International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Blockchain Based Cross Chain Trusted Clinical Records Sharing System

[1]Dr. Chandrshekhar Goswami, [2]Sreenivasulu Reddy L., [3]Dr. A. Pankajam, [4]Priyadarsini K., [5]Vivek Dadasaheb Solavande, [6]Dr. Adapa Gopi

Submitted: 27/05/2023 **Revised**: 15/07/2023 **Accepted**: 28/07/2023

Abstract: The progress of clinical informatization depends greatly on the trustworthy exchange of electronic healthcare records, which are sensitive and important private data assets for patients. The longer access time, problematic cross-domain trustworthy exchange, and insecure storage of patient clinical record data are all discussed in this study. Designing a cross-chain trustworthy sharing solution for electronic clinical records based on the Fabric alliance chain required the use of blockchain and edge computing in this work. The system is separated into patient mobile applications, hospital online applications, and RFID electronic tag wristbands, with clinical record encryption and authentication, cross-chain trustworthy sharing, remote authorization, and other features. Additionally, in order to accomplish tailored privacy protection, a system for controlling the flow of private data using patients as the main source is proposed in this work. This mechanism is based on a biometric key and a secret algorithm. In order to establish reliable access and control, the master-slave multi-chain layered cross-chain paradigm based on the upgraded PBFT consensus algorithm for the main Chain and PoVT consensus algorithm for the slave Chain is employed

Keywords: *Blockchain, Edge Computing, Clinical Records, Consensus Algorithm, Fabric Alliance Chain*

1. Introduction

At present, with the popularization of medical information system, most hospitals at home and abroad use it to realize the information management of the whole hospital process, including the storage and processing of electronic medical records of patients. Traditional medical information systems usually use B/S or C/S architecture centres. The main reasons are: first, centralized architecture and relational data storage cannot guarantee the absolute security of medical record data, and different medical information systems implement different levels of information security protection standards. , storage service providers are not sufficiently credible and reliable, the system rights management mechanism is not strict, the division of role rights is not clear, and data leaks caused by third-party internal attacks emerge in an endless stream [2], according to the 2020 white paper on cyber security in the medical industry [3]] data show that over 280,000 pieces of patient medical data from 14 domestic central servers are exposed to the Internet; second, the storage format of electronic medical records is inconsistent with the dependent environment, the interoperability of medical information systems in various hospitals is low, and the storage of patient data is relatively scattered and Controlled by different subjects, data sharing is difficult to coordinate and manage, and in the process of cross-domain sharing, the confidentiality, integrity, and availability of data cannot be guaranteed, and the reliability is questionable; third, the data access cycle is long, and access to medical record data requires medical information system

A series of links, such as identity authentication, access control, key generation and certificate issuance, may cause network congestion and prolong the data access cycle when the amount of access is large. Obtain historical medical record data within the system, delaying accurate first aid.

[1]*Associate Professor, Department of CSE, School of Computing, MIT ADT University, Pune- 412201, Maharashtra, India Email: shekhar.goswami358@gmail.com*

[2]*Associate Professor, Department of Mathematics, School of Advanced Sciences, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India Email: sreenivasulureddy.svu@gmail.com*

[3]*Associate Professor, Department of Business Administration, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India Email: ambipankaj@gmail.com*

[4]*Department of Data Science and Business Systems, School of Computing, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, Chennai- 603203, Tamil Nadu, India Email: priyadak@srmist.edu.in*

[5]*Assistant Professor, Department of Computer Science and Engineering, Bharati Vidyapeeth Deemed to be University, Department of Engineering and Technology, Navi Mumbai, India Email: viveksolavande@gmail.com*

[6]*Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur- 522502, Andhra Pradesh, India Email: dr.adapagopi@gmail.com*

Corresponding Author: Dr. Chandrshekhar Goswami (shekhar.goswami358@gmail.com)

Blockchain technology provides a secure distributed framework for electronic medical records to be controlled, trusted, and shared. Its decentralization and non-tampering characteristics align with the trend of distributed and secure data storage [4], and it is a perfect solution for data exchange. At present, the application research of the combination of blockchain and intelligent medical treatment at home and abroad has made significant progress. For example, HealthNautica's product e-Orders[5] uses blockchain technology to improve the security of patient data, which is convenient for both doctors and patients to identify and communicate with each other. It can be traced back and cannot be tampered with[6]; BitHealth[7] uses blockchain technology to store medical data and can restore it from any node around the world; Gem and Philips jointly develop an enterprise-level blockchain medical application Gem HealthNetwork [8], the application is based on blockchain technology to protect patient privacy and is conducive to the sharing of electronic medical record information [9]. However, the above research still has shortcomings: First, it is difficult to adapt to the high-speed production and high-frequency concurrent sharing of domestic medical data. , it is not suitable for the complex and rich text information environment in the era of big data, and the implementation cost is high; second, it does not reflect the authority control of the data flow with patients as the main body and cannot realize the controllable and personalized privacy protection of patients; third, it does not entirely Use the computing power of patient equipment and integrating edge computing technology highlights the shortcomings of single blockchain architecture.

With the gradual enhancement of data processing and computing power of edge devices, edge computing has been introduced into Internet application systems as an extension of the cloud [10]. The solution for cross-domain sharing of medical records takes the patient as the main body to control the sovereignty of private data assets and the flow of information, reflects the individualized privacy protection of patients, improves medical efficiency and reduces operating costs, and contributes to the construction of digital India.

2. Overall System Design

2.1. System Architecture Design

The overall architecture design of the electronic medical record cross-chain trusted sharing system is shown in Figure 1. The hospital node centre server is the basic business of the system, such as providing support for appointment registration, user management, etc., and uses B/S architecture to communicate with the patient and the hospital. , the client initiates a request to the server's standard RESTful interface to exchange data in JSON format. The server is developed using the SSM (SpringMVC+Spring+MyBatis) framework set and interacts with the local database that stores the patient's basic information. The system is built through the patient's mobile application and the electronic label emergency aid bracelet. The edge computing environment provides computing power and storage functions and reads and writes data through RFID or NFC. The master-slave multi-chain hierarchical cross-chain blockchain network and IPFS distributed P2P storage network support the core medical record business of the system.

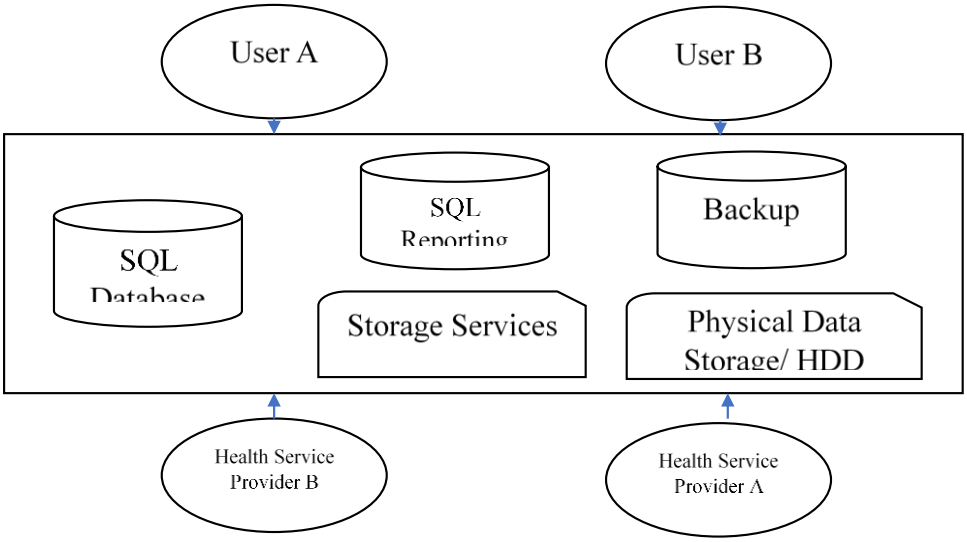


Fig 1: Overall Architecture of Electronic Medical Record

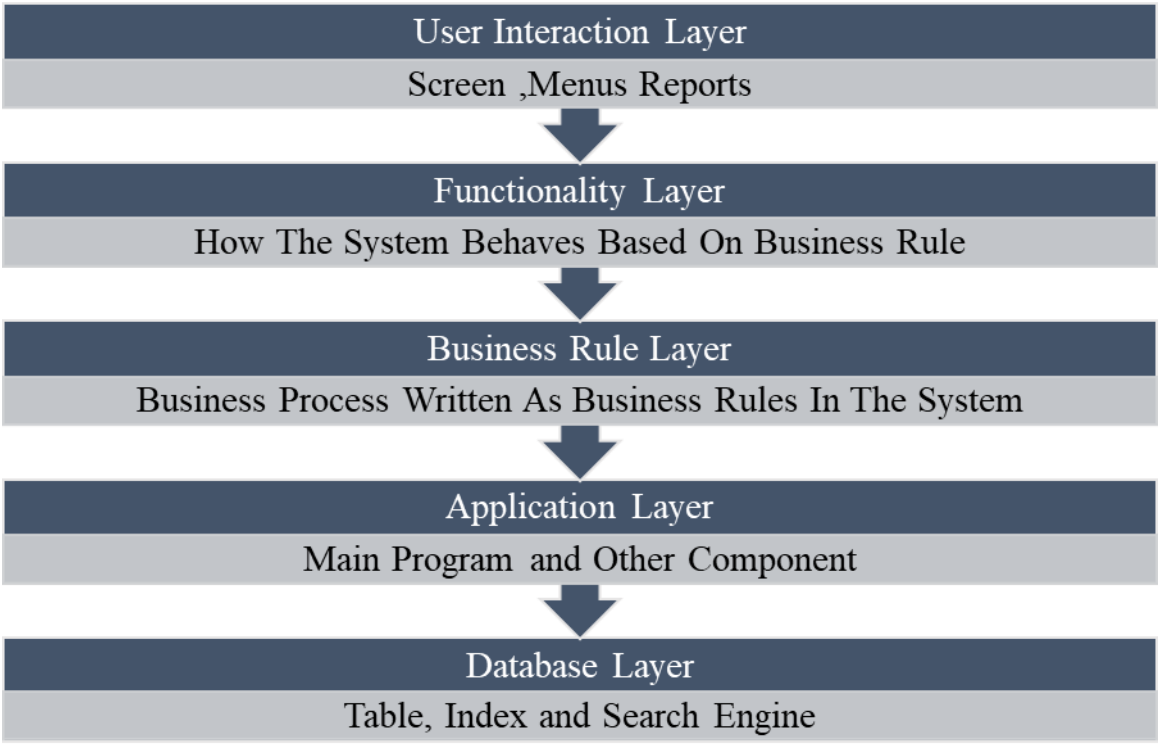


Fig 2: Five-Layer Architecture

In addition, the five-layer architecture design of the core medical record business is shown in Figure 2, which is divided into the user layer, application layer, core business layer, network layer and data storage layer, and the system architecture design is refined from the perspective of different user roles and functional requirements.

2.2. System Function Module Design

After market analysis and research and user demand analysis, the following software functional structure is designed, with a total of three application platforms and 20 functional modules..

I. Patient Mobile Application Terminal Functional Module

(1). Medical record centre: The remote authorization module handles the authorization request of doctors to view remote medical records; the medical record download module retrieves the historical medical record files and downloads, decrypts, and verifies the signatures for patients to view; the medical record destruction module permanently deletes the historical medical records and files of patients.

(2). Appointment centre: The registration and payment module allows patients to view the doctor's schedule and make an appointment for registration and payment; the appointment list displays the patient's appointment record.

(3). Personal centre: The information management module provides addition, deletion, modification and checking of personal basic information; the key management module manages the validity period of the patient's biometric key, encrypted records, etc.; the biometric management module collects the patient's biometrics and performs local and offline encryption. key export.

II. Functional Modules of Hospital Web Application

(1). Medical record centre: The medical record uploading module uploads and uploads the signed and encrypted medical record files of the system by the hospital node; the medical record downloading module retrieves the historical medical record and downloads it to the local by the hospital node; the medical record request module is used by doctors to remotely send patients Initiate a medical record sharing request authorization.

(2). Diagnosis centre: The doctor's consultation module is used by doctors to inquire and fill in the medical records of the patients to be diagnosed; the auxiliary examination module is used by doctors to issue auxiliary examination application forms;

(3). Monitoring centre: The system management module is for administrators to manage the system; the data statistics module supports exporting various data of the system in the form of multi-format files; the visualization module provides a large screen for data monitoring.

III. First Aid Auxiliary Bracelet Module

(1). Medical record reading and writing: Support the writing and encryption of basic patient information, encrypted medical record index and other information into the bracelet.

(2). Electronic fence: support setting the induction point electronic fence strategy to limit the range of activities.

(3). Statistics of people flow: It supports counting the number of people passing through the points through the induction points.

2.3. System Core Business Process Design

The core business of this system is the signature, encryption, uploading and uploading of electronic medical records, as well as retrieval, downloading, decryption and signature verification of medical records. 4. Among them, after the hospital node is validly registered with the CA, it locally generates the hospital node public and private key pair ‹PKhos, SKhos›, submits the identity information and public key PKhos to the CA, issues a digital certificate and returns to the hospital node server. Patient mobile application When the client needs to verify the digital signature of the encrypted medical record hospital node, it applies for a digital certificate to the hospital node server and confirms its validity, and then obtains the hospital node public key PKhos for verification. Kiris is the patient's biometric key, which is locally offline by the patient's mobile application client Export.

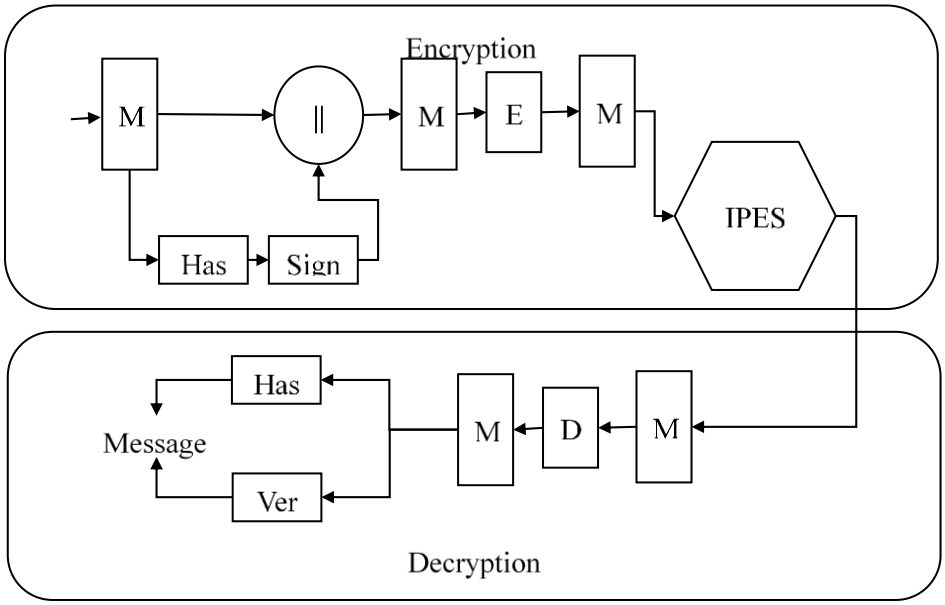


Fig 3 Encryption and Decryption approach

2.3.1. Medical Record Signature, Encryption, Upload And On-Chain

After the doctor completes the patient's diagnosis, the hospital web application generates the patient's plaintext electronic medical record. The hospital node first uses the national secret SM3 algorithm to calculate the digest value for the plaintext data, and then uses the hospital node private key SKhos and uses the national secret SM2 algorithm to sign the digest value. The signed digest value SigSKhos (Hash (M)) is obtained; after the plaintext data and the signed digest value are spliced together, the biometric symmetric key Kiris is used and the national secret SM4 algorithm is used to encrypt the data symmetrically, and the result is completed. Signature authentication and encrypted medical record data EKiris (SigSKhos (Hash(M)).

After the plaintext medical record data is signed and encrypted, the encrypted medical record file emr-DataEncrypted is uploaded to the IPFS distributed P2P storage network, and the unique index Hash value related to the file content is obtained; the hospital node packages this Hash value and user basic information for the easy query as a block, call the smart contract and start the consensus algorithm to upload to the master-slave multi-chain layered cross-chain network.

2.3.2. Medical record search, download, decryption and signature verification

When the patient himself needs to view the historical medical record, or after the doctor obtains the patient's remote authorization, the hospital node server calls the smart contract to query the historical medical record on the chain according to the keyword. After the query is successful, download the encrypted medical record file emrDataEncrypted in the IPFS distributed P2P storage network according to the index Hash value. Use the symmetric key Kiris to decrypt the medical record data, then verify the digest signature, and use the hospital node public key PKhos to get the digest to be compared. The

plaintext medical record data is calculated by the national secret SM3 algorithm to obtain the digest value H, and the comparison and verification stage is entered. If H and H' are completely consistent, the comparison and verification are passed, and the medical record data is true and valid, otherwise, it fails. The ciphertext medical record data decryption And the description of the signature verification algorithm is shown in Algorithm 1.

Algorithm 1 Decryption and signature verification algorithm of ciphertext medical record data based on national secrets Input: ciphertext medical record data emrDataEncrypted, hospital node public key PKhos, biometric symmetric key Kiris

Output: plaintext medical record data emrData

(1). Symmetric decryption: use the SM4 decryption algorithm to decrypt the ciphertext data into emrDataPlainText;
(2). Dismantling: take the last 32 bytes of emrDataPlainText as emrDataHashSig, and the rest as emrData;
(3). Calculate the summary of plaintext medical record data: use the SM3 summary algorithm to calculate the Hash value emrDataHash;
(4). Verify signature: use SM2 signature verification algorithm, input emrData, emrDataHashSig, PKhos for verification;
(5). If the verification fails in step 4, output null and end; otherwise, output emrData and end.

In addition, when a patient encounters an emergency outside the hospital, the emergency personnel scan the patient's emergency aid bracelet, read the Hash index of the patient's medical history, and then directly download the encrypted medical record file. The patient's iris is scanned on-site without the consent of the patient. The feature derives the biological key Kiris to complete the subsequent steps to achieve accurate first aid.

3. Key Technologies and Implementation of The System

3.1. Biometric-Based Key Derivation Algorithm

The iris has rich and unique texture features. Among various keys derived from biometrics, the iris key is longer and can meet the requirements of general symmetric encryption algorithms for key length (≥56 bits), which becomes the iris feature. Unique advantages of exporting biometric keys.

In terms of iris feature extraction biological key research, The Author proposed a private template scheme in 1988 [11], which extracts typical iris features directly as a key, but there is no experimental result, only at the theoretical level. The representative work is error-correcting code-based [12] and context-based iris feature key generation technology [13], but the above work has the following problems: First, the extracted iris feature template is stored in the cloud, and there are The second is that the generated keys are all from the outside, not from the iris feature itself. The scheme adopted in this system is: on the basis of iris preprocessing, use Haar wavelet three-layer decomposition to extract iris features, and use random mapping function to extract iris features from the iris. The 128-bit symmetric encryption key is directly extracted from the feature, which is used for the national secret SM4 symmetric encryption algorithm to realize the personalized privacy protection of patients. The algorithm description is shown in algorithm 2.

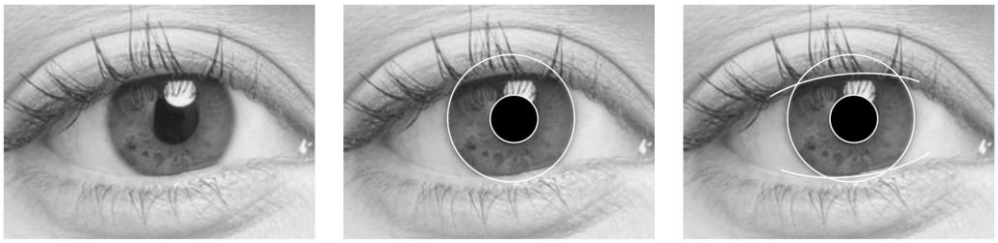
Algorithm 2 Key derivation algorithm based on iris features Input: iris image img

Output: 128-bit key for the national secret SM4 symmetric encryption algorithm

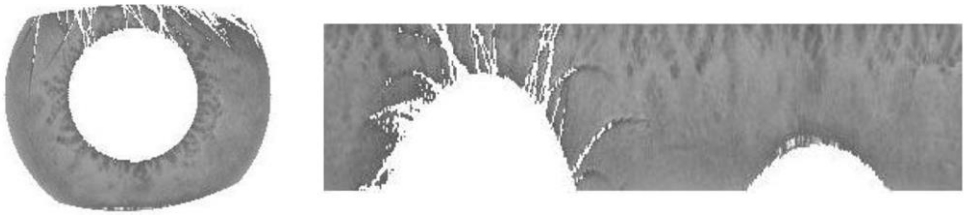
(1). Iris image preprocessing: After preprocessingimg, a normalized image img_tmp is obtained, with a size of 100 × 400;
(2). Image segmentation: take the 40×200 area R4 at the upper right of the img_tmp image;
(3). Two-dimensional Haar wavelet three-layer decomposition: take the HL3, LH3, HH3 regions of the result, a total of 375 wavelet coefficients;
(4). Feature encoding: The feature vector C composed of "0~1" thresholded wavelet coefficients is a binary code;
(5). Key derivation: extract the 128-bit symmetric cryptographic key P from C through a random mapping function;
(6). Output P, end.

