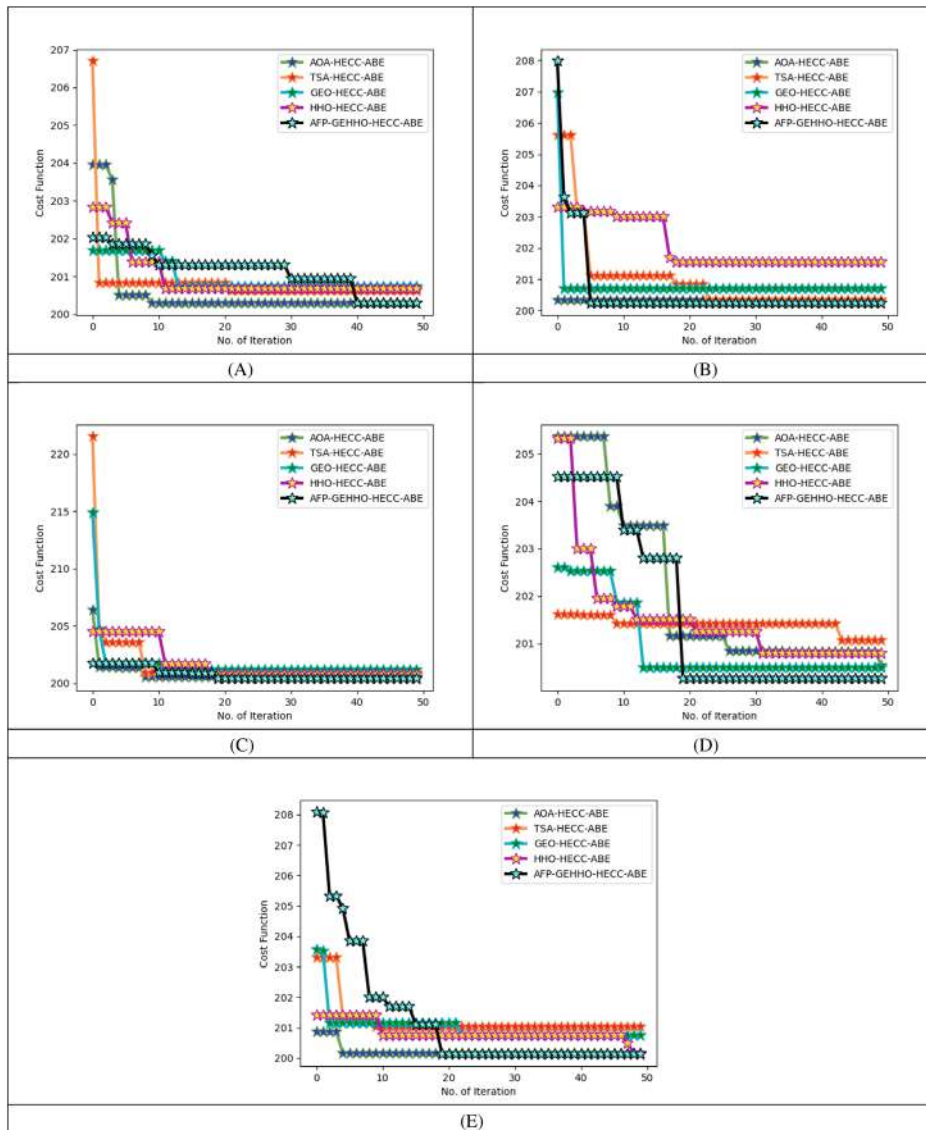


FIGURE 10 Convergence evaluation of the suggested encryption scheme with respect to “(A) block size 5, (B) block size 10, (C) block size 15, (D) block size 20, and (E) block size 25”.

### 6.7 | Evaluation of the deployed trust verification model

The evaluation of the deployed trust verification model with respect to existing algorithms and classifiers is shown in Figures 11 and 12, respectively. The MSE of the deployed AFP-GEHHO-ADLSTM-AN framework for trust verification of users is 12.35%, 17.44%, 8.97%, and 12.35% lesser than the AOA-ADLSTM-AN, TSA-ADLSTM-AN, GEO-ADLSTM-AN, and HHO-ADLSTM-AN algorithms respectively at an activation function of ReLU.

