BIBLIOGRAPHIC INFORMATION SYSTEM

Journal Full Title: Journal of Biomedical Research & Environmental Sciences

Journal NLM Abbreviation: J Biomed Res Environ Sci

Journal Website Link: https://www.jelsciences.com

Journal ISSN: 2766-2276

Category: Multidisciplinary

Subject Areas: Medicine Group, Biology Group, General, Environmental Sciences

Topics Summation: 133

Issue Regularity: Monthly

Review Process: Double Blind

Time to Publication: 21 Days

Indexing catalog: IndexCopernicus ICV 2022: 88.03 | GoogleScholar | View more

Publication fee catalog: Visit here

DOI: 10.37871 (CrossRef)

Plagiarism detection software: iThenticate

Managing entity: USA

Language: English

Research work collecting capability: Worldwide

Organized by: SciRes Literature LLC

IndexCopernicus ICV 2022: 83.03

Manuscript should be submitted in Word Document (.doc or .docx) through

Online Submission

form or can be mailed to support@jelsciences.com

Vision: Journal of Biomedical Research & Environmental Sciences main aim is to enhance the importance of science and technology to the scientific community and also to provide an equal opportunity to seek and share ideas to all our researchers and scientists without any barriers to develop their career and helping in their development of discovering the world.

JOURNAL OF BIOMEDICAL RESEARCH & ENVIRONMENTAL SCIENCES
ISSN: 2766-2276
SUBJECT AREA(S): PUBLIC HEALTH
DOI: 10.37871

OPINION

A Unified Framework for Secure Healthcare Data Sharing: Integrating Federated Learning, Blockchain, and Quantum Cryptography

Jeremie Ruvunangiza* and Carlos Valderrama

Polytechnic Faculty, University of Mons, Belgium

Abstract

As the demand for secure and efficient data sharing in healthcare continues to grow, there is a pressing need for innovative solutions that ensure data privacy, integrity, and accessibility in multiple institutions. This study proposes a unified framework that integrates three cutting-edge technologies, federated learning, blockchain, and quantum cryptography, to address the complex challenges of secure data sharing in the healthcare sector. Federated learning enables decentralized data analysis by maintaining sensitive patient information locally, significantly reducing the risk of data breaches. Blockchain technology adds an immutable and transparent ledger to securely track data exchanges, ensuring compliance with stringent data governance standards. Quantum cryptography enhances the security of data transmission using quantum mechanics principles to prevent unauthorized access and guarantee the confidentiality of shared information. The proposed framework successfully combines these advanced technologies to fortify the security of healthcare data sharing. Promote collaborative analysis while maintaining patient privacy, leading to better patient outcomes and fostering greater trust among healthcare providers. By synergizing federated learning, blockchain, and quantum cryptography, the proposed framework represents a significant advance in secure healthcare data sharing. Not only does it address the urgent need for data security, it also supports global collaboration necessary to tackle healthcare challenges on an international scale.

Abbreviations

FL: Federated Learning; BC: Blockchain; QC: Quantum Cryptography; QKD: Quantum Key Distribution; HCP: Healthcare Provider; PHI: Protected Health Information; GDPR: General Data Protection Regulation; HIPAA: Health Insurance Portability and Accountability Act

Introduction

The healthcare industry is at the forefront of a digital revolution, with data-driven technologies that transform patient care, medical research, and operational efficiency. As healthcare systems around the world become

***Corresponding author(s)**

Jeremie Ruvunangiza, Polytechnic Faculty, University of Mons, Belgium

Email: jeremiebiringanine.ruvunangiza@student.umons.ac.be

DOI: 10.37871/jbres1993

Submitted: 30 August 2024

Accepted: 05 September 2024

Published: 11 September 2024

Keywords

- Federated Learning
- Blockchain technology
- Quantum cryptography
- Healthcare data privacy
- Secure data sharing
- Medical records
- Quantum-resistant encryption

