Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 4-B, pp. 1323–1333
DOI : 10.47974/JIOS-1993

BHPEC : Design of an efficient model for blockchain-based healthcare privacy enhancement in clinical settings

Rubana A. Khan *
Bhavna Sharma †
Department of Computer Science and Engineering
JECRC University
Jaipur 303905
Rajasthan
India

Nita M. Thakare §
Department of Computer Technology
Priyadarshini College of Engineering Nagpur
Nagpur 440019
Maharashtra
India

Abstract

In the fast-changing health technology domain, the need for an improvement in privacy and efficiency in the clinical scenario has become very critical. Traditional blockchain models, revolutionary in themselves, have numerous limitations for healthcare applications in areas like nonoptimal energy efficiency, latency, compromised privacy levels, throughput limitations, inconsistent packet delivery, and jitter levels. This paper comes up with an innovative "Proof of Healthcare Privacy" consensus mechanism (PoHP) and a low complexity Coot Optimization model that enhances the scalability of blockchains. This proposed model has been tested empirically at different clinical settings, which shows very impressive results with an increase in energy, efficiency, while reducing the delay and enhancing privacy levels. The model also increases the throughput, the packet delivery ratio and reducing jitter when compared to the blockchain methods available. The proposed model significantly enhances privacy and operational efficiencies in blockchain applications for healthcare.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Blockchain technology, Healthcare privacy, Consensus mechanisms, Coot optimization, Clinical data management.*

* *E-mail:* **rubi.tarannum@gmail.com (Corresponding Author)**
† *E-mail:* **bhavna.sharma@jecrcu.edu.in**
§ *E-mail:* **nitathakre14@gmail.com**

1. Introduction

The invention of blockchain technology has come to herald a new arena of data management and security using a decentralized, ledger tamper-proof process system. It found its way into different sectors, and healthcare stands out as a critical area ripe for transformations. Another set of claims, which blockchain technology is supposed to secure against, posits that the current healthcare infrastructure is subjected to challenges entailing data breaches, ineffectiveness in critical data handling, and privacy, among others. Current blockchain implementations in the health care domain are primarily focused on patient data [1, 2, 3] security and its authentication. Although these are great accomplishments, it most often shadows performance indicators like energy efficiency, latency on the blockchain, and its scalability levels. These limitations hamper the practical applicability of blockchain in dynamic clinical environments where the volume of data and the need for real-time processing are constantly escalating for different scenarios. Having identified these challenges [4, 5, 6]. Various methods proposed highlighting the role of blockchain in diverse computing paradigms [7, 8, 9], optimization techniques in blockchain for healthcare [10, 11, 12, 13, 14], a cloud-IIoT-based HER[15, 16, 17] and federated learning and blockchain [18].

The present paper introduces a novel model adapted for fulfilling the needs of healthcare, viz. the Proof-of-Healthcare-Privacy (PoHP) consensus mechanism. The PoHP consensus mechanism is introduced to achieve the optimization of temporal and spatial privacy performance in the miner nodes.

Further enhancing the effectiveness of this model is the low-complexity Coot Optimization model, which is integrated for deployed blockchain for the sidechaining. This integration is very vital since it gives the increased scalability in the blockchain. The integration guarantees that blockchain supports the rising data needs of modern healthcare settings without the performance levels being compromised. It comes with higher energy efficiency, reduced latencies, an improved level of privacy, higher throughputs, and improved packet delivery ratios.

2. Design of the Proposed Security Model Process

This section is focused on discussing design of an efficient model meant for blockchain-based privacy enhancement in clinical settings. According to figure 1, proof of Healthcare Privacy-based consensus is

presented in the proposed model. To that end, as shown in equation 1 below, the proposed model computes an Iterative Privacy Trust Rank for each node,

$$IPTR = \frac{1}{NC}\sum_{i=1}^{NC}\frac{P(Rx,i)^2}{d(i)*P(Tx,i)*E(i)} \tag{1}$$

Where, NC represents total number of previous communications, $P(Rx)$ & $P(Tx)$ represents number of successfully received & transmitted packets, $d(i)$ & $E(i)$ represents the delay & energy needed during previous communications.

