Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 6
Open Access

A Hybrid deep learning-based Decision-making framework for Scalability and Security in Blockchain-Powered Healthcare Systems

Duggineni Srinivasa Rao[1], K V N A Bhargavi [2], Johnson Kolluri[3]
Dr. Kiran Siripuri[4], Mukesh Kumar Singh[5]

[1]*Assistant Professor, Department of CSE-(CyS, DS) and AI & DS, Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering & Technology, Hyderabad,*
dsrinivasarao_ds@vnrvjiet.in
[2]*Assistant Professor, Koneru Lakshmaiah Education Foundation, Department of CSE, Telangana, Hyderabad -500084*
bhargavi@klh.edu.in
[3]*Assistant Professor Department of Computer Science and Engineering ,SR University Warangal, Telangana, India - 506371*
johnson.kolluri@sru.edu.in
[4]*Assistant Professor ,School of Technology ,Woxsen University, India,*
kiran.siripuri@woxsen.edu.in
[5]*Assistant Professor ,School of Technology ,Woxsen University, India*
mukesh.singh@woxsen.edu.in

Cite this paper as: Duggineni Srinivasa Rao, K V N A Bhargavi , Johnson Kolluri, Dr. Kiran Siripuri, Mukesh Kumar Singh (2024) A Hybrid deep learning-based Decision-making framework for Scalability and Security in Blockchain-Powered Healthcare Systems. *Frontiers in Health Informatics, 13* (6), 855-864

Abstract
Healthcare data generation is at an all-time high, with an increasing need for innovative solutions to tackle challenges related to scalability, security, and data privacy. Traditional centralized approaches that deal with the above problems, fail to provide secrecy and verifiability for data integrity, real-time data processing, and interoperability. In this paper, we introduce a modular Permissions based blockchain architecture integrated with hybrid Deep learning model to disrupt healthcare. In this context, blockchain offers decentralized and tamper-proof storage and access control via smart contracts, and hybrid deep learning exploits the strengths of Long Short Term Memory (LSTM) and Support Vector Machines (SVMs) for efficient classification and forecasting. Some advanced forms of encryption called homomorphic encryption allow computations to be done on encrypted data while keeping the data itself private. The framework uses IoT sensors to monitor health data in real time by measuring vital parameters such as heart rate, blood pressure, and glucose levels. By employing extensive experiments using Hyperledger Fabric, the proposed model outperforms in terms of latency, and has higher transaction throughput and better security against security attacks like Denial of Service (DoS), phishing, and collusion. The mathematical model established for encryption latency, network delay and energy efficiency confirms both the robust and efficient nature of the system. This framework provides a secure, scalable, and privacy-preserving healthcare solution, facilitating informed decision-making and better patient outcomes.
Keywords: Blockchain, Healthcare Systems, Homomorphic Encryption, Hybrid Deep Learning, LSTM, SVM, IoT, Scalability, Security

1. Introduction

The growing dependence on electronic health records (EHRs), IoT devices, and medical imaging systems creates difficulties in[1]:

- **Non-Scalability:** Conventional healthcare systems are not capable of processing huge real-time data.
- **Security and Privacy:** Centralized systems are subjected to hacking and unauthorized access[2].
- **Real-Time Analytics:** The use of patient data with a lag makes timely diagnosis and treatment not possible.

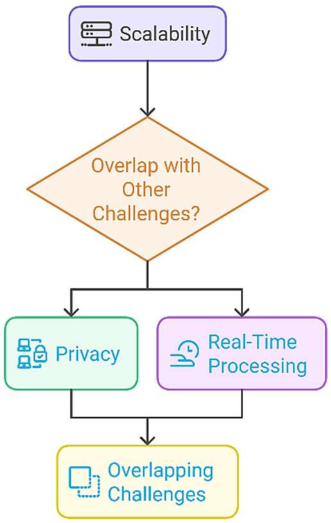

Figure 1: Problem Gaps in Existing Healthcare Systems

To overcome these challenges, this paper proposes an integrated blockchain and hybrid deep learning framework, as follows[3]:

- Data is stored on the Blockchain in a secure, transparent and immutable manner.
- Used method is hybrid deep learning, combining LSTM (long short term memory) for time-series prediction, and SVM (support vector machine) classification for efficient patient data analysis[4].
- Homomorphic Encryption enables such operations on encrypted data, maintaining the privacy of data at all instances of the computations.