MEDICINE GROUP

PUBLIC HEALTH

VOLUME: 5 ISSUE: 9 - SEPTEMBER, 2024

Scan Me

How to cite this article: Ruvunangiza J, Valderrama C. A Unified Framework for Secure Healthcare Data Sharing: Integrating Federated Learning, Blockchain, and Quantum Cryptography. J Biomed Res Environ Sci. 2024 Sept 11; 5(9): 1081-1088. doi: 10.37871/jbres1993, Article ID: JBRES1993, Available at: https://www.jelsciences.com/articles/jbres1993.pdf

increasingly interconnected, the ability to securely share sensitive patient data has become a critical priority [1]. Medical problems, such as pandemics and chronic diseases, are no longer confined to isolated regions, but are global phenomena requiring collaborative international responses [2,3]. Using advanced technologies such as Federated Learning (FL), Blockchain (BC) and Quantum Cryptography (QC) offers innovative solutions to securely collaborate while maintaining patient privacy and compliance with regulatory [4,5]. However, the global nature of medical data sharing introduces significant challenges related to privacy, security, and data governance [6,7]. Traditional data exchange methods, which often rely on centralized systems, expose sensitive patient information to numerous risks, including unauthorized access, data breaches, and misuse [8,9]. These risks are exacerbated by the varying regulatory requirements in different countries, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe, which complicates secure data sharing across borders [10,11].

To address these challenges, this paper proposes a unified framework that integrates FL, BC, and QC. This framework is designed to meet the urgent need for secure, scalable, and efficient global health care data sharing, ensuring that patient privacy is protected while allowing collaborative analysis necessary to combat global health issues [12,13].

FL enables decentralized data analysis, allowing healthcare institutions worldwide to collaboratively train machine learning models without exposing their underlying data. This is critical given the fragmented nature of healthcare data between institutions and the sensitive information contained in electronic health records [14,15]. BC enhances this framework by providing a decentralized, immutable ledger that ensures data integrity and traceability, addressing concerns about trust and accountability in shared environments [16,17]. QC further strengthens data security by using quantum mechanics to protect against advanced cyber threats, including those posed by quantum computing [18,19]. Quantum Cryptography, especially through Quantum Key Distribution (QKD), plays a vital role in securing communication channels. QKD uses principles of quantum mechanics to ensure that encryption keys are transmitted securely, protecting sensitive data transmissions from quantum-level threats.

By integrating these advanced technologies, the proposed framework offers a robust solution to the sharing of global healthcare data. Not only does it address the pressing need for data security, it also supports the global collaboration necessary to tackle healthcare challenges on an international scale. This framework represents a significant step forward in bridging the gap between data security and accessibility, facilitating a new era of global healthcare innovation [20].

Literature Review

Existing approaches

Traditional Healthcare Data Security: Traditional methods for securing healthcare data rely largely on centralized systems and classical cryptographic techniques, such as digital signatures and elliptic curve cryptography. Although these methods have been effective, they face significant limitations in terms of scalability, privacy, and resistance to emerging threats such as quantum computing. Blockchain has been introduced as a decentralized alternative, providing immutability and transparency. However, traditional blockchain systems are vulnerable to quantum attacks due to their reliance on classical cryptography.

Quantum-safe blockchain: The quantum blockchain paper by Chehimi M, et al. [21] proposes a novel quantum blockchain network designed to withstand quantum computer attacks. This approach uses quantum entanglement and quantum cryptographic principles to secure the blockchain, making it resistant to quantum threats. The quantum blockchain provides a new level of security but does not integrate Federated Learning (FL), which limits its applicability in scenarios that require collaborative data processing between decentralized entities, such as healthcare.