As per figure 1, this rank is updated for each communication iteration, and based on this updated rank, the model estimates an Iterative Relative Rank between 2 miners via equation 2,

$$IRR(i,j) = \sqrt{IPTR(i)*IPTR(j)} \tag{2}$$

This rank is estimated for all node pairs, and based on it, the model estimates Iterative Rank Threshold via equation 3,

$$IR(th) = \frac{1}{NN^2}\sum_{i=1}^{NN}\sum_{j=1}^{NN}IRR(i,j) \tag{3}$$

Node pairs with $IRR(i, j) < IR(th)$ are removed, while others are retained to perform consensus. These nodes are tested for their temporal & spatial privacy levels, which are estimated via equations 4, 5, 6, & 7 as follows,

$$DSn = \sum_{i=1}^{N} wi \cdot \int_0^{Dn} exp(-si(x))dx \tag{4}$$

Where, Dn designates the data elements in node n, and Sn are the sensitivity parameters with N different types of data samples. Each type of data would have a weight wi and sensitivity function si(x), integrated over the data range sets. The exponential term exp(−si(x)) denotes the decaying effect of sensitivity while processing every data element sets.

The weighting of each data type adds complexity by prioritizing certain sensitive data elements over others.

$$ACPn = \frac{1}{N}\sum_{i=1}^{N}\left(1-\frac{\partial pi}{\partial ri}\right) \tag{5}$$

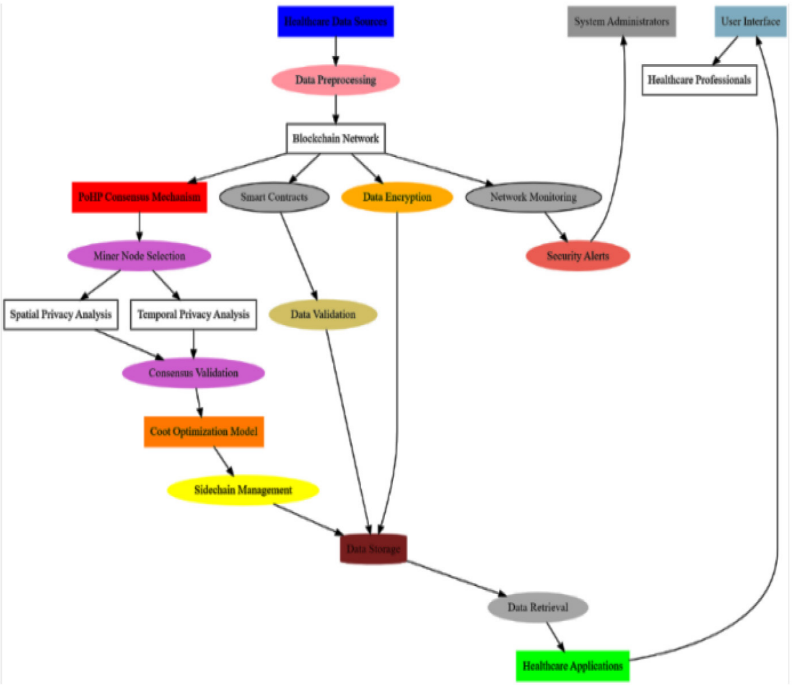

Figure 1

Model Architecture of the Proposed PoHT based Consensus Process

Herein, Pn denotes the set of privacy policies, whereas the derivative measures the rate of change of policy pi with respect to rule ri. The average over N of the sum of such derivatives measures how fast access controls adapt to changes in the policies. In particular, it is what makes the process complex: considering small changes in access rules that would impact adherence to privacy policies, which is a very important issue in dynamic scenarios of access control.

$$ESn = \int_0^{Kn} \frac{dk}{1 + exp(-ek(x))} dx \tag{6}$$

Where, Kn is the encryption key strength, and the function ek(x) will represent how good the encryption algorithm is in relation to the key strength. So the integration over the key strength range divided by the exponential term will reflect the robustness of the encryption algorithm in relation to levels of key strengths.

$$ADn = \sum_{i=1}^{M} ai \cdot \left(\frac{dmi(x)}{dx} \right)^{x=Dn} \tag{7}$$

In this equation, Dn represents the data set in node n, the function mi (x) represents the masking function corresponding to the ith method sets. The derivative $\frac{dmi(x)}{dx}$ at $x=Dn$ measures the rate at which the data is masked or anonymized for different use cases. The sum over all anonymization methods provides the overall effectiveness of the data anonymization process. The perplexity of the process results from how it quantifies the effectiveness of a set of multiple anonymization methods. It looks at the instantaneous change in data masking at the specific data point Dn sets. These levels are then fused to achieve final privacy level via equation 8,

$$PLn = \frac{DSn + ACPn + ESn + ADn}{4} \tag{8}$$

This overall privacy level, PLn, of node n is then calculated as mean value computed among data sensitivity evaluation, access control efficiency, encryption strength and also anonymization effectiveness. It is only then those nodes which have higher levels of privacy are selected to do PoHT consensus for the addition of new blocks in decentralized chains. While doing so, the model is estimating sidechain activation threshold, SAT, via equation 9:

$$SAT = \frac{d(i+1) * E(i+1)}{d(i) * E(i)} \tag{9}$$

Where, i stands for block number which is added to the current chains. When adding blocks, if SAT>2, then the model activates Coot optimizer so as to be in a position to increase speed all at the same time keeping it energy efficient in the process of mining. The Coot optimizer does this job, through stochastically breaking the current blockchain into 2 parts, of which the length of each part is estimated via equation 10,

$$SL = STOCH\left(\frac{LC * LR}{2}, \frac{LC}{2} \right) \tag{10}$$

Where, SL represents length of the current sidechain, LC is length of the current chain, while LR represents learning rate of the Coot optimization process. Using this sidechain length, the model estimates Coot fitness via equation 11,

$$fc = \frac{1}{ND}\sum_{i=1}^{ND}\frac{THR(i)*PDR(i)}{d(i)*E(i)} \tag{11}$$

Where, THR & PDR represents the throughput & packet delivery ratio of mining process, which is estimated for mining ND dummy blocks. This process of estimating new sidechain length is done for NC such Coot particles, and based on these particles, model estimate Coot fitness threshold via equation 12,

$$fth = \frac{1}{NC}\sum_{i=1}^{NC} fc(i)*LR \tag{12}$$

Based on this, Coot particles with fc>fth are passed to the Next Iteration, while other particles are removed from the current iteration, and replaced with new particles via equations 10 & 11, which assists in adding stochasticity to the sidechaining process. The process is then repeated for NI Iteration Sets, and after these iterations the model selects Coot particles with highest fitness to segregate the sidechains. In the selected chain configuration, the sidechain with a lower size is used for adding new blocks and is marked as a current chain, while the larger length chain is archived for future retrieval operations. Because of this, the model can enhance QoS with higher privacy levels maintained during mining & communication operations.

4. Result Analysis & Comparisons

The PoHP consensus mechanism and the Coot Optimization model set a new paradigm of blockchain applications to healthcare with a focus on privacy, security, and scalable efficiency.

Experiments in this paper are conducted on an all-round setup to test the performance of the BHPEC model in enhancing privacy in blockchain-based healthcare applications. The simulations, run on Network Simulator NS-3, mimic the typical clinical setting and consider BHPEC against other blockchain models like BCGeo[4], PCTB[16], and Federated Learning[18]. In these experiments, Figure 2 shows the scale of communications will be changed from 10,000 up to 104,000 communications, testing under different load conditions and measuring key metrics such as delay, energy consumption, throughput, packet delivery ratio, and jitter. It provides an objective and rigid enough setup to show the potential of BHPEC in improving privacy and operational efficiencies in blockchain applications in healthcare.