### 6.8 | Time requirement examination of the suggested cryptography scheme

The time requirement by the generated cryptography scheme is compared with the other cryptography schemes as given in Figures 13 and 14. The encryption time required by the AFP-GEHHO-HECC-ABE cryptography scheme is 72.41%,

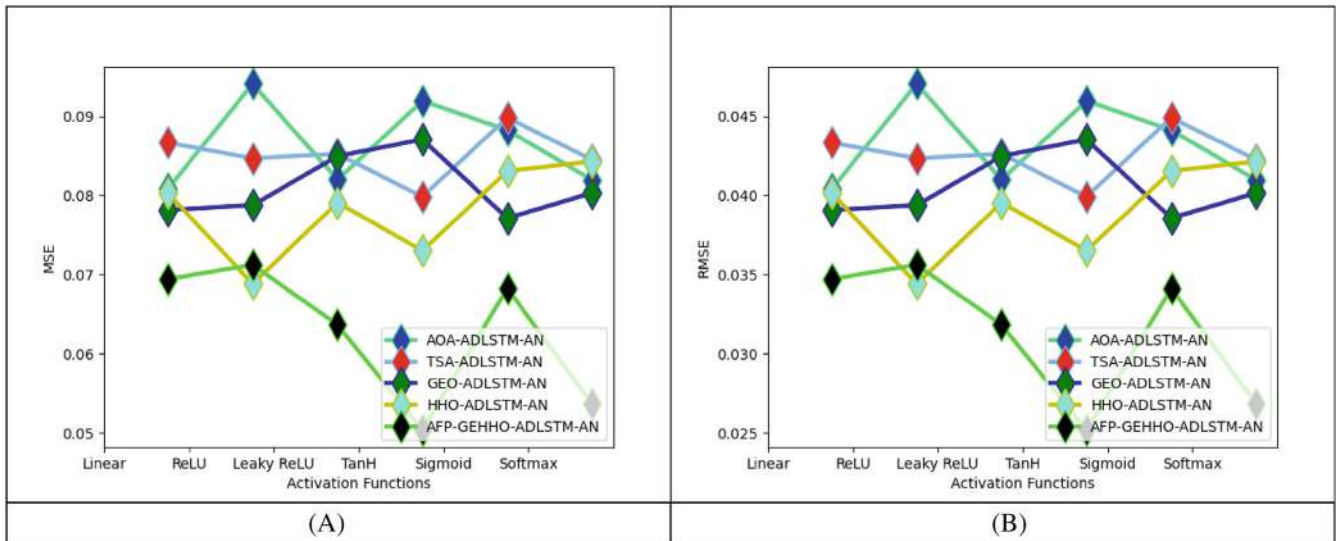


FIGURE 11 Algorithmic evaluation of the deployed trust verification model in terms of “(A) MSE, and (B) RMSE”.

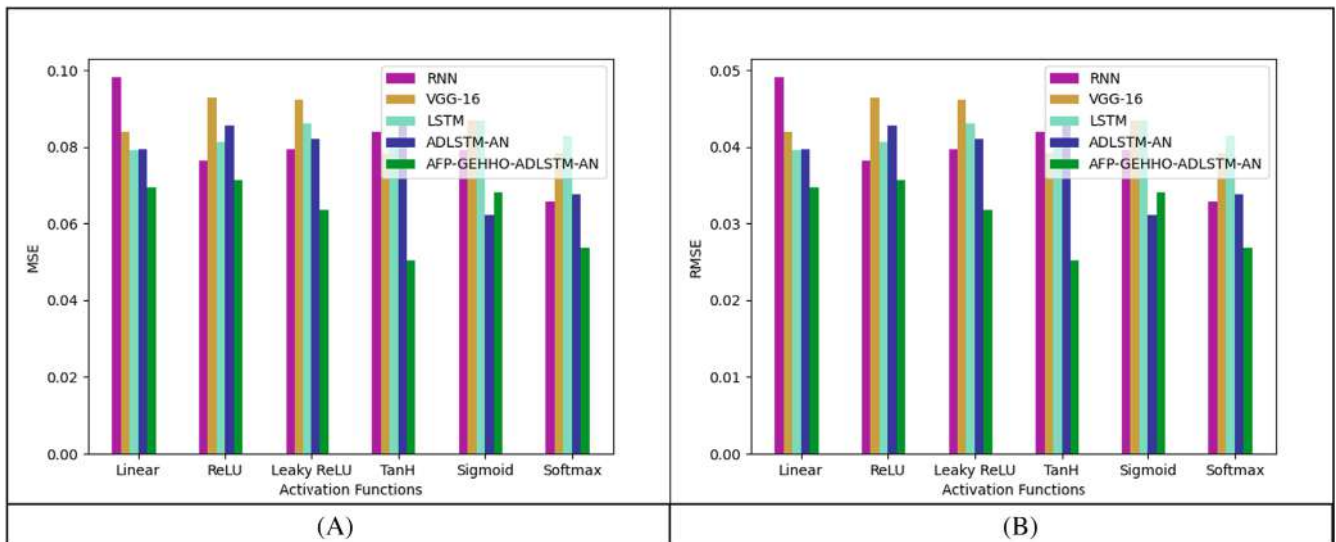


FIGURE 12 Classifier analysis of the proposed trust verification framework in terms of “(A) MSE, and (B) RMSE”.