Federated learning in healthcare: The QuantumFed paper explores the adaptation of Federated Learning to quantum computing environments, proposing a framework that allows quantum nodes to collaboratively train a global model without sharing raw data [22]. Although this approach addresses the challenges of data privacy and computational efficiency in quantum environments, it does not integrate Blockchain (BC) or Quantum Cryptography (QC). As a result, the framework lacks the comprehensive security needed for practical

applications in healthcare, particularly against quantum threats.

Need for integration: Existing research, while innovative, does not provide a unified solution that combines FL, BC, and QC for the sharing of data in healthcare. The quantum blockchain approach is secure against quantum attacks but does not support the collaborative data processing required in healthcare. On the other hand, the QuantumFed framework focuses on federated learning in quantum environments but does not address data integrity or quantum-safe communication. Therefore, there is a clear need for a unified framework that integrates these technologies to ensure secure, scalable, and privacy-preserving healthcare data sharing in the face of both classical and quantum threats.

Proposed framework

Federated Learning (FL) component: Federated Learning (FL) enables decentralized and privacy-preserving healthcare data processing by allowing multiple institutions to collaboratively train machine learning models without sharing sensitive patient data. In this approach, each participating entity (such as hospitals or research centers) processes its local data and only shares model updates with a central aggregator, ensuring that the raw data never leave the local environment [23]. This method not only preserves patient privacy, but also improves the security of data processing by minimizing the risk of exposure. Compared to the other frameworks, which focus on quantum environments, our approach is specifically designed for healthcare applications. Citefedquantum integrates FL with additional security layers provided by Blockchain (BC) and Quantum Cryptography (QC), offering a more practical and secure solution for healthcare data sharing.

Blockchain (BC) component: Blockchain technology in our framework ensures data integrity and transparency within the healthcare ecosystem by providing a decentralized, immutable ledger that records all transactions and data exchanges. This ledger guarantees that any alterations or updates to the data are transparent and verifiable by all stakeholders, thus fostering trust in the shared data [24].

Although blockchain secures the integrity of the data once they are recorded in the ledger, there are potential security concerns during the transmission of data between healthcare institutions before it is stored on the blockchain. To address this, the Quantum Key Distribution (QKD) is used to secure the communication channels through which data and model updates are transmitted between entities. QKD ensures that any eavesdropping attempts on these transmissions can be detected, guaranteeing that the data remains untampered with before being committed to the blockchain.

Unlike the quantum blockchain framework, which focuses primarily on resisting quantum attacks within the blockchain itself, our approach improves the security of Federated Learning (FL) by integrating Blockchain (BC) with Quantum Cryptography (QC), particularly QKD, to protect data transmissions [25]. This integration allows for a more robust verification process, ensuring that the data used in federated learning is accurate, traceable, and securely transmitted between different healthcare institutions.

Once data is securely transmitted using QKD, the blockchain ledger ensures that it remains immutable and transparent, providing accountability and trust across the healthcare network. This dual approach - QKD to secure data transmission and Blockchain to ensure data integrity - creates a highly secure system for data sharing in healthcare.

Quantum Cryptography (QC) component: Quantum Cryptography (QC) plays a crucial role in securing communication channels within the proposed framework, particularly against quantum attacks that could compromise traditional cryptographic methods. QC, through mechanisms such as Quantum Key Distribution (QKD), provides an additional layer of security that is future-proof against the computational power of quantum computers.

Quantum Key Distribution (QKD) is essential in securing the exchange of encryption keys between healthcare institutions during data transmissions. QKD ensures that any eavesdropping attempts are detected, as the act of measuring quantum bits (qubits) alters their state, thereby alerting the system to potential security breaches. This mechanism guarantees that the encryption keys remain confidential even in the presence of advanced quantum computing threats [26].

By integrating QKD with Federated Learning (FL) and Blockchain (BC), the framework ensures that all data transmissions, especially those involved in federated learning model updates and blockchain transactions, are fully secure. QKD strengthens

communication channels by providing quantum-level encryption that protects against classical and quantum-based attacks.

This integration not only secures the overall system but also positions it as a cutting-edge solution for secure healthcare data sharing in the quantum era. Using QKD, the framework future proofs sensitive data communications, ensuring that they remain resilient against both current and emerging cyber threats.

Integration of components

Unified system architecture: The proposed framework integrates Federated Learning (FL), Consortium Blockchain (BC) and Quantum Cryptography (QC) into a unified architecture designed to enhance the security, privacy, and trustworthiness of healthcare data sharing. In this architecture, FL enables decentralized data processing across multiple healthcare institutions without sharing sensitive patient data. The Consortium Blockchain serves as the foundation for ensuring data integrity, transparency, and controlled access among a predefined group of trusted healthcare stakeholders, such as hospitals, research centers, and regulatory bodies [1]. The blockchain records all transactions related to model updates and data sharing in an immutable ledger, ensuring that only authorized participants can validate and view transactions [27]. QC is integrated to secure communication channels, using Quantum Key Distribution (QKD) to protect against potential quantum threats, thereby securing the data transmission between FL nodes and blockchain participants.

Workflow: The workflow within the integrated framework begins with the local collection and processing of data in each participating healthcare institution. Each institution trains its machine learning models locally, ensuring that sensitive patient data remain within its local environment [28,29].

Once the model is trained, the quantum key distribution (QKD) is used to secure the transmission of model updates between institutions. QKD ensures that the encryption keys used to secure these updates are protected and that any attempt to intercept or tamper with the data is immediately detected [30]. This guarantees that the model updates are transmitted securely and without compromise.

The updates are then recorded on the Blockchain (BC), where all transactions related to model updates and data sharing are immutably stored. The blockchain ensures that only authorized participants can validate and audit these transactions, providing transparency and accountability to all stakeholders [31].

Finally, the global model is updated with the aggregated results of all institutions and redistributed to the participating institutions. This iterative process allows for continuous learning and improvement of the model while ensuring the privacy and security of patient data through QKD-secured transmissions and blockchain-enabled data integrity.

scenario: Consider the management of a global pandemic as an application scenario for the proposed framework. Healthcare providers in different regions must collaborate in real time to develop predictive models for disease spread, treatment efficacy, and resource allocation. Each institution uses FL to train models on its local data without sharing sensitive patient information. These model updates are then securely transmitted using QC to prevent interception or tampering. The Consortium blockchain records all model updates and transactions, ensuring that only trusted healthcare providers within the consortium can validate and verify the data, maintaining data integrity and transparency [32]. The global model, which is continuously updated with the input of various institutions, enables a coordinated and effective response to the pandemic. This scenario demonstrates the potential of the framework to facilitate secure, privacy-preserving, and transparent data sharing in critical healthcare settings, ensuring that data remain trustworthy and actionable throughout the global consortium.

Security and privacy analysis

Quantum resistance: The integration of Quantum Cryptography (QC) within the proposed framework significantly enhances its resistance to quantum attacks, a growing concern as quantum computing continues to evolve. QC, specifically through Quantum Key Distribution (QKD), provides a level of security that is theoretically unbreakable by quantum computers, ensuring that all data transmissions within the framework are protected against future quantum threats [26]. This integration is critical to protect healthcare data shared between institutions, particularly during the federated learning process,

where sensitive information is at play. The use of QC in this context not only future proofs the system but also addresses the limitations of traditional cryptographic methods, which are vulnerable to quantum attacks [33]. This aspect of the framework sets it apart from other approaches, such as the quantum blockchain discussed earlier, which focuses on quantum-resistant data storage but does not integrate a comprehensive quantum-secure communication layer.

