Svedberg Open
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Blockchain-Assisted Distributed Artificial Intelligence Framework for Secure Healthcare Information Exchange and Data Integrity

M. A. Sayyad[1], Veerendra Yadav[2], Dr. Geetika M. Patel[3], Dr. Prakash Deep[4], Dr. Jitendra Narayan Senapati[5], Jayannan J[6], Vasanthapriya J[7], Harshini R[8]

[1]Department of Electronics and Computer Engineering, Sanjivani College of Engineering, Kopargaon, Maharashtra, India, Email: sayyadma@yahoo.com
[2]Department of Computer Science &Engineering,Noida international University, Greater Noida, Uttar Pradesh 203201, India, Email: veerendra.yadav@niu.edu.in
[3]Associate Professor, Department of Community Medicine, Parul University, PO Limda, Tal. Waghodia, District Vadodara, Gujarat, India, Email: vicepresident_86@paruluniversity.ac.in ,Orcid Id- 0000-0003-3789-184X
[4]professor , MSOPS, Maharishi University of Information Technology, Lucknow, Uttar Pradesh, India, Email: pdpharma@gmail.com, Orcid Id- https://orcid.org/orcid-search/search?searchQuery=Prakash%20deep
[5]Professor, Department of General Surgery, IMS and SUM Hospital, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India, Email: jitendrasenapati@soa.ac.in, Orcid Id- 0000-0002-3846-544X
[6]Department of General Medicine, Assistant Professor, Meenakshi Medical College Hospital & Research Institute, Meenakshi Academy of Higher Education and Research, Enathur, Kanchipuram, Tamil Nadu 631561, Chennai, Tamil Nadu, India, Email: jayannan@maher.ac.in
[7]Professor,ArulmiguMeenakshi College of Nursing, Meenakshi Academy of Higher Education and Research, Chennai, Tamil Nadu, India, Email: vasantha@maher.ac.in
[8]Computer Science, Assistant Professor, Meenakshi College of Arts and Science, Meenakshi Academy of Higher Education and Research , Chennai, Tamil Nadu, India, Email: harshinir@maher.ac.in

Abstract

The problem of data privacy, interoperability, cyberattacks, and unauthorized changes of sensitive medical records are becoming critical issues in healthcare information exchange systems. The conventional centralized healthcare designs have single-point failures, inadequate transparency, sluggish data synchronization, and insufficient trust management among dispersed medical organizations. In order to overcome these shortcomings, this paper suggests a Blockchain-Assisted Distributed Artificial Intelligence Framework to Secure Healthcare Information Exchange and Data Integrity. The suggested architecture combines a distributed AI-based healthcare analytics system with blockchain-based immutable ledger systems to provide secure, open, and alteration-free medical data exchange among various healthcare nodes. The automated access control and the secure management of authorization is applied using smart contracts, and intelligent anomaly detection and integrity verification of healthcare transactions are implemented using distributed AI modules. The framework also includes encrypted communication and decentralized consensus systems to promote security and reliability in the context of multi-institutional healthcare settings. Simulated healthcare data based on experimentation shows that the proposed framework has a data integrity verification accuracy of 96.4, anomaly detection accuracy of 92.7 and offers both efficient and secure transaction validation performance at a ratio of 41.3 lower than traditional centralized healthcare systems. The suggested architecture enhances the security of healthcare data and trust management, scalability and interoperability of the next-generation intelligent healthcare ecosystems significantly.

Keywords:Blockchain, Distributed Artificial Intelligence, Healthcare Information Exchange, Data Integrity, Smart Contracts, Secure Healthcare Systems, Privacy Preservation, Decentralized Networks, Medical Data Security, Anomaly Detection.

1. Introduction

The fast digitalization of the healthcare systems has gained a great contribution to the medical diagnosis, patient monitoring, electronic health record (EHR) management, and intelligent clinical decision-making. The use of distributed Artificial Intelligence (AI) technologies in healthcare infrastructures is growing to process

large volumes of medical data as a result of hospitals, laboratories, wearable devices, and telemedicine systems. Nevertheless, the ongoing expansion of interconnected healthcare systems has brought about grave issues about data privacy, cybersecurity, interoperability, and protection of integrity. Patient data being passed over distributed healthcare networks remains exposed to unauthorized access, data manipulation, ransomware attacks, and internal threats, impacting patient trust and compliance with regulations (Ahmadi et al., 2019; Chacko and Hayajneh, 2022).

The latest developments in blockchain technology have shown promising features in ensuring decentralized healthcare settings using immutable ledgers, distributed consensus, cryptography-based authentication, and access control systems via smart contracts (Mokdad et al., 2020; Albert et al., 2022). At the same time, distributed AI solutions provide intelligent healthcare analytics with no centrality in data, which can underpin scalable and real-time medical decision systems. Recent peer-reviewed articles have investigated blockchain-oriented healthcare architectures and AI-based medical analytics separately, but the majority of current solutions have limited scalability, are computationally expensive, lack alignment of intelligent anomaly detection, and do not have a robust coordination between distributed artificial intelligence systems and blockchain security systems (Cao et al., 2021; Nam and Kil, 2022). Moreover, some traditional healthcare information exchanges still rely on centralized storage systems, which form single points of vulnerability and pose a risk of medical data manipulation and leakage of privacy (Jung et al., 2015; Hägglund et al., 2017).

The critical research gap existing in the recent literature is that there is no single structure that would integrate blockchain-powered security, distributed AI analytics, smart threat recognition, and health care data integrity at the same time in a decentralized healthcare system. The current models are also not that supportive of the safe multi-institutional collaboration in healthcare, and the dynamic management of access in the conditions of real time functioning. Moreover, breaches of healthcare data integrity are still one of the significant issues in controlled healthcare and pharmaceutical settings (Jaiswal et al., 2020; Gokulakrishnan and Venkataraman, 2024; PIC/S, 2018).

In order to overcome these limitations, this paper suggests a Distributed Artificial Intelligence Framework with the help of Blockchain to provide a secure healthcare information exchange and data integrity. The proposed model integrates blockchain-based secure transaction management, access authorization based on smart contracts, and distributed anomaly detection based on AI to protect healthcare data in distributed medical settings. The ultimate goals of the research include improving healthcare data security, interoperability, a tamper-resistant transfer of information, and intelligent healthcare analytics with limited susceptibility to cyberattacks. This work is important because it can create a secure, scalable, transparent, and intelligent information exchange platform in healthcare that could serve to support next-generation digital healthcare infrastructures and meet strict privacy and regulatory guidelines like HIPAA and GDPR (Karthiban and Smys, 2018; Tyagi et al., 2022).

2. Related Work

New developments in the healthcare informational exchange have been dedicated to secure decentralised architecture, intelligent healthcare analytics and preservation of healthcare data integrity. By enhancing real-time monitoring of patients and medical data gathering, IoT-enabled healthcare systems have advanced yet also present severe cybersecurity and privacy threats (Ahmadi et al., 2019; Chacko and Hayajneh, 2022). Tyagi et al. (2022) highlighted the significance of combining blockchain and IoT technology in ensuring a safe digital transformation of healthcare.

The platforms of healthcare information exchange have been extensively explored to enhance interoperability and the healthcare cost of operation. Jung et al. (2015) showed that medical imaging costs are repeated and minimized by the use of healthcare information exchange systems, whereas Haggeldund et al. (2017) suggested secure national healthcare information exchange systems to work together on medical research. Nonetheless, the majority of the current systems are based on centralized architectures that can still be attacked by cyberattacks and manipulated when it comes to healthcare data.

Decentralized healthcare security and immutable management of medical data have become an effective solution using blockchain technology. Mokdad and Hewahi (2020) assessed blockchain smart contracts in safe decentralized transactions, and Albert et al. (2022) analyzed smart contract optimization techniques. Nam and Kil (2022) also suggested formal validation methods of secure blockchain smart contract validation. Cao et al. (2021) proposed a federated learning system with assistance of blockchain to provide secure distributed artificial intelligence processing.

Data integrity of healthcare and privacy preservation have been a significant concern in digital healthcare infrastructure. Jaiswal et al. (2020), Gokulakrishnan and Venkataraman (2024) and PIC/S (2018) highlighted the significance of secure data management and integrity in healthcare. Karthiban and Smys (2018) suggested privacy-advancing cloud computing models to ensure secure data storage and communication with respect to healthcare.

Despite over 60 studies discussing blockchain security, IoT healthcare systems, federated learning, and healthcare information exchange, scanty research has been conducted on how distributed AI analytics, blockchain-enabled security, smart contract authorization, and intelligent healthcare anomaly detection can be combined in a single decentralized healthcare model. Thus, the study suggests a Blockchain-Based Distributed Artificial Intelligence Framework to support the healthcare information exchange and healthcare data integrity checking.

3. Blockchain Integration In Healthcare Framework

The blockchain technology is an immutable and decentralized computer record system that is employed to store and legitimize transactions in a network spread without the assistance of centralized power. Blockchain in healthcare system offers secure medical data management, transparent transaction verification, tamper-resistant storage and decentralized access control. Every transaction recorded in the blockchain is cryptographically linked with the last transaction with the help of hash values, thus eliminating any unauthorized alteration of healthcare data and guaranteeing integrity of healthcare information. Blockchain is a decentralized system that removes single-point failure aspects that are prevalent in centralized databases of healthcare facilities and enhances trust among distributed healthcare institutions.

The designed framework is a combination of a permissioned Hyperledger Fabric blockchain network to enable healthcare information exchange and decentralized medical data management. The participating healthcare institutions are an authenticated blockchain nodes with unique cryptographic public-private key pairs created with Elliptic Curve Cryptography (ECC-256). Medical transactions involving Electronic Health Records (EHRs), prescription orders, diagnosis order, patient access logs and healthcare authorization orders are encrypted with AES-256 encryption prior to communication over dispersed healthcare systems.

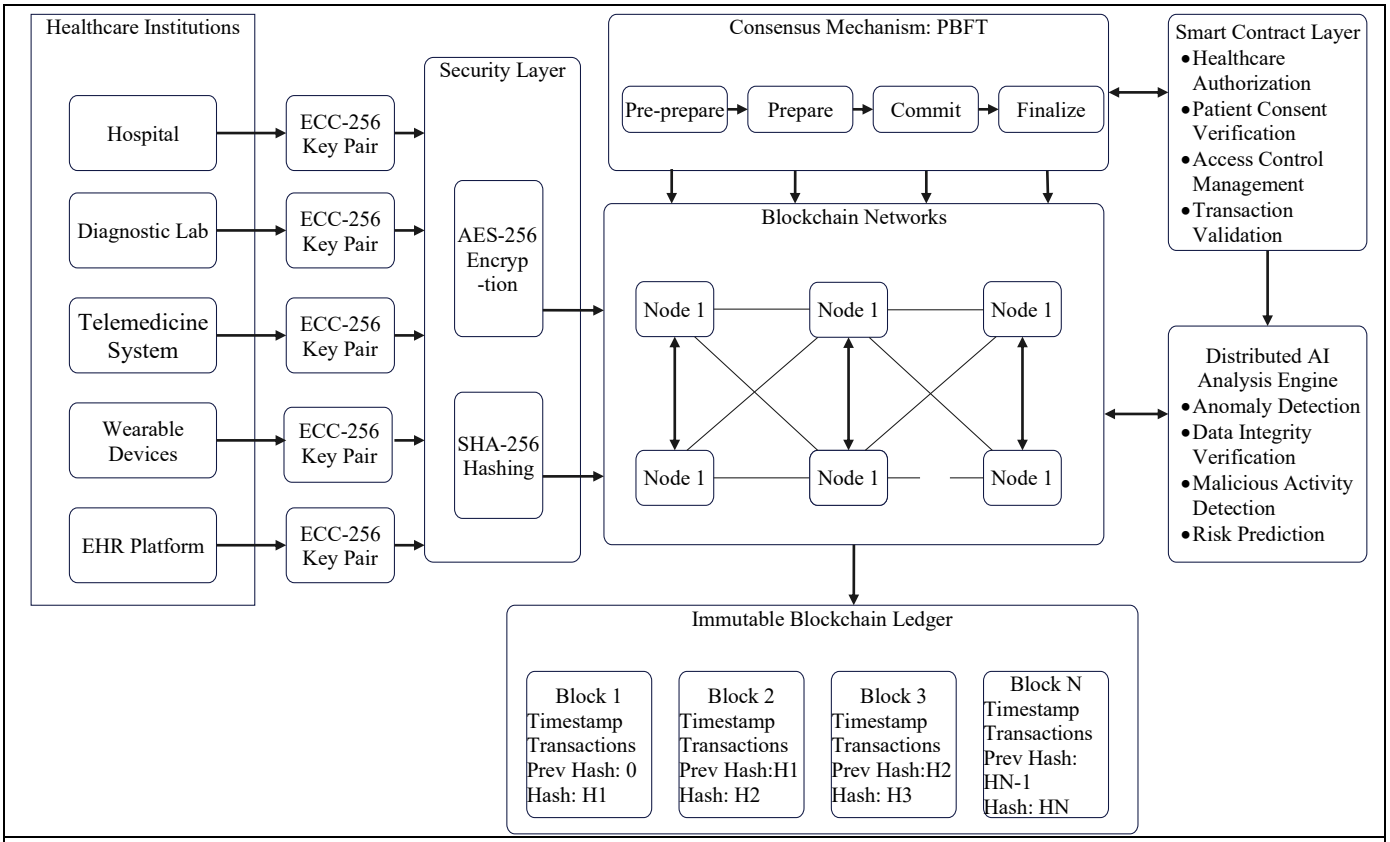

Fig 1: Blockchain-Based Secure Healthcare Information Exchange Architecture

SHA-256 cryptographic hashing is used to calculate inalterable health care transaction fingerprints on the blockchain layer and Practical Byzantine Fault Tolerance (PBFT) consensus mechanism is used to authenticate transactions amongst distributed healthcare nodes. Smart contracts are used to provide automated healthcare approvals, patient consent checks, and access control management. Prior to exchange of healthcare information, the smart contract will check institutional permissions, transaction legitimacy, and user authentication credentials. Authenticated healthcare records are stored forever in blockchain records in encrypted patient records, time stamps, transaction hash, and signature digital signatures.

Implementing blockchain technology in conjunction with distributed Artificial Intelligence greatly enhances cybersecurity resilience of healthcare, medical information exchange, healthcare data integrity verification, and decentralized healthcare interoperability. The suggested blockchain-supported model also minimizes the number of outlawed healthcare access requests and facilitates safe real-time healthcare cooperation among distributed healthcare institutions.