3.1.1. Iris image pre-processing

Iris preprocessing includes iris acquisition, iris ring localization, eyelid detection, eyelash detection, and iris ring rectangle normalization, and its purpose is to extract the effective iris area for feature extraction. The preprocessing process is shown in Figure 4.



(A) Eye Image (B) Iris Ring Localization (C) Eye Detection



(D) Eyelash Detection (E) Iris Ring Rectangle Normalization

Fig 4 Irisimagepre-processing

3.1.2. Extraction and coding of iris characteristic coefficients

The iris texture features are mainly concentrated in the third layer, and the two-dimensional Haar wavelet three-layer decomposition is performed on the iris feature area, as shown in Figure 5.

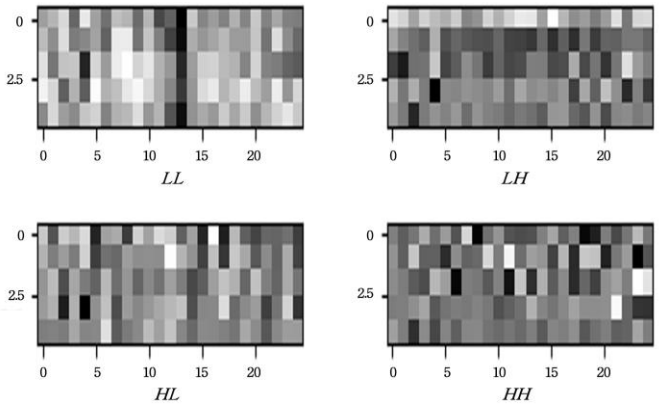


Fig 5. Results of Haar three-level wavelet decompositionof iris image

The frequent changes in iris texture feature cause the details of grey image changes to be mainly concentrated in high-frequency coefficients. If the low-level high-frequency coefficients are used as iris feature coefficients, the feature vector space will be too large, and the coding efficiency and key derivation speed will be reduced. Therefore, the high-frequency coefficients of the third layer are extracted as the iris feature vector C, and there are 25 × 5 × 3 = 375 wavelet coefficients in total, and the results are listed in Table 1.

Table 1: Irish Features Extraction

Child Images	1	2	3	4		22	23	24	25
LH 3	45.26	38.96	21.45	39.89	…	43.88	5.25	56.55	52.23
	25.68	8.95	-2.89	-6.89	…	-8.25	5.63	5.25	-8.00
	…	…	…	…	…	…	…	…	…
	18.12	5.69	-35.78	5.69	…	9.25	11.45	5.50	8.35
HL 3	48.56	-45.56	51.50	35.56	…	-31.72	-28.56	-23.45	-73.73
	35.56	-15.25	15.25	-15.56	…	1	-35.85	28.86	-61.25
	…	…	…	…	…	…	…	…	…

	-12.82	-9.36	-15.74	22.56	…	-43.85	-5.3	15.45	15.89
HH 3	5.26	-5.63	-1.36	20.69	…	-18	-5.35	25.36	-2.45
	10.55	-10.56	28.88	-10	…	1	14.63	-43.87	14.56
	…	…	…	…	…	…	…	…	…
	15.61	5.12	-30.45	8.88	…	-9.56	11.56	18.45	4.25

To facilitate the processing of the random mapping function, set 0 as the threshold to convert the feature vector C into a binary code. The encoding rule of the iris feature vector element C(i) is shown in formula (1):

$$\boldsymbol{C}(i) = \begin{cases} 0, \boldsymbol{C}(i) < 0, 1 \leqslant i \leqslant 375 \\ 1, \boldsymbol{C}(i) \geqslant 0, 1 \leqslant i \leqslant 375 \end{cases}$$

After encoding the thresholded feature vector C' through a random mapping function, a 128-bit symmetric cryptographic key is obtained, as shown in Figure 6.

p	0	1	1	0	0	0	0	0	1	1	0	0	0	0	1	1
	1	0	0	1	0	0	1	0	1	1	0	0	1	1	1	1
	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	0
	0	1	0	0	1	0	0	1	0	1	0	0	0	1	1	1
	0	1	0	0	1	1	0	0	1	0	0	1	1	0	0	0
	0	0	1	0	0	1	0	0	0	0	1	0	0	1	0	1
	0	1	0	1	1	1	0	0	1	0	0	1	0	0	1	0
	1	1	0	0	1	0	0	1	0	1	0	0	1	0	0	1

Fig 6: Biometric Key Extraction

3.2. Master-Slave Multi-Chain Hierarchical Cross-Chain Model

The cross-chain consensus algorithm can improve the throughput and scalability of the blockchain, and enhance the transaction processing capability. This system builds a master-slave multi-chain split based on the improved PBFT consensus algorithm [14] for the main chain and the PoVT consensus algorithm for the slave chain. Layer cross-chain model. This model uses cross-chain technology based on the notary mechanism. The slave chain is responsible for packaging and verifying medical record data blocks, and the main chain is responsible for sorting, consensus and uploading the blocks uploaded from the slave chain. The model structure is shown in the figure 7 is shown.

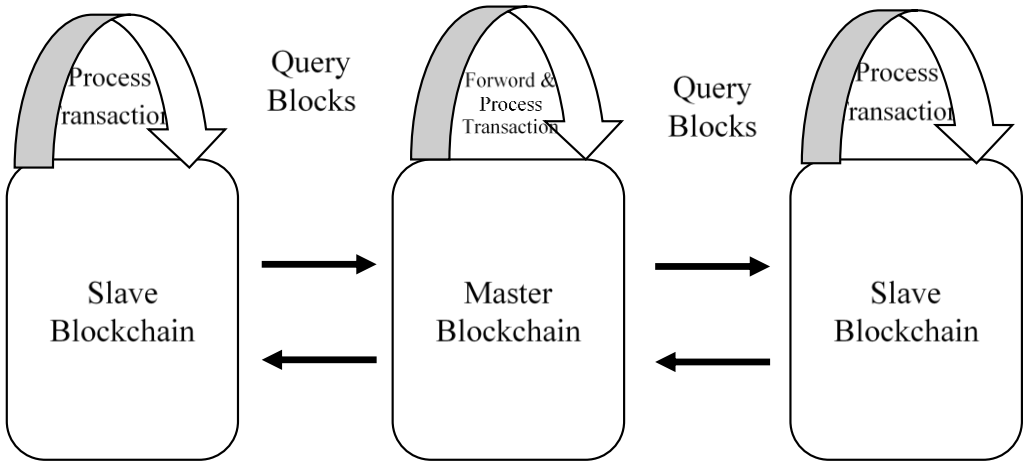


Fig 7: Master Slave Multichain Hierarchy

3.2.1. Slave Chain Consensus

The slave chain adopts a PoVT consensus mechanism based on a voting mechanism and a credit mechanism. The consensus mechanism adopts a voting mechanism to select block-producing nodes, which ensures the reliability of nodes participating in the consensus and reduces the impact of node rights and interests on the distribution of accounting rights. , thereby increasing the difficulty of launching rights smashing attacks, double-spending attacks, private mining attacks, etc. on the system. The slave chain completes the packaging and uploading of data blocks within a time slice, and after a cycle ends, the representative of the slave chain node uploads all data blocks in this cycle to the main chain network. The slave chain nodes are divided into 5 types of roles: ordinary nodes, election nodes, production nodes, alternate nodes, and representative nodes. The ordinary nodes do not participate in any consensus and are responsible for synchronizing the latest data The block is sent to the local; the electoral node verifies and votes on the data block; the production node packs the medical record data and basic patient information into blocks; the alternate node is responsible for replacing the production node or the electoral node to become the role to continue when the production node or the election node cannot provide services Exercising the mission; the representative node is responsible for uploading the confirmed data blocks of its main body to the main chain network in each cycle. Select some nodes from the production nodes, election nodes, and candidate nodes to form a consensus node set N, set N The middle node is allowed to have the dual identities of the main chain node and the slave chain node at the same time. After the set N is formed, the PoVT consensus algorithm is used to determine the number of the production node that generates the block in each time slot, and a pseudo-random number is generated by running the Mersenne rotation algorithm. As the number of the representative node constituting the main chain, the data block is uploaded to the main chain network.

3.2.2. Main chain consensus

The main chain adopts an improved PBFT consensus mechanism. Based on the PBFT consensus mechanism, the checkpoint protocol cancels the step of regularly checking and clearing certificates, and the node synchronization process uses the method of requesting blocks from other nodes and verifying the synchronization to complete; The view switching protocol uses a timeout mechanism to switch views based on the block generation protocol. The improved PBFT consensus does not require three-stage mutual communication between nodes, which reduces communication consumption.

The representative node uploads the confirmed block data in its slave chain to the main chain network and then participates in the improved PBFT consensus of the main chain. After the consensus is completed, each representative node saves the main chain block to the local network. The main chain block saved by a representative node contains block data from different slave chains, which can be queried by other nodes in the slave chain where it is located, so as to complete the data cross-chain between different slave chains.

4. System Analysis

4.1. Security Analysis

(1) Data security: The system processes and stores users' primary low-sensitive data and important sensitive data in different ways. The essential low-sensitive data is stored in the hospital's local database, and fields such as user passwords are processed by "hash and salt" Post-storage. Critical and sensitive medical record data is processed by a series of encryption and authentication mechanisms based on biometrics and national secret algorithms. The most vital symmetric encryption key is derived from the image of the patient's iris. As a result, the medical record data is safe and reliable. In addition, the RFID electronic tag in the edge computing device uses the NTag213 chip, and the password protection mode is turned on. It uses 128-bit ECC encryption. The electronic title will permanently lock when the password is tried and wrong 50 times. Sex is higher.

(2) System operation security: The core network architecture of the system adopts a distributed and P2P structure design. Through the joint maintenance of all nodes, single-point attacks can be avoided to a certain extent; the main chain in the master-slave multi-chain layered cross-chain network is improved. In addition, the PBFT consensus algorithm supports 3f+1 node fault tolerance, which can better ensure the system's stability.

4.2. Efficiency Analysis

The SimPy simulator is used to model the core blockchain network of the system and the operation process of edge computing. The standard PBFT consensus algorithm and H-PBFT algorithm are selected for comparison.

First, compare the throughput and delay when the number of system nodes is 20, 50, and 100. It can be seen from Figure 8 and Figure 9 that the system's performance using the standard PBFT consensus algorithm decreases with the increase in the number of nodes. This is because the system's performance using the H-PBFT consensus algorithm has been improved. This system combines edge computing technology with the blockchain system and adopts the master-slave multi-chain hierarchical cross-chain model. The experimental

results show that the system has the best indicators, throughput, and time. Second, comparing the change in CPU occupancy rate with time, the results are shown in Figure 10. It can be seen from the results that over time, the CPU occupancy rate of the system using the standard PBFT consensus algorithm continues to increase. The CPU occupancy rate of the H-PBFT algorithm has a similar trend, which has been maintained at about 82% for a long time. The CPU occupancy rate of this system has been dramatically improved and can be kept below 20%.

Table 2 Throughput Data

No of Nodes	System using PBFT algorithm	System using H-PBFT algorithm	Huiwen system
20	3500	5500	7500
50	2500	5000	6500
100	1500	4500	6500

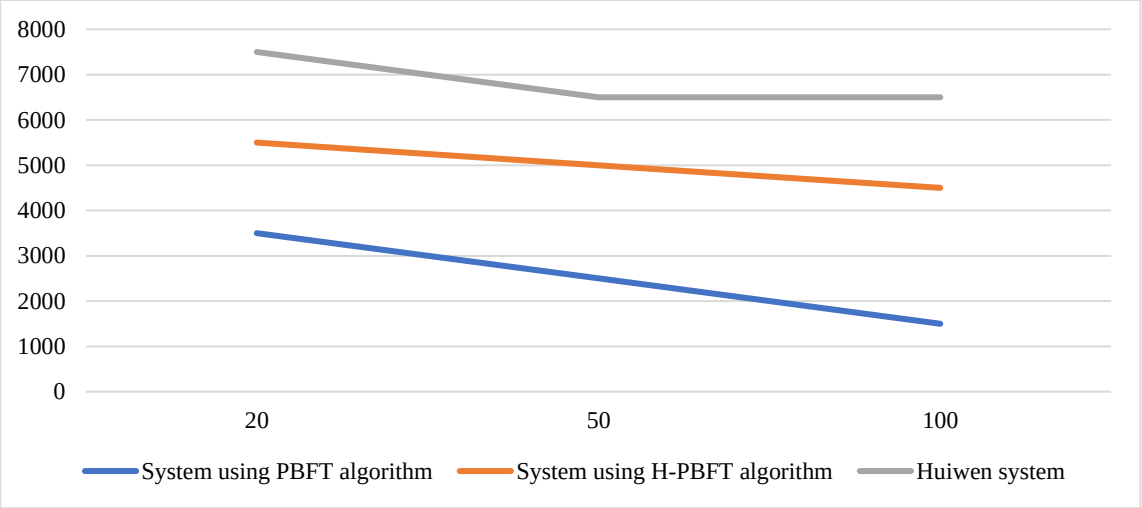


Fig 8 Throughput graph

Table 3: Time Delay data

No of Nodes	System using PBFT algorithm	System using H-PBFT algorithm	Huiwen system
20	675	625	425
50	875	725	580
100	1120	780	675