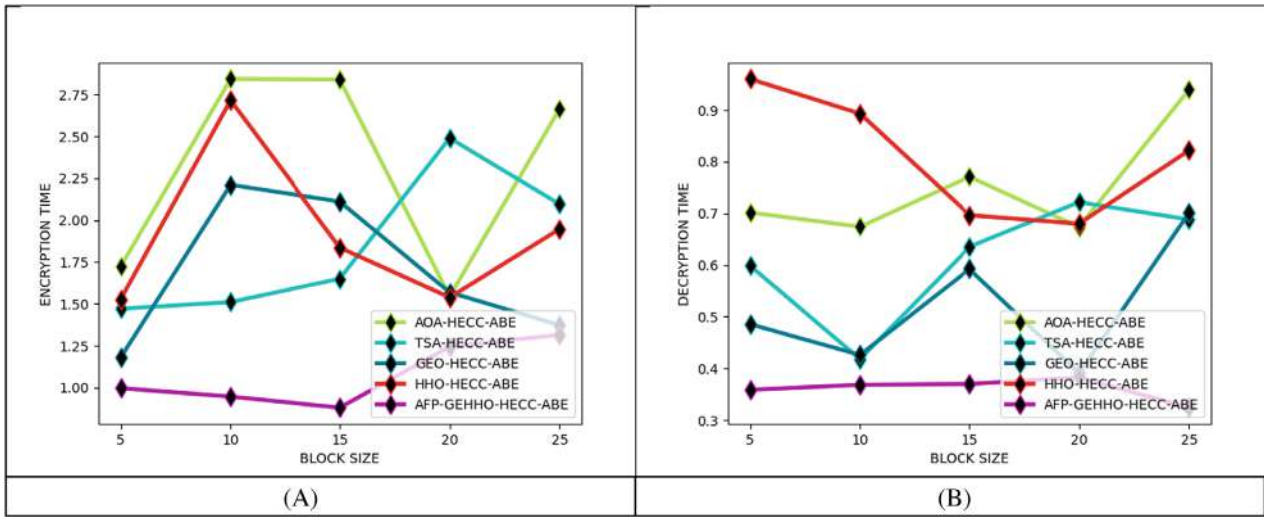


FIGURE 13 Time requirement-based evaluation of the suggested model with respect to “(A) encryption time, and (B) decryption time”.

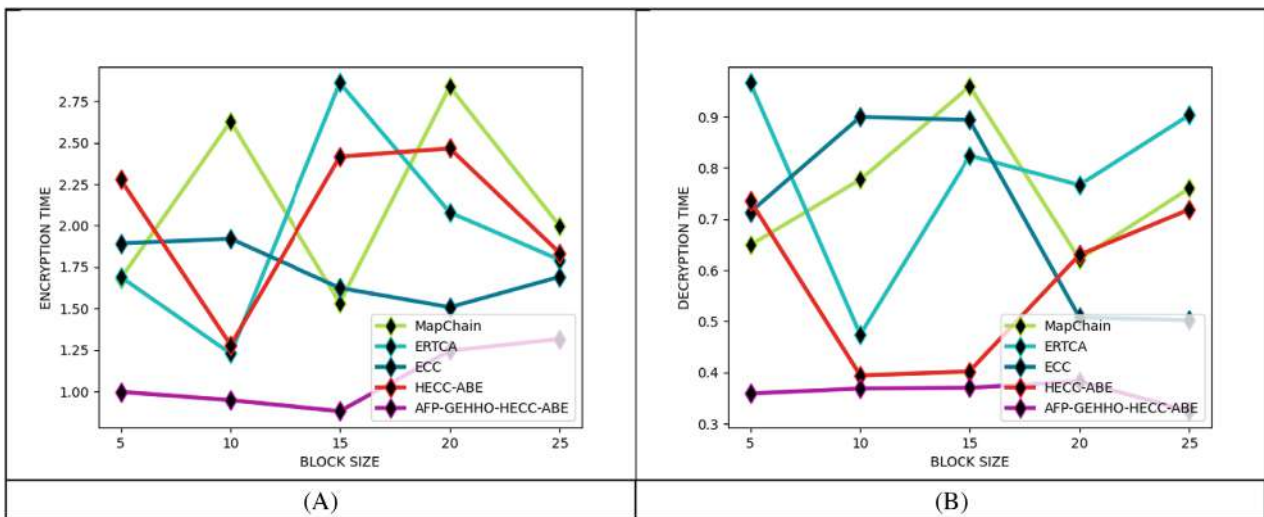


FIGURE 14 Time requirement-based evaluation of the suggested model with respect to “(A) encryption time, and (B) decryption time”.