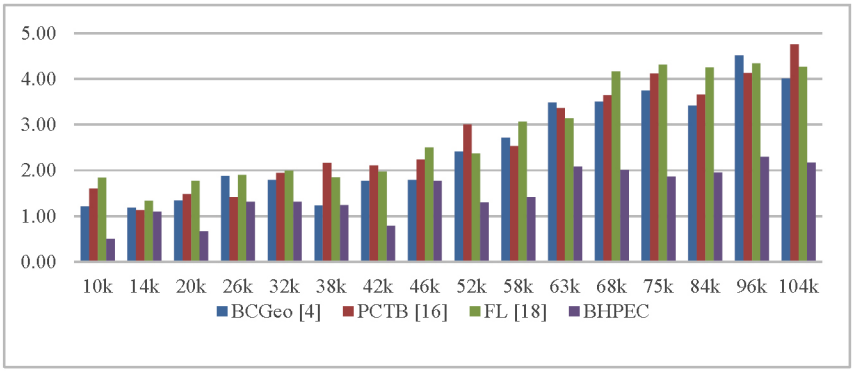

Figure 2

Delay needed for communication of data packets in Healthcare Deployments

Figure 3 depicts BHPEC produced a delay of only 0.51 ms at the 10k mark in communications, way shorter than BCGeo [4], PCTB [16], and FL [18], that posted delays of 1.21 ms, 1.60 ms, and 1.84 ms respectively. This efficiency holds up even when the communication complexity becomes very large, and BHPEC manages a delay of 1.31 ms at the 32k mark, with FL at 1.99 ms and remaining competitive with the other models.

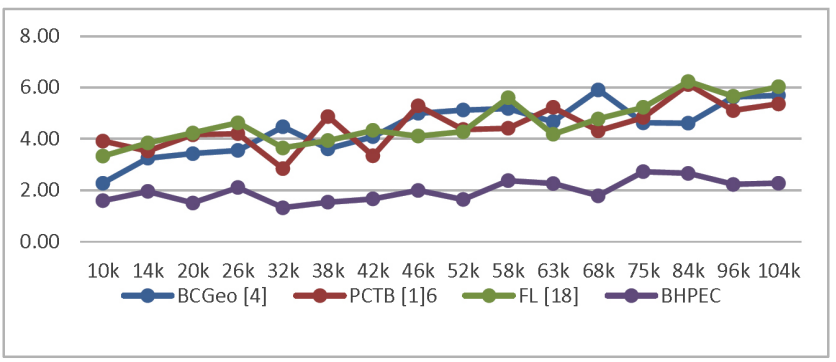

Figure 3

Energy needed for communication of data packets in Healthcare Deployments

Showing better energy efficiency at all scales of communication, the BHPEC model forms an ideal solution for energy-sensitive healthcare applications. For instance, at the 10k communications scale, BHPEC requires only 1.59 mJ, way below that used by BCGeo[4], PCTB[16], and FL[18] with 2.28 mJ, 3.92 mJ, and 3.33 mJ, respectively.

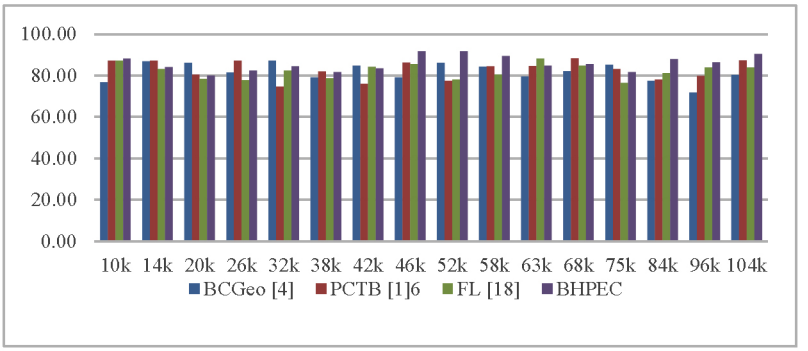

Figure 4

PDR obtained for communication of data packets in Healthcare Deployments

In Figure 4, the data indicates that BHPEC is outstandingly very high in terms of PDR, showing the ratio of data packets delivered successfully at different communication scales. BHPEC obtains a PDR of 88.13% at the 10k level of communication, which is slightly higher than other competitive models such as BCGeo[4] with 76.71%, PCTB[16] with 87.12%, and FL[18] with 87.15% for different scenarios.