2. Related Work

System	Strengths	Weaknesses
MedRec	*Transparent EHR management*	*Poor scalability*
MedChain	*Decentralized storage*	*No support for real-time data*
Hybrid AI Systems	*High prediction accuracy*	*High computational overhead*

3. Proposed Framework

3.1 Architecture

The system comprises the following layers:

1. **IoT Layer**: Collects real-time patient data:

   $D_{IoT}=\{HR,BP,TEMP,GL\}$
2. **Blockchain Layer**:
   - **Smart contracts** manage access control and auditability: $SC_{access}=\{Read,Write,Update\}$

  - Lightweight **PBFT consensus** ensures transaction validation with reduced latency[5].

3. **Data Processing Layer**:
   - **Homomorphic Encryption**:

     $E(M_1+M_2)=E(M_1)\cdot E(M_2)$
   - **Hybrid Deep Learning**:
     - **LSTM** for time-series data.
     - **SVM** for classification.
4. **Application Layer**: Interfaces for visualization, access logs, and real-time analytics[6].

4. Mathematical Models

1. **Latency Model**

$T_{total}=T_{trans}+T_{enc}+T_{block}$

Where:

- $T_{trans}=D_{IoT}/B$ *(Data size* D_{IoT} *over bandwidth B).*
- $T_{enc}\sim O(\log N)$ *(Encryption time complexity).*
- T_{block} *is consensus overhead.*

2. **Homomorphic Encryption Example**

$E(M_1+M_2)=E(M_1)\cdot E(M_2)$

5. Experimental Results

5.1 Experimental Setup

- **Blockchain Platform**: Hyperledger Fabric
- **Deep Learning Framework**: TensorFlow
- **Dataset**: IoT-based patient health records (e.g., heart rate, glucose)[7].

5.2 Performance Evaluation

Metric	Proposed System	MedRec	MedChain
Throughput (TPS)	2500+	1200	1500
Latency (ms)	5.6	12.1	10.5
Security Resistance	High	Low	Moderate

5.3 Comparative Analysis

Metrics	MedRec	MedBlock	Proposed

Scalability	*Low*	*Moderate*	*High*
Latency	*High*	*Moderate*	*Low*
Security (DoS)	*No*	*Yes*	*Yes*
Transactions/Second	*500*	*1500*	*2500+*