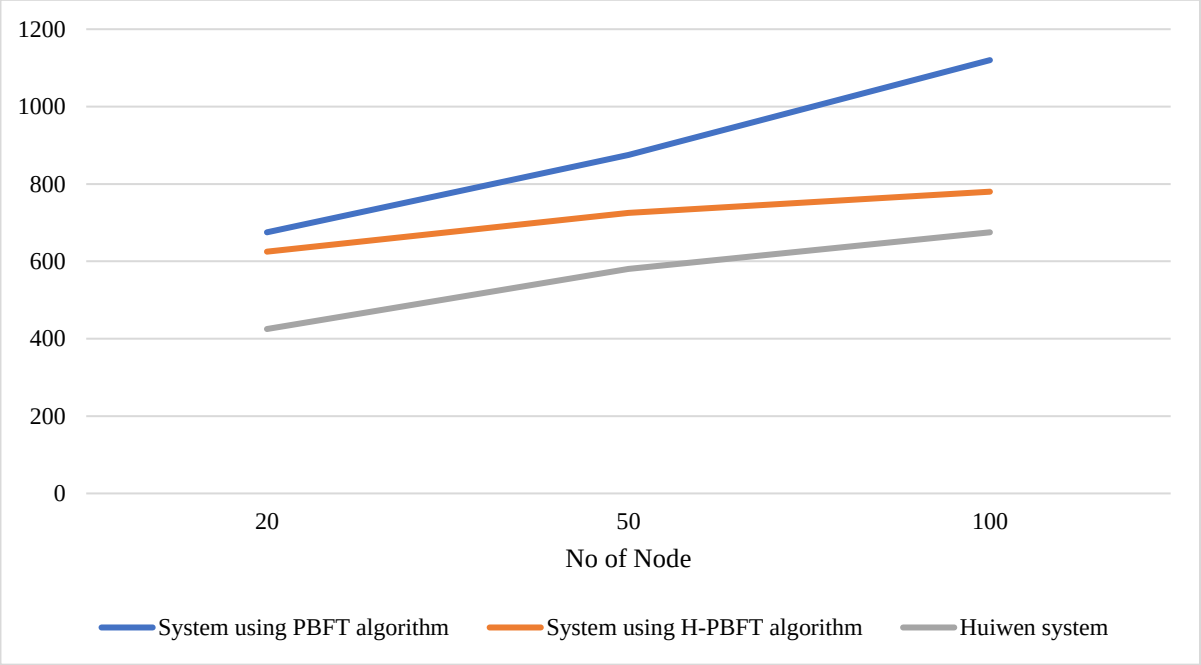


Fig 9: Time Delay graph

Table 4: CPU Utilization

No of Nodes	System using PBFT algorithm	System using H-PBFT algorithm	Huiwen system
70	104	83	18
65	105	85	20
60	103	84	21
55	105	85	18
50	101	85	21
45	102	83	19
40	105	84	19
35	75	85	20
30	60	66	19
25	55	46	18
20	45	42	19
15	24	23	20
10	9	15	10
5	5	8	8
0	3	5	5

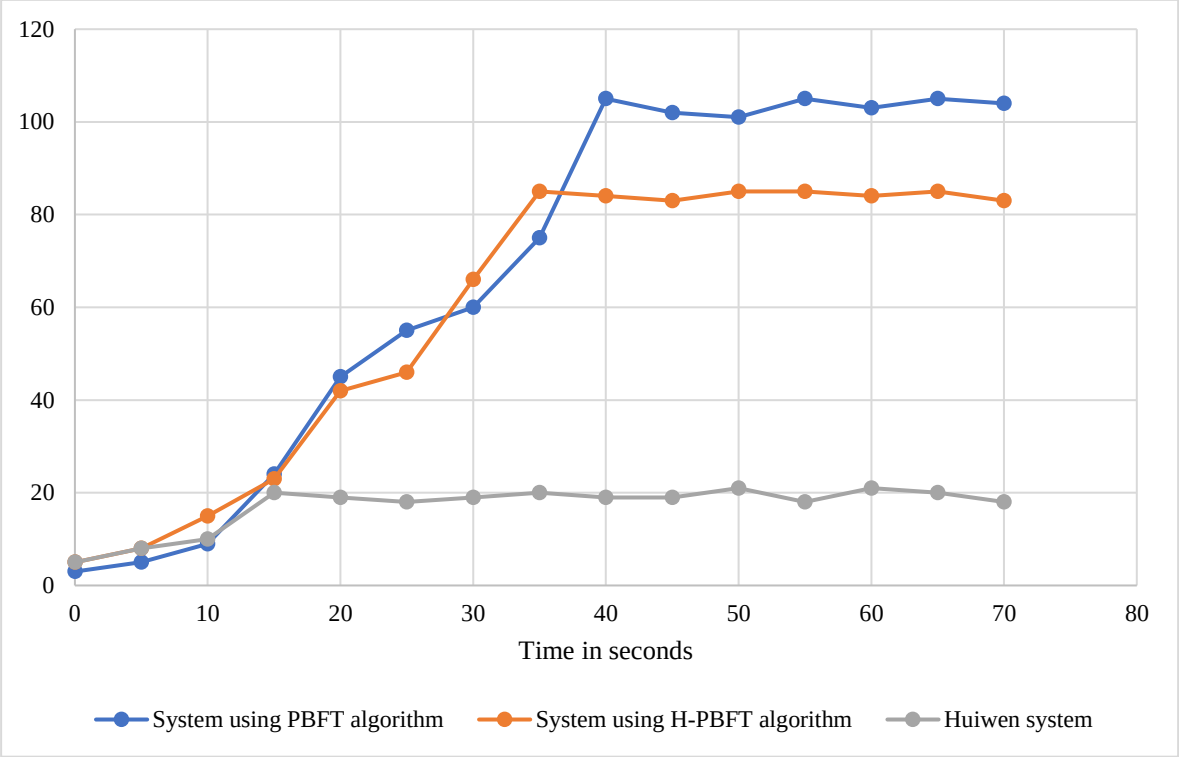


Fig 10: CPU Utilization Graph

The mainstream similar electronic medical record data sharing systems are analyzed and compared from five aspects: consensus algorithm, chain structure, system efficiency (throughput, delay, CPU occupancy rate), data sharing, and whether to integrate edge computing.

5. Conclusion

This paper integrates blockchain and edge computing technology, designs and implements a cross-chain trusted sharing system for electronic medical records, derive keys from patient biometrics, and realize personalized privacy protection. It has strong security and practicability and provides a Powerful decentralized network and abundant edge computing and storage resources. Of course, this system still has many deficiencies. Exploring the combination of blockchain and edge computing technology still faces significant challenges, such as integrating

References

[1] S. Ozcan and S. Unalan, "Blockchain as a General-Purpose Technology: Patentometric Evidence of Science, Technologies, and Actors," in IEEE Transactions on Engineering Management, vol. 69, no. 3, pp. 792-809, June 2022, doi: 10.1109/TEM.2020.3008859.

