Texila International Journal of Public Health
ISSN: 2520-3134
DOI: 10.21522/TIJPH.2013.12.04.Art069

A Blockchain-Based, Efficient, and Privacy-Preserving Data Exchange System for mHealthcare that Includes Trust Authentication

Krishnamoorthy R.* and Kaliyamurthie K. P.
CSE, Bharath Institute of Higher Education and Research, Chennai, India

Abstract

The mobile healthcare (mHealthcare) paradigm provides promise to enhance the delivery of healthcare services through remote diagnostics and medical data interchange. But problems like unapproved access and data leaks continue. Although there are still problems, attribute-based encryption (ABE) is a useful cryptographic method for protecting data exchange in mHealthcare. To address these problems, this study provides an effective data sharing strategy that also protects privacy. The mHealthcare service users activity has been monitored for malicious analysis in which the authentication of the users is analysed using convolutional reinforcement fuzzy neural network. the trained and classified output gives security analysis based on healthcare data modelling then the network privacy is enhanced. In order to protect user privacy, it hides a portion of the access policy, adds an offline method for generating keys and encrypting data in mHealthcare, and uses blockchain technology to provide decentralized, reliable verification of data access rights. The enhanced security and efficiency of the method are confirmed by security proofs and experimental outcomes. Proposed technique attained detection accuracy 96%, data privacy analysis of 94%, recall of 90%, RMSE of 60% based on mHealthcare dataset analysis.

Keywords: *ABE, Blockchain Technology, Convolutional Reinforcement, Fuzzy Neural Network, mHealthcare.*

Introduction

Novelty of the work Data are a valuable asset in the digital economy and are essential for stimulating economic growth and innovation in a range of sectors. Individual users have amassed a substantial amount of healthcare data, especially in medical industry due to the extensive use of electronic medical records (EMRs), the rise in popularity of smart medical devices, and the development in health-tracking apps. Relevant organisations, like data centres and medical research institutes, use machine learning (ML) as well as deep learning (DL) methods to extract critical data from these data. This information can help with disease diagnosis, epidemic prevention, and further improvement of healthcare services [1]. As a result, one important strategy for promoting the advancement of medical research is to encourage people to share their healthcare data with medical research organisations. The majority of personal health data is kept on cloud servers or other centralised sites. There are drawbacks to this management and storage strategy. The server failure can have disastrous effects for services that store and share data. Furthermore, using external storage results in an unclear attribution of data ownership. The operator of the cloud server may claim ownership or control of the data, which would prevent the user from directly managing or modifying their data. Internet of Things (IoT) technology and 5G have emerged in IoT era [2]. A popular application of 5G and IoT

Received: 11.09.2024 ***Accepted: 05.11.2024*** ***Published on: 27.12.2024***
****Corresponding Author: r.krishcse@gmail.com***

technology is mobile health (mHealthcare), providing patients with more convenient and efficient services. Wearable technology is used by mHealthcare to collect patient medical records (MR), which are then stored in cloud service providers (CSPs). Because patient privacy is contained in online medical records, data owners in mHealthcare systems want to protect their information and limit who can access it. Therefore, a solution capable of providing precise access control is essential for mHealthcare systems [3]. It has been introduced ABE technique, which can simultaneously perform one-to-many access control and fine-grained data encryption. Therefore, this is one of the technologically reasonable solutions to the above problem. Many factors related to access policy make it possible to divide ABE into two types: CP-ABE and KP-ABE. To store data in CP-ABE, the data owner creates an access policy with a set of attributes. Only users with all access policy credentials have decryption privileges. This function only meets the needs of mHealthcare systems in protecting data privacy [4]. Securing the confidentiality and security of shared data is one of the main issues telemedicine. Health data privacy is also associated with a number of legal, economic, ethical, technological issues. Strict laws and regulations like GDPR (General Data Protection Regulation) as well as HIPAA (Health Insurance Portability and Accountability Act) prohibit hospitals from sharing sensitive data with other healthcare institutions in order to construct data analytics models because they are concerned about privacy. Novel technologies like the IoT, Blockchain, AI, ML, Big Data, and more recent technologies like Federated learning are integrated into healthcare to provide suitable solutions because of these data privacy problems [5].

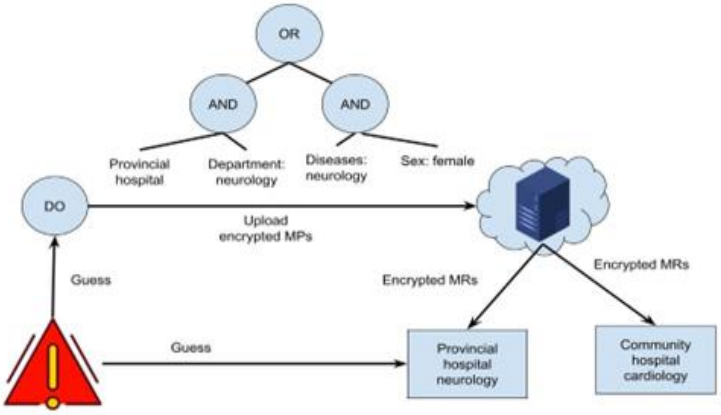


Figure 1. mHealthcare Data-Sharing System Combined with Traditional CP-ABE

However, access policy in conventional CP-ABE systems remains explicit and only encrypts data to a finer degree. mHealthcare method access policy also covers sensitive information of data owners. The data owner (DO) encrypts his MR using access policy ("Hospital: Provincial Hospital" AND "Department: Neurology") OR ("Disease: Neurology"). AND "Gender: Female" in Figure 1, depicts a simplified mHealthcare system with traditional.

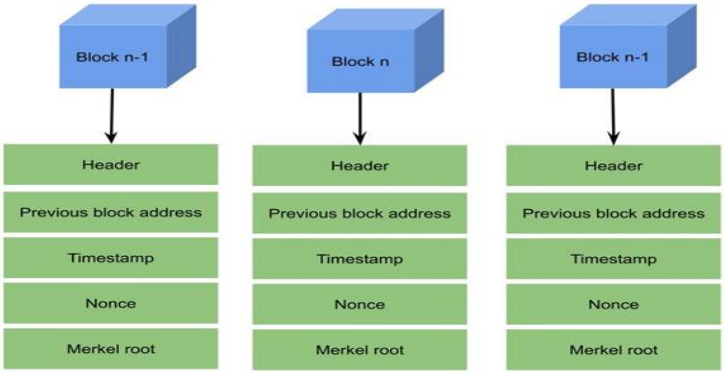


Figure 2. Blockchain Structure

CP-ABE. Anyone can see that the data requestor (DR) is a patient with a neurological disease or a neurologist working at a provincial hospital because the access policy is clearly stipulated. It can also be assumed that data owner is a patient hospitalized in a provincial hospital, where he is being treated for a neurological disease. Therefore, privacy of data owners as well as data recipients will be violated. Therefore, it is imperative that the explicit [7] access policy be hidden. Only way for the recipient of the data blockchain-based mHealthcare data exchange is an attractive concept, but there are several obstacles to its widespread implementation. Current research efforts address these challenges through different approaches, providing valuable insights for your proposed system.

Attribute-Based Encoding

ABE design is initiated by fuzzy identity-based encryption (IBE) method. It was the first company to provide one-to-many access control by hiding the recipient's identity, which gave rise to idea of attribute-based encryption (ABE). Work [8] presented first KP-ABE system with this special structure and converted to know whether it is authorized or not if explicit attribute values in access policy are obfuscated is to decrypt the ciphertext rather than directly [6] inspect the attribute values. increases the unnecessary computational costs of unauthorized users. Some solutions address this vulnerability by adding an authentication step to verify user access before complete decryption. Concentration and opacity are issues that arise throughout the authentication process.

Effective

The CP-ABE scheme was developed by [9], who also provided a security proof for the method using the corresponding model. This scheme is based on basic mathematical assumptions. The CP-ABE technique is based on common mathematical assumptions also described by [10]. involved in the decoding step to the CSP. However, CSP is not always reliable. A redundancy checking component was added to the ciphertext by allowing users to confirm the detection accuracy of CSP decoding results. However, this technique doubles the length of the ciphertext compared to doubles the computational and storage costs.

Materials and Methods

Structure of access

Given an attribute party set U, let it be. If A $\subseteq$ 2U is a collection and B $\in$ A, then C $\in$ 2U and C $\in$ A, then A $\in$ B. A monotone collection A without empty set is called a monotone access structure of U and is written as A $\subseteq$ 2U \ {$\emptyset$}.

Bilinear Pairings

Assume that two cyclic multiplicative groups of prime order p are represented by G and GT. A procedure e: G × G $\longrightarrow$ If GT

possesses following features, it is referred to be bilinear mapping:

•Bilinear: for all g, w ∈ G and a, b ∈ Z∗, e(ga, wb) = e(g, w)ab.

•Nondegenerate: e(w, w) /= 1 occurs for any w ∈ G.

•Computable: In polynomial time, all operations in G, GT, and e: G × G −→ GT can be computed.

Blockchain

It was thanks to Bitcoin that we started thinking about blockchain. The title and body of the block form structure of block. As shown in Figure 2, each block has a header that stores hash value of previous block as well as feature data of current block, such as root of Merkle tree. Block body contains actual transaction data, stored in a way that allows the Merkle tree to prevent tampering with transactions within the block [11]. A distributed ledger is created when blocks are connected in a single direction based on chronological order.

Proposed Model

As illustrated in Figure 3, the system presented in this chapter is composed of five entities: the Blockchain Consortium (CB), the Trusted Authority (TA), the Cloud Service Provider (CSP), the Data Owner (DO), and the Data Requester (DR) [12].

TA: All entities in system fully trust TA as a trusted authority. The task of managing user registration belongs to the TA. •CSP: Made up of several processing and storage servers, a CSP is a collection of semi-trusted cloud servers. •CB: Users can execute and query transactions on this trusted and distributed platform [13]. This article uses blockchain to record access policy and authentication ciphertext. Additionally, it can perform distributed as well as trusted authentication for data requesters because it carries smart contracts.

DO: The organization responsible for creating and uploading the ciphertext is the DO at CSP [14].

Once the notification and access policy are in place, DO first produces offline ciphertext and then final ciphertext. By sending ciphertext address, authentication ciphertext, access policy to blockchain as a storage transaction (Txstorage), DO can perform secure and reliable data exchange. •DR: A Designated Representative (DR) is an entity with certain characteristics that require access to shared data. DR calls the smart contract to confirm authorization before starting the decryption process.

Overview of Proposed Scheme

The suggested scheme has 7 methods.

1. Not online.KeyGen(PK, MSK) → SKoff: TA creates offline key SKoff as output, given the inputs PK and MSK.
2. On the internet.KeyGen(PK, SKoff, S = (IS, LS)) → (SKS, SKAuth): TA provides the secret key tuple (SKS, SKAuth) as outputs, where SKS is decryption key and SKAuth is authentication key, given the inputs of PK, SKoff, attribute set S = (IS, LS).
3. Not online.Enc(PK) → CToff: DO creates offline ciphertext CToff as output given the PK as the input.
4. (TKs) → TKGenout(PK, SKS) UK): Using the PK and SKS as inputs, DR produces the transformation keys that are outsourced and the outputs are the user's decryption key for the UK.
5. Transformout (TKs, CTA, and PK)) → CTout: With the TKs, CTA, and PK as the sources, The output of CSP is the modified ciphertext CTout.
6. DecryptDR(PK, CTout, UK) → Mr or ⊥: DR retrieves the message Mr or ⊥ as the output given the PK, CTout, and UK.
7. MVerify(PK, CTA, Mr) → TorF: The algorithm returns T if the inputs are PK, CTA, and Mr. and the commitment value

of Mr. equals the commitment value of M in CTA. If not, F is the result of the algorithm.

mHealthcarecare Service User Activity Analysis using Convolutional Reinforcement Fuzzy Neural Network (ConRFuz-NN)

The several receptive layers can process the sections of input layer. To create an output with a high resolution of original image, these networks are configured so that there is overlap of input area. Convolutions and pooling are two techniques used by CNNs for feature detection. Following the extraction of features [15], every fully connected layer functions as a classifier. Since a fully connected CNN is not required, there is less coupling between convolutional layers and pooling layers [16]. Convolution is used when combining two mathematical functions so that the outcome is likewise a function. Convolution is applied across input by sliding filter. Matrix multiplication is done for each place, and the output is added up on to feature map.

