Sādhanā (2023)48:206
https://doi.org/10.1007/s12046-023-02249-2

Secure and privacy in healthcare data using quaternion based neural network and encoder-elliptic curve deep neural network with blockchain on the cloud environment

P SUGANTHI[1,*] and R KAVITHA[2]

[1]Department of CSBS, Thiagarajar College of Engineering, Madurai, India
[2]Department of IT, Velammal College of Engineering and Technology, Madurai, India
e-mail: suga.pathma@gmail.com

MS received 13 July 2022; revised 8 June 2023; accepted 8 July 2023

Abstract. The security and privacy of healthcare data are crucial aspects within the healthcare industry, as accurate diagnoses rely on medical professionals accessing patient healthcare data. Similarly, patients often require access to their data. However, ensuring that sensitive health data is shared securely while prioritizing privacy is essential. This paper proposes an innovative solution called the quaternion based neural network, Advanced Data Security Architecture in Healthcare Environment (ADSAH), which combines Elliptical curve cryptography (ECC) with a blockchain mechanism and a Deep Fuzzy Based Neural Network (DFBNN) to safeguard cloud-stored health data. The proposed approach begins by encoding the input medical data using an encoder and then encrypting the encoded data using ECC techniques. The secret key for encrypting the data is securely stored within a blockchain framework. The key is divided into blocks to enhance security, and the SHA algorithm is employed to identify key events within these blocks. These key events are subsequently stored in a cloud storage system. A modified genetic algorithm is utilized to generate the encryption and decryption key. This algorithm is explicitly tailored to secure healthcare data. Authorized patients or physicians can access medical data using the secret key to decrypt and retrieve the necessary information. The performance of the proposed network is evaluated by considering factors such as time and cost and is compared against existing studies. The evaluation demonstrates notable improvements, including a reduction in the time required for the encryption and decryption process, as well as a decrease in transaction and execution costs when compared to previous research. By incorporating ECC with a blockchain mechanism and DNN, the ADSAH approach offers an advanced solution for ensuring the security and privacy of cloud-stored health data. It provides robust encryption and facilitates efficient and cost-effective access to authorized individuals while safeguarding sensitive health information.

Keywords. Healthcare data; security; deep neural network; improved quaternion based neural network; blockchain mechanism; elliptic curve cryptography.

1. Introduction

The healthcare industry is of paramount importance as it delivers vital medical services and continually strives to enhance patient outcomes through technological advancements, innovative treatments, and public health initiatives [1]. Despite these advancements, ensuring the security and privacy of patient data remains a pressing concern within the healthcare sector. While healthcare professionals require access to patient healthcare data for accurate diagnoses and effective treatments, it is equally vital to prioritize the secure and private sharing of sensitive health information [2]. Protecting patient's privacy is imperative to maintain trust and confidentiality in healthcare interactions. To address these concerns, robust measures must be implemented to safeguard patient data against unauthorized access, breaches, and misuse. Achieving a balance between data accessibility and privacy preservation is paramount in the healthcare industry, as it allows for effective healthcare delivery while respecting patient rights [3].

Therefore, comprehensive and reliable solutions are needed to establish stringent security measures and ensure the utmost privacy protection in the healthcare data ecosystem. Maintaining patient data privacy has become increasingly challenging with the digitization of healthcare records and the widespread use of cloud storage systems [4, 5]. Existing techniques for securing healthcare data often need to be revised to address privacy concerns

[*] For correspondence

Published online: 23 September 2023

adequately [6]. These techniques may need more robust encryption mechanisms, efficient access controls, and secure storage methods [7, 8]. As a result, healthcare organizations face the risk of data breaches, unauthorized access, and misuse of sensitive patient information [9]. This paper proposes a novel solution called the Advanced Data Security Architecture in Healthcare Environment (ADSAH) to address these challenges and enhance the security and privacy of cloud- stored health data. ADSAH combines Elliptical curve cryptography (ECC) [10] with a blockchain mechanism and deep Fuzzy Based Neural Network (DFBNN) [11] to provide a comprehensive and practical approach to safeguarding patient data [12, 13]. The ADSAH technique presents numerous advantages in overcoming the shortcomings of current privacy protection methods. It leverages advanced encryption techniques, specifically Elliptical curve cryptography (ECC), to establish a robust layer of data security and ensure the utmost confidentiality of sensitive information. Through integrating a blockchain framework, ADSAH provides a secure storage mechanism for encryption keys, enhancing critical management practices and mitigating the risk of unauthorized access. Additionally, ADSAH integrates a modified genetic algorithm [14, 15], enabling efficient encryption and decryption processes that significantly reduce time requirements and enhance overall system performance. This combination of cutting-edge encryption, secure key storage, and optimized algorithms makes ADSAH an effective solution for bolstering data privacy in healthcare settings. Through integrating ECC (blockchain) and DNN, the proposed ADSAH enables secure access and retrieval of medical data for authorized individuals like patients and physicians. This integration ensures efficient and controlled data sharing while upholding patient privacy. By addressing the limitations of existing methods, ADSAH provides a comprehensive and advanced solution to safeguard patient data in cloud-based healthcare environments. The incorporation of ECC strengthens data security, while the utilization of DNN-based DFBNN processes the encrypted data using deep learning capabilities and fuzzy logic to handle uncertainty and imprecision. It performs analysis and decision-making tasks on the encrypted data while preserving its confidentiality. By utilizing the proposed ADSAH, healthcare organizations can protect patient data effectively while facilitating seamless and protected access for authorized users.

The main contributions of the paper are as follows.

- Introducing a ground-breaking approach called the Advanced Data Security Architecture in Healthcare Environment (ADSAH) that addresses the secure handling of patient data within healthcare settings.
- The ADSAH technique incorporates Elliptical Curve Cryptography (ECC) with a blockchain mechanism, Deep Fuzzy Based Neural Network (DFBNN), to ensure healthcare data's seamless and efficient transfer.
- Within the Blockchain mechanism, the keys are converted into blocks, and subsequently, the SHA algorithm is employed to recognize and process them.

The experiments are conducted to demonstrate the effectiveness of the proposed technique.

1.1 *Blockchain*

Recent growth of blockchain technology assists in solving the interoperability challenges in healthcare and plays a major role in maintaining patient's record at the centre of ecosystem. Thereby, blockchain improves the privacy, security and interoperability. Generally, blockchain can be used in sharing and accessing the medical record of patients and also in remote monitoring. Blockchain is used in medical data management system which permits patients to maintain ownership over the available records.

The main advantages of using the blockchain are

- Single point failure and performance bottlenecks are avoided.
- Patients may view and manage their data.
- The blockchain guarantees the consistency, precision, simplicity, completeness, and timeliness of medical data history.
- The patient network participants may see every step of the blockchain procedure.
- The data insertions are also unchangeable. Unauthorised alterations have been discovered.

1.2 *Privacy preservation*

The major focus is on how to completely manage privacy problems and forecast efficacy, especially when it comes to sensitive medical data kept in third parties. As a result, in order to prevent the loss of privacy associated with medical data, data mining techniques for privacy preservation should be developed. Accordingly, Machine Learning (ML) algorithms possess innate abilities of effective learning. Such abilities could be employed in blockchain for enhancing the smartness of the chain. This integration could also be valuable in enhancing the security of blockchain distributed ledger. With the ability in predicting the system behavior, using various ML algorithms optimizes blockchain mechanisms. No privacy preservation approach currently in use provides the necessary privacy protection. It is quite effective, practical and useful. The capacity of blockchain to provide adequate privacy protection is represented by security analysis. The objective of the study involves:

1. To use improved quaternion based neural network cryptography, elliptical curve cryptography to generate

keys, encrypt data, and decode data in order to protect shared data.

2. To implement blockchain technology, which converts keys into blocks and then recognises them using the ADSHA algorithm.
3. To put the encrypted data in a cloud storage system and provide authorised patients and clinicians access to it.

1.3 *Novelty of the proposed system*

Proposed framework permits the clinicians for transferring their data in encrypted format to cloud which hosts the corresponding network. A neural network is fed with input (plain text) and neurally based pseudo-random numbers (in vector form). Results of process include weights and cipher text in hidden-layers. In accordance with the changes in weight based on the pseudo-random number, cipher text alters in accordance with it. Hence, this permits the model to be highly secured. The study proposes Modified Genetic Algorithm, wherein, based on fitness-function, keys are generated and these keys are utilized for encryption. Such encrypted predictions could be sent to secret-key owner who could decrypt them. The proposed system is highly secured as the training-input adjusts its weight in accordance with the trained data.

As the model quickly and easily provides overall output, plain text encryption is accomplished easily for producing cipher text in less time with the updated key-generation approach. With the use of several nodes and hidden layers, it enhances the model complexity, thereby affording high cryptosystem security. The keys generated with Modified Genetic Algorithm are integrated with the hidden weights. Thus, even when an intruder attempts to hack any data, it is not possible to decrypt it. Owner of the data could possess confidence upon their data as it is safely stored in cloud. The proposed system seems to exist as a potential-source for the public-key cryptographic approaches which does not rely on the number theoretic-operations and possess memory and time complexities. The outcomes reveal the better performance of the proposed system while comparison with conventional studies in accordance with security. In blockchain, third-parties are not needed for verifying the transactions. The consensus approaches are utilized for maintaining the consistency of data on the blockchain networks. The ethereum possess 3 kinds of consensus approaches (PoS-Proof of Stake, PoW-Proof of Work and PoA-Proof of Authority). In this study, PoW consensus approach is executed in the fusion-chain with Ethereum as it assists only PoW. This approach is implemented with full-node type, block creation and block validation, wherein, CPU overhead tends to increase. To ensure the smooth and effective transfer of healthcare data, the ADSAH approach combines Elliptical Curve Cryptography (ECC) with a blockchain mechanism known as Deep Fuzzy Based Neural Network (DFBNN).

2. Related works

This study aims to evaluate the performance of various encryption and decryption schemes for securing medical data transmitted wirelessly. The study assesses the execution time, throughput, average data rate, and information entropy of encryption schemes such as Blowfish, DES, AES, RC4, RSA, ECC, CBE, MTLM, and CEC [16]. This paper proposes a hybrid cryptographic algorithm combining RC4, ECC, and SHA-256 to enhance the security of sensitive information in IoT-based intelligent irrigation systems. By encrypting the RC4 key with ECC and applying SHA-256 for hashing, the proposed scheme ensures data integrity and protection against known attacks [17]. This paper addresses the privacy and efficiency challenges in IoT devices and applications that rely on continuous data collection. The paper presents a hybrid approach where the initial layers of a deep neural network are run on the IoT device, and the output is sent to the cloud for further processing. To ensure privacy, the paper introduces Siamese fine-tuning to prevent unwanted inferences in the data [18]. This paper uses blockchain technology to enhance healthcare systems by improving health record management, insurance billing, and data security. It explores solutions such as Hyperledger Fabric, Composer, Docker Container, and Hyperledger Caliper to measure the performance of blockchain-based systems. This paper aims to propose GuardHealth, a decentralized Blockchain system for innovative electronic medical records (EMRs), ensuring secure and privacy-preserving data sharing. GuardHealth focuses on managing confidentiality, authentication, and data preservation while utilizing consortium Blockchain, smart contracts, and a trust model with Graph Neural Network (GNN) for malicious node detection [19]. The proposed framework addresses the challenges of log record protection and real-time anomaly detection in IoT systems. By leveraging Blockchain and smart contracts, it ensures data integrity and automates anomaly detection, overcoming issues with high communication overhead and tampering vulnerability in existing methods [20]. This paper addresses the privacy and control issues associated with centralized health data storage in IoT systems. The proposed scheme, Healthchain, utilizes blockchain technology to preserve the privacy of health data by encrypting it and implementing fine-grained access control [21]. This paper aims to shed light on the constraints of conventional health information technology in delivering personalized and patient- centric care. It underscores the transformative potential of blockchain technology in overcoming these limitations by offering decentralized and secure solutions for data access, storage, and payment systems in healthcare

[22]. This study aims to address the security vulnerabilities in a multiserver authentication scheme proposed by Wang *et al* to manage the increasing number of users in a mobile network. The authors demonstrate the insecurity of Wang *et al* scheme against various attacks and propose an improved scheme to mitigate these security weaknesses [23]. The focus is on addressing the security, privacy, and trust issues in intelligent healthcare, a crucial aspect of smart cities. The authors propose a human-in- the-loop-aided (HitL-aided) scheme to preserve privacy in intelligent healthcare. The scheme incorporates a block design technique to obfuscate health indicators and introduces the concept of human-in-the-loop to enable privacy-controlled access to health reports [24]. This paper aims to address the research challenge of achieving efficient data search and sharing in cloud-assisted IoT systems while ensuring sensor data security in healthcare applications. The authors propose a solution called proxy re-encryption with equality test (PRE- ET) by combining the concepts of proxy re-encryption (PRE) and public key encryption with equality test (PKE-ET) [25]. This paper aims to address the security and privacy concerns in IoT-enabled healthcare infrastructure by proposing a novel encryption scheme. The scheme combines elliptic curve cryptography, Advanced Encryption Standard (AES), and Serpent to secure healthcare data [26]. The paper discusses using cryptographic algorithms for access contro l in IoMT-based healthcare systems, emphasizing algorithms like RC6, elliptic curve digital signature, and SHA256 for data integrity. It highlights how adopting high-security algorithms enhances availability and confidentiality and protects sensitive information from implantable devices, strengthening healthcare services [27]. This research addresses the challenge of storing and securely transferring healthcare data by proposing the LRO-S encryption method. This method combines lionized remora optimization and improved security algorithms to generate secure keys for the serpent encryption algorithm [28]. This paper addresses the security concerns in transmitting ECG data to cardiologists for telecardiology services. The proposed method focuses on securing the ECG transmission using a triple data encryption standard (3-DES) for encryption and a water cycle optimization (WCO) algorithm for authentication [29]. This research addresses the security concerns in healthcare data and services by proposing a content-aware DNA computing system for encrypting medical images [30]. This research addresses the security and privacy concerns of storing and accessing patients' health data in cloud computing environments. The vulnerability of patient data to various cyberattacks necessitates the implementation of encryption mechanisms to protect sensitive health information. This paper proposes a hybrid cryptography approach to securely share health data over the cloud, ensuring data privacy and secrecy [31–33].

2.1 *Significance of blockchain in healthcare sector*

As the study focuses on blockchain in healthcare, significance and usage of blockchain in healthcare as claimed by conventional studies are presented to afford a comprehensive view about it in existing researches [34–36].

The recommended study has explained about the significance of blockchain in health care during pandemic situation. The application of blockchain technology includes digital data storage, public surveillance system, disease control, supporting the supply chain of medical parts, healthcare instruments tracking, enhanced the transparency during treatment of patients, assist in storing and transferring the information related to treatment, helps in efficient healthcare management and provides better healthcare protection [37, 38].

2.2 *Research gap*

The recommended study has confessed that blockchain technology is prone to have information decay, lack of scalability and non-standardization. Hence, the new approaches may be integrated with blockchain technology to overcome the existing drawbacks.

As the healthcare services are complex in nature, the blockchain technology is still in a budding stage. Therefore, more empirical base is needed to make the existing mechanism highly conclusive and emphatic which may reduce the complexity of the existing system.

Scalability acts as a major limitation, as validation needs more time because of the authorization of transactions from majority of nodes. Additionally, complexity of blockchain and need for extensive network of users is considered as another disadvantage. And also, privacy preservation acts as a major limitation in using blockchain technology in health care.

3. Methodology

Through the implementation of the proposed work improved quaternion neural network cryptography is used to encrypt the shared healthcare data in order to achieve strong security. The ADSAH, a robust security framework is established for encrypting shared health data. This approach incorporates key generation, encryption, and decryption processes to optimize complexity and execution time. The overall process is depicted in figure 1, showcasing the seamless flow of data security measures. In the ADSAH framework, private medical data uploaded by physicians is encrypted using the ECC encryption technique. The secret key associated with the encrypted data is securely stored using blockchain technology, utilizing a block-based storage approach. Key events within these blocks are identified using the SHA algorithm, bolstering

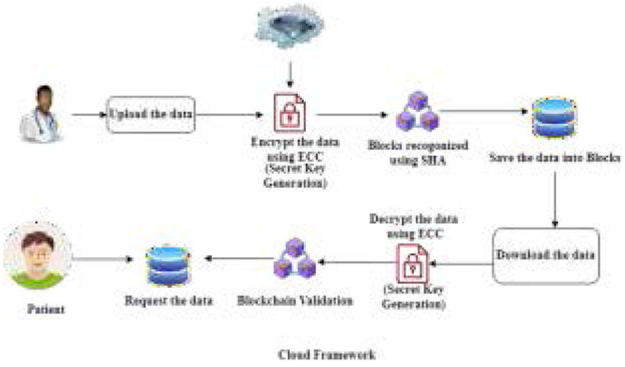
Upload the data
Encrypt the data using ECC (Secret Key Generation)
Blocks recognized using SHA
Save the data into Blocks
Download the data
Decrypt the data using ECC
(Secret Key Generation)
Blockchain Validation
Request the data
Patient
Cloud Framework

Figure 1. An implementation framework for the proposed methodology.

security measures. The encrypted and secured data is then stored in a cloud storage system, ensuring its accessibility and integrity. Using the secret key, authorised patients or medical professionals can access the medical information. The data is decrypted using the ADSAH encryption and decryption processes, enabling the retrieval of secure medical data. The data remains protected and stored within the cloud environment throughout the process, safeguarding its confidentiality and privacy (figures 2 and 3).

3.1 *Proposed ADSAH*

3.1.1 *Elliptic curve cryptography (ECC) algorithm:*

In hospital management, the security of user-related data, encompassing patient information, medical records, and medication details, holds immense significance. However, hospitals encounter significant challenges in ensuring data security. To tackle this issue, this paper proposes the adoption of the elliptic curve cryptography (ECC) algorithm for encryption and decryption processes. ECC is an asymmetric cryptographic algorithm that utilizes private and public keys for encryption and decryption operations. One notable advantage of ECC over non-ECC algorithms like RSA and DSA is its ability to provide equivalent security with smaller key sizes. In other words, ECC achieves the same level of protection as different algorithms while requiring shorter key lengths. The name “elliptic curve cryptography” stems from using elliptic curves as the foundation of its mathematical framework. Elliptic curves are described by cubic functions, specifically equations of degree 3. The equation of an elliptic curve follows the form $y^2 = x^3 + (a * x) + b$, where a and b are constants defining the curve. The coordinates of the elliptic curve equation are represented as (x_1, y_1), (x_2, y_2) and so on [32]. By harnessing the power of elliptic curves and their underlying mathematical principles, the ECC algorithm provides a secure and efficient solution for encrypting and decrypting sensitive user data within the realm of hospital management. It offers robust security while minimizing the required key sizes, making it appropriate for safeguarding confidential information within healthcare systems.

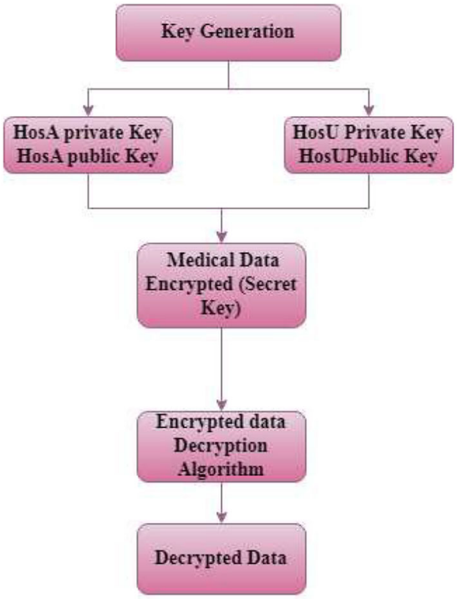

Figure 2. ECC Encryption process workflow.

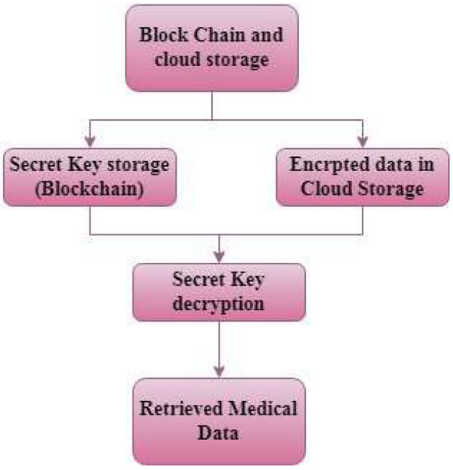
Block Chain and cloud storage
Secret Key storage (Blockchain)
Encrpted data in Cloud Storage
Secret Key decryption
Retrieved Medical Data

Figure 3. ECC Decryption process workflow.

The process begins by initiating the algorithm. For each user, their username and password are obtained. If the user’s credentials are authenticated, they are granted access to a secret key within the system. This authentication check is performed iteratively, allowing multiple users to be established. If a user is found invalid during the authentication process, the algorithm proceeds to handle this case. It displays a message indicating the user is invalid and then exits the algorithm. Once the authentication process is completed, the algorithm moves on to the next phase, which involves storing the data securely in a cloud storage system using blockchain technology. This integration ensures the data integrity and provides a secure and decentralized storage solution. After the data is securely stored, the algorithm reads the plain text data. The next step involves initiating the ECC encryption process in the Edge Server. During this process, public and private keys are generated using Algorithm 1, which will be crucial for the subsequent encryption and decryption operations. Following key generation, the algorithm performs the encryption process using Algorithm 2. This process transforms the plain text data into an encrypted form, ensuring its confidentiality and protection against unauthorized access. To enable the decryption of the encrypted data, a request for the decryption process is made in the Edge Server. If the user is authenticated for decryption, the algorithm performs the decryption process using Algorithm 3. This process utilizes the previously generated keys to decrypt the encrypted data and retrieve the original plaintext. Once the decryption process is completed, the data is securely stored in the cloud server and blockchain technology. This dual storage approach enhances the security and persistence of the data. Finally, authenticated users are granted access to view their data securely. This ensures privacy and confidentiality by restricting data access only to authorized individuals

Algorithm 1- public, private, and secret Key Generation

```
Input: User $HosU$ data; Key size: 516 bits
Output: public, private, and secret key of $HosU\&HosA$
Step 1: create $E$
Step 2: generate $G$
Step 3: for-each User $HosU$ do;
Step 4: create private and public keys of $HosA$
Step 5: create private key$N_{HosA}$ of $HosA$; where $N_{HosA} <$ n
Step 6: compute public key $P_{HosA}$ of $HosA$; where $P_{HosA} = N_{HosA}(G)$
Step 7: create the private key and Public key of $HosU$
Step 8: create private key $N_{HosU}$of $HosU$; where $N_{HosU} < n$
Step 9: compute public key $P_{HosU}$ of $HosU$; where $P_{HosU} = N_{HosU} * G$
Step 10: create a secret key of $HosA$; $kHosA = N_{HosA} * P_{HosU}$
Step 11: create secret key of $N_{HosU}$; $kHosU = N_{HosU} * P_{HosA}$
Step 12: end for-each;
```

According to Algorithm 1, the aim is to generate public, private, and secret keys for Hospital Users *HosU* and the Hospital Authority *HosA*. The key size is specified as 516 bits. First, a variable E is created. Then, a point G is generated. For each Hospital User *HosU* in the system, the algorithm proceeds a private key and public key are created for the Hospital Authority *HosA*. The private key is denoted as N_{HosA}, where N_{HosA} is a randomly generated value that is less than the total number of keys n. The public key of *HosA*, denoted as P_{HosA}, is computed as the scalar multiplication of N_{HosA} and G: $P_{HosA} = N_{HosA}(G)$. Similarly, private and public keys are created for the Hospital User *HosU*. The private key for *HosU* is denoted as N_{HosU}, and it is randomly generated such that $N_{HosU} < n$. The public key of *HosU*, denoted as P_{HosU}, is computed as $P_{HosU} = N_{HosU} * G$. To establish the secret key for each entity, the algorithm performs the following calculations: The secret key of HosA, kHosA, is computed as the scalar multiplication of N_{HosA} and P_{HosU}: *HosA*; $kHosA = N_{HosA} * P_{HosU}$. Similarly, the secret key of *HosU*, *kHosU*, is computed as $kHosU = N_{HosU} * P_{HosA}$. These steps are repeated for each Hospital User in the system.

Algorithm 2- plain text PT to cipher text CP_{pt}

```
Input: plain text $PT$
Output: cipher text $CP_{pt}$
Step 1: read $PT$
Step 2: encode $PT -> EP => EP_{pt}$
Step 3: compute $CP$
Step 4: compute $CP_{pt}$; $CP_{pt} = \{K * G, EP_{pt} + K * P_{HosU}\}$
Step 5:compute $X - coordinate = K * G$; $Y - coordinate = EP_{pt} + K * P_{HosU}$
```

The algorithm 2 takes a plain text message *PT* as input and aims to produce a cipher text CP_{pt} as output. First, the plain text message *PT* is read. Next, the plain text message *PT* is encoded, resulting in an encoded message EP_{pt}, which represents the transformed version of the original message using a specific encoding scheme. Then, the algorithm proceeds to compute the cipher text *CP*. The cipher text CP_{pt} is calculated using the formula: $CP_{pt} = \{K * G, EP_{pt} + K * P_{HosU}\}$, where K is a randomly generated scalar value, G is a predefined point, and P_{HosU} is a public key associated with the Hospital User. The computation of CP_{pt} involves two components: the X-coordinate and the Y-coordinate. The X- coordinate is determined by multiplying $K * G$, while the Y-coordinate is obtained by adding $EP_{pt} + K * P_{HosU}$.

```
**Algorithm 3-** cipher text $CP_{pt}$ **to** plain text PT
**Input**: Cipher text
**Output**: Plain text
Step 1: get cipher point $CP_{pt}$ at receiver end
Step 2: compute $Z = KG * N_{HosU}$
Step 3: subtract $Z$ from $Y$ coordinates and compute the following:
Step 4: $HosU < -EP_{pt} + K * P_{HosU} - (Z)$
Step 5: $HosU < -EP_{pt} + K * P_{HosU} - (KG * N_{HosU})$
Step 6: $HosU < -EP_{pt} + K * P_{HosU} - K * P_{HosU}$ where $P_{HosU} = N_{HosU} * G$
Step 7: $HosU < -EP_{pt}$
```

The algorithm 3 aims to decrypt a cipher text and retrieve the original plain text message. Given the cipher text, the receiver obtains the cipher point CP_{pt} as an input. To decrypt the cipher text, the receiver computes Z by multiplying the predefined point $KG * N_{HosU}$ associated with the Hospital User. Next, the algorithm subtracts Z from the Y coordinates of the cipher point and performs the following computations:

$$HosU < -EP_{pt} + K * P_{HosU} - (Z)$$

$$HoSU < -EP_{pt} + K * P_{HosU} - (KG * N_{HosU})$$

$$HosU < -EP_{pt} + K * P_{HosU} - K *$$

P_{HosU} where $P_{HosU} = N_{HosU} * G$ Finally, the algorithm simplifies the expression to: $HosU < - EP_{pt}$

3.1.2 *Deep fuzzy based neural network (DFBNN):* In this section we discussed about the DFBNN which is based On Deep Neural Network (DNN) concept. The proposed ADSAH technique employs a combination of ECC and DFBNN algorithms for secure data analysis and decision-making. It starts by encrypting the data using ECC, which utilizes elliptic curves and cryptographic keys to ensure confidentiality during transmission or storage. The encrypted data, along with other relevant information, is securely stored, such as in a blockchain or secure database. The DFBNN, which combines deep learning and fuzzy logic, is then used for data analysis. The figure 4 depicts the DFBNN architecture, which is made up of several layers, nodes, and fuzzy rules, and it is trained on labeled data to learn patterns and relationships in the encrypted data. The DFBNN processes the encrypted data using deep learning capabilities and fuzzy logic to handle uncertainty and imprecision. It performs analysis and decision-making tasks on the encrypted data while preserving its confidentiality. When the analysis is complete, the encrypted results are retrieved, and the private key associated with ECC encryption is used to decrypt the data back to its original form, allowing for interpretation or further use.

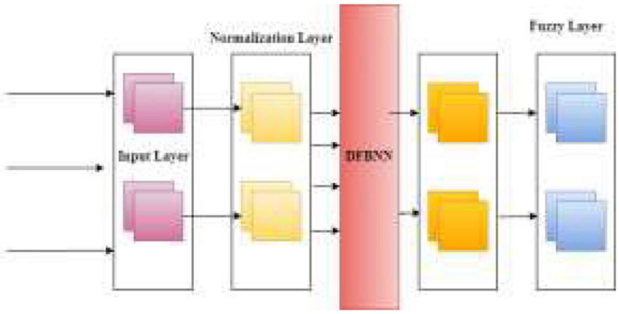

Figure 4. DFBNN Architecture.

```
Step 1: Initialization:
        $DaTr$ = Data for training (scene data and situation labels).
        $DaTr_m$ = $m$ number of training data $DaTr$.
        $X_i$ = For input $X$, ith input of the scene data
        $\hat{X}_i$ = Input normalized data.
        $F_{train}()$ = Function to train the hidden layers of deep network
        $Fun_{act}$ =Activation function for the deep neural network
        $DNN_{imp}$ = Improved deep neural network (DNN)
        $F_{norml}()$ =For input normalization
        $F_{fuzz\_out}$ =Output Fuzzification
        $Fout\_DNN_{imp}$ =Training of the $DNN_{imp}$
Step 2: Offline training of the $DNN_{imp}$
Step 3: $i \leftarrow 0$;
Step 4: $do\ i++$
Step 5:             $\hat{X}_i \leftarrow F_{norm}(DaTr)$;
Step 6:               $F_{train}(Fun_{act}, \hat{X}_i)$;
Step 7: $while\ i > DaTr_m$is false go back to line 2
Step 8: $Ftrain_{DNN_{imp}(DNN_{imp},DaTr)}$;
Step 9: Online training of the $DNN_{imp}$:
Step 10:    $t \leftarrow 0$;
Step 11:    $do\ t++$
Step 12:        $\hat{X}_i$ ←Normalized $(X_i)$;
Step 13:        $\hat{b_i} \leftarrow Fout_{DNN_{imp}}(\hat{X}_i, DNN_{imp})$;
Step 14:        $p_i \leftarrow F_{fuzz_{out}}(\hat{b_i})$;
Step 15:        $while\ DaTr \geq DaTr_{max}$is false, go back to line 9
```

The algorithm starts with an initialization step, where the necessary variables and functions are defined. These include the training data $DaTr$, the number of training data $DaTr_m$, input variables X_i normalized input data $\hat{X}_i$, functions for training the hidden layers of the deep network

F_{train}, activation function for the deep neural network Fun_{act}, the improved deep neural network DNN_{imp}, functions for input normalization F_{norml} and output fuzzification F_{fuzz_out}, and the training of the improved DNN $Fout\_DNN_{imp}$. In the offline training phase, the DNN_{imp} is trained using the training data $DaTr$. Then, in a loop starting from Step 3, the algorithm iterates through the training process. Each iteration involves normalizing the input data and training the hidden layers of the deep network. The loop continues until the condition $i > DaTr_m$ is false, and then DNN_{imp} is further trained. The online training phase begins with initializing the variable t. In the subsequent loop, the algorithm performs online training. It involves normalizing the input data and obtaining the output of the DNN_{imp} $\widehat{b_i}$ for the normalized input. Fuzzifying the output p_i using $F_{fuzz_{out}}\left(\widehat{b_i}\right)$ and repeating the process until the condition $DaTr \geq DaTr_{max}$ is false. The algorithm continues to iterate through the online training phase until the desired criteria for the maximum number of training data $DaTr_{max}$ or the maximum number of iterations $DaTr_{max}$ are met. the training of the improved DNN $Fout\_DNN_{imp}$. In the offline training phase, the DNN_{imp} is trained using the training data $DaTr$. Then, in a loop starting from Step 3, the algorithm iterates through the training process. Each iteration involves normalizing the input data and training the hidden layers of the deep network. The loop continues until the condition $i > DaTr_m$ is false, and then DNN_{imp} is further trained. The online training phase begins with initializing the variable t. In the subsequent loop, the algorithm performs online training. It involves normalizing the input data and obtaining the output of the DNN_{imp} $\hat{b_i}$ for the normalized input. Fuzzifying the output pi using $F_{fuzz_{out}}(\hat{b_i})$ and repeating the process until the condition $DaTr \geq DaTr_{max}$ is false. The algorithm continues to iterate through the online training phase until the desired criteria for the maximum number of training data $DaTr_{max}$ or the maximum number of iterations $DaTr_{max}$ are met.

3.1.3 *Modified genetic algorithm (GA):* As we discussed earlier, in the context of the proposed ADSAH system, a modified genetic algorithm can be used to generate encryption and decryption keys. The genetic algorithm is a search and optimization technique inspired by natural selection and genetics. Figures 5 and 6 illustrates the process of key generation using genetic algorithm [14].

Figure 7 represents the framework for the practical implementation of the model. The cloud framework will be based on the hospital networks. The doctors could create new files and add them to the network, which will be protected using the proposed techniques. The files stored in the cloud server would be accessed by the patient based on privacy, and they could only read the data.

Algorithm 2- Modified Genetic Algorithm for Key Generation

```
P(t) − Pop(i)
Input: Initialised the data
Output: Generated Key
   i ← 0
   Init_Population [Pop(i)]; Initialises the population.
   Eval_Population [Pop(i)]; Evaluates the population.
   While not terminating,
   do
           Pop'(i)
     ← Variation [Pop(i)]; Creates new solutions
      Eval_Population [Pop'(t)]; Evaluates the new solutions
           Pop(i + 1) ← ApplyGeneticOperators
             [Pop'(i)U Q]; Next, generation pop.
                     i ← i + 1;
                   end while.
   Population having maximum fitness value
                 is selected as key.
```

4. Results and discussion

This part presents the findings from the performance analysis, comparison analysis, and environmental setup conducted during the execution of the proposed system.

4.1 *Environmental setup*

In our proposed work, the evaluation is conducted by implementing programs using the Java programming language version 1.8. The computer system used for the evaluation consists of an Intel Core i5 processor with a clock speed of 3.30 GHz. It is equipped with 8 GB of RAM and runs on the Windows 8 operating system, which is a 64-bit OS. This specific hardware and software configuration is chosen to provide a suitable computing environment for our experiments. The Intel Core i5 processor offers a good balance between performance and cost, while the 8 GB of RAM ensures sufficient memory capacity for running the programs and handling the computational tasks involved for training and evaluation. By utilizing this, we can execute our programs efficiently and collect relevant data to evaluate the performance of the proposed ADSAH.

4.2 *Comparative analysis*

4.2.1 *Uploading time:* According to figure 8, for the data size of 1MB, ADSAH achieves an uploading time of 3.98 milliseconds, which is significantly lower than the other methods such as CE (5.6 ms), LR (10.89 ms), RCE (5.6 ms), DOM (5.6 ms), and ECC-CRT (4.38 ms). This indicates that ADSAH has optimized the uploading process for faster data transfer. As the data size increases to 2MB, ADSAH still maintains its superiority with an uploading time of 6.2 ms, outperforming CE (8.68 ms), LR (16.24 ms), RCE (8.68 ms), DOM (8.68 ms), and ECC-CRT (5.42

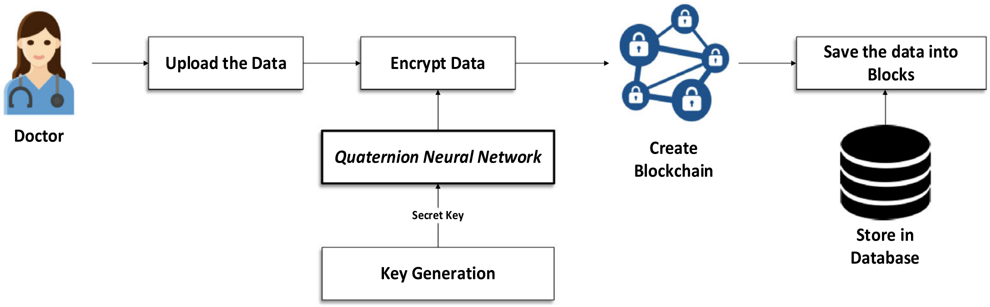

Figure 5. Key generation for the doctor.

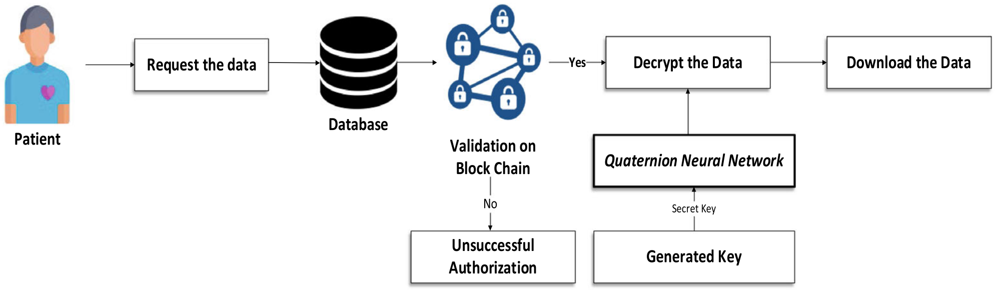

Figure 6. Key generation for the patient.

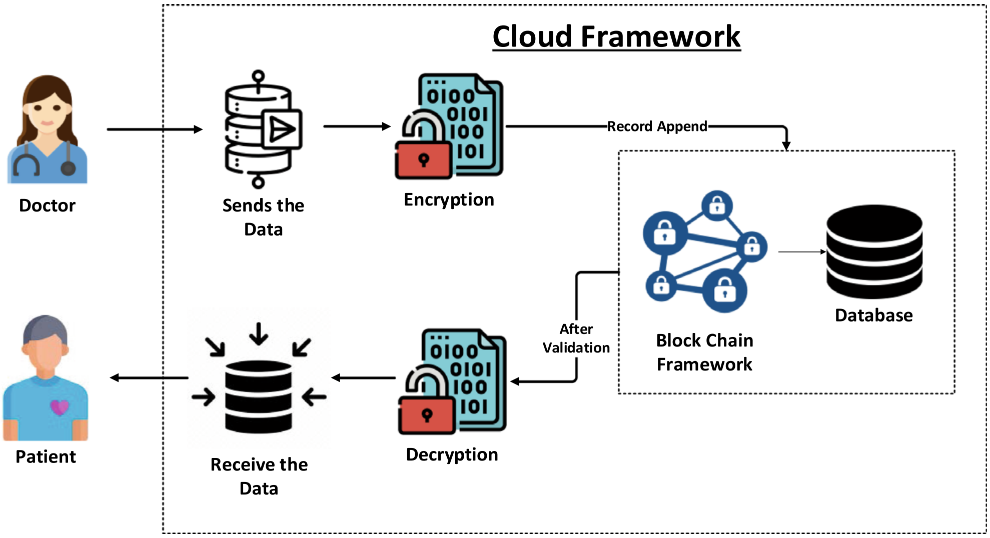

Figure 7. An implementation of overall framework.

ms). The trend continues as the data size grows. For 4MB, 6MB, 8MB, and 10MB, ADSAH consistently exhibits lower uploading times compared to the other methods. This demonstrates that ADSAH has been designed to efficiently handle larger data sizes and minimize the time required for data uploading.

4.2.2 *Downloading time:* ADSAH, the proposed method, demonstrates faster data retrieval compared to other methods for a data size of 1MB, achieving a downloading time of 3.23ms. This superiority is maintained as the data size increases to 2MB, with ADSAH recording a downloading time of 4.89ms,

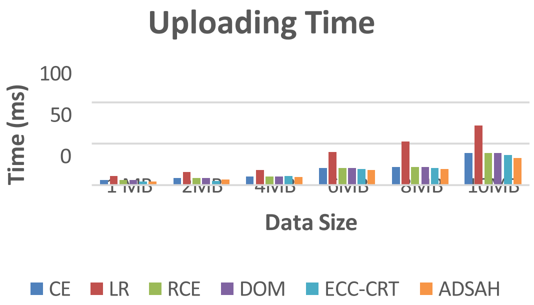

Figure 8. Uploading time.

outperforming the alternative methods. This trend continues for larger data sizes, such as 4MB, 6MB, 8MB, and 10MB. When it comes to the data size of 10 MB it achieving the time with 31.98 ms when compared with the other CE, LR, RCE, DOM, ECC-CRT as 34.92 ms, 34.92ms, 34.92ms, 35ms, 33.89ms respectively, was clearly depicted in figure 9. Where ADSAH consistently exhibits lower downloading times compared to the other methods. These findings highlight the efficiency and effectiveness of ADSAH in facilitating faster data retrieval, regardless of the data size.

4.2.3 *Encryption time comparison:* Figure 10 represents the encryption time comparison for different encryption methods at various input data sizes (in KB), the term of time evaluated in terms of (milliseconds). The encryption times are provided for the following methods: 3DES & ECC & SHA-256, RC4 & 3DES & SHA-256, AES & RC4 & SHA-256, AES & 3DES & SHA-256, RC4 & AES & SHA-256, and the proposed ADSAH method. By analyzing the figure, we can observe that the proposed ADSAH method consistently demonstrates lower encryption times compared to the other encryption methods for all data sizes. This indicates that ADSAH is more efficient in terms of encryption time. For example, at a data size of 200 KB, the proposed ADSAH method has an encryption time of 19.63 ms, while the other methods range from 28 ms to 35 ms. Similarly, at larger data sizes, such as 1000 KB, the proposed ADSAH method has an encryption time of 100.63 ms, outperforming the other methods with encryption times ranging from 119 ms to 168 ms. These results highlight the efficiency of the proposed ADSAH method in terms of encryption time. It offers faster encryption compared to the other methods, making it a more time-effective solution for securing data.

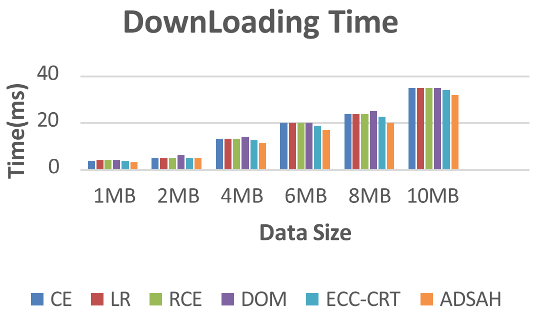

Figure 9. Downloading time.

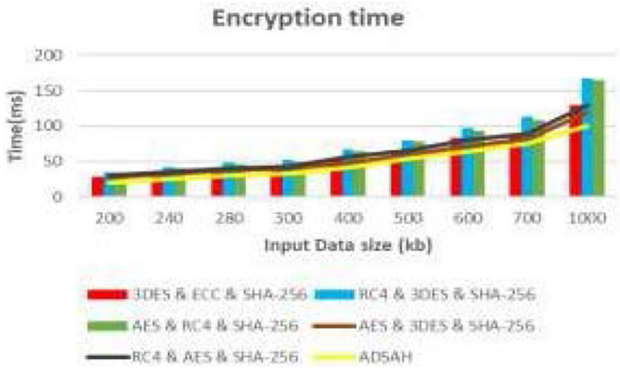

Figure 10. Encryption time comparison of the proposed model.

4.2.4 *Decryption time:* Figure 11 represents the decryption time comparison for different decryption methods at various input file sizes (in KB). The decryption times are provided for the following methods: 3DES & ECC & SHA-256, RC4 & 3DES & SHA- 256, AES & RC4 & SHA-256, AES & 3DES & SHA-256, RC4 & AES & SHA-256, and the proposed ADSAH method. By analyzing figure 8, we can observe that the proposed ADSAH method consistently demonstrates lower decryption times compared to the other decryption methods for all file sizes. This indicates that ADSAH is more efficient in terms of decryption time. For example, at a file size of 200 KB, the proposed ADSAH method has a decryption time of 17.66 ms, while the other methods range from 28 ms to 33 ms. Similarly, at larger file sizes, such as 1000 KB, the proposed ADSAH method has a decryption

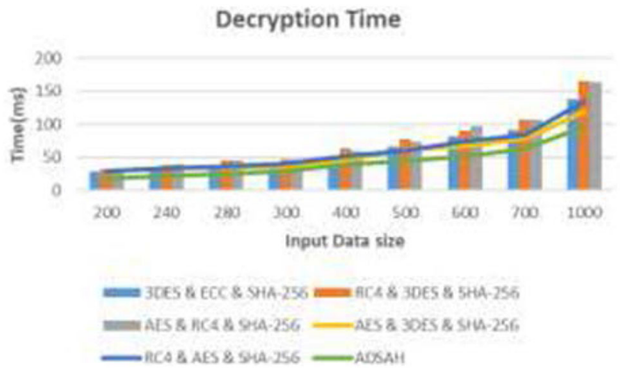

Figure 11. Decryption time comparison of the proposed model.

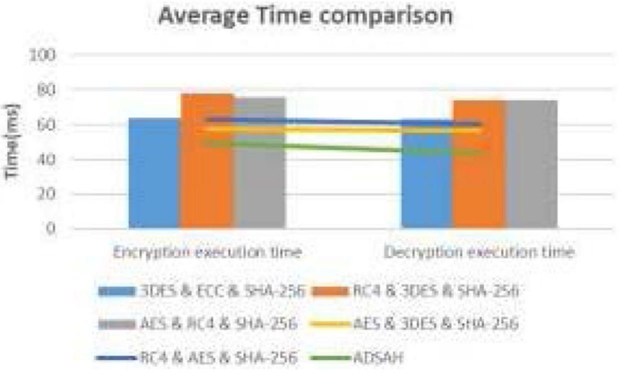

Figure 12. Average time comparison for encrypting and decrypting a file for the proposed model and the previous model.

time of 96.82ms, outperforming the other methods with decryption times ranging from 120 ms to 165 ms. These results highlight the efficiency of the proposed ADSAH method in terms of decryption time. It offers faster decryption compared to the other methods, making it a more time-effective solution for retrieving secured data. By minimizing the decryption time, ADSAH enhances the overall efficiency of the system, enabling quick access to decrypted data while ensuring its security.

4.2.5 *Average time comparison:* Figure 12 presents the average time comparison for encryption and decryption execution using different methods: 3DES & ECC & SHA-256, RC4 & 3DES & SHA-256, AES & RC4 & SHA-256, AES & 3DES & SHA-256, RC4 & AES & SHA- 256, and the proposed ADSAH method. In terms of encryption execution time, the proposed ADSAH method demonstrates the best performance with an average time of 49.28 ms. It outperforms the other methods, which range from 57.44 ms to 77.88 ms. This indicates that ADSAH offers faster encryption execution, making it more efficient in terms of time. Similarly, in terms of decryption execution time, the proposed ADSAH method shows superior performance with an average time of 43.44 ms. The other methods have average times ranging from 56.33 ms to 74.33 ms. Once again, ADSAH outperforms the alternatives, providing faster decryption execution. The performance of the proposed ADSAH method can be attributed to its optimized encryption and decryption algorithms, which are specifically designed to minimize execution time while maintaining data security. By reducing the average time required for encryption and decryption, ADSAH enhances the overall performance of the system, enabling efficient and timely data processing From table 1, it has been observed that, Scheme I has regarded to afford security for different attack methods like user anonymity, offline password attacks, stolen smart card attacks and server impersonation attack. Similarly, Scheme II has considered to afford security to offline password attacks, stolen smart card attacks, replay attacks, three factor secrecy and perfect forward secrecy. On contrary, the proposed method has considered to provide security for all the kinds of considered attacks as depicted in table 1 which confirms its ability than other schemes.

Table 2. Comparison of computation cost.

Scheme	Overall computation cost (ms)
Existing algorithm	74.33
Proposed algorithm	49.28

In addition, comparison has been performed in accordance with computational cost and the outcomes are shown in table 1.

From table 2, it has been revealed that, the existing methods have consumed high computational cost in comparison with the proposed system. Lower the computational cost, higher is the efficacy of the method. Hence, the proposed algorithm has been found to be effective than conventional algorithms.

Table 1. Security Performance comparison.

Attack methods	Scheme I	Scheme II	Proposed Method
User anonymity	√	×	√
Offline password attacks	√	√	√
Stolen smart card attacks	√	√	√
Known session- specific temporary information attack	×	×	√
User impersonation attack	×	×	√
Server impersonation attack	×	×	√
Replay attacks	√	√	√
Perfect forward secrecy	×	√	√
Three-factor secrecy	×	√	√

5. Conclusion

The suggested new novel solution improved quaternion based neural network and ADSAH with a blockchain mechanism maintained in a cloud environment secures private health data. The innovative approach to addressing the security and privacy risks associated with cloud-based healthcare data. To reduce complexity and time, the proposed cryptography approach performed the key generation, encryption, and decryption processes.

The blockchain system is used to manage multiple hash events, where the secret key is saved and handled by the ADSAH algorithm. A further enhancement in security is provided by the updated genetic algorithm's key generation process. The data is encrypted and kept securely in the cloud. Using the secret key, the authorised patient or doctor can access the confidential health information, after which the data is decrypted. The assessment findings demonstrate that compared to the previous study, the suggested approach reduces the time required for encryption and decryption. Comparatively, the cost of transaction and execution was also decreased as a result of the complexity reduction. It addresses the security and privacy challenges associated with healthcare data, providing a promising solution for the healthcare industry.