[2] C. Xu, Y. Qu, T. H. Luan, P. W. Eklund, Y. Xiang and L. Gao, "A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm for Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 6, pp. 4371-4384, 15 March15, 2022, doi: 10.1109/JIOT.2021.3103275.

[3] H. Xiong et al., "On the Design of Blockchain-Based ECDSA With Fault-Tolerant Batch Verification Protocol for Blockchain-Enabled IoMT," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5, pp. 1977-1986, May 2022, doi: 10.1109/JBHI.2021.3112693.

[4] M. N. M. Bhutta et al., "A Survey on Blockchain Technology: Evolution, Architecture and Security," in IEEE Access, vol. 9, pp. 61048-61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

[5] W. Liang, D. Zhang, X. Lei, M. Tang, K. -C. Li and A. Y. Zomaya, "Circuit Copyright Blockchain: Blockchain-Based Homomorphic Encryption for IP Circuit Protection," in IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 3, pp. 1410-1420, 1 July-Sept. 2021, doi: 10.1109/TETC.2020.2993032.

[6] J. Ren, J. Li, H. Liu and T. Qin, "Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT," in Tsinghua Science and Technology, vol. 27, no. 4, pp. 760-776, Aug. 2022, doi: 10.26599/TST.2021.9010046.

[7] H. M. Kim, H. Turesson, M. Laskowski and A. F. Bahreini, "Permissionless and Permissioned, Technology-Focused and Business Needs-Driven: Understanding the Hybrid Opportunity in Blockchain Through a Case Study of Insolar," in IEEE Transactions on Engineering Management,

vol. 69, no. 3, pp. 776-791, June 2022, doi: 10.1109/TEM.2020.3003565.

[8] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao and Y. Xiang, "A Blockchained Federated Learning Framework for Cognitive Computing in Industry 4.0 Networks," in IEEE Transactions on Industrial Informatics, vol. 17, no. 4, pp. 2964-2973, April 2021, doi: 10.1109/TII.2020.3007817.

[9] S. Xu, X. Chen and Y. S. Khatri, F. A. Alzahrani, M. T. J. Ansari, A. Agrawal, R. Kumar and R. A. Khan, "A Systematic Analysis on Blockchain Integration With Healthcare Domain: Scope and Challenges," in IEEE Access, vol. 9, pp. 84666-84687, 2021, doi: 10.1109/ACCESS.2021.3087608.26, no. 6, pp. 845-856, Dec. 2021, doi: 10.26599/TST.2020.9010043.

[10] J. Zhou, G. Feng and Y. Wang, "Optimal Deployment Mechanism of Blockchain in Resource-Constrained IoT Systems," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8168-8177, 1 June1, 2022, doi: 10.1109/JIOT.2021.3106355.

[11] X. Cai et al., "A Sharding Scheme-Based Many-Objective Optimization Algorithm for Enhancing Security in Blockchain-Enabled Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7650-7658, Nov. 2021, doi: 10.1109/TII.2021.3051607.

[12] Tharatipyakul and S. Pongnumkul, "User Interface of Blockchain-Based Agri-Food Traceability Applications: A Review," in IEEE Access, vol. 9, pp. 82909-82929, 2021, doi: 10.1109/ACCESS.2021.3085982.

[13] S. K. Ezzat, Y. N. M. Saleh and A. A. Abdel-Hamid, "Blockchain Oracles: State-of-the-Art and Research Directions," in IEEE Access, vol. 10, pp. 67551-67572, 2022, doi: 10.1109/ACCESS.2022.3184726.

[14] A. Omar, R. Jayaraman, M. S. Debe, K. Salah, I. Yaqoob and M. Omar, "Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts," in IEEE Access, vol. 9, pp. 37397-37409, 2021, doi: 10.1109/ACCESS.2021.3062471.

[15] M. S. Farooq, U. Iftikhar and A. Khelifi, "A Framework to Make Voting System Transparent Using Blockchain Technology," in IEEE Access, vol. 10, pp. 59959-59969, 2022, doi: 10.1109/ACCESS.2022.3180168.

[16] S. -J. Hsiao and W. -T. Sung, "Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks," in IEEE Access, vol. 9, pp. 72326-72341, 2021, doi: 10.1109/ACCESS.2021.3079708.

[17] T. Meng, Y. Zhao, K. Wolter and C. -Z. Xu, "On Consortium Blockchain Consistency: A Queueing Network Model Approach," in IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 6, pp. 1369-1382, 1 June 2021, doi: 0.1109/TPDS.2021.3049915.

[18] T. H. Tran, H. L. Pham, T. D. Phan and Y. Nakashima, "BCA: A 530-mW Multicore Blockchain Accelerator for Power-Constrained Devices in Securing Decentralized Networks," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 68, no. 10, pp. 4245-4258, Oct. 2021, doi: 10.1109/TCSI.2021.3102618.

[19] S. E. Chang and Y. Chen, "When Blockchain Meets Supply Chain: A Systematic Literature Review on Current Development and Potential Applications," in IEEE Access, vol. 8, pp. 62478-62494, 2020, doi: 10.1109/ACCESS.2020.2983601.

[20] L. Yan, S. Yin-He, Y. Qian, S. Zhi-Yu, W. Chun-Zi and L. Zi-Yun, "Method of Reaching Consensus on Probability of Food Safety Based on the Integration of Finite Credible Data on Block Chain," in IEEE Access, vol. 9, pp. 123764-123776, 2021, doi: 10.1109/ACCESS.2021.3108178.

[21] J. Indumathi et al., "Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unlimited Health Care Services (BC IoMT U6 HCS)," in IEEE Access, vol. 8, pp. 216856-216872, 2020, doi: 10.1109/ACCESS.2020.3040240.

[22] H. Zhi, H. Ge and Y. Wang, "Cooperative Communication Method Based on Block Chain for a Large Number of Distributed Terminals," in IEEE Access, vol. 10, pp. 11679-11695, 2022, doi: 10.1109/ACCESS.2022.3145444.

[23] X. Fu, H. Wang and Z. Wang, "Research on Block-Chain-Based Intelligent Transaction and Collaborative Scheduling Strategies for Large Grid," in IEEE Access, vol. 8, pp. 151866-151877, 2020, doi: 10.1109/ACCESS.2020.3017694.

[24] L. Askari, F. Musumeci and M. Tornatore, "Reprovisioning for latency-aware dynamic service chaining in metro networks," in Journal of Optical Communications and Networking, vol. 12, no. 11, pp. 355-366, November 2020, doi: 10.1364/JOCN.400149.

[25] D. Samanta et al., "Cipher Block Chaining Support Vector Machine for Secured Decentralized Cloud Enabled Intelligent IoT Architecture," in IEEE Access, vol. 9, pp. 98013-98025, 2021, doi: 10.1109/ACCESS.2021.3095297.

[26] E. Ram and Y. Cassuto, "On the Decoding Performance of Spatially Coupled LDPC Codes With Sub-Block Access," in IEEE Transactions on

Information Theory, vol. 68, no. 6, pp. 3700-3718, June 2022, doi: 10.1109/TIT.2022.3152104.