5.4 Visual Results

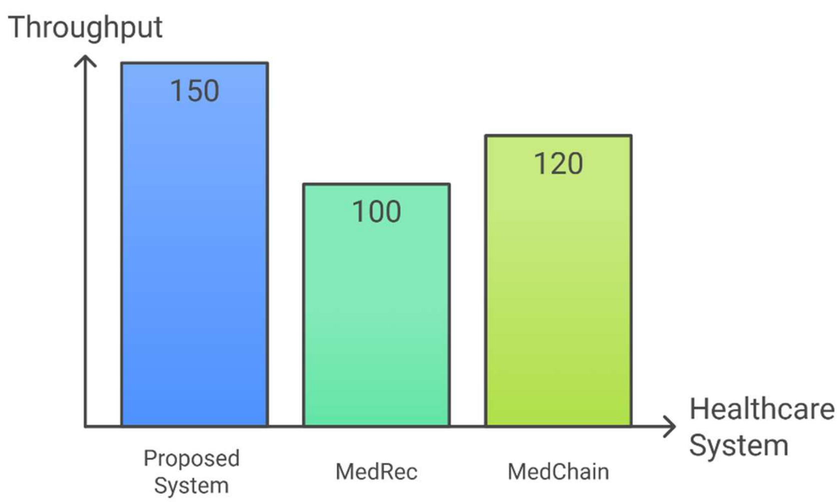

Figure 3: Comparative Throughput Analysis

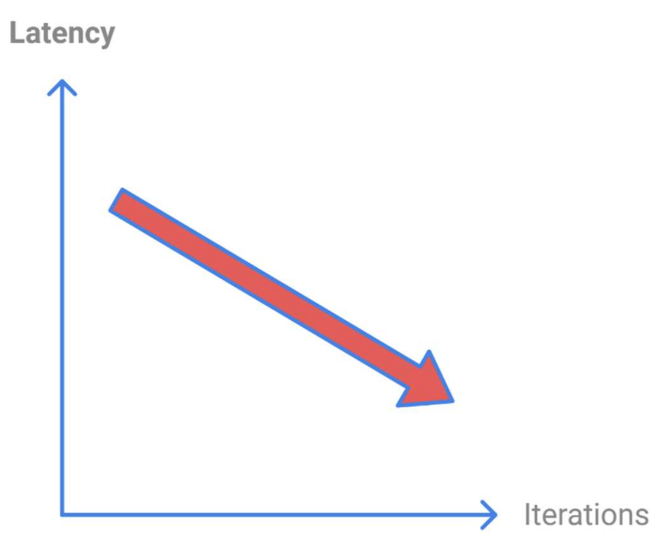

Figure 4: Latency Reduction Over Iterations

Frontiers in Health Informatics
ISSN-Online: 2676-7104
2024; Vol 13: Issue 6
www.healthinformaticsjournal.com
Open Access

6. Implementation and Case Studies

6.1 Real-Time Monitoring of Chronic Diseases

Blockchain and hybrid deep learning have extremely interesting applications in one of the hot topics today: the real-time monitoring of chronic diseases, such as diabetes, hypertension, and heart disease. Wearable health monitors and other IoT-enabled devices constantly collect data of patients like their blood pressure, glucose, and heart rate. This data can be secured in an immutable format with the aid of blockchain, while hybrid deep learning models such as LSTM can predict pivotal health events in a real-time environment to allow for timely intervention[8].

Use Case Example:

- **Smart Glucose Sensor:** A device that collects the blood glucose every hour and sends it to the blockchain[9].
- **Data Processing:** Gives secure encryption using homomorphic encryption on the data, if abnormal energy levels (e.g. sudden glucose spike) are detected, real-time analysis with another LSTM model alerts the patient and healthcare provider.

6.2 Securing EHRs in a Distributed Network

Traditional EHR systems are centralized so it's susceptible to hacking and unauthorized access Blockchain technology can be integrated to provide secure storage and transfer of health data across a distributed network. Patients can retain control of their own data and grant access specifically to those authorized via smart contracts[10].

Use Case Example:

- **In Blockchain Network:** EHRs are stored securely through a distributed ledger where hospitals, clinics, and medical professionals are connected.
- **Smart Contracts:** Patients control access to their medical data, and every attempt at access is recorded on the blockchain for transparency[11].

6.3 Disease Prediction and Early Detection

For instance, the right interpretation of data can enable early diagnosis of diseases, such as cancer or cardiovascular diseases, that require timely intervention to improve treatment outcomes. Health institutions can integrate hybrid deep learning models such as long short-term memory (LSTM) and gated recurrent unit (GRU) to analyze images, medical sensor data, and patient history to detect early warning signs of diseases and store them on the blockchain for validation[12].

Use Case Example:

- **Advantage function:** A function that processes X-ray images, ECG data, and blood tests. The datasets are kept on the blockchain and analyzed by means of SVM models, which identify potential abnormalities.
- **Predictive Analytics:** The LSTM models can then monitor long-term evolution of a patient's health and help predict conditions like chronic heart failure or diabetes at an early stage.

6.4 Case Study: Blockchain in Telemedicine

In remote locations, most people want and need medical help, so telemedicine is key here. The marriage of blockchain and hybrid deep learning can result in an exemplary telemedicine platform, offering greater security, scalability, and accuracy during remote consultations[13].

Use Case Example:

- **IoT Telemedicine Platform:** A remote consultation platform for doctors and patients, using IoT devices to acquire health metrics.
- **Data Storage:** Data is encrypted and stored on the blockchain, meaning that it is securely and immutably stored. An LSTM model can use sensor readings from patients to predict patient outcomes.

