

Privacy-preserving AI-driven healthcare analytics in post-quantum clouds

Asma A. Hussain [§]

*Department of Dermatology, Venerology, Leprosy
Krishna Institute of Medical Sciences
Krishna Vishwa Vidyapeeth (Deemed to be University)
Karad 415539
Maharashtra
India*

Chetan Kumar Sharma [†]

*School of Sciences
Noida International University
Greater Noida 201312
Uttar Pradesh
India*

Sekkeri Venu Gopal ^{*}

*Department of Computer Science and Engineering
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India*

Saurabh Bhattacharya [‡]

*School of Computer Science and Engineering
Galgotias University
Greater Noida 203201
Uttar Pradesh
India*

[§] E-mail: drasmaarif.5aug@gmail.com

[†] E-mail: chetan.sharma@niu.edu.in

^{*} E-mail: s.venugopal@vardhaman.org (Corresponding Author)

[‡] E-mail: babu.saurabh@gmail.com

J. Monisha [®]

*Department of Management Studies
Meenakshi College of Arts and Science
Meenakshi Academy of Higher Education & Research
Chennai 600078
Tamil Nadu
India*

P. Varalakshmi [#]

*Department of Electrical & Electronics Engineering
Pragati Engineering College
Kakinada 533437
Andhra Pradesh
India*

Abstract

Healthcare analytics leverages Artificial Intelligence and Cloud Computing in disease prediction, Clinical Decisions Making, Personalized Treatment and Remote Monitoring. However, having all of the information in a single place increases the risk of medical information being breached, misused, accessed and new threats in the quantum era. This study aims at designing an AI-powered healthcare analytics system with privacy in post-quantum cloud computing era. Incorporates Federated learning, Differential privacy, Secure aggregation, Post quantum key encapsulation, Quantum resistant digital signature, Role based access control and Explainable Artificial Intelligence. Patients' data is kept locally and a global model is trained collaboratively by healthcare institutions. Differential privacy preserves the contribution of the individual, secure aggregation presents the institutional update in an obscure manner and post quantum mechanisms secure authentication and communication. An evaluation based on a diabetes dataset demonstrates the framework's ability to classify with 92.94% accuracy with a reduction in membership-inference and gradient-reconstruction risks while using simulation. The latency, memory consumption and communications overhead of security mechanisms are high, but they are kept under control.

Subject Classification: 81P94.

Keywords: Healthcare analytics, Post-quantum cryptography, Federated learning, Differential privacy, Cloud security, Patient privacy, Explainable AI.

1. Introduction

The accelerated digitalization of healthcare has led to a huge amount of sensitive data to be generated, from Electronic Health Records (EHRs), medical imaging systems, through to wearable devices, genomics platforms and IoMT

[®] E-mail: jmonishamba@maher.ac.in

[#] E-mail: pvaralakshmi@outlook.com

applications [1]. These complex and varied sets of data can be processed by AI to aid in disease prediction, clinical decisