Journal of Information Systems Engineering and Management
2025, 10 (2)

e-ISSN: 2468-4376

https://jisem-journal.com/

Research Article

Adaptive Feature Centric Trust Analysis Model for Improved Data Security on EHR Data Using Blockchain

Mr. Vijayakumar M[1*], Dr Balapriya S[2], Mr. Ashok M[3], Mrs. Sudha R[4]

[1*]*Assistant Professor, Department of Computer Science and Engineering, Sathiyabama Institute of Science and Technology, Tamil Nadu, India*

[1*]*Email: vijayakumar.m.cse@sathyabama.ac.in*

[2]*Assistant Professor, Computer Science and Engineering, Sathyabama Institute of Science and Technology, Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai -119, Tamil Nadu, India*

[3]*Assistant Professor/Cse, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu, India*

[4]*Assistant Professor, Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India*

ARTICLE INFO

Received: 14 Oct 2024

Revised: 17 Dec 2024

Accepted: 31 Dec 2024

ABSTRACT

Recent development of cloud encourages the healthcare organizations to perform data management and access through variety of services. However, there are number of security issues challenges the QoS of the healthcare systems. To handle the security issues and to enforce data security of Electronic Healthcare Record various approaches are defined in literature. The methods adapt different factors methods like data encryption, key based authentication, and profile based restriction and behavior analysis to restrict the malformed access. However, the methods are inclined to produce poor accuracy in access restriction and QoS maximization. To handle this issue, an Adaptive Feature Centric Trust Analysis Model with Blockchain (AFCTAM-BC) is presented in this article. The method keeps track of feature access performed by any user towards access restriction. By classifying the features of services and healthcare records under different level of sensitivity. Accordingly, the method applies AFCTAM algorithm to measure the trust of any user against the access of different features of healthcare record. The method computes sensitive and non-sensitive Feature Centric Trust Score (FCTS) according to the historic access records. Based on these values, the method computes Access Clearance Measure (ACM) to grant or deny the service access. Further, the method adapts Class Level Data Encryption (CLDE) to generate the blockchain which restrict the malformed access of any user to which the user has no access. The proposed AFCTAM model improves the performance of data security, access restriction and QoS of the healthcare system.

Keywords: Cloud, Healthcare Systems, EHR data security, blockchain, AFCTAM-BC, FCTS, ACM, CLDE.

.

INTRODUCTION

The increased growth of information technology and cloud support variety of organizations to maintain their data in cloud with least cost. This encourages the healthcare organizations to maintain their entire data in cloud with least cost. The healthcare organizations maintains variety of data in cloud like professional, personal, diagnosis, and health records of various users of the environment. These data has been used for variety of purposes like data analysis, disease prediction and recommendation generation. The data analysis model would fetch the data to analyze the rate of curing performed by the organization against any disease and others also. Similarly, the disease prediction models would fetch the data to predict the possible disease affected by any person. The recommendation systems would analyze the data in cloud to produce recommendation of medicines and treatment for any person. The access of cloud data is performed in two ways like read and write. The presence of malicious nodes in the environment would perform variety of threats on the data like modification attack, intrusion attack and so on. For example, if the healthcare system monitors the patient health information like blood pressure, sugar and

temperature through different bio sensors. Then the data sensed has been transmitted to the model which in turn save the records in the cloud and produce treatment option for the person. If there is an malicious node in the path exist, then if the node performs modification attack on data, then the system would produce wrong health medicine recommendation and affect the performance and trust of the model. Similarly, each threat has different impact on the performance of the model and affects the medical condition of the person as well. This must be considered in keen and the data security must be enforced on EHR data. Also, the healthcare organization would maintain variety of information about the patient where not all of them can be exposed to the all users. There will be sensitive information and private information present in the EHR data, which must be secured from illegal access. To enforce this privacy and to preserve that, efficient data security measures should be adapted.

To enforce data security there are number of approaches are available in literature like access restriction based on profile, behavior, and history where data encryption schemes like attribute based encryption, public key encryption and others also available. Such methods are not tamper proof and would compromise with adversaries. To overcome these security issues, modern blockchain can be adapted. The blockchain techniques are more tamper proof and restrict the malformed access in block level and the user with concern key belongs to the data in a specific block only can read the original data. By adapting such methods, the performance of data security can be improved. Also, in terms of records, there will be number of features and each would have different access restriction. By enforcing feature level access restriction, the data security of cloud can be further improved. This article focused on designing such model to improve the data security. By considering all these, an Adaptive Feature Centric Trust Analysis Model with blockchain (AFCTAM-BC) is presented in this article. The method analyze the user trust on feature level using the FCTAM algorithm by computing Feature Centric Trust Score (FCTS) on both sensitive and non-sensitive features to compute Access Clearance Measure (ACM). Similarly, the data has been encoded on each block of chain using Class Level Data Encryption (CLDE) algorithm. The detailed working of the proposed AFCTAM-BC model has been briefed in the next section.

RELATED WORKS

Number of data security methods are prescribed in literature and explored in this section in detail.

A patient centric health information exchange model is presented in [1], which uses blockchain smart contract features to protect patient data and privacy in a personalized way.

A blockchain based personalized access control EHR-sharing scheme is presented in [2], which uses CPABE towards personalized access control for data owners. Also, a interactive zero knowledge proof protocol is used between owners and users to perform authentication.

A blockchain based data sharing framework is presented in [3], for the support of healthcare organization which consider the factors of healthcare, security and blockchain.

A multilevel blockchain security model is presented in [4], which uses Lattice Based Access Control (LBAC) and smart contract based blockchain towards the data security of EHR data. The user has been authenticated with Ethereum Virtual Machine (EVM) envision model using smart contracts.

An confidentiality preserving with blockchain model (CP-BDHCA) is presented in [5], which uses HCA-ECC for secure key communication within the entities and uses a two-step authentication framework HCA-RSAE is used.

Anblockchain based secure and efficient data management model (EdgeMediChain) is presented in [6], which supports both edge computing and blockchain to ensure data security.

An hybrid blockchain architecture is presented in [7], which uses attribute based signature aggregation (ABSA) scheme and multi-authority attribute-based encryption (MA-ABE) with Paillierhomomorphic encryption (HE) to secure patient data.

A deep learning with blockchain model is presented in [8], towards ensuring the privacy of healthcare data. The method classifies the data using CNN and blockchain is used with crypto based federated learning model to eliminate the malicious users.

A Patient's E-Healthcare Records Management System (PRMS) is presented in [9], which is focused on the reduction of latency and increase of throughput.

A Decentralized Self-Management of data Access Control (DSMAC) is presented in [10], which uses blockchain based Self Sovereign Identity (SSI) model to enforce privacy preservation and uses role based access control policies towards access restriction.

An hybrid deep learning and homomorphic encryption based model is presented in [11], which uses HE to perform data encryption to challenge phishing attacks. Also, deep learning models are used to classify the devices in IIoMT networks.

An EHR sharing and drug supply chain management framework is presented in [12], which prioritize patient orient healthcare by providing access control on health information.

A patient centric privacy preservation framework is presented in [13], which uses three blockchain platforms using smart contract to find the suitable platform.

A detailed analysis on artificial intelligence based healthcare system using blockchain is presented in [14], which analyzes the issues and challenges in adapting AI in blockchain healthcare.

A permissioned blockchain based system is presented in [15], which gives a web based interface for the access and uses hybrid data management. The method encrypts the data using public key infrastructure based asymmetric encryption and digital signatures to secure shared EHR data.

A blockchain-inspired secure and reliable data exchange architecture is presented in [16], which uses BigchainDB, Tendermint, Inter-Planetary-File-System (IPFS), MongoDB, and AES encryption algorithms.

A systematic review is presented in [17], which present a detailed introduction on blockchain security on electronic healthcare records and future challenges in detail.

A flexible fine grained access control model is presented in [18], which uses CPABE, permission token, dual key regression and blockchain to enforce data security in EHRdata.

A blockchain based model is presented in [19], which uses smart contracts for service automation and uses blockchain-based distributed data storage system to enforce security. A decentralized selective ring based access control scheme is used for access restriction.

A privacy preserving scheme based on blockchain and swarm exchange techniques is presented in [20], named BioTHR which uses blockchain and swarm nodes to enforce secure transmission. Also the method uses autonomous encryption-decryption mechanism to secure EHR data.

All the methods suffer to achieve higher accuracy in access restriction and data security.

ADAPTIVE FEATURE CENTRIC TRUST ANALYSIS MODEL BASED EHR DATA SECURITY MODEL (AFCTAM-BC)

The proposed Adaptive Feature Centric Trust Analysis Model with Blockchain (AFCTAM-BC) model keeps track of feature access performed by any user towards access restriction [21]. The model classifies the features accessed by the services under different sensitivity level. Accordingly, the method applies AFCTAM algorithm to measure the trust of any user against the access of different features of healthcare record. The method computes sensitive and non-sensitive Feature Centric Trust Score (FCTS) according to the historic access records. Based on these values, the method computes Access Clearance Measure (ACM) to grant or deny the service access. Further, the method adapts Class Level Data Encryption (CLDE) to generate the blockchain which restrict the malformed access of any user to perform access restriction.

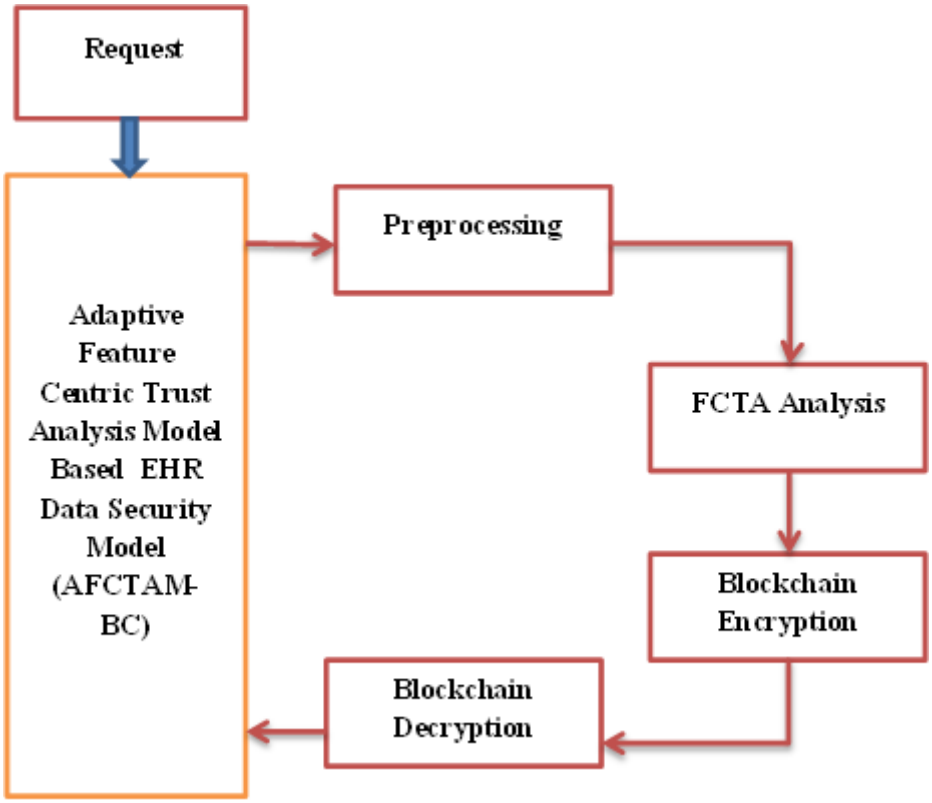

Figure 1: Architecture of AFCTAM-BC Model

The functional architecture of proposed AFCTAM-BC model is presented in Figure 1 and the functional components are briefed in this section.

Preprocessing:

In this stage, the model receives the user request and collects the traces of user available in the data base. From the records fetched, the method finds the set of features in the access trace. By traversing through each record, the method finds the missing values and incomplete records and eliminate from the set. Such normalized set has been used to perform further analysis.

Algorithm:

Given: Access Record set ARS

Obtain: Normalized set Ns.

Start

Read Request R and ARS.

User U =UserId$\in R$

User access set Uas = $\sum_{i=1}^{Size(ARS)} ARS(i).UserId == U$

Feature set FeaS=$(\sum_{i=1}^{size(Uas)} Features(Uas(i)) \ni Feas) \cup Feas$

For each record r

If $r \ni Features(Feas)$ then

Uas = Uas$\cap r$

End

End

Ns =Uas

Stop

The preprocessing algorithm collects the records of user and normalizes the data to perform further analysis.

FCTA Analysis:

The FCTA analysis algorithm read the service taxonomy and finds the features required for the service access. Using the features identified, the method finds the sensitivity of each feature. Using them, the method collects the access grant of users and compute sensitive and non-sensitive Feature Centric Trust Score (FCTS). Using both the values, the method computes Access Clearance Measure (ACM) to perform access restriction.

Algorithm:

Given: Normalized record set Nrs, Service Taxonomy ST, Service S

Obtain: ACM

Start

Read Nrs, ST, and S.

Find features required frs = $\sum_{i=1}^{size(ST)} Features(ST(i)).Required == S$

Find sensitive feature set Sfs = $\sum_{i=1}^{Size(Frs)} Frs(i).FeatureType == Sensitive$

Find Non-Sensitive Feature set Nsfs = $\sum_{i=1}^{Size(Frs)} Frs(i).FeatureType == Non-Sensitive$

Compute Sensitive Feature centric trust score SFCTS = $\frac{\sum_{j=1}^{Size(Sfs)} \sum_{i=1}^{size(ST)} Count(SFS(i)==ST(i)\&\&\ ST(i).UState==Grant)\&\&ST(i).User==U}{Size(SFS)}$

Compute Non-Sensitive Feature centric trust score NSFCTS = $\frac{\sum_{j=1}^{Size(NSfs)} \sum_{i=1}^{size(ST)} Count(NSFS(i)==ST(i)\&\&\ ST(i).UState==Grant)\&\&ST(i).User==U}{Size(NSFS)}$

Compute ACM = SFCTS×NSFCTS

Stop

The FCTA analysis algorithm computes the ACM value for the user based on which access restriction is performed.

BLOCKCHAIN GENERATION

The blockchain generation algorithm checks the ACM value of the user towards the service access and based on that the service data has been collected. Further, the data has been applied with the Class level data encryption scheme. The class level encryption scheme selects a distinct key and scheme for the feature and encrypt the data. Encrypted data has been added to the data block of the chain and hash code is generated according to the index of each key and scheme used. Generated chain has been given to the user to perform decryption.

Algorithm:

Given: ACM, Service S

Obtain: Blockchain B

Start

Read ACM and S.

If ACM>Th then

Service data Sd= access service and collect data.

Identify no of features on the service data Nf = $Count(\sum Features \in sd)$

Generate chain B with number of blocks Nf.

For each feature f

Key k = $\underset{i=1}{\overset{size(ST)}{Random(ST(i).Feature == F \;\&\&\; ST(i).Key)}}$

Scheme s = $\underset{i=1}{\overset{size(ST)}{Random(ST(i).Scheme == F \;\&\&\; ST(i).scheme)}}$

Cipher text ct = Perform encryption (f.value, k, s)

Add ct to block b.

Hash code FHC = $\underset{i=1}{\overset{size(ST)}{indexof(ST(i).Key == k)}} + "\#" + \underset{i=1}{\overset{size(ST)}{indexof(ST(i).Scheme == s)}}$

Add FHC to the hashcode block.

End

Stop

The block chain generation algorithm validates the access of user and applies class level data encryption to produce the blockchain.

Blockchain Decryption:

The user receives the blockchain and at each block the hash code has been reversed and the indexes of key and schemes are identified. Using the index, concern scheme and key are obtained from the set provided earlier. At each block, the method applies decryption according to the scheme and key identified and original data has been given to the user.

Algorithm:

Given: Blockchain B, Scheme set Scs, Key set Kes

Obtain: Original data D

Start

Read B, Scs, Kes.

For each block b

Index set Is = Split(HashCode, #)

Key k = $Kes(Is(0))$

Scheme s = SCS(IS(1))

Original text Ot = Perform decryption (b.value, k, s)

Add ot to data D.

End

Stop

The blockchain decryption algorithm finds the key and scheme for each block using the index obtained from the hash code. Accordingly, original text is obtained by decrypting each block of data.

RESULTS AND DISCUSSION:

The proposed AFCTAM-BC model has been implemented and its performance is evaluated under various scenarios and metrics. Obtained results are presented in this section.

Table 1: Experimental Setup

Key Factors	Value
Tool Used	Advanced Java
Number of Services	500
Number of Features	100
Total Traces	2 lakhs.

The evaluation conditions considered for the performance evaluation of proposed model is presented in Table 1 and the performance of method is measured against various performance metrics and compared with the result of other approaches.

Table 2: Performance on Access Restriction

Access Restriction Efficiency Vs. Number of Services			
	100 Service	200 Services	300 Services
CP-BDHCA	68	76	81
EdgeMediChain	72	79	84
BioTHR	78	84	89
AFCTAM-BC	89	94	98

The efficacy of methods in restricting malformed access has been counted at various scenarios and plotted in Table 2, and the proposed AFCTAM-BC model has produced higher accuracy than others.

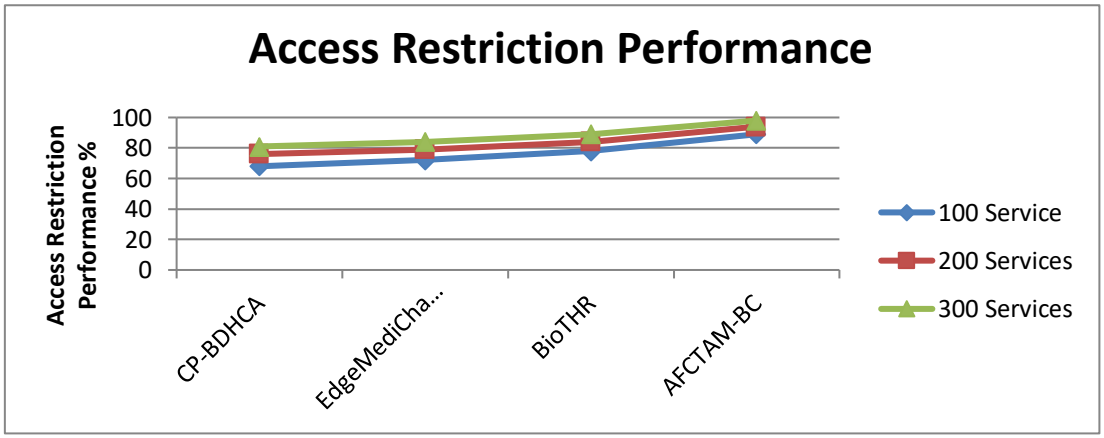

Figure 2: Access Restriction Performance

Efficiency in access restriction achieved by various approaches are measured and pictured in Figure 2, where the AFCTAM-BC model shows higher accuracy in all test cases.

Table 3: Performance in Data Security

Data Security Efficiency Vs Number of Services			
	100 Service	200 Services	300 Services
CP-BDHCA	72	78	83
EdgeMediChain	75	82	87
BioTHR	79	84	89
AFCTAM-BC	88	94	98

The efficacy of methods in enforcing data security is measured for various schemes and plotted in Table 3, and the AFCTAM-BC model has achieved higher data security performance than others.

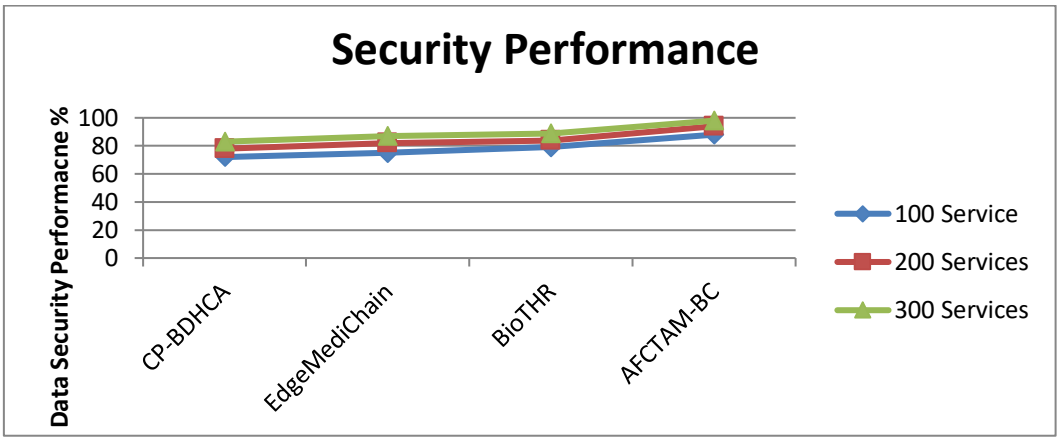

Figure 3: Performance on Data Security

The performance in data security enforcement is measured for various approaches under different scenario and pictured in Figure 3, and the AFCTAM-BC model has achieved higher data security performance in all test cases than others.

Table 4: Data Encryption / Decryption Performance

Data Encryption/Decryption Efficiency Vs Number of Services			
	100 Services	200 Service	300 Services
CP-BDHCA	68	74	80
EdgeMediChain	72	79	85
BioTHR	77	83	89
AFCTAM-BC	86	91	97

The efficiency in data encryption and decryption is measured for various approaches under different scenario and presented in Table 4, and the AFCTAM-BC model has achieved higher performance in all test cases than others.

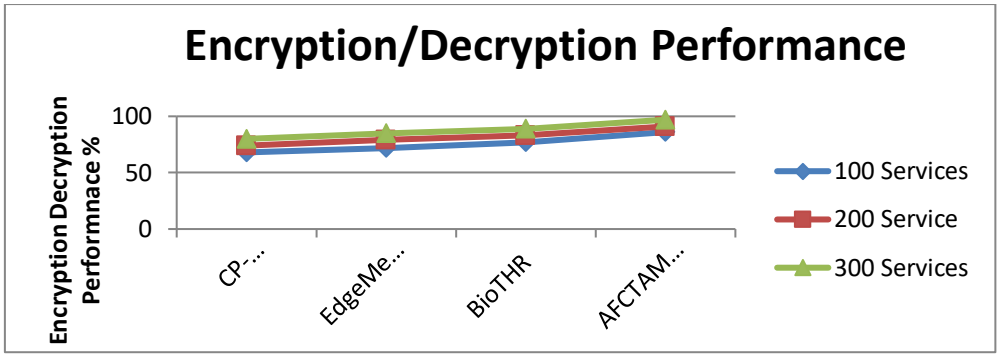

Figure 4: Data encryption decryption performance

The efficiency in data encryption and decryption is measured for various approaches under different scenario and presented in Figure 4, and the AFCTAM-BC model has achieved higher efficiency in all test cases than others.

CONCLUSION

This paper presents a novel adaptive feature centric trust analysis model with blockchain (AFCTAM-BC) towards data security in electronic healthcare records. The model applies preprocess to normalize the data belongs to the user. According to the access history of user, the method finds the features and applies feature trust analysis to measure access control measure (ACM). Based on the value of ACM, the user access has been restricted or allowed. Further, the method generates blockchain with the data obtained from service access and applies class level data encryption (CLDE) to store the data block with the chain. The user in turn receives the blockchain and performs data encryption to obtain the result. The proposed model improves the performance of data security, access restriction and data encryption.

REFERENCES

[1] Zhuang Y, Sheets LR, Chen YW, Shae ZY, Tsai JJ, Shyu CR. A patient-centric health information exchange framework using blockchain technology. IEEE journal of biomedical and health informatics. 2020 May 8; 24(8):2169-76.

[2] Wang H, Xie Y, Liu Y, Li X, Dorje P. Data verifiable personalized access control electronic healthcare record sharing based on blockchain in IoT environment. IEEE Internet of Things Journal. 2023 Oct 23;11(4):5696-707.

[3] Alzahrani AG, Alhomoud A, Wills G. A framework of the critical factors for healthcare providers to share data securely using blockchain. Ieee Access. 2022 Mar 25; 10:41064-77.

[4] Haritha T, Anitha A. Multi-level security in healthcare by integrating lattice-based access control and blockchain-based smart contracts system. IEEE Access. 2023 Oct 16; 11:114322-40.

[5] Ghayvat H, Pandya S, Bhattacharya P, Zuhair M, Rashid M, Hakak S, Dev K. CP-BDHCA: Blockchain-based Confidentiality-Privacy preserving Big Data scheme for healthcare clouds and applications. IEEE Journal of Biomedical and Health Informatics. 2021 Jul 14; 26(5):1937-48.

[6] Akkaoui R, Hei X, Cheng W. EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange. IEEE access. 2020 Jun 19; 8:113467-86.

[7] Guo H, Li W, Nejad M, Shen CC. A hybridblockchain-edge architecture for electronic health record management with attribute-based cryptographic mechanisms. IEEE Transactions on Network and Service Management. 2022 Jun 24; 20(2):1759-74.

[8] Alzubi JA, Alzubi OA, Singh A, Ramachandran M. Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning. IEEE Transactions on Industrial Informatics. 2022 Jul 7; 19(1):1080-7.

[9] Zala K, Thakkar HK, Jadeja R, Singh P, Kotecha K, Shukla M. PRMS: design and development of patients' E-healthcare records management system for privacy preservation in third party cloud platforms. IEEE Access. 2022 Aug 11; 10:85777-91.

[10] Saidi H, Labraoui N, Ari AA, Maglaras LA, Emati JH. DSMAC: Privacy-aware Decentralized Self-Management of data Access Control based on blockchain for health data. IEEE Access. 2022 Sep 19; 10:101011-28.

[11] Ali A, Pasha MF, Guerrieri A, Guzzo A, Sun X, Saeed A, Hussain A, Fortino G. A novel homomorphic encryption and consortium blockchain-based hybrid deep learning model for industrial internet of medical things. IEEE Transactions on Network Science and Engineering. 2023 Jun 14; 10(5):2402-18.

[12] Javan R, Mohammadi M, Beheshti-Atashgah M, Aref MR. A scalable multi-layered blockchain architecture for enhanced EHR sharing and drug supply chain management. arXiv preprint arXiv:2402.17342. 2024 Feb 27.

[13] Tanwar N, Thakur J. Patient-centric soulbound NFT framework for electronic health record (EHR). Journal of Engineering and Applied Science. 2023 Dec; 70(1):33.

[14] Shinde R, Patil S, Kotecha K, Potdar V, Selvachandran G, Abraham A. Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions. Transactions on Emerging Telecommunications Technologies. 2024 Jan; 35(1):e4884.

[15] Dubovitskaya A, Baig F, Xu Z, Shukla R, Zambani PS, Swaminathan A, Jahangir MM, Chowdhry K, Lachhani R, Idnani N, Schumacher M. ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. Journal of medical Internet research. 2020 Aug 21; 22(8):e13598.

[16] Kumar M, Raj H, Chaurasia N, Gill SS. Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. Internet of Things and Cyber-Physical Systems. 2023 Jan 1; 3:309-22.

[17] Kiania K, Jameii SM, Rahmani AM. Blockchain-based privacy and security preserving in electronic health: a systematic review. Multimedia Tools and Applications. 2023 Jul; 82(18):28493-519.

[18] Chen D, Zhang L, Liao Z, Dai HN, Zhang N, Shen X, Pang M. Flexible and fine-grained access control for ehr in blockchain-assisted e-healthcare systems. IEEE Internet of Things Journal. 2023 Oct 30; 11(6):10992-1007.

[19] Egala BS, Pradhan AK, Badarla V, Mohanty SP. Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet of Things Journal. 2021 Feb 12; 8(14):11717-31.

[20] Ray PP, Chowhan B, Kumar N, Almogren A. BIoTHR: Electronic health record servicing scheme in IoT-blockchain ecosystem. IEEE Internet of Things Journal. 2021 Jan 11; 8(13):10857-72.

[21] Geeitha S, Ravishankar K, Cho J, Easwaramoorthy SV. Integrating cat boost algorithm with triangulating feature importance to predict survival outcome in recurrent cervical cancer. Scientific Reports. 2024 Aug 27; 14(1):19828.