5. Conclusion & Future Scope

The proof of Healthcare Privacy consensus mechanism, incorporated with the Coot Optimization model, has greatly improved the key metrics regarding energy efficiency by 10.5%, a reduction in communication delay of 9.5%, and increased throughput of 3.9%. Also, it has less jitter coupled with further improvements in the packet delivery ratios. The high degree of privacy and efficiency that BHPEC is going to bring will revolutionize healthcare service delivery in regard to ensuring the highest level of security in handling patient data and operational effectiveness. It is through the ability of BHPEC to offer more secure and robust digital health solutions that marked improvements in healthcare informatics can be made. This presents a framework for supporting changing modern health-care needs. Some key areas in future research include the integration of BHPEC with IoMT, artificial intelligence, machine learning, etc., which further extend its capability. Other critical themes that would require further research include BHPEC scalability within bigger and more complicated healthcare networks, adaptability to several healthcare

systems across the globe, and interoperability with pre-installed healthcare information systems.

References

[1] B. Ren, L. T. Yang, Q. Zhang, J. Feng and X. Nie, "Blockchain-Powered Tensor Meta-Learning-Driven Intelligent Healthcare System With IoT Assistance," in IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, pp. 2503-2513 (1 Sept.-Oct. 2023), doi: 10.1109/TNSE.2022.3227317.

[2] Md. A. Islam, Md. A. H. Jacky, Md. Al-Amin, Md. S. Miah, Md. M. I. Khan, Md. I. Hossain, "Distributed Ledger Technology Based Integrated Healthcare Solution for Bangladesh," in IEEE Access, vol. 11, pp. 51527-51556 (2023), doi: 10.1109/ACCESS.2023.3279724.

[3] R. Myrzashova, S. H. Alsamhi, A. V. Shvetsov, A. Hawbani and X. Wei, "Blockchain Meets Federated Learning in Healthcare: A Systematic Review With Challenges and Opportunities," in IEEE Internet of Things Journal, vol. 10, no. 16, pp. 14418-14437, 15 Aug.15 (2023), doi: 10.1109/JIOT.2023.3263598.

[4] S. R. Mallick, R. K. Lenka, V. Goswami, S. Sharma, A. K. Dalai, H. Das; R. K. Barik, "BCGeo: Blockchain-Assisted Geospatial Web Service for Smart Healthcare System," in IEEE Access, vol. 11, pp. 58610-58623 (2023), doi: 10.1109/ACCESS.2023.3283776.

[5] A.Lakhan, M. A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, A. Vidyarthi, A. Alkhayyat, W. Wang, "Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare," in *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 2, pp. 664-672 (Feb. 2023), doi: 10.1109/JBHI.2022.3165945.

[6] L. D. Costa, B. Pinheiro, W. Cordeiro, R. Araújo and A. Abelém, "SecHealth: A Blockchain-Based Protocol for Securing Health Records," in IEEE Access, vol. 11, pp. 16605-16620 (2023), doi: 10.1109/ACCESS.2023.3245046.

[7] J. Li, D. Li and X. Zhang, "A Secure Blockchain-Assisted Access Control Scheme for Smart Healthcare System in Fog Computing," in IEEE Internet of Things Journal, vol. 10, no. 18, pp. 15980-15989, 15 Sept.15 (2023), doi: 10.1109/JIOT.2023.3268278.