[27] S. Khan, M. A. Irfan, A. Arif, A. Ali, Z. A. Memon and A. Khaliq, "Reversible-Enhanced Stego Block Chaining Image Steganography: A Highly Efficient Data Hiding Technique," in Canadian Journal of Electrical and Computer Engineering, vol. 43, no. 2, pp. 66-72, Spring 2020, doi: 10.1109/CJECE.2019.2938844.

[28] R. G.S. and M. Dakshayini, "Block-chain Implementation of Letter of Credit based Trading system in Supply Chain Domain," 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), 2020, pp. 1-5, doi: 10.23919/ICOMBI48604.2020.9203485.

[29] Veeraiah V., Kumar K. R., Lalitha K. P., Ahamad S., Bansal R. and Gupta A., (2022). Application of Biometric System to Enhance the Security in Virtual World. 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 719-723.doi: 10.1109/ICACITE53722.2022.9823850.

[30] Babu, S.Z.D. et al. (2022). Analysation of Big Data in Smart Healthcare. In: Gupta, M., Ghatak, S., Gupta, A., Mukherjee, A.L. (eds) Artificial Intelligence on Medical Data. Lecture Notes in Computational Vision and Biomechanics, vol 37. Springer, Singapore. https://doi.org/10.1007/978-981-19-0151-5_21

[31] Bansal R., Gupta A., Singh R. and Nassa V. K., (2021). Role and Impact of Digital Technologies in E-Learning amidst COVID-19 Pandemic. 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), pp. 194-202.doi: 10.1109/CCICT53244.2021.00046.

[32] Dushyant, K., Muskan, G., Gupta, A. and Pramanik, S. (2022). Utilizing Machine Learning and Deep Learning in Cyber security: An Innovative Approach", in Cyber security and Digital Forensics, M. M. Ghonge, S. Pramanik, R. Mangrulkar,D. N. Le, Eds, Wiley, https://doi.org/10.1002/9781119795667.ch12

[33] Gupta A., Singh R., Nassa V. K., Bansal R., Sharma P. and Koti K., (2021) Investigating Application and Challenges of Big Data Analytics with Clustering. 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), pp. 1-6.doi: 10.1109/ICAECA52838.2021.9675483.

[34] Kaushik, K., Garg, M., Annu, Gupta, A. and Pramanik, S. (2021). Application of Machine Learning and Deep Learning in Cyber security: An Innovative Approach, in Cybersecurity and Digital Forensics: Challenges and Future Trends, M. Ghonge, S. Pramanik, R. Mangrulkar and D. N. Le, Eds, Wiley, 2021.

[35] Pandey, B.K. et al. (2022). Effective and Secure Transmission of Health Information Using Advanced Morphological Component Analysis and Image Hiding. In: Gupta, M., Ghatak, S., Gupta, A., Mukherjee, A.L. (eds) Artificial Intelligence on Medical Data. Lecture Notes in Computational Vision and Biomechanics, vol 37. Springer, Singapore.https://doi.org/10.1007/978-981-19-0151-5_19

[36] Pathania, V. et al. (2022). A Database Application of Monitoring COVID-19 in India. In: Gupta, M., Ghatak, S., Gupta, A., Mukherjee, A.L. (eds) Artificial Intelligence on Medical Data. Lecture Notes in Computational Vision and Biomechanics, vol 37. Springer, Singapore. https://doi.org/10.1007/978-981-19-0151-5_23

[37] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Review on Comparative study of 4G, 5G and 6G Networks," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1830-1833, doi: 10.1109/IC3I56241.2022.10073385.

[38] V. Jain, S. M. Beram, V. Talukdar, T. Patil, D. Dhabliya and A. Gupta, "Accuracy Enhancement in Machine Learning During Blockchain Based Transaction Classification," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 536-540, doi: 10.1109/PDGC56933.2022.10053213.

[39] V. Talukdar, D. Dhabliya, B. Kumar, S. B. Talukdar, S. Ahamad and A. Gupta, "Suspicious Activity Detection and Classification in IoT Environment Using Machine Learning Approach," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 531-535, doi: 10.1109/PDGC56933.2022.10053312.

[40] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Scalable Platform to Collect, Store, Visualize and Analyze Big Data in Real- Time," 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India, 2023, pp. 1-6, doi: 10.1109/ICIPTM57143.2023.10118183.

[41] M. Dhingra, D. Dhabliya, M. K. Dubey, A. Gupta and D. H. Reddy, "A Review on Comparison of Machine Learning Algorithms for Text Classification," 2022 5th International Conference

on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1818-1823, doi: 10.1109/IC3I56241.2022.10072502.

[42] D. Mandal, A. Shukla, A. Ghosh, A. Gupta and D. Dhabliya, "Molecular Dynamics Simulation for Serial and Parallel Computation Using Leaf Frog Algorithm," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 552-557, doi: 10.1109/PDGC56933.2022.10053161.

[43] V. V. Chellam, S. Praveenkumar, S. B. Talukdar, V. Talukdar, S. K. Jain and A. Gupta, "Development of a Blockchain-based Platform to Simplify the Sharing of Patient Data," 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India, 2023, pp. 1-6, doi: 10.1109/ICIPTM57143.2023.10118194.

[44] Lalitha Kumari, P. et al. (2023). Methodology for Classifying Objects in High-Resolution Optical Images Using Deep Learning Techniques. In: Chakravarthy, V., Bhateja, V., Flores Fuentes, W., Anguera, J., Vasavi, K.P. (eds) Advances in Signal Processing, Embedded Systems and IoT . Lecture Notes in Electrical Engineering, vol 992. Springer, Singapore. https://doi.org/10.1007/978-981-19-8865-3_55

[45] Sindhwani, N. et al. (2023). Comparative Analysis of Optimization Algorithms for Antenna Selection in MIMO Systems. In: Chakravarthy, V., Bhateja, V., Flores Fuentes, W., Anguera, J., Vasavi, K.P. (eds) Advances in Signal Processing, Embedded Systems and IoT . Lecture Notes in Electrical Engineering, vol 992. Springer, Singapore. https://doi.org/10.1007/978-981-19-8865-3_54

[46] Patil, A. ., & Govindaraj, S. K. . (2023). ADL-BSDF: A Deep Learning Framework for Brain Stroke Detection from MRI Scans towards an Automated Clinical Decision Support System. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 11–23. https://doi.org/10.17762/ijritcc.v11i3.6195

[47] Sofia Martinez, Machine Learning-based Fraud Detection in Financial Transactions , Machine Learning Applications Conference Proceedings, Vol 1 2021.

[48] Jain, V., Beram, S. M., Talukdar, V., Patil, T., Dhabliya, D., & Gupta, A. (2022). Accuracy enhancement in machine learning during blockchain based transaction classification. Paper presented at the PDGC 2022 - 2022 7th International Conference on Parallel, Distributed and Grid Computing, 536-540. doi:10.1109/PDGC56933.2022.10053213 Retrieved from www.scopus.com