46.67%, 63.64%, and 69.23% lesser than the AOA-HECC-ABE, TSA-HECC-ABE, GEO-HECC-ABE, and HHO-HECC-ABE algorithms, respectively at a block size of 10.

### 6.9 | Memory consumption evaluation

The memory consumption of the designed cryptography scheme is compared with the other cryptography schemes as given in Figure 15. The encryption time required by the AFP-GEHHO-HECC-ABE cryptography scheme is 6.54%, 12.28%, 4.76%, and 10.71% lesser than the MapChain, ERTCA, ECC, and HECC-ABE cryptography schemes, respectively at a block size of 5.

### 6.10 | Examination of the deployed user authentication model

The algorithm-based evaluation of the implemented user authentication model is given in Table 2, and the classifier-based evaluation of the implemented user authentication framework is given in Table 3. The accuracy of the implemented

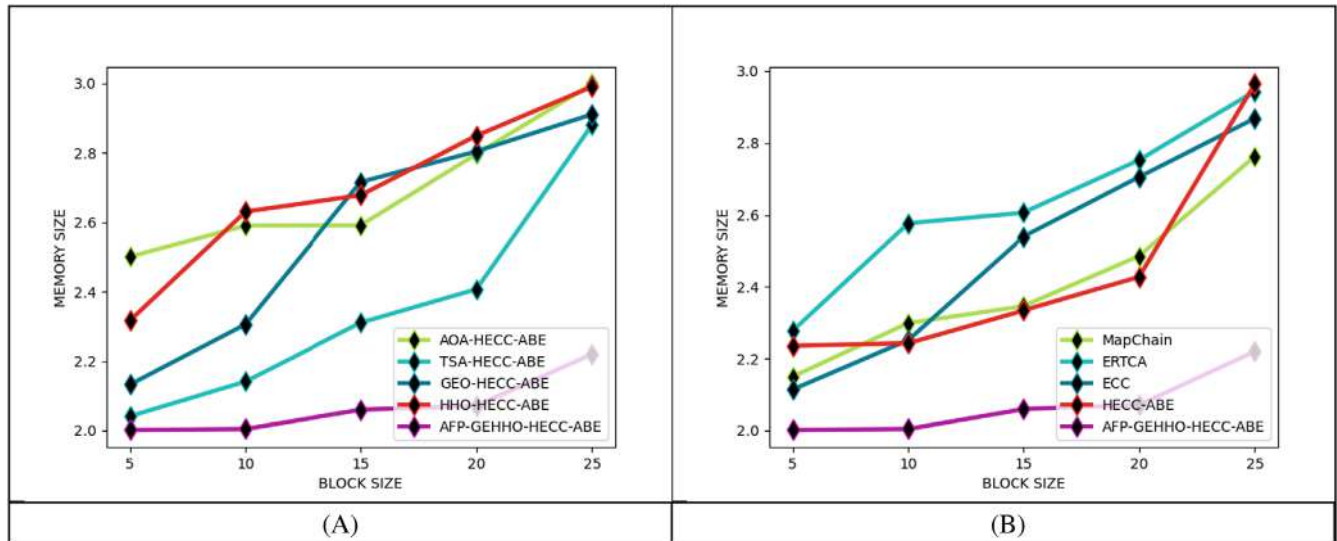


FIGURE 15 Memory consumption-based analysis of the generated framework with respect to “(A) various algorithms, and (B) different classifiers”.

TABLE 2 Algorithmic examination of the deployed user authentication model.

Terms/ Algorithm	AOA- ADLSTM-AN <sup>37</sup>	GEO- ADLSTM-AN <sup>33</sup>	TSA- ADLSTM-AN <sup>38</sup>	HHO- ADLSTM-AN <sup>35</sup>	AFP-GEHHO- ADLSTM-AN
NPV	93.182	95.376	94.253	94.798	95.954
Recall	93.750	95.833	94.792	95.313	96.354
Specificity	94.798	95.376	94.798	94.798	95.954
F1-Score	94.488	95.833	95.039	95.313	96.354
FPR	5.202	4.624	5.202	5.202	4.046
Precision	95.238	95.833	95.288	95.313	96.354
FDR	4.762	4.167	4.712	4.688	3.646
FNR	6.250	4.167	5.208	4.688	3.646
MCC	0.885	0.912	0.896	0.901	0.923
Accuracy	94.247	95.616	94.795	95.068	96.164

AFP-GEHHO-ADLSTM-AN framework for user authentication is 13.96%, 7.01%, 9.01%, and 7.67% higher than the RNN, VGG-16, LSTM, and AD-LSTM-AN classifiers, respectively.