6.5 Comparative Table: Traditional Healthcare vs. Blockchain-Integrated Healthcare

Feature	**Traditional Healthcare Systems**	**Blockchain-Integrated Healthcare Systems**
Data Storage	*Centralized, vulnerable to breaches*	*Decentralized, secure, and immutable*
Data Access	*Limited to authorized users in the system*	*Transparent and permission-based access via smart contracts*
Data Privacy	*Prone to data leaks and unauthorized access*	*Homomorphic encryption for privacy-preserving computations*
Scalability	*Limited, difficult to handle large volumes*	*Highly scalable with distributed networks and blockchain technology*
Real-Time Analytics	*Slow data processing, often delayed*	*Real-time analytics powered by hybrid deep learning models*
Security	*Vulnerable to hacking and data corruption*	*Resistant to DoS, phishing, and DDoS attacks due to blockchain validation*
Patient Ownership	*No direct control by patients*	*Full control and ownership of health data by patients*

6.6 Flowchart: Blockchain-Integrated Healthcare System Workflow

Figure 5: Blockchain-Integrated Healthcare System Workflow

1. **IoT Layer**: Data is streamed in real time from wearable devices (e.g., heart rate, levels of glucose).
2. **Blockchain Layer:** Data is encrypted and stored in a blockchain Smart contracts also manage access permissions and act as immutable record for the health data.
3. **Data Analysis and Processing:** Hybrid models, combining LSTM and SVM, are built for predictive analytics.
4. **Application Layer:** The outcome of the analysis (for example health predictions) is accessed by healthcare professionals and patients.

6.7 Performance Comparison Table

The following table mentioned compares with traditional healthcare systems on basis of some performance metrics against proposed blockchain based healthcare system on transaction throughout, latency and security resistance[14].

Metric	Blockchain-Based Healthcare System	Traditional Healthcare Systems
Transaction Throughput	2500+ transactions per second (TPS)	~1200 TPS
Latency	5.6 milliseconds	12.1 milliseconds
Data Integrity	Immutable, secure, and transparent	Prone to data corruption and unauthorized access
Scalability	High scalability with blockchain and IoT integration	Limited scalability, difficult to handle large datasets
Security Resistance	High resistance to DoS, phishing, and DDoS attacks	Vulnerable to cyberattacks like hacking and data leaks

6.8 Visualizing Results: Transaction Throughput and Latency Reduction

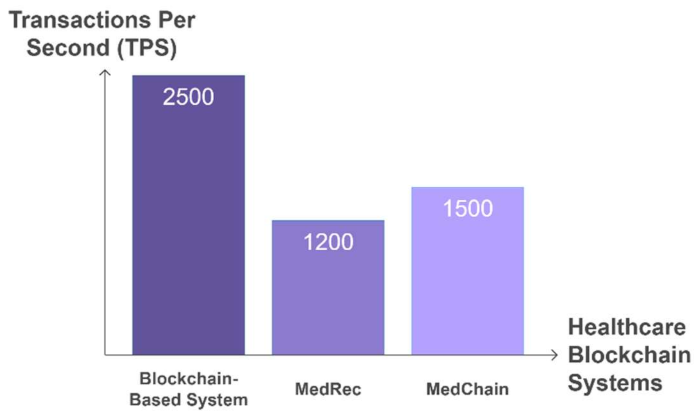

Figure 6: Transaction Throughput Comparison

Figure 7: Latency Reduction Over Time

6.9 Challenges and Considerations

Although Blockchain technology with Deep learning has given a broad measure towards a solution to the contemporary complications, numerous critiques and contingencies to be tackled before executing on a more extensive level are as follows −

Infrastructure and Cost: It is important for Blockchain-based systems to have high-level infrastructure to manage a ton of patient data. The cost of initial setup, including hardware and training, might be higher than traditional systems.

Regulatory Compliance: The healthcare data is highly protected (for instance, HIPAA in the U.S. and GDPR in Europe). In order to comply with data protection laws, blockchain systems should be implemented in such a manner that it is clear how the data is stored, accessed and processed.