[8] V. Agarwal and S. Pal, "HierChain: A Hierarchical-Blockchain-Based Data Management System for Smart Healthcare," in *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 2924-2934, 15 Jan.15 (2024), doi: 10.1109/JIOT.2023.3295847.

[9] Z. A. E. Houda, A. S. Hafid, L. Khoukhi and B. Brik, "When Collaborative Federated Learning Meets Blockchain to Preserve Privacy in Healthcare," in I*EEE Transactions on Network Science and Engineering,* vol. 10, no. 5, pp. 2455-2465 (1 Sept.-Oct. 2023), doi: 10.1109/TNSE.2022.3211192.

[10] V. Stephanie, I. Khalil, M. Atiquzzaman and X. Yi, "Trustworthy Privacy-Preserving Hierarchical Ensemble and Federated Learning in Healthcare 4.0 With Blockchain," in *IEEE Transactions on Industrial Informatics,* vol. 19, no. 7, pp. 7936-7945 (July 2023), doi: 10.1109/TII.2022.3214998.

[11] F. F. Alruwaili, B. Alabduallah, H. Alqahtani, A. S. Salama, G. P. Mohammed and A. A. Alneil, "Blockchain Enabled Smart Healthcare System Using Jellyfish Search Optimization With Dual-Pathway Deep Convolutional Neural Network," in *IEEE Access*, vol. 11, pp. 87583-87591 (2023), doi: 10.1109/ACCESS.2023.3304269.

[12] J. Liu, W. Jiang, R. Sun, A. K. Bashir, M. D. Alshehri, Q. Hua, K. Yu, "Conditional Anonymous Remote Healthcare Data Sharing Over Blockchain," in *IEEE Journal of Biomedical and Health Informatics,* vol. 27, no. 5, pp. 2231-2242 (May 2023), doi: 10.1109/JBHI.2022.3183397.

[13] J. A. Alzubi, O. A. Alzubi, A. Singh and M. Ramachandran, "Cloud-IIoT-Based Electronic Health Record Privacy-Preserving by CNN and Blockchain-Enabled Federated Learning," in I*EEE Transactions on Industrial Informatics,* vol. 19, no. 1, pp. 1080-1087 (Jan. 2023), doi: 10.1109/TII.2022.3189170.

[14] S. Thapliyal, M. Wazid, D. P. Singh, A. K. Das, S. Shetty and A. Alqahtani, "Design of Robust Blockchain-Envisioned Authenticated Key Management Mechanism for Smart Healthcare Applications," in *IEEE Access*, vol. 11, pp. 93032-93047 (2023), doi: 10.1109/ACCESS.2023.3310264.

[15] J. Liu, Y. Fan, R. Sun, L. Liu, C. Wu and S. Mumtaz, "Blockchain-Aided Privacy-Preserving Medical Data Sharing Scheme for E-Healthcare System," in *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21377-21388, 15 Dec.15 (2023), doi: 10.1109/JIOT.2023.3287636.

[16] N. K. Dewangan and P. Chandrakar, "Patient-Centric Token-Based Healthcare Blockchain Implementation Using Secure Internet of Medical Things," in *IEEE Transactions on Computational Social Systems,* vol. 10, no. 6, pp. 3109-3119 (Dec. 2023), doi: 10.1109/TCSS.2022.3194872.

[17] A. Alnuaimi, D. Hawashin, R. Jayaraman, K. Salah and M. Omar, "Trustworthy Healthcare Professional Credential Verification Using Blockchain Technology," in *IEEE Access,* vol. 11, pp. 109669-109688 (2023), doi: 10.1109/ACCESS.2023.3322359.

[18] O. Samuel, A. B. Omojo, A.M. Onuja,Y. Sunday, P. Tiwari, D. Gupta, G. Hafeez, A. S. Yahaya, O. J. Fatoba, S. Shamshirband, "IoMT: A COVID-19 Healthcare System Driven by Federated Learning and Blockchain," in *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 2, pp. 823-834 (Feb. 2023), doi: 10.1109/JBHI.2022.3143576.

Received October, 2024