## 6.11 | Statistical evaluation of the user authentication model

The statistical evaluation of the implemented user authentication model is tabulated in Table 4. The best of the implemented AFP-GEHHO-ADLSTM-AN user authentication model is 94%, 94%, 76%, and 76% less than the TSA-ADLSTM-AN, HHO-ADLSTM-AN, AOA-ADLSTM-AN, and GEO-ADLSTM-AN algorithms, respectively.

## 6.12 | Comparison of the recommended trust verification model

The comparison of the recommended trust verification model is tabulated in Tables 5 and 6 with respect to various algorithms and classifiers, respectively. The MSE of the recommended AFP-GEHHO-ADLSTM-AN framework

TABLE 3 Classifier-based examination of the deployed user authentication model.

Terms/ Classifiers	RNN <sup>39</sup>	VGG16 <sup>31</sup>	LSTM <sup>28</sup>	ADLSTM- AN <sup>29</sup>	AFP-GEHHO- ADLSTM-AN
FPR	16.185	10.405	11.561	10.405	4.046
Accuracy	84.384	89.863	88.219	89.315	96.164
NPV	83.333	89.080	86.932	88.068	95.954
Precision	85.340	90.576	89.418	90.476	96.354
Specificity	83.815	89.595	88.439	89.595	95.954
MCC	0.687	0.797	0.764	0.786	0.923
FNR	15.104	9.896	11.979	10.938	3.646
F1-Score	85.117	90.339	88.714	89.764	96.354
FDR	14.660	9.424	10.582	9.524	3.646
Recall	84.896	90.104	88.021	89.063	96.354

TABLE 4 Statistical evaluation of the user authentication model.

Measures/ Algorithm	TSA- ADLSTM-AN <sup>38</sup>	HHO- ADLSTM-AN <sup>35</sup>	AOA- ADLSTM-AN <sup>37</sup>	GEO- ADLSTM-AN <sup>33</sup>	AFP-GEHHO- ADLSTM-AN
Best	0.001	0.001	0.00025	0.00025	0.00006
Standard deviation	0.008	0.001	0.008	0.013	0.006
Worst	0.034	0.004	0.047	0.059	0.022
Median	0.001	0.001	0.004	0.00025	0.00006
Mean	0.005	0.002	0.007	0.005	0.003

TABLE 5 Algorithmic comparison of the recommended trust verification framework.

Terms/ Algorithm	TSA- ADLSTM-AN <sup>38</sup>	AOA- ADLSTM-AN <sup>37</sup>	HHO- ADLSTM-AN <sup>35</sup>	GEO- ADLSTM-AN <sup>33</sup>	AFP-GEHHO- ADLSTM-AN
MD	2.055	1.986	1.849	1.918	1.233
TWONORM	0.858	0.843	0.793	0.737	0.652
RMSE	0.045	0.044	0.042	0.039	0.034
MAE	0.012	0.011	0.010	0.009	0.007
INFINITYNORM	0.248	0.241	0.234	0.249	0.240
SMAPE	0.023	0.023	0.021	0.022	0.014
ONENORM	4.205	4.099	3.614	3.320	2.473
MSE	0.090	0.088	0.083	0.077	0.068
MASE	13.048	12.888	11.248	10.282	7.750



TABLE 6 Classifier comparison of the recommended trust verification framework.

Terms/ Classifiers	VGG16 <sup>31</sup>	RNN <sup>39</sup>	ADLSTM-AN <sup>29</sup>	LSTM <sup>28</sup>	AFP-GEHHO-ADLSTM-AN
RMSE	0.043	0.040	0.031	0.044	0.034
MD	1.918	1.712	1.644	1.781	1.233
MSE	0.087	0.079	0.062	0.087	0.068
MASE	12.385	10.136	7.417	12.405	7.750
MAE	0.011	0.009	0.007	0.011	0.007
TWONORM	0.830	0.755	0.595	0.831	0.652
ONENORM	3.927	3.242	2.406	3.954	2.473
SMAPE	0.022	0.020	0.019	0.020	0.014
INFINITYNORM	0.248	0.248	0.234	0.234	0.240

TABLE 7 Statistical analysis.