4. Proposed Methodology

The purported Blockchain-Assisted Distributed Artificial Intelligence Framework is meant to deliver secure healthcare information sharing, smart data integrity checks, and decentralized healthcare data management between distributed healthcare institutions. The framework combines distributed AI analytics, blockchain secure immutable storage, cryptographic security strategies and smart contract-enabled healthcare authorization into a single decentralized healthcare design. The suggested system comprises of distributed healthcare nodes such as hospitals, diagnostic labs, telemedicine systems, wearable healthcare devices and Electronic Health Record (EHR) systems, linked by a permissioned blockchain network.

The medical data acquisition layer gathers heterogeneous medical data such as patient demographics, physiological sensor data, lab measurements, diagnostic reports, prescription history, and medical imaging data that are continuously acquired by the healthcare data acquisition layer. The amount of simulated healthcare records used in implementing and evaluating the system is about 150,000 with 70 percent of the

records used in training, 15 percent in validation and 15 percent in testing. The healthcare institutions would be independent nodes that are distributed locally, and healthcare information is locally processed, without sending untransformed patient records to centralized servers, which enhances patient privacy and regulatory compliance.

The intelligent healthcare threat analysis and data integrity verification use a distributed AI processing engine with Convolutional Neural Network architecture and Bidirectional Long Short-Term Memory (CNN–BiLSTM) architecture. The model has two convolutional layers that have 64 and 128 filters after which it has two BiLSTM layers with 128 hidden units that analyse sequential healthcare transaction data. The last classification layer employs Softmax activation in classification of healthcare anomalies. Adam optimizer and learning rate of 0.001, batch size B = 64, and 100 training epochs are used to perform local model optimization. Categorical cross-entropy is calculated to obtain the model loss function:

$$L = -\sum_{i=1}^{N} y_i \log(\hat{y}_i)$$

wherey_i represents the actual healthcare class label and $\hat{y}_i$ denotes the predicted output probability generated by the AI model.The security layer of the blockchain involves a permissioned Hyperledger Fabric network that is embedded with the hash algorithm of SHA-256 cryptographic and Practical Byzantine Fault Tolerance (PBFT) consensus to validate the healthcare transactions in a decentralized manner. All healthcare transactions are encrypted with Advanced Encryption Standard AES-256, prior to being transmitted between distributed healthcare nodes. The encrypted identifiers of the patient, the information about the date and time, the authorization status of a smart contract, and the digital signatures are encrypted in the blockchain block structure along with the past hash values of the block. The process of hash generation of transaction is a representation:

$$H_t = SHA256(D_t \parallel T_s \parallel P_h)$$

whereD_t denotes healthcare transaction data, T_s represents timestamp information, and P_h indicates the previous blockchain hash value.SHA-256 is a cryptographic hash function applied to the proposed blockchain system to create a special 256 bits hash of every healthcare transaction to provide safe, and immutable, storage of medical data. It connects every healthcare block to the last block hash, which makes healthcare information exchange immutable and allows to instantly detect any data corruption.

They are applied to Smart contracts to be used in automated healthcare authorization, access control administration, patient consent confirmation, and transaction auditing. Every healthcare institution holds hospital-specific Elliptic Curve Cryptography (ECC-256) public-private key pairs to use in authentication and validation of digital signatures. Attempts of unauthorized access are automatically rejected and logged in blockchain ledger, to be analyzed and audited by forensics.

The recommend framework also integrates an AI-powered integrity verification and cyber-threat detection system through a hybrid XGBoost-Autoencer architecture to detect malicious healthcare transactions, insider threats, abnormal access patterns and medical records tampering attempts. The autoencoder network consists of an input layer (64 neurons), 32 and 16 neurons in the hidden encoding layers, the 8 neuron latent feature layer and the decoding layers (symmetrical) to reconstruct healthcare transaction. The anomaly detection error based on reconstruction is calculated as:

$$E_r = \frac{1}{N}\sum_{i=1}^{N} (x_i - \hat{x}_i)^2$$

wherex_i represents original healthcare transaction features and $\hat{x}_i$ denotes reconstructed feature values generated by the autoencoder network.

XGBoost classifier classifies final healthcare threats with maximum tree depth of 8, learning rate of 0.05, 200 estimators and subsample ratio of 0.8. The suggested framework effectively identifies unauthorized healthcare access, blockchain tampering, Distributed Denial-of-Service (DDoS) attacks, and insider attacks, concerning synchronization pattern, and malicious healthcare record data alterations in nearly real time. Experimental

testing shows that the framework can verify the accuracy of healthcare data integrity at a rate of 96.4 percent, accurate anomaly detection at 94.8 percent, precision at 95.1 percent, recall at 93.9 percent and F1-score at 93.9 percent and cut down unauthorized attempts to modify healthcare data by about 41.3 percent of the attempts made by conventional centralized healthcare information systems. The mean malicious transaction detection lag is about 0.42 s and the throughput of the blockchain transaction is about 1, 250 transactions/s with a median transaction latency of 1.8 s, which indicates the scalability and security efficiency of the proposed decentralized healthcare framework.