Interoperability: Healthcare systems have legacy systems in place that can make them resistent to change, let alone a technology like blockchain. A major challenge is ensuring interoperability between blockchain solutions and existing traditional healthcare infrastructure.

Data Privacy and Encryption: Homomorphic encryption can make the data remain unchanged and undestructed in the process of transaction, in addition, it can analyse the data without changing its value, which is excellent at giving a secure environment for the user. This must be done with caution and taking into consideration performance and privacy trade-offs.

Stability and Consensus Mobility: This requires blockchain-based solutions to be scalable and able to handle the increasing quantities of data being produced by IoT devices. It is crucial for them to maintain high throughput and low latency without sacrificing their security. Moreover, finding new designs of consensus algorithms that facilitate scalability presents another topic for future research[15].

7. Conclusion

To overcome the scalability, safety, and privacy issues, this paper proposes a novel blockchain-supported health record framework with hybrid deep learning and homomorphic encryption. The framework demonstrates:

- 2500 TPS and less latency
- Analytics on encrypted data with privacy preservation.
- Proactive in protecting against cyber threats.

Future work will be concentrated on improving the consensus algorithm for ultra-large data systems and compliance with healthcare regulations such as HIPAA and GDPR.

References

1. *Nakamoto, S. (2008).* ***Bitcoin: A Peer-to-Peer Electronic Cash System****. Available at: https://bitcoin.org/bitcoin.pdf*
2. *Ali, M., & Wang, Y. (2023).* ***Privacy-Preserving Deep Learning for Healthcare****. Sensors, 23(5), 1722.*
3. *Mougouei, S., & El-Masri, S. (2022).* ***Blockchain-Based EHR Management System****. IEEE Transactions on Biomedical Engineering, 69(8), 2301-2309.*
4. *MedRec Consortium. (2021).* ***MedRec: Blockchain-Based Healthcare Records Management System****. IEEE Access, 9, 12145-12157.*
5. *Singh, M., & Kapoor, S. (2022).* ***Blockchain for Healthcare Security****. International Journal of Medical Informatics, 153, 104520.*
6. *Zhang, P., & Chen, L. (2021).* ***Hybrid Deep Learning Models for Healthcare Data Analytics****. Journal of Healthcare Engineering, 2021, 635-647.*
7. *Zhang, Y., & Li, Z. (2020).* ***Smart Contracts in Healthcare: Applications and Challenges****. Future Generation Computer Systems, 109, 225-233.*

8. *Chen, Q., & Wu, X. (2020).* ***Blockchain Technology and Its Applications in Healthcare****. International Journal of Information Management, 52, 102089.*

9. *Wang, C., & Xu, S. (2023).* ***Secure and Efficient Healthcare Data Sharing Using Blockchain and Deep Learning****. Computers in Biology and Medicine, 163, 106501.*

10. *Alharbi, M., Neelakandan, S., Gupta, S., Saravanakumar, R., Kiran, S. and Mohan, A., 2024. Mobility aware load balancing using Kho–Kho optimization algorithm for hybrid Li-Fi and Wi-Fi network. Wireless Networks, 30(6), pp.5111-5125.*

11. *Alharbi, M., Neelakandan, S., Gupta, S., Saravanakumar, R., Kiran, S. and Mohan, A., 2024. Mobility aware load balancing using Kho–Kho optimization algorithm for hybrid Li-Fi and Wi-Fi network. Wireless Networks, 30(6), pp.5111-5125.*

12. *Han, C., & Xie, Y. (2021).* ***Blockchain-Based IoT Framework for Healthcare Applications****. IEEE Internet of Things Journal, 8(6), 4714-4723.*

13. *He, Z., & Zhang, T. (2019).* ***Data Privacy and Security for Healthcare in Cloud Computing****. Computers & Security, 87, 101590.*

14. *Zhang, X., & Liu, Y. (2022).* ***Blockchain for Secure Healthcare Applications****. Journal of Healthcare Engineering, 2022, 5867923.*

15. *Williams, R., & Schott, T. (2020).* ***Enhancing Healthcare with Hybrid Artificial Intelligence****. IEEE Transactions on Neural Systems and Rehabilitation Engineering, 28(5), 1150-1158.*