Pooling Layer: Between CNN and after convolution layer, a pooling layer is added. This layer's primary objective is to reduce dimensionality in order to minimise computation as well as number of specifications. Max pooling is most crucial type of pooling. It is employed to select highest value present in every window [17].

1. **Fully Connected Layer:** In which classifies input images, comes in last after convolutional and pooling layers. The activation functions of neurons connected to the previous layer are present in a fully connected layer. Since malware attacks are common in 5G, IoT, healthcare domains, the next section will focus on using ANN, also known as DL classifier CNN, to detect malware attacks [18]. It will not only identify malware but also offer information security for identifying and categorising bad code.
2. Despite the fact that each organisation has personal data or information, both are subject to numerous attacks. Because of this, a lot of assailants or criminals learn new tactics every time they attack target [19]. Security providers are attempting to fight against these kinds of attacks in a number of ways, but they are unable to do so due to the billions of malware that are identified each month. As a result, methods like deep learning are essential for maintaining privacy and security [20].
3. The learning problem is formulated as a contextual bandit problem, which we solve with a one-step Markov decision process. Formally, we construct a policy network that receives zx as the input state and produces a categorical distribution as the policy, indicating which model should be used for anomaly detection. Given the contextual data (zx) of an input data (x), where zx is a representation of the input data, and AD models that have been trained and deployed at the HEC system's K layers by eqn (1)

$$\pi_\theta(\mathbf{a} \mid \mathbf{z_x}) = \prod_{k=1}^{K} s_k^{a_k} \quad (1)$$

where actions recorded as a one-hot vector that specifies which model to complete task are denoted by a = ($a1$, $a2$, $\cdots$, aK), $ak \in \{0, 1\}$. The likelihood vector s = ($s1$, $s2$, $\cdots$, sK) = $f\theta$ (zx), $sk \in [0, 1]$, represents the chance of choosing each model k. When k = arg max$k$ (sk), we set ak = 1; otherwise, we set ak = 0, we indicate chosen action as |a| = k. With parameters θ, the policy network $Z\theta$ (.) is constructed as a neural network. We describe the contextual information of input data using extracted features zx rather than raw input data x, to minimize size of the policy network and make it operate quickly on IoT devices. The goal of training policy network is to identify best possible policy $\pi\theta *$ that maximises expected reward of chosen action by mapping

an input state to an action. In order to reduce negative anticipated reward, we train policy network utilizing policy gradient technique by eqn (2)

$$\min\mathcal{L}(\theta) = -\underset{\mathbf{a}\sim\pi_\theta}{\mathbb{B}}[R(\mathbf{a},\mathbf{z_x})] \quad (2)$$

where R(a, zz) is the action's reward function for a certain state, zx. Gradient of L (θ) can be obtained in this manner by eqn (3)

$$\nabla_\theta\mathcal{L} = -\int R(\mathbf{a},\mathbf{z_x})\nabla_\theta\pi_\theta(\mathbf{a}\mid\mathbf{z_x})d\mathbf{a} = -\int R(\mathbf{a},\mathbf{z_x})\frac{\nabla_\theta\pi_\theta(\mathbf{a}|\mathbf{z_x})}{\pi_\theta(\mathbf{a}|\mathbf{z_x})}\pi_\theta(\mathbf{a}\mid\mathbf{z_x})d\mathbf{a} = -\int R(\mathbf{a},\mathbf{z_x})\nabla_\theta\log\pi_\theta(\mathbf{a}\mid\mathbf{z_x})\pi_\theta(\mathbf{a}\mid\mathbf{z_x})d\mathbf{a} = -\underset{\mathbf{a}\sim\pi_\theta}{\mathbb{B}}\left[R(\mathbf{a},\mathbf{z_x})\nabla_\theta\log\left(\pi_\theta(\mathbf{a}\mid\mathbf{z_x})\right)\right] \quad (3)$$

We use a reinforcement comparison using an independent baseline (a˜, zx) to decrease volatility of reward value as well as improve rate of convergence. Empirical evidence suggests that using baseline (a˜, zx) as best observed reward accelerates the rate of convergence [21]. To avoid the over-fitting issue, we additionally include a ℓ2-norm regularisation term in loss function. Thus, we rewrite L (θ) as follows by eqn (4)

$$\mathcal{L}(\theta) = -\underset{\mathbf{a}\sim\pi_\theta}{\mathbb{B}}[R(\mathbf{a},\mathbf{z_x}) - R(\tilde{\mathbf{a}},\mathbf{z_x})] + \frac{\gamma}{2}\parallel\theta\parallel_2 \quad (4)$$

where the parameter "γ" is regularised. This can be rewritten as follows by selecting a baseline (a◦, zx) that is unaffected by output actions by eqn (5)

$$\mathcal{L}(\theta) = -\underset{\mathbf{a}\sim\pi_\theta}{\mathbb{B}}[R(\mathbf{a},\mathbf{z_x})] + R(\tilde{\mathbf{a}},\mathbf{z_x}) + \frac{\gamma}{2}\parallel\theta\parallel_2 \quad (5)$$

As with initial objective function, we minimise (3) by computing gradient of L (θ) as follows using policy gradient technique with reinforce method by eqn (6)

$$\nabla_\theta\mathcal{L} = -\underset{\mathbf{a}\sim\pi_\theta}{\mathbb{B}}\left[\left(R(\mathbf{a},\mathbf{z_x}) - R(\tilde{\mathbf{a}},\mathbf{z_x})\right)\nabla_\theta\log\left(\pi_\theta(\mathbf{a}\mid\mathbf{z_x})\right)\right] + \gamma\theta = -\underset{\mathbf{a}\sim\pi_\theta}{\mathbb{E}}\left[\left(R(\mathbf{a},\mathbf{z_x}) - R(\tilde{\mathbf{a}},\mathbf{z_x})\right)\nabla_\theta\sum_{k=1}^{K} a_k\log(s_k)\right] + \gamma\theta \quad (6)$$

Any classification issue contains m training patterns $x_p = (\dot{x}_{p1},\dots,x_{pn},C_p), p = 1,2,\dots,m$. We employ fuzzy rules of following kind in this work:

Rule R_j : If x_1 is A_{j1} and ... and x_n is A_{jn} $x_p = (\dot{x}_{p1},\dots,x_{pn},C_p), p = 1,2,\dots,m$ then Class $= C_j$ with RW_j

Fuzzification model: In order to convert the three distinct input variables—direct, indirect, and past trust—into fuzzy sets, we create membership functions for trust that are trapezoidal and trapezoidal by eqn (7)

$$\mu_H(x;a,b) = \begin{cases} 0; & x < a \\ \dfrac{x-a}{b-a}; & a \le x \le b \\ 1; & x > b \end{cases}$$

$$\mu_A(x;c,d,e) = \begin{cases} 0; & x < c \\ \frac{x-c}{d-c}; & c \le x \le d \\ \frac{e-d}{e-d}; & d < x < e \\ 0; & x \ge e \end{cases} \quad (7)$$

It indicates the extent to which an element x in R is a member of a fuzzy set (H; A or L).

Development of Fuzzy rule base: Three linguistic labels serve as the membership functions for proving legitimacy of acquired overall trust for a fog node as well as the trust values.

Defuzzification: For each membership function, crisp value of overall trust is provided by mean of the centroids of gravity by eqn (8)

$$\text{overall trust} = \frac{\sum_{x=a}^{b}\mu_R(x)\times x}{\sum_{x=a}^{b}\mu_R(x)} \quad (8)$$

Specifications for Proposed System and Scheme

The provided strategy is explained in depth in this section. The mHealthcare system consists of five phases: (1) privacy-preserving data access; (2) privacy-preserving MRs sharing; (3) system initialization; and (4) decryption outsourcing. The specifics of the algorithms used in the aforementioned five steps will be presented.

1. Privacy-preserving MRs sharing;

To produce offline secret key, TA performs the first method as shown below before retrieving the user attribute set. To produce final secret key, TA performs the second

process as follows after receiving attribute set S = (IS, LS) provided by user.

OfflineKeyGen: TA generates an offline key for each user in the system by randomly selecting the elements ε, εi, Li › Zp, where i e [1, U].

(K0, K1, K2,i, K3,i, K4,i, K5,i}ie[1,U]) is the value of SKoff.

2. Decryption outsourcing

To ascertain if a user is authorised, the authentication step is employed. The decryption process must only be continued by authorized users.

The Authen Smart Contract Algorithm 3 input is as follows: (A, ρ), S = (IS, LS), CTA, CTAuth, SKAuth;

Algorithm - Smart Contract of Authen

1: get matrix A and extract map ρ;

2. Determine the minimum authorized attributes set I and the constant set {wi};

3: 0<j if Cr = œieIe(Cr, Kr)wiI

4: give back True; 5: None

6: produce True or False; return False;

•Authentication: As shown in the algorithm, the data requester invokes an authentication contract before decryption to confirm whether it is authorized to access data or not. The method returns True if the user is authorized, indicating that they can proceed with the decryption step. Otherwise, the algorithm will produce False.

There are three stages in the decoding process. The user's kill switch and decryption key are first generated by DR. The ciphertext is then modified by the CSP using a switch. After extracting message from ciphertext [22], the DR validates transformation result provided by CSP. •TKGenout: Person requesting the data executes the algorithm. DR r R

Z∗ and set the user to the conversion key and the decryption key to UK = r

TKS= [1,|I |] TK0, TK1, TK2,i, TK3,i, TK4,i}I.

Results and Discussion

Experimental setup: With a 1.2 GHz processor, 4 GB RAM, and 4*ARM Cortex A-53, the following model can be accomplished. The human activity recognition model is implemented using Keras and Python 3.8.8. Keras uses layers of Dense, Dropout, and Flatten to construct the model. The vector's dimensions can be altered using the dense layer. Additionally, this layer manipulates the vector's scale, translation, and rotation. A 1.2 GHz processor, 4 GB RAM, and 4*ARM Cortex A-53 are required to run the following model. Python 3.8.8 and Keras are used to implement the human activity recognition model. Dense, Dropout and Flatten layers are used by Keras to construct the model. To alter the vector's dimensions, apply the dense layer. Additionally, this layer modifies the vector's rotation, scaling, and translation.

Table 1. Parameters and Values

Parameter	Value
batch size	64
epoch	20
num classes	25

A performance study of the proposed scheme, Table 1 as well as several other PHP-CP-ABE strategies in terms of functionality and computational cost, is provided in this section. We repeat the experiments thirty times for every access policy as well as user attribute list, using average do test results. Experimental results of the strategies in terms

of computational cost are clearly shown in Fig. 3 and Fig. 4 shows that, in systems (Cui et al. 2018; GHu et al. 2020), cost of online key generation as well as online encryption increases significantly with increasing scale. user attribute model or online encoding. This difference improves significantly with the size of the properties. Based on Fig. 4,5,6 it is clear that this scheme (Y. Zhang, 2018) has a larger authentication cost than the method (G. Hu et al. 2020) and provided scheme. Scheme with highest authentication cost is scheme (G. Hu et al).

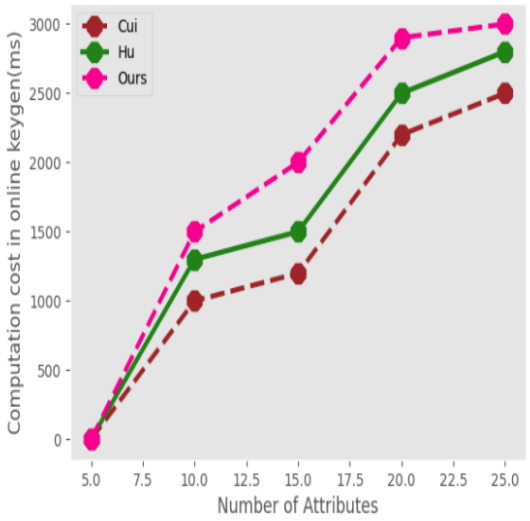


Figure 3. Computation Overhead in Online Keygen

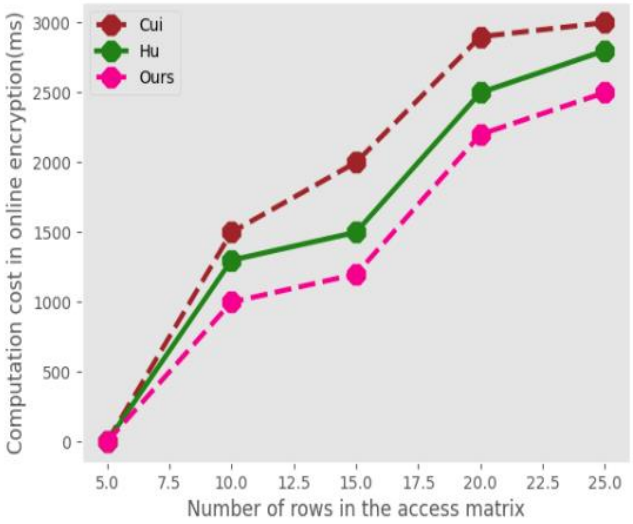


Figure 4. Computation Overhead in Online Encryption

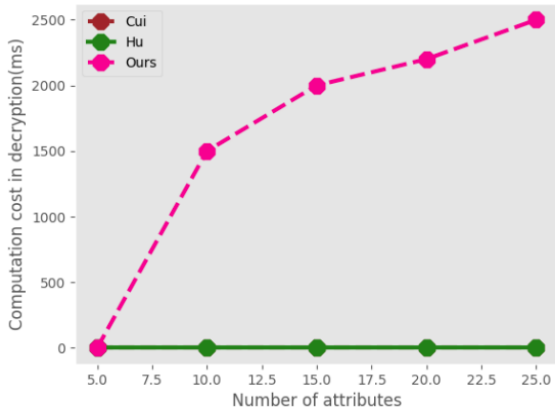


Figure 5. Computation overhead in authentication

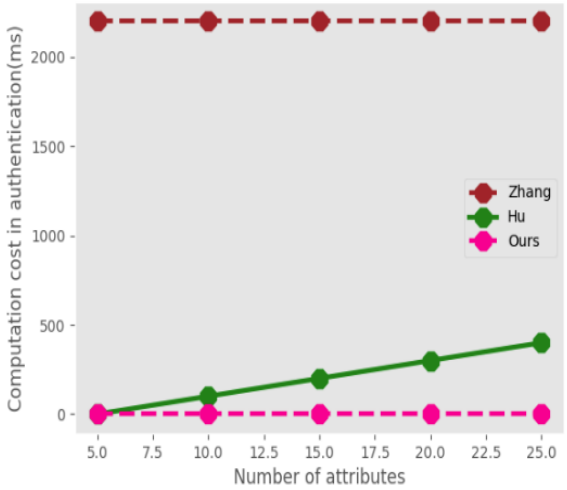


Figure 6. Computation Overhead in User Decryption

Although it remains constant in the presented figure, it has a positive linear correlation with the characteristic scale. according to Figure Average time required for: (a) computational cost in online keyGen; (b) computational cost in online encryption; (c) computational cost during authentication; (d) the computational cost of user decoding.

Under the same conditions, the given method has the lowest computational cost, but the decoding cost increased further in the study of Cui et al. (2018) had a positive linear correlation with the user characteristics scale. In summary, it is clear that proposed technique is better than Cui et al. (2018) and G. Hu et al. (2020) in all respects, showing that it is most suitable for mHealthcare systems consisting of a large number of mobile devices.

Blockchain: Hyperledger Fabric 2. 4, installed on Docker 20. 107 platform and Ubuntu18. 04 64-bit operating system with AMD Ryzen r7-5800H processor running at 3. 20 GHz makes up the test configuration. In Fabric, peer nodes execute contracts as well as reach consensus with other peer nodes on blockchain using a consensus method. Client nodes create transactions through smart contracts [23]. The time it takes for a transaction to be confirmed on blockchain or consensus time of transaction nodes is what we need to measure. We performed ten simulations for each step, using the average value to represent the experimental results. As shown in Figure 7, there is a positive correlation between number of transactions as well as blockchain reaction time.

Dataset description: CPRD General practitioners (GPs) are the primary point of contact for healthcare in the UK National Health Service, over 98% of population is registered with one. A network of general practitioners in UK provides deidentified longitudinal primary care data to CPRD service, which then links those data to administrative databases for area-based health care, secondary care, other services.

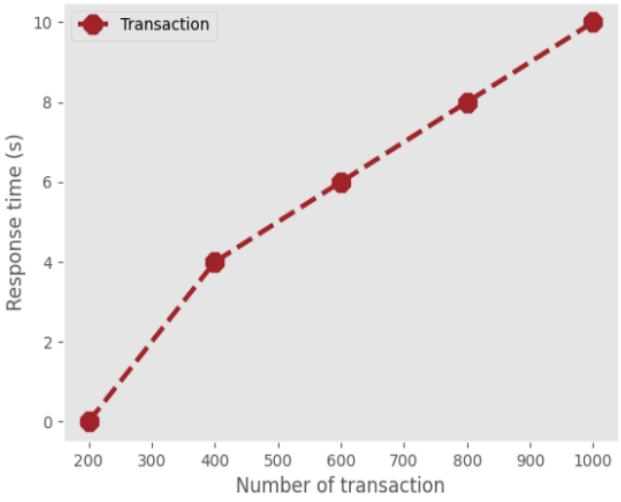


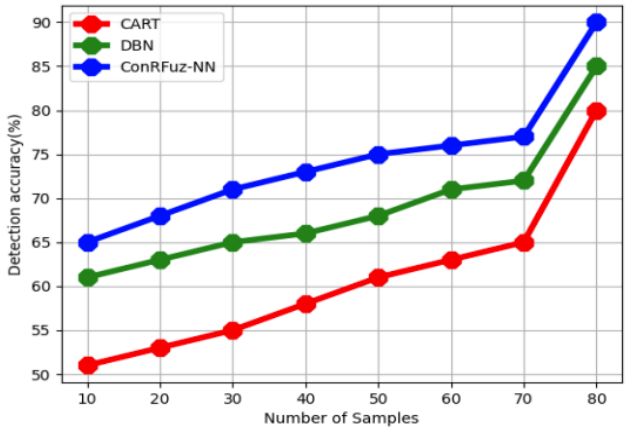
Figure 7. Response Time of Transaction

Table 2. Comparative Based on mHealthcarecare Dataset

Parameters	Techniques	Detection accuracy	Data privacy analysis	Recall	RMSE
CPRD	**CART**	80	73	70	65
	DBN	85	78	75	67
	ConRFuz-NN	90	83	83	60
COPD	**CART**	89	79	85	71
	DBN	93	87	88	68
	ConRFuz-NN	96	94	90	60

Table 2 shows comparative based on mHealthcarecare dataset. Here dataset utilized are CPRD public dataset and COPD EHR dataset.

Each EHR has an ICD-9 clinical event sequence that is longitudinal and high-dimensional. Obesity, diabetes, COPD are the traits that have been chosen. Python as well as Keras DL API with a TensorFlow backend are utilized to method setup.



S

Figure 8. Detection Accuracy

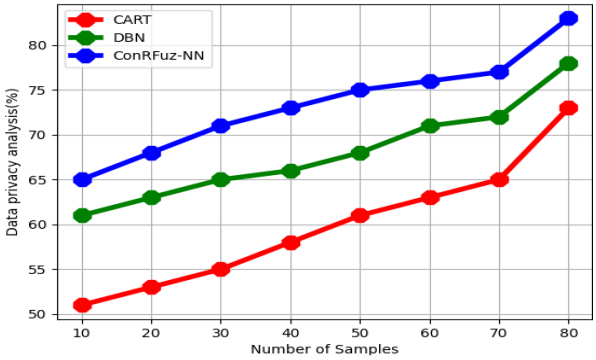


Figure 9. Data Privacy Analysis

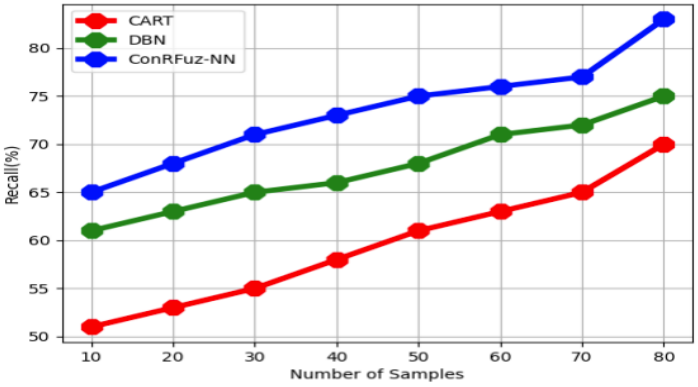


Figure 10. Recall

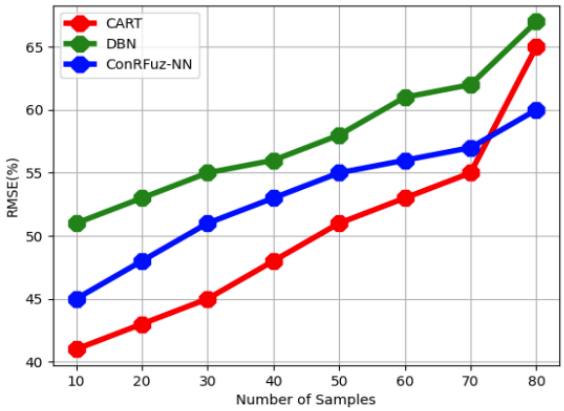


Figure 11. RMSE

The Figure 8-11 shows comparative for CPRD dataset. Here proposed technique attained detection accuracy of 90%, data privacy analysis of 83%, recall of 83%, RMSE of 60%; existing CART attained detection accuracy of 80%, data privacy analysis of 73%, recall of 70%, RMSE of 65%, DBN attained detection accuracy of 85%, data privacy analysis of 78%, recall of 75%, RMSE of 67%.

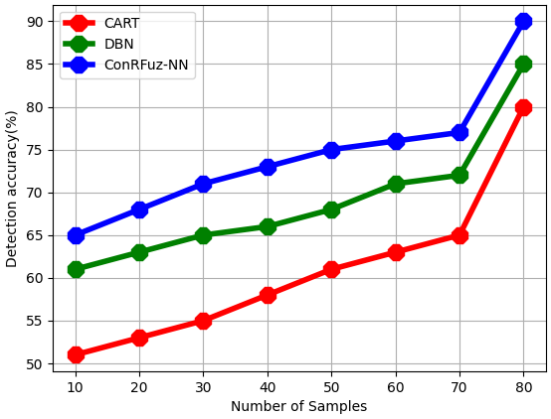


Figure 12. Detection Accuracy

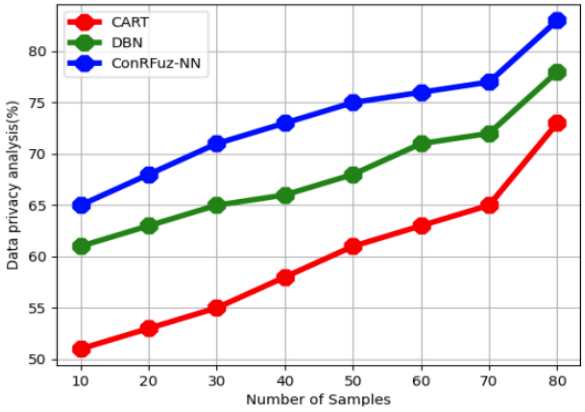


Figure 13. Data Privacy Analysis

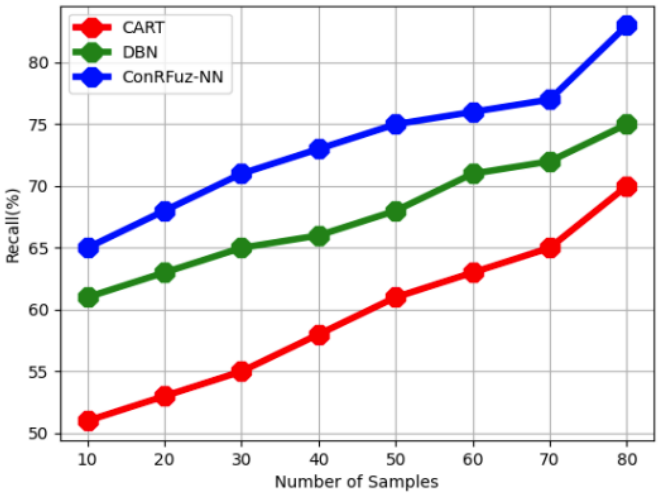


Figure 14. Recall

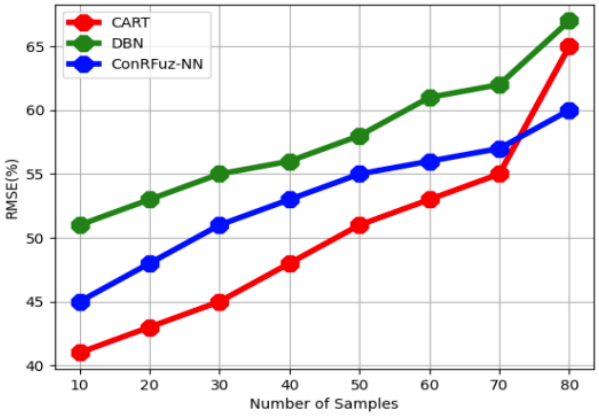


Figure 15. RMSE

The Figure 12 - 15 shows comparative for COPD dataset. Here proposed technique detection accuracy 96%, data privacy analysis of 94%, recall of 90%, RMSE of 60%; existing CART attained detection accuracy of 89%, data privacy analysis of 79%, recall of 85%, RMSE of 71%, DBN attained detection accuracy of 93%, data privacy analysis of 87%, recall of 88%, RMSE of 68%.

Conclusion

In addition to offering mHealthcare scenarios with fine-grained access control, the suggested system may also conceal characteristics in access policies to better safeguard user privacy. Unquestionable authentication outcomes are also obtained using access rights authentication based on blockchain. Furthermore, the effective encryption and decryption techniques in mHealthcare are highly beneficial to consumers of IoT devices. Moreover, we provide explicit demonstrations that, under the specified conditions, the approach is selectively secure. Convolutional reinforcement fuzzy neural networks are used to assess user authentication in order to monitor the activity of mHealthcare service users for harmful analysis. After receiving security analysis based on healthcare data modelling from the trained and classed output, network privacy is improved. The theoretical and experiment analysis results attest to the scheme's increased efficiency and practicality. To put it succinctly, this approach has several potential applications in mHealthcare settings. Malicious individuals could be exploiting keys in user groups with similar features in actual

application settings. The SC and the blockchain are utilised to guarantee impartial and independent anonymous authentication. It is imperative to recognise the constraints of our suggested plan, nevertheless. In order to achieve large-scale healthcare data sharing, we will concentrate on the task of improving our scheme's capacity to manage the growing volume of healthcare data and support highly concurrent users.

References

[1]. Xu, X., Peng, H., Bhuiyan, M. Z. A., Hao, Z., Liu, L., Sun, L., & He, L. 2021. Privacy-preserving federated depression detection from multisource mobile health data. *IEEE transactions on industrial informatics*, *18*(7), 4788-4797. DOI: 10.1109/TII.2021.3113708

[2]. Altameem, A., Kovtun, V., Al-Ma'aitah, M., Altameem, T., Fouad, H., & Youssef, A. E. 2022. Patient's data privacy protection in medical healthcare transmission services using back propagation learning. *Computers and Electrical Engineering*, *102*, 108087. https://doi.org/10.1016/j.compeleceng.2022.108087

[3]. Hennebelle, A., Ismail, L., Materwala, H., Al Kaabi, J., Ranjan, P., & Janardhanan, R. 2024. Secure and privacy-preserving automated machine learning operations into end-to-end integrated IoT-edge-artificial intelligence-blockchain monitoring system for diabetes mellitus prediction. *Computational and Structural Biotechnology Journal*, *23*, 212-233. DOI: 10.1016/j.csbj.2023.11.038

[4]. Wang, W., Li, X., Qiu, X., Zhang, X., Brusic, V., & Zhao, J. 2023. A privacy in smart healthcare systems. *Information Processing & Management*, *60*(1), 103167. https://doi.org/10.1016/j.ipm.2022.103167

[5]. Motahari, D., Arif, S., Mohboubi, A., & ur Rehman, S. 2020, November. Investigation of Mobile Machine Learning Models to Preserve the Effectiveness of User Privacy. In *2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA)* pp. 1-7. IEEE. DOI:10.1109/CITISIA50690.2020.9397489

[6]. Sahinbas, K., & Catak, F. O. 2023. Secure multi-party computation-based privacy-preserving data analysis in healthcare IoT systems. In *Interpretable Cognitive Internet of Things for Healthcare* pp. 57-72. Cham: Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-031-08637-3_3

[7]. Sinaci, A. A., Gencturk, M., Alvarez-Romero, C., Erturkmen, G. B. L., Martinez-Garcia, A., Escalona-Cuaresma, M. J., & Parra-Calderon, C. L. 2024. Privacy-preserving federated machine learning on FAIR health data: A real-world application. *Computational and Structural Biotechnology Journal*. https://doi.org/10.1016/j.csbj.2024.02.014

[8]. Boulemtafes, A., Derhab, A., & Challal, Y. 2022. Privacy-preserving deep learning for pervasive health monitoring: a study of environment requirements and existing solutions adequacy. *Health and Technology*, *12*(2), 285-304. https://link.springer.com/article/10.1007/s12553-022-00640-3

[9]. Kang, J. J., Dibaei, M., Luo, G., Yang, W., & Zheng, X. 2020, December. A privacy-preserving data inference framework for internet of health things networks. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* pp. 1209-1214. IEEE. DOI: 10.1109/TrustCom50675.2020.00162

[10]. Deng, H., Qin, Z., Sha, L., & Yin, H. 2020. A flexible privacy-preserving data sharing scheme in

Conflict of Interest

The author hereby declares that there is no conflict of interest.

Acknowledgement

The authors would like to thank Bharath Institute of Higher Education and Research (Deemed to be a university), for providing research facilities to carry out this work.

cloud-assisted IoT. *IEEE Internet of Things Journal*, *7*(12), 11601-11611. https://ieeexplore.ieee.org/document/9105096

[11]. Jayaram, R., & Prabakaran, S. 2021. Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system. *Egyptian Informatics Journal*, *22*(4), 401-410. https://doi.org/10.1016/j.eij.2020.12.003

[12]. Abdo, M. A., Abdel-Hamid, A. A., & Elzouka, H. A. 2020, December. A cloud-based mobile healthcare monitoring framework with location privacy preservation. In *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)* (pp. 1-8). IEEE. https://ieeexplore.ieee.org/document/9311999

[13]. Liang, J., Qin, Z., Xue, L., Lin, X., & Shen, X. 2021. Efficient and privacy-preserving decision tree classification for health monitoring systems. *IEEE Internet of Things Journal*, *8*(16), 12528-12539. DOI: 10.1109/JIOT.2021.3066307

[14]. Zhu, D., Zhu, H., Huang, C., Lu, R., Feng, D., & Shen, X. 2023. Efficient and Accurate Cloud-Assisted Medical Pre-Diagnosis With Privacy Preservation. *IEEE Transactions on Dependable and Secure Computing*. DOI: 10.1109/TDSC.2023.3263974

[15]. Othman, S. B., Almalki, F. A., Chakraborty, C., & Sakli, H. 2022. Privacy-preserving aware data aggregation for IoT-based healthcare with green computing technologies. *Computers and Electrical Engineering*, *101*, 108025. https://doi.org/10.1016/j.compeleceng.2022.108025

[16]. Aminifar, A., Rabbi, F., Pun, V. K. I., & Lamo, Y. 2021, November. Monitoring motor activity data for detecting patients' depression using data augmentation and privacy-preserving distributed learning. In *2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC) pp. 2163-2169. IEEE.* DOI: 10.1109/EMBC46164.2021.9630592

[17]. Guduri, M., Chakraborty, C., & Margala, M. 2023. Blockchain-based federated learning technique for privacy preservation and security of smart electronic health records. *IEEE Transactions on Consumer Electronics*. DOI: 10.1109/TCE.2023.3315415

[18]. Li, C., Dong, M., Xin, X., Li, J., Chen, X. B., & Ota, K. 2023. Efficient privacy-preserving in IoMT with blockchain and lightweight secret sharing. *IEEE Internet of Things Journal*. DOI: 10.1109/JIOT.2023.3296595

[19]. Xu, G., Qi, C., Dong, W., Gong, L., Liu, S., Chen, S., & Zheng, X. 2022. A privacy-preserving medical data sharing scheme based on blockchain. *IEEE Journal of Biomedical and Health Informatics*, *27*(2), 698-709. DOI: 10.1109/GLOBECOM42002.2020.9348251

[20]. Abdelfattah, S., Badr, M. M., Mahmoud, M., Abualsaud, K., Yaacoub, E., & Guizani, M. 2023. Efficient and privacy-preserving cloud-based medical diagnosis using an ensemble classifier with inherent access control and micro-payment. *IEEE Internet of Things Journal*. DOI:10.1109/JIOT.2023.3303429

[21]. Patruni, M. R., & Humayun, A. G. 2024. PPAM-mIoMT: a privacy-preserving authentication with device verification for securing healthcare systems in 5G networks. *International Journal of Information Security*, *23*(1), 679-698. https://doi.org/10.1007/s10207-023-00775-y

[22]. Iwaya, L. H., Ahmad, A., & Babar, M. A. 2020. Security and privacy for mHealthcare and uHealth systems: a systematic mapping study. *IEEE Access*, *8*, 150081-150112. DOI: 10.1109/ACCESS.2020.3015962

[23]. Long, G., Shen, T., Tan, Y., Gerrard, L., Clarke, A., & Jiang, J. 2021. Federated learning for privacy-preserving open innovation future on digital health. In Humanity Driven AI: Productivity, Well-being, *Sustainability and Partnership (pp. 113-133). Cham: Springer International Publishing.* https://doi.org/10.48550/arXiv.2108.10761