Comparison with existing systems: Compared to existing systems, such as the quantum Fed framework and the quantum blockchain approach, the proposed framework offers a more holistic solution to the security of healthcare data. QuantumFed primarily addresses federated learning in quantum environments, but lacks the integration of blockchain for data integrity and transparency, as well as QC for secure communication. However, the quantum blockchain approach, while robust against quantum threats, does not incorporate federated learning, limiting its applicability in collaborative healthcare settings. The proposed framework, by integrating FL, BC and QC, not only ensures secure data processing and transmission, but also maintains transparency and accountability between all participating entities. This comprehensive approach addresses the key weaknesses in existing systems, providing a more secure and efficient solution for the sharing of healthcare data.

Privacy preservation: The preservation of privacy is a core principle of the proposed framework, particularly in the context of federated learning. By allowing for decentralized model training, FL ensures that raw patient data remain within the local environment of each healthcare institution, reducing the risk of data breaches and unauthorized access [23]. The addition of blockchain technology further enhances privacy by providing an immutable record of all transactions, ensuring that only authorized entities can access or modify the data. This is particularly important in maintaining patient trust and complying with stringent data protection regulations such as HIPAA and GDPR [34]. QC adds another layer of privacy by securing communication channels between institutions, preventing any interception or manipulation during data transmission. This multilayered approach to privacy preservation ensures that patient data are protected throughout the entire data sharing process, from local processing to global model aggregation.

In summary, the integration of FL, BC, and QC in the proposed framework provides a robust solution to ensure the security and privacy of healthcare data. By addressing the limitations of existing systems and offering a comprehensive approach to data protection, this framework stands out as a significant advance in the field of secure healthcare data sharing.

Challenges and future work

Technical challenges: Implementing the proposed framework presents several technical challenges, particularly related to the integration of Federated Learning (FL), Consortium Blockchain (BC) and Quantum Cryptography (QC). One of the primary challenges is the complexity of coordinating and managing the interactions between these technologies in a way that ensures optimal performance and security. For example, ensuring that quantum cryptographic protocols operate seamlessly with the blockchain infrastructure and federated learning processes requires sophisticated algorithms and precise synchronization. In addition, the scalability of the framework is a significant concern, especially as the number of participating healthcare institutions increases [35]. The computational overhead associated with quantum cryptography and the need for consensus in a consortium blockchain could lead to latency issues, potentially slowing down data sharing and model training processes [36,37]. Addressing these technical challenges will require ongoing research and development to optimize the framework's efficiency without compromising security.

Regulatory and ethical considerations: The adoption of this framework in real-world healthcare settings also raises several regulatory and ethical considerations. Compliance with data protection regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe is paramount. These regulations impose strict requirements on how patient data is collected, stored, and shared, and any deviation could result in legal consequences [38]. The use of blockchain technology, which involves immutable records, poses a challenge to the right to be forgotten, a key provision under GDPR. Furthermore, the deployment of quantum cryptography, while improving security, may raise concerns about accessibility and fairness, particularly in regions with limited technological infrastructure. Ensuring that the framework is ethically sound and

complies with relevant regulations will be crucial to its successful implementation.

Future research directions: Future research should focus on several areas to improve the proposed framework and address its current limitations. One critical area is the development of more efficient quantum cryptographic protocols that can be seamlessly integrated with blockchain and federated learning systems. Research should also explore ways to improve the scalability of the framework, such as optimizing consensus mechanisms in consortium blockchains or developing more lightweight quantum cryptography solutions [39]. Another important direction is the exploration of additional use cases beyond healthcare, where secure, decentralized data sharing is critical, such as in finance, supply chain management, and smart cities. Furthermore, as quantum computing technology continues to advance, it will be important to continually assess and update the framework to ensure that it remains secure against new threats [40]. Finally, interdisciplinary research involving legal scholars, ethicists, and technologists will be essential to address the regulatory and ethical challenges associated with the deployment of this framework in real-world environments.

Although the proposed framework offers significant advances in secure healthcare data sharing, its implementation will require overcoming several technical, regulatory, and ethical challenges. By addressing these challenges and pursuing further research, the framework can be refined and expanded to provide a robust solution for secure, decentralized data sharing across various domains.

Conclusion

In this paper, we proposed a unified framework that integrates Federated Learning (FL), Consortium Blockchain (BC), and Quantum Cryptography (QC) to enhance the security and privacy of healthcare data sharing. This framework addresses the critical need for a secure, scalable, and efficient solution in an increasingly interconnected healthcare ecosystem, where the sharing of sensitive patient data is essential for effective collaboration and response to global health challenges.

The integration of FL allows healthcare institutions to collaboratively train machine learning models without compromising patient privacy by ensuring that raw data remain localized. Consortium blockchain technology ensures the integrity, transparency and traceability of all data exchanges and update models within a controlled group of trusted participants, promoting trust and accountability in the system. Quantum cryptography further strengthens the security of the framework by protecting communication channels against quantum threats, making the system resilient to future advances in quantum computing.

The framework not only offers a significant advancement over existing approaches, such as the QuantumFed framework and quantum blockchain technologies, but also provides a comprehensive solution that combines the strengths of these technologies while addressing their limitations. By doing so, it sets a new standard for secure healthcare data sharing, particularly in scenarios that require global collaboration, such as during pandemics and other public health emergencies.

However, the implementation of this framework is not without challenges. Technical hurdles, such as the complexity of integration and scalability, must be overcome, and regulatory and ethical considerations must be carefully navigated to ensure compliance with data protection laws like HIPAA and GDPR. Future research should focus on optimizing the performance of the framework, exploring new use cases, and addressing the evolving threats posed by advances in quantum computing.

In conclusion, the proposed framework represents a significant step forward in the field of secure healthcare data sharing. It provides a robust and innovative solution that not only improves the security and privacy of sensitive data, but also supports the global collaboration necessary to address complex healthcare challenges. As the landscape of healthcare continues to evolve, the adoption of such integrated frameworks will be crucial to ensure that data security keeps pace with technological advancements, ultimately leading to better patient outcomes and more effective healthcare delivery on a global scale.

References

1. Mäntymäki M, Tandon A, Dhir A, Najmul Islam AKM. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Elsevier BV. 2020;122:103290. doi: 10.1016/j.compind.2020.103290.

2. Schwalbe N, Wahl B, Song J, Lehtimaki S. Data Sharing and Global Public Health: Defining What We Mean by Data. Front Digit Health. 2020 Dec 14;2:612339. doi: 10.3389/fdgth.2020.612339. PMID: 34713073; PMCID: PMC8521885.

3. Taghizade S, Chattu VK, Jaafaripooyan E, Kevany S. COVID-19 Pandemic as an Excellent Opportunity for Global Health Diplomacy. Front Public Health. 2021 Jul 12;9:655021. doi: 10.3389/fpubh.2021.655021. PMID: 34322467; PMCID: PMC8310918.

4. Scheibner J, Raisaro JL, Troncoso-Pastoriza JR, Ienca M, Fellay J, Vayena E, Hubaux JP. Revolutionizing Medical Data Sharing Using Advanced Privacy-Enhancing Technologies: Technical, Legal, and Ethical Synthesis. J Med Internet Res. 2021 Feb 25;23(2):e25120. doi: 10.2196/25120. PMID: 33629963; PMCID: PMC7952236.

5. Zhang R, Xue R, Liu L. Security and privacy for healthcare blockchains. Cornell University. 2021. doi: 10.48550/arXiv.2106.06136.

6. Abdulrahman H, Poh N, Burnett J. Privacy preservation, sharing and collection of patient records using cryptographic techniques for cross-clinical secondary analytics. 2014. doi: 10.1109/cicare.2014.7007847.

7. Kim D, Kim H, Kwak J. Secure sharing scheme of sensitive data in the precision medicine system. 2020;64:1527-53. doi: 10.32604/cmc.2020.010535.