Algorithms/ Terms	GEO-HECC-ABE <sup>33</sup>	AOA-HECC-ABE <sup>37</sup>	TSA-HECC-ABE <sup>38</sup>	HHO-HECC-ABE <sup>35</sup>	AFP-GEHHO-HECC-ABE
Block size 5					
Worst	201.689	203.953	206.697	202.837	202.035
Best	200.727	200.291	200.631	200.685	200.290
Standard deviation	0.406	0.964	0.843	0.643	0.526
Mean	200.966	200.598	200.832	200.987	201.142
Median	200.727	200.291	200.631	200.685	201.301
Block size 10					
Standard deviation	0.878	0.000	1.311	0.743	1.333
Worst	206.966	200.341	205.611	203.315	207.979
Median	200.695	200.341	200.326	201.564	200.232
Mean	200.820	200.341	201.018	202.098	200.628
Best	200.695	200.341	200.326	201.564	200.232
Block size 15					
Median	201.171	200.551	200.911	200.785	200.387
Worst	214.856	206.414	221.531	204.497	201.715
Mean	201.619	200.784	201.721	201.725	200.739
Best	201.171	200.551	200.911	200.779	200.387
Standard deviation	1.964	0.854	3.000	1.503	0.520
Block size 20					
Median	200.495	201.154	201.426	201.254	200.259
Mean	200.974	202.105	201.410	201.546	201.603
Worst	202.611	205.363	201.615	205.326	204.513
Best	200.495	200.535	201.071	200.791	200.259
Standard deviation	0.823	1.746	0.154	1.109	1.783
Block size 25					
Mean	201.019	200.219	201.242	200.859	201.291
Best	200.747	200.162	201.026	200.159	200.128
Worst	203.579	200.874	203.304	201.427	208.081
Standard deviation	0.551	0.193	0.616	0.308	2.010
Median	200.747	200.162	201.026	200.752	200.128

for trust verification is 24.22%, 22.73%, 18.07%, and 11.69% less than the TSA-ADLSTM-AN, AOA-ADLSTM-AN, HHO-ADLSTM-AN, and GEO-ADLSTM-AN algorithms, respectively.

### 6.13 | Statistical analysis

The statistical analysis of the recommended cryptography scheme is tabulated in Table 7. The worst of the recommended AFP-GEHHECC-ABE cryptography scheme is 2.21%, 3.59%, 2.35%, and 3.3% higher than the GEO-HECC-ABE, AOA-HECC-ABE, TSA-HECC-ABE, and HHO-HECC-ABE algorithms, respectively for block size 25.

## 7 | CONCLUSION

A secure data storage model for storing healthcare data in blockchain was designed using a deep learning approach and was implemented successfully. Wearable sensors were used by IoT networks to gather healthcare data from the patient. Before storing the medical data onto the blockchain, the user's authentication was initially validated. The user's biometrics and private information were gathered, and these details were supplied into the user authentication structure constructed by AD-LSTM-AN. Once the user's authentication was confirmed, then the user's trust was verified. The same AD-LSTM-AN-based verification structure was used to verify the historical data that has been stored and retrieved by the user, together with their previous transactions, in this phase. The healthcare data were then sent to the HECC-ABE cryptography schemes for data encryption once the authentication and trust of the person who attempts to store the data were confirmed. An AFP-GEHHECC algorithm was used for optimizing the keys of the cryptography scheme. The encrypted data of the authorized user with a high level of trust was stored in the blockchain platform. The same processes were done in reverse order whenever a user needed to retrieve the stored medical information from the blockchain. The effectiveness of secure data storage in blockchain was tested through various experimental simulations. The experimental results suggested that the deployed secure data storage system for healthcare IoT in blockchain has an accuracy of 13.96%, 7.01%, 9.01%, and 7.67% higher than the RNN, VGG-16, LSTM, and AD-LSTM-AN classifiers, respectively. From the results, it was confirmed that the security provided by this model in storing the healthcare IoT-related medical data in blockchain is more secure, effective, accurate, and precise, has less error, and minimizes the time and memory requirements. The major issue of this research work is depicted as follows. In this developed medical health record system, the doctors or hospitals have access to a patient's records, and also the healthcare sector gets affected. Here, if the patient wants to see his medical records, it has been a lengthy and inconvenient procedure. Additionally, the developed system needs to add more data security methods and approaches that can help to create a way for new features. In the future, we will add more advanced data security methods and approaches to reduce the lengthy procedure of the medical health record system. Accordingly, we will try to apply our developed method to other types of real-world applications.

### DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

### ORCID

Anil Kumar Dubey  <https://orcid.org/0000-0002-8992-3463>

### REFERENCES

1. Ren J, Li J, Liu H, Qin T. Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT. *Tsinghua Sci Technol.* 2022;27(4):760-776.
2. Prasad AVK. Deep learning based optimization for detection of attacks in IoT. *J Netw Commun Syst.* 2021;4(2):31-36.
3. Chinaei MH, Gharakheili HH, Sivaraman V. Optimal witnessing of healthcare IoT data using blockchain logging contract. *IEEE Internet Things J.* 2021;8(12):10117-10130.
4. Abou-Nassar EM, Iliyasa AM, El-Kafrawy PM, Song O-Y, Bashir AK, El-Latif AAA. DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. *IEEE Access.* 2020;8:111223-111238.
5. Sabu S, Ramalingam HM, Vishaka M, Swapna HR, Hegde S. Implementation of a secure and privacy-aware E-health record and IoT data sharing using blockchain. *Global Trans Proc.* 2021;2(2):429-433.
6. Janaiah B. Attack detection in IoT using DBN based optimization algorithm. *J Netw Commun Syst.* 2022;5(1):40-49.

7. Shukla S, Thakur S, Hussain S, Breslin JG, Jameel SM. Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model. *Internet Things*. 2021;15:100422.
8. Liu L, Li Z. Permissioned blockchain and deep reinforcement learning enabled security and energy efficient healthcare internet of things. *IEEE Access*. 2022;10:53640-53651.
9. Yazdinejad A, Srivastava G, Parizi RM, Dehghantanha A, Choo K-KR, Aledhari M. Decentralized authentication of distributed patients in hospital networks using blockchain. *IEEE J Biomed Health Inform*. 2020;24(8):2146-2156.
10. ElRahman SA, Alluhaidan AS. Blockchain technology and IoT-edge framework for sharing healthcare services. *Soft Comput*. 2021;25:13753-13777.
11. Kumar A, Krishnamurthi R, Nayyar A, Sharma K, Grover V, Hossain E. A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. *IEEE Access*. 2020;8:118433-118471.
12. Kumar R, Kumar P, Tripathi R, Gupta GP, Islam AKMN, Shorfuazzaman M. Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems. *IEEE Trans Industr Inform*. 2022;18(11):8065-8073.
13. Ray PP, Chowhan B, Kumar N, Almogren A. BIoTHR: electronic health record servicing scheme in IoT-blockchain ecosystem. *IEEE Internet Things J*. 2021;8(13):10857-10872.
14. Zhang J, Yang Y, Liu X, Ma J. An efficient blockchain-based hierarchical data sharing for healthcare internet of things. *IEEE Trans Industr Inform*. 2022;18(10):7139-7150.
15. Ray PP, Dash D, Salah K, Kumar N. Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases. *IEEE Syst J*. 2021;15(1):85-94.
16. Yongjoh S, So-In C, Kompunt P, Muneesawang P, Morien RI. Development of an internet-of-healthcare system using blockchain. *IEEE Access*. 2021;9:113017-113031.
17. Gohar AN, Abdelmawgoud SA, Farhan MS. A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and IoT. *IEEE Access*. 2022;10:92137-92157.
18. Ray PP, Kumar N, Dash D. BLWN: blockchain-based lightweight simplified payment verification in IoT-assisted e-healthcare. *IEEE Syst J*. 2021;15(1):134-145.
19. Mayer AH, Rodrigues VF, Costa CA, Righi RR, Roehrs A, Antunes RS. FogChain: a fog computing architecture integrating blockchain and internet of things for personal health records. *IEEE Access*. 2021;9:122723-122737.
20. Demirbaga U, Aujla GS. MapChain: a blockchain-based verifiable healthcare service management IoT-based big data ecosystem. *IEEE Trans Netw Serv Manag*. 2022;19(4):3896-3907.
21. Bataineh MR, Mardini W, Khamayseh YM, Yassein MMB. Novel and secure blockchain framework for health applications in IoT. *IEEE Access*. 2022;10:14914-14926.
22. Aujla GS, Jindal A. A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring. *IEEE J Sel Areas Commun*. 2021;39(2):491-499.
23. Zulkifl Z, Khan F, Tahir S, et al. FBASHI: fuzzy and blockchain-based adaptive security for healthcare IoTs. *IEEE Access*. 2022;10:15644-15656.
24. Hossein KM, Esmaeili ME, Dargahi T, Khonsari A, Conti M. BCHealth: a novel blockchain-based privacy-preserving architecture for IoT healthcare applications. *Comput Commun*. 2021;180:31-47.
25. Sharmila AH, Jaisankar N. Edge intelligent agent assisted hybrid hierarchical blockchain for continuous healthcare monitoring & recommendation system in 5G WBAN-IoT. *Comput Netw*. 2021;200:108508.
26. Rathee G, Sharma A, Saini H, Kumar R, Iqbal R. A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimed Tools Appl*. 2020;79:9711-9733.
27. Arul R, Alroobaea R, Tariq U, Almulihi AH, Alharithi FS, Shoaib U. IoT-enabled healthcare systems using block chain-dependent adaptable services. *Personal Ubiquitous Comput*. 2021.
28. Tran L, Hoang T, Nguyen T, Kim H, Choi D. Multi-model long short-term memory network for gait recognition using window-based data segment. *IEEE Access*. 2021;9:23826-23839.
29. Schoene AM, Lacey G, Turner AP, Dethlefs N. Dilated LSTM with attention for classification of suicide notes. Proceedings of the Tenth International Workshop on Health Text Mining and Information Analysis (LOUHI 2019). 2019 136-145.
30. Zhang H, Zhang Q, Shao S, Niu T, Yang X. Attention-based LSTM network for rotatory machine remaining useful life prediction. *IEEE Access*. 2020;8:132188-132199.
31. Campos-Leal JA, Yee-Rendón A, Vega-López IF. Simplifying VGG-16 for plant species identification. *IEEE Latin Am Trans*. 2022;20(11):2330-2338.
32. Zhang Y, He D, Choo K-KR. BaDS: blockchain-based architecture for data sharing with ABS and CP-ABE in IoT. *Wirel Commun Mob Comput*. 2018;2018:9.
33. Mohammadi-Balani A, Nayeri MD, Azar A, Taghizadeh-Yazdi M. Golden eagle optimizer: a nature-inspired metaheuristic algorithm. *Comput Ind Eng*. 2021;152:107050.
34. Amor N, Noman MT, Petru M, Sebastian N. Comfort evaluation of ZnO coated fabrics by artificial neural network assisted with golden eagle optimizer model. *Sci Rep*. 2022;12(6350):6350.
35. Elgamal ZM, Yasin NBM, Tubishat M, Alswaiti M, Mirjalili S. An improved Harris hawks optimization algorithm with simulated annealing for feature selection in the medical field. *IEEE Access*. 2020;8:186638-186652.
36. Hu H, Ao Y, Bai Y, Cheng R, Xu T. An improved Harris's hawks optimization for SAR target recognition and stock market index prediction. *IEEE Access*. 2020;8:65891-65910.