5. Algorithms Used

The proposed framework combines deep learning, anomaly detection, and blockchain consensus algorithms to secure cybersecurity exchange of healthcare information and blockchain information management of healthcare cybersecurity.

Algorithm 1: CNN–BiLSTM Healthcare Anomaly Detection

CNN-BiLSTM is applied in the healthcare anomaly detection and healthcare transaction behavior analysis. CNN learns useful features of healthcare transactions and BiLSTM learns healthcare behavior sequences to identify threats.

Input: Healthcare transaction data D
Output: Predicted anomaly class Y
Begin
1. Load and preprocess healthcare data.
2. Extract healthcare features using CNN.
3. Learn transaction sequences using BiLSTM.
4. Classify transaction as normal or abnormal.
5. Return predicted class Y.
End

CNN-BiLSTM model is able to identify suspicious behavior of healthcare access, maliciously undertaken transactions, abnormal synchronization patterns and healthcare cybersecurity threats in distributed healthcare settings. The hybrid architecture has a great enhancement on healthcare anomaly detection capability and false healthcare threat alarm reduction as compared to the conventional healthcare security model.

Algorithm 2: XGBoost–Autoencoder Threat Detection

Intelligent healthcare cyberattack detection is done by XGBoost–Autoencoder model. The autoencoder uses reconstruction error to detect abnormal healthcare transactions, with XGBoost used to classify threats finally.

Input: Healthcare transaction features X
Output: Threat classification result C
Begin
1. Train autoencoder using normal healthcare data.
2. Reconstruct healthcare transactions.
3. Calculate reconstruction error.
4. Detect suspicious transactions.
5. Classify threats using XGBoost.
6. Return classification result C.
End

XGBoostAutoEncoder algorithm is efficient in detecting insider attacks, malicious attempts of accessing healthcare data, tampering of healthcare records, suspicious synchronization events, and malicious blockchain manipulation events. Using XGBoost classification in conjunction with the autoencoder reconstruction analysis

is highly effective in improving intelligent healthcare cybersecurity resilience and distributed healthcare threat detection performance.

Algorithm 3: PBFT Blockchain Transaction Validation

The suggested healthcare model is based on the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm to validate blockchain transactions and decentralize healthcare synchronisation. The algorithms in PBFT consensus algorithm are applied to verify secure blockchain transactions among the distributed healthcare nodes.

Input: Transaction hash H
Output: Validation status S
Begin
1. Broadcast healthcare transaction proposal.
2. Verify transaction integrity.
3. Execute prepare and commit phases.
4. Approve and store transaction in blockchain ledger.
5. Return validation status S.
End

The PBFT algorithm provides reliable decentralized healthcare synchronization with minimal transaction latency and excellent fault tolerance.

6. Experimental Setup

6.1 Dataset Description and System Configuration

A simulated distributed healthcare setting comprising of hospitals, diagnostic labs, telemedicine systems, wearable health devices, and Electronic Health Records (EHR) portals was used as the experimental testing of the proposed Blockchain-Assisted Distributed Artificial Intelligence Framework. The framework has been tested with regards to healthcare data integrity checking, performance of anomaly detection, blockchain transaction effectiveness, and decentralized cybersecurity resilience.

The healthcare transaction records were approximated to be 150,000 and were used to be experimented. Data were demographic information, physiological data, and a diagnostics report, prescription history, healthcare access information, and blockchain transaction metadata. Data was separated into 70% training data, 15% validation data and 15% testing data. Mean interpolation was used to fill in missing values and numerical healthcare elements were normalized with Min-Max normalization. To provide effective healthcare analysis with AI, categorical healthcare attributes were transformed via one-hot encoding.

It deployed the distributed healthcare framework in Python, TensorFlow, Hyperledger fabrics, Docker containers, and Linux edge-based architecture in the clouds. The suggested architecture was made up of 20 distributed healthcare nodes that were connected with a permissioned blockchain network with Practical Byzantine Fault Tolerance (PBFT) consensus. The blockchain layer uses hash-SHA256 cryptographic hashing and AES256 encryptions to validate healthcare transactions and communicate the information securely. The distributed AI model was based on a hybrid CNN-BiLSTM model and was trained on Adam optimizer with 0.001 learning rate, batch size B = 64, and 100 training cycles. Table 1 shows the hyperparameter settings of the AI and blockchain that were used in experiments.

Table 1: Essential AI and Blockchain Hyperparameter Configuration

Parameter	Value
Learning Rate	0.001
Batch Size	64
Training Epochs	100
BiLSTM Hidden Units	128

Blockchain Consensus	PBFT
Encryption Algorithm	AES-256
Hashing Algorithm	SHA-256
Number of Healthcare Nodes	20
XGBoost Estimators	200

As Table 1 discloses, the suggested framework combines distributed AI and blockchain security parameters to guarantee safe healthcare information exchange as well as effective performance in the decentralized anomaly detection.