8. Pisani E, Aaby P, Breugelmans JG, Carr D, Groves T, Helinski M, Kamuya D, Kern S, Littler K, Marsh V, Mboup S, Merson L, Sankoh O, Serafini M, Schneider M, Schoenenberger V, Guerin PJ. Beyond open data: realising the health benefits of sharing data. BMJ. 2016 Oct 10;355:i5295. doi: 10.1136/bmj.i5295. PMID: 27758792; PMCID: PMC6616027.

9. Khan RA, Shah SM. Secondary use of electronic health record: Opportunities and challenges. Institute of Electrical and Electronics Engineers. 2020;8:136947-65. doi: 10.1109/access.2020.3011099.

10. Dankar FK. Practices and challenges in clinical data sharing. Cornell University. 2023. doi: 10.48550/arXiv.2304.06509.

11. Porwal S, Srijith K. Nair SK, Dimitrakos T. Regulatory impact of data protection and privacy in the cloud. Springer Science+Business Media. 2011;290-299. doi: 10.1007/978-3-642-22200-9_23.

12. Bhavin M, Tanwar S, Sharma N, Tyagi S, Kumar N. Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications. 2023. doi: 10.1016/j.jisa.2020.102673.

13. Selvarajan S, Mouratidis H. A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. Sci Rep. 2023 May 2;13(1):7107. doi: 10.1038/s41598-023-34354-x. Erratum in: Sci Rep. 2023 Jun 9;13(1):9409. doi: 10.1038/s41598-023-36573-8. PMID: 37131047; PMCID: PMC10154383.

14. Bhatia AS, Neira DEB. Federated hierarchical tensor networks: A collaborative learning quantum AI-driven framework for healthcare. Cornell University. 2024. doi: 10.48550/arXiv.2405.07735.

15. Xu J, Glicksberg BS, Su C, Walker P, Bian J, Wang F. Federated learning for healthcare informatics. Springer Science+Business Media. 2020;5:1-19. doi: 10.1007/s41666-020-00082-4.

16. Nguyen LT, Nguyen LD, Hoang T, Bandara D, Wang Q, Lu Q, Xu X, Zhu L, Popovski P, Chen S. Blockchain-empowered trustworthy data sharing: Fundamentals, applications, and challenges. 2023. doi: 10.48550/arXiv.2303.06546.

17. Chen L, Yang J-J, Wang Q, Niu Y. A framework for privacy-preserving healthcare data sharing. 2012 IEEE 14th international conference on e-health networking, applications and services (healthcom). IEEE. 2012;341-6. doi: 10.1109/HealthCom.2012.6379433.

18. Science & tech spotlight: Securing data for a post-quantum world. 2023.

19. Barker W, Polk W, Souppaya M. Getting ready for post-quantum cryptography: Exploring challenges associated with adopting and using post-quantum cryptographic algorithms 2021. doi: 10.6028/nist.cswp.15.

20. Vithanwattana N, Karthick G, Mapp G, George C, Samuels A. Securing future healthcare environments in a post-COVID-19 world: moving from frameworks to prototypes. J Reliab Intell Environ. 2022;8(3):299-315. doi: 10.1007/s40860-022-00180-7. Epub 2022 Jul 9. PMID: 35967078; PMCID: PMC9362615.

21. Chehimi M, Saad W. Quantum federated learning with quantum data. ICASSP 2022-2022 IEEE international conference on acoustics, speech and signal processing (ICASSP). IEEE. 2022;8617-21. doi: 10.1109/ICASSP43922.2022.9746622.

22. Xia Q, Li Q. Quantumfed: A federated learning framework for collaborative quantum training. 2021 IEEE global communications conference (GLOBECOM). IEEE. 2021;1-6. doi: 10.1109/GLOBECOM46510.2021.9685012.

23. Sarmadi A, Fu H, Krishnamurthy P, Garg S, Khorrami F. Privacy-preserving collaborative learning through feature extraction. Cornell University. 2022. doi: 10.48550/arXiv.2212.06322

24. Zou R, Lv X, Zhao J. SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. Elsevier BV. 2021;58:102604-4. doi: 10.1016/j.ipm.2021.102604.