37. Abualigah L, Diabat A, Mirjalili S, Elaziz MA, Gandomi AH. The arithmetic optimization algorithm. *Comput Methods Appl Mech Eng*. 2021;376:113609.
38. Kiran MS. TSA: tree-seed algorithm for continuous optimization. *Expert Syst Appl*. 2015;42(19):6686-6698.
39. Kim J, Lee Y, Kim E. Accelerating RNN transducer inference via adaptive expansion search. *IEEE Signal Process Lett*. 2020;27:2019-2023.
40. Sethia D, Sahu R, Yadav S, Kumar R. Attribute revocation in ECC-based CP-ABE scheme for lightweight resource-constrained devices. Paper presented at: 2021 International Conference on Communication, Control and Information Sciences (ICCISc), Idukki, India. 2021.
41. Ersoy M, Gürfidan R. Blockchain-based asset storage and service mechanism to metaverse universe: metarepo. *Emerg Telecommun Technol*. 2023;34(1).
42. Gürfidan R, Ersoy M. A new approach with blockchain based for safe communication in IoT ecosystem. *J Data Inf Manag*. 2022;4:49-56.
43. Gürfidan R, Ersoy M. Blockchain-based music wallet for copyright protection in audio files. *J Comput Sci Technol*. 2021;21(1):e2.
44. Amara M, Siad A. Elliptic curve cryptography and its applications. Paper presented at: 7th international workshop on systems, Signal Processing and their Applications (WOSSPA). 2011 247-250.
45. Rana A, Reddy A, Shrivastava A, Verma D, Ansari MS, Singh D. Secure and smart healthcare system using IoT and deep learning models. Paper presented at: 2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS). 2022 915-922.
46. Jayashri N, Rampur V, Gangodkar D, Abirami M, Balarengadurai C, Kumar NA. Improved block chain system for high secured IoT integrated supply chain. *Meas: Sensors*. 2023;25:100633.

**How to cite this article:** Dubey AK, Ramanjaneyulu N, Saraswat M, Brammya G, Govindasamy C, Ninu Preetha NS. HECC-ABE: A novel blockchain-based IoT healthcare data storage using hybrid cryptography schemes with key optimization by hybrid meta-heuristic algorithm. *Trans Emerging Tel Tech*. 2023;e4839. doi: 10.1002/ett.4839