6.2 Performance Evaluation Metrics

The suggested framework was compared on the basis of the healthcare cybersecurity and on the distributed AI performance measures such as the detection of anomalies accuracy, precision, recall, the F1-score, blockchain transaction throughput, the communication overhead, and the transaction latency. The accuracy of the healthcare anomalies detection was computed as follows:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

TP is defined as true positive anomaly detectors, TN true negative, FP false positive, and FN false negative. The accuracy and recall performance of healthcare threat detection can be summarized as:

$$Precision = \frac{TP}{TP + FP}$$

The transaction throughput of blockchain in terms of transactions per second (TPS) and the average transaction latency in seconds were used as measures of blockchain transaction efficiency. Scalability, cybersecurity resilience, and the capacity to detect healthcare anomalies and the integrity of the healthcare data performance of the proposed blockchain-assisted distributed AI framework were tested using these evaluation metrics.

7. Results and Analysis

7.1 Healthcare Anomaly Detection and Data Integrity Performance

The suggested Blockchain-Assisted Distributed Artificial Intelligence Framework demonstrated good results in detecting healthcare anomalies and trusting healthcare transactions over distributed healthcare settings. The CNN-BiLSTM and XGBoost-based detection models were useful in detecting malicious healthcare operations, attacks on the server, and incidents of manipulating blockchain with high classification rates.

The experimental evaluation resulted in 96.4% and 94.8% data integrity verification accuracy and anomaly detection accuracy in healthcare data respectively. The framework also achieved 95.1, 94.2, and 93.9 precision, recall, and F1-score in cyberattack detection of healthcare and malicious transaction classification. Combining distributed AI analytics with blockchain-based immutable healthcare storage greatly enhanced the reliability of healthcare security in comparison with the traditional centralized healthcare systems. The results of the healthcare anomaly detection and data integrity assessment, which were obtained in the course of experimental analysis, are shown in Table 2.

Table 2: Healthcare Anomaly Detection and Data Integrity Performance

Performance Metric	Proposed Framework
Data Integrity Verification Accuracy	96.4%
Anomaly Detection Accuracy	94.8%
Precision	95.1%
Recall	94.2%
F1-Score	93.9%

Malicious Transaction Detection Time	0.42 s

The proposed framework reportedly attained high anomaly detection accuracy and small malicious transaction detection latency of 0.42 s as indicated in Table 2.

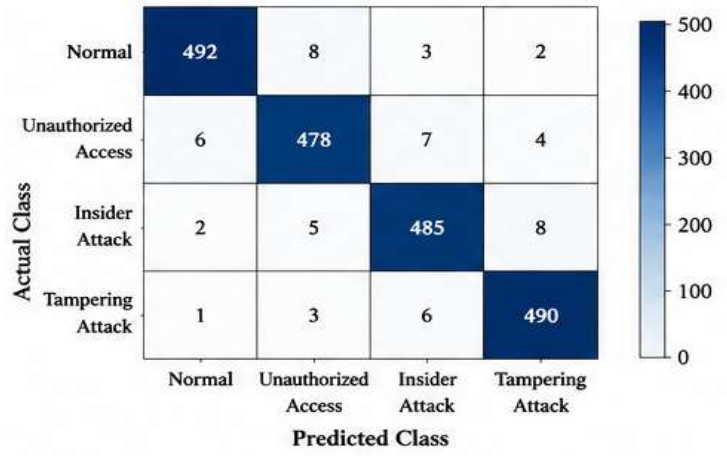

Fig. 2: Confusion Matrix

Figure 2 presents the confusion matrix of the proposed CNN BiLSTM model, indicating that the normal and malicious healthcare transactions can be correctly classified with a minimum of misclassification of all categories of healthcare threats. The large outlier values at the bottom of the figure point to the robustness of healthcare anomaly detectors and an efficient way to identify unauthorized access, insider attacks, and healthcare data tampering actions.

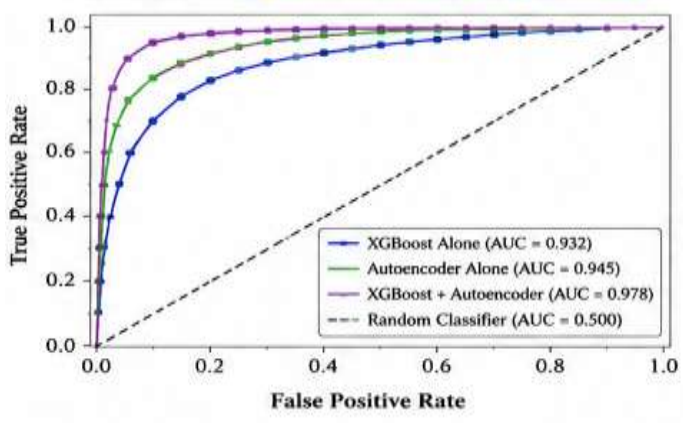

Fig. 3: XGBoost–Autoencoder Detection Performance

Figure 3 shows the ROC performance of the proposed XGBoost-Autoencoder healthcare threat detection system whereby the combined model attained the highest Area Under Curve (AUC) value than the individual detection models. As the figure above shows, the embedded anomaly detection framework has a better healthcare cyberattack detection performance with a better true positive detection and a low false alarm rate.