25. Gurung D, Pokhrel SR, Li G. Decentralized quantum federated learning for metaverse: Analysis, design and implementation. Cornell University. 2023. doi: 10.48550/arXiv.2306.11297.

26. Wang J, Huberman B. A guide to global quantum key distribution networks. Cornell University. 2020. doi: 10.48550/arXiv.2012.14396.

27. Zhang P, Schmidt DC, White J. A pattern sequence for designing blockchain-based healthcare information technology systems. Cornell University. 2020. doi: 10.48550/arXiv.2010.01172.

28. Liu D, Miller T, Sayeed R, Mandl KD. FADL: Federated-autonomous deep learning for distributed electronic health record. arXiv preprint arXiv:181111400. 2018. doi: 10.48550/arXiv.1811.11400.

29. Xu J, Glicksberg BS, Su C, Walker P, Bian J, Wang F. Federated

learning for healthcare informatics. Journal of healthcare informatics research. 2021;5:1-19.

30. Jain N, Hoff U, Gambetta M, Rodenberg J, Gehring T. Quantum key distribution for data center security–a feasibility study. arXiv preprint. 2023. doi: 10.48550/arXiv.2307.13098

31. Goh E, Kim D-Y, Lee K, Oh S, Chae J-E, Kim D-Y. Blockchain-enabled federated learning: A reference architecture design, implementation, and verification. IEEE Access. 2023. doi: 10.48550/arXiv.2306.10841.

32. Dara T, Joong-Sun L, Hiroyuki S, Anushka W, Naoko T, Takashi O, Nagaaki O. Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability.2020;26:3-3. doi: 10.4258/hir.2020.26.1.3.

33. Zhang Y, Zhang C, Zhang C, Fan L, Zeng B, Yang Q. Federated learning with quantum secure aggregation. Cornell University. 2022. doi: 10.48550/arXiv.2207.07444.

34. Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and Trustable Electronic Medical Records Sharing using Blockchain. AMIA Annu Symp Proc. 2018 Apr 16;2017:650-659. PMID: 29854130; PMCID: PMC5977675.

35. Yoo JH, Jeong H, Lee J, Tai-Myoung C. Federated learning: Issues in medical application. Cornell University. 2021. doi: 10.48550/arXiv.2109.00202.

36. Bhavin M, Tanwar S, Sharma N, Tyag S, Neeraj k. Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications. 2020. doi: 10.1016/j.jisa.2020.102673.

37. Pandey PSAJK. Secure quantum computing for healthcare sector: A short analysis. Cornell University. 2022. doi: 10.48550/arXiv.2211.10027.

38. Simon PDAF, Simon F. Differences between Europe and the united states on AI/digital policy: Comment response to roundtable discussion on AI. SAGE Publishing. 2020;4:247028972090710-0. doi: 10.1177/2470289720907103.

39. Dev Gurung, Shiva Raj Pokhrel, Gang Li. Performance analysis and evaluation of post quantum secure blockchained federated learning. Cornell University. 2023. doi: 10.48550/arXiv.2306.14772.

40. Nitin Jain, Ulrich Hoff, Marco Gambetta, Jesper Rodenberg, Tobias Gehring. Quantum key distribution for data center security- A feasibility study Cornell University. 2023. doi: 10.48550/arXiv.2307.13098.

How to cite this article: Ruvunangiza J, Valderrama C. A Unified Framework for Secure Healthcare Data Sharing: Integrating Federated Learning, Blockchain, and Quantum Cryptography. J Biomed Res Environ Sci. 2024 Sept 11; 5(9): 1081-1088. doi: 10.37871/jbres1993, Article ID: JBRES1993, Available at: https://www.jelsciences.com/articles/jbres1993.pdf