References

[1] Duan X, Guo D, Liu N, Li B, Gou M and Qin C 2020 A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network. *IEEE Access* 8: 25777–25788

[2] Itoo S, Khan A A, Kumar V, Alkhayyat A, Ahmad M and Srinivas J 2022 CKMIB: Construction of key agreement protocol for cloud medical infrastructure using blockchain. *IEEE Access* 10: 67787–67801

[3] Zala K, Thakkar H K, Jadeja R, Singh P, Kotecha K and Shukla M 2022 PRMS: design and development of patients' E-healthcare records management system for privacy preservation in third party cloud platforms. *IEEE Access* 10: 85777–85791

[4] Haddad A, Habaebi M H, Islam M R, Hasbullah N F and Zabidi S A 2022 Systematic review on AI-blockchain based E-healthcare records management systems. *IEEE Access*. https://doi.org/10.1109/ACCESS.2022.3201878

[5] Madine M M, Salah K, Jayaraman R, Yaqoob I, Al-Hammadi Y, Ellahham S and Calyam P 2020 Fully decentralized multi-party consent management for secure sharing of patient health records. *IEEE Access* 8: 225777–225791

[6] Gupta D N, Kumar R and Ansari S H 2022 Federated learning for an IoT application. In: *Federated Learning for IoT Applications*, Springer International Publishing, Cham, pp. 53–66

[7] Rasina Begum B and Chitra P 2021 ECC-CRT: an elliptical curve cryptographic encryption and Chinese remainder theorem based deduplication in cloud. *Wirel. Pers. Commun.* 116(3): 1683–1702

[8] Hamza R, Yan Z, Muhammad K, Bellavista P and Titouna F 2020 A privacy-preserving cryptosystem for IoT E-healthcare. *Inf. Sci.* 527: 493–510

[9] Ilokah M and Eklund J M 2020 A secure privacy preserving cloud-based framework for sharing electronic health data. In: *2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*, IEEE, pp. 5592–5597

[10] Christo M S, Jesi V E, Priyadarsini U, Anbarasu V, Venugopal H and Karuppiah M 2021 Ensuring improved security in medical data using ECC and blockchain technology with edge devices. *Secur. Commun. Netw.* 2021: 1–13

[11] Kwabena O A, Qin Z, Zhuang T and Qin Z 2019 Mscryptonet: multi-scheme privacy-preserving deep learning in cloud computing. *IEEE Access* 7: 29344–29354

[12] An J, Fu L, Hu M, Chen W and Zhan J 2019 A novel fuzzy-based convolutional neural network method to traffic flow prediction with uncertain traffic accident information. *IEEE Access* 7: 20708–20722

[13] Amosov O S, Ivanov Y S and Amosova S G 2019 Recognition of abnormal traffic using deep neural networks and fuzzy logic. In: *2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, IEEE, pp. 01–05

[14] Soni A and Agrawal S 2013 Key generation using genetic algorithm for image encryption. *Int. J. Comput. Sci. Mob. Comput. (IJCSMC)* 2(6): 376–383

[15] Tanwar S, Parekh K and Evans R 2020 Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* 50: 102407

[16] Adedeji K B, Nwulu N I, Aigbavboa C and Gbadamosi S L 2019 Assessment of encryption and decryption schemes for secure data transmission in healthcare systems. In: *2019 IEEE AFRICON*, IEEE, pp. 1–6

[17] Mousavi S K, Ghaffari A, Besharat S and Afshari H 2021 Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems. *J. Ambient Intell. Human. Comput.* 12: 2033–2051

[18] Osia S A, Shamsabadi A S, Sajadmanesh S, Taheri A, Katevas K, Rabiee H R, Lane N D and Haddadi H 2020 A hybrid deep learning architecture for privacy-preserving mobile analytics. *IEEE Internet of Things J.* 7(5): 4505–4518

[19] Wang Z, Luo N and Zhou P 2020 GuardHealth: blockchain empowered secure data management and graph convolutional network enabled anomaly detection in smart healthcare. *J. Parallel Distrib. Comput.* 142: 1–12

[20] Wu T Y, Yang L, Lee Z, Chen C M, Pan J S and Islam S H 2021 Improved ECC-based three-factor multiserver authentication scheme. *Secur. Commun. Netw.* 20(21): 1–14

[21] Xie X, Fang Y, Jian Z, Lu Y, Li T and Wan G 2020 Blockchain-driven anomaly detection framework on edge intelligence. *CCF Trans. Network.* 3: 171–192

[22] Xu J, Xue K, Li S, Tian H, Hong J, Hong P and Yu N 2019 Healthchain: a blockchain-based privacy preserving scheme for large-scale health data. *IEEE Internet of Things J.* 6(5): 8770–8781

[23] Yaeger K, Martini M, Rasouli J and Costa A 2019 Emerging blockchain technology solutions for modern healthcare infrastructure. *J. Sci. Innov. Med.* 2(1)

[24] Yassein H R, Abidalzahra A A and Al-Saidi N M 2021 A new design of NTRU encryption with high security and performance level. In: *AIP Conference Proceedings*, Vol. 2334, No. 1, AIP Publishing LLC, p. 080005

[25] Zhou T, Shen J, He D, Vijayakumar P and Kumar N 2020 Human-in-the-loop-aided privacy-preserving scheme for smart healthcare. *IEEE Trans. Emerg. Top. Comput. Intell.* 6(1): 6–15

[26] Li W, Jin C, Kumari S, Xiong H and Kumar S 2022 Proxy re-encryption with equality test for secure data sharing in Internet of Things-based healthcare systems. *Trans. Emerg. Telecommun. Technol.* 33(10): e3986

[27] Das S and Namasudra S 2022 A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure. *Comput. Electr. Eng.* 101: 107991

[28] Nagarajan S M, Deverajan G G, Kumaran U, Thirunavukkarasan M, Alshehri M D and Alkhalaf S 2021 Secure data transmission in internet of medical things using RES-256 algorithm. *IEEE Trans. Ind. Inform.* 18(12): 8876–8884

[29] Almalawi A, Khan A I, Alsolami F, Abushark Y B and Alfakeeh A S 2023 Managing security of healthcare data for a modern healthcare system. *Sensors* 23(7): 3612

[30] Raheja N and Manocha A K 2022 IoT based ECG monitoring system with encryption and authentication in secure data transmission for clinical health care approach. *Biomed. Sign. Process. Control* 74: 103481

[31] Wu Y, Zhang L, Berretti S and Wan S 2022 Medical image encryption by content-aware DNA computing for secure healthcare. *IEEE Trans. Ind. Inform.* 19(2): 2089–2098

[32] Karuppiah S V and Gurunathan G 2021 Secured storage and disease prediction of E-health data in cloud. *J. Ambient Intell. Human. Comput.* 12: 6295–6306

[33] Boumezbeur I and Zarour K 2022 Improving privacy-preserving healthcare data sharing in a cloud environment using hybrid encryption. *Acta Inform. Prag.* 3: 361–379

[34] Jiang H, Wang M, Zhao P, Xiao Z and Dustdar S 2021 A utility-aware general framework with quantifiable privacy preservation for destination prediction in LBSs. *IEEE/ACM Trans. Netw.* 29(5): 2228–2241

[35] Qiao F, Li Z and Kong Y 2023 A privacy-aware and incremental defense method against GAN-based poisoning attack. *IEEE Trans. Comput. Soc. Syst.*

[36] Han S, Ding H, Zhao S, Ren S, Wang Z, Lin J, Zhou S 2023 Practical and robust federated learning with highly scalable regression training. *IEEE Trans. Neural Networks Learn Syst.*

[37] Luan D, Liu A, Wang X, Xie Y, Wu Z, Zhang W 2022 Robust two-stage location allocation for emergency temporary blood supply in postdisaster. *Discrete Dyn. Nat. Soc.*

[38] Song Y, Xin R, Chen P, Zhang R, Chen J, Zhao Z 2023 Identifying performance anomalies in fluctuating cloud environments: A robust correlative-GNN-based explainable approach. *Future Gener. Comput. Syst.* 145: 77–86