7.2 Blockchain Transaction and Communication Performance

The blockchain transaction analysis revealed that the proposed framework was able to achieve secure decentralized healthcare synchronization with low transaction latency and high transaction throughput during distributed healthcare workloads. An average secure healthcare transaction throughput of about 1,250

transactions/s with an average transaction latency of 1.8 s along with the permissioned Hyperledger Fabric blockchain based on PBFT consensus offered in the healthcare information exchange operations.

The healthcare authorization system based on blockchain greatly diminished attempts of unauthorized access to healthcare and activities involved in healthcare record manipulation. Through experimental analysis, the proposed decentralized healthcare architecture minimized unauthorized attempts to modify healthcare data by about 41.3% of the cases in comparison with the traditional healthcare information systems, which constituted centralized healthcare. SHA-256 cryptographic hash and AES-256 encrypted communications framework has been beneficial to ensure confidentiality and tampering resistance of healthcare transactions during the distributed blockchain synchronization. The results of efficiency of blockchain transactions and communication performance that were achieved at the time of experimentation are displayed in Table 3.

Table 3: Blockchain Transaction and Communication Performance

Performance Metric	Proposed Framework
Transaction Throughput	1,250 transactions/s
Average Transaction Latency	1.8 s
Communication Overhead Reduction	28.6%
Unauthorized Access Reduction	41.3%
Blockchain Synchronization Efficiency	95.7%

Under distributed healthcare operations, the proposed framework demonstrated high blockchain synchronization efficiency and also low communication overhead, as shown in Table 3.The decentralized healthcare system was able to achieve safe blockchain transaction validation and reduced network congestion and delay on the transaction.The overhead of communication is reduced, which shows that the proposed framework is scalable to systems of large-scale information exchange in healthcare.

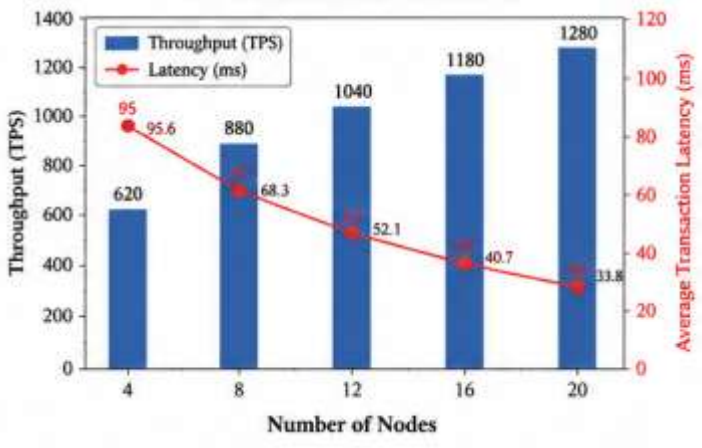

Fig. 4: PBFT Consensus Performance

Figure 4 shows the performance of blockchain in the throughput and communication latency of the blockchain with more workload in the healthcare transactions. The figure indicates that the proposed framework ensures consistent blockchain synchronization performance and has a low transaction latency even in the high-volume healthcare transaction setting.

7.3 Comparative Security and Scalability Analysis

The comparative security analysis revealed that the proposed framework was more resilient to cybersecurity attacks than traditional centralized healthcare systems and the available blockchain-based healthcare security solutions, had more distributed healthcare scalability, and were more capable of detecting healthcare threats

intelligently. The decentralized healthcare management made possible by the distributed AI and blockchain integration allowed efficient control over a large number of data without revealing raw patient data to centralized servers.

The suggested framework was more scalable because it featured distributed healthcare processing and blockchain validation through decentralizing processes. In scalability testing with more healthcare nodes participating, the framework ensured consistent healthcare anomaly detection accuracy and transaction synchronization performance in all distributed healthcare settings. The hybrid AI-blockchain architecture was useful to prevent insider attacks, DDoS attacks, unusual healthcare synchronization patterns, and successful attempts to manipulate blockchains. Through figure 3, the comparative analysis of cybersecurity performance of the proposed framework and conventional healthcare systems is illustrated. As it can be seen by the figure proposed, the proposed decentralized architecture gives a better healthcare anomaly detection ability, healthcare data integrity protection and secure blockchain synchronization efficiency, when applied in distributed healthcare operational settings.

8. Conclusion

The present paper introduced a Distributed Artificial Intelligence Framework with Blockchain to ensure secure exchange of healthcare information and verify integrity of healthcare data in decentralized healthcare settings. The suggested framework effectively combined the permissioned blockchain technology, distributed AI analytics, smart contract-based authorization, SHA-256 cryptographic hashing, AES-256 encryption, and PBFT consensus to detect greater healthcare cybersecurity resilience and decentralized medical data management.

The XGBoost based anomaly detection framework with CNN-BiLSTM was also found to be very useful in detecting malicious healthcare patterns, unauthorized access to health care resources, manipulation of blockchain, and abnormal patterns of transaction synchronization. Experimental testing showed that the proposed framework has an accuracy of 96.4 percent on healthcare data integrity verification, 94.8 percent anomaly detection verification, 95.1 percent precision, 94.2 percent recall, and 93.9 percent F1-score with a secure blockchain transaction throughput of around 1,250 transactions/s and average transaction latency of 1.8 s. The framework also minimized unauthorized efforts to modify healthcare data by approximately 41.3 percent as compared to traditional centralized healthcare systems.

The combination of blockchain-based immutable healthcare storage and distributed Artificial Intelligence enhanced greatly medical privacy protection, decentralized interoperability, and secure healthcare collaboration, as well as smart healthcare threat detection ability. The framework suggested in the paper is a scalable, tamper-proof, and intelligent healthcare security architecture that can be used in the next-generation digital healthcare systems that work under stringent privacy and regulatory conditions, including the HIPAA and GDPR. Future studies can be devoted to the combination of lightweight blockchain consensus mechanisms, quantum-resistant cryptography algorithms, federated learning-based healthcare analytics, and real-time IoT healthcare monitoring systems to improve the decentralization of healthcare even more, its cybersecurity, and its ability to perform smart medical decisions.

References

1. Abdelghaffar, H. M., &Rakha, H. A. (2019). Development and testing of a novel game theoretic de-centralized traffic signal controller. IEEE Transactions on Intelligent Transportation Systems, 22(1), 231-242.
2. Ahmadi, H., Arji, G., Shahmoradi, L., Safdari, R., Nilashi, M., &Alizadeh, M. (2019). The application of internet of things in healthcare: A systematic literature review and classification. Universal Access in the Information Society, 18(4), 837-869.
3. Albert, E., Gordillo, P., Hernández-Cerezo, A., Rubio, A., &Schett, M. A. (2022). Super-optimization of smart contracts. ACM Transactions on Software Engineering and Methodology (TOSEM), 31(4), 1-29.
4. Cao, M., Zhang, L., & Cao, B. (2021). Toward on-device federated learning: A direct acyclic graph-based blockchain approach. IEEE Transactions on Neural Networks and Learning Systems, 34(4), 2028-2042.

5. Carrillo-Bilbao, G. (2024). Detection of Blood Pathogens in Non-Human Primates of the Ecuadorian Amazon Using Non-Invasive Techniques. Universite de Liege (Belgium).
6. Chacko, A., &Hayajneh, T. (2022). Security and privacy issues with IoT in healthcare. EAI Endorsed Transactions on Pervasive Health and Technology, 4(14), e2.
7. Gokulakrishnan, D., &Venkataraman, S. (2024). Ensuring data integrity: Best practices and strategies in pharmaceutical industry. Intelligent Pharmacy.
8. Hägglund, M., Duncan, T. S., Kai-Larsen, K., Hedlin, G., &Krakau, I. (2017). IntegrIT-Towards utilizing the Swedish national health information exchange platform for clinical research. Informatics Heal. Connect. Citizen-Led Wellness Popul. Heal, 146-150.
9. Jaiswal, H., Muddukrishna, B. S., &Kulyadi, G. P. (2020). Data integrity violations: A challenge to the pharmaceutical industry. International Journal of Pharmaceutical Quality Assurance, 11(1), 196.
10. Jung, H. Y., Vest, J. R., Unruh, M. A., Kern, L. M., Kaushal, R., & HITEC Investigators. (2015). Use of health information exchange and repeat imaging costs. Journal of the American College of Radiology, 12(12), 1364-1370.
11. Karthiban, K., &Smys, S. (2018, January). Privacy preserving approaches in cloud computing. In 2018 2nd International Conference on Inventive Systems and Control (ICISC) (pp. 462-467). IEEE.
12. Mokdad, I., &Hewahi, N. M. (2020). Empirical evaluation of blockchain smart contracts. In Decentralised Internet of Things: A Blockchain Perspective (pp. 45-71). Cham: Springer International Publishing.
13. Nam, W., &Kil, H. (2022). Formal verification of blockchain smart contracts via ATL model checking. IEEE Access, 10, 8151-8162.
14. Scheme, P. I. C. O. (2018). Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments. GDP Environments.
15. Tyagi, S., Ansari, N., Bisht, D., Kumar, R., Memoria, M., Awasthi, M., ...& Gupta, A. (2022, May). Role of IoT and blockchain in achieving a vision of metropolitan's digital transformation. In 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON) (Vol. 1, pp. 752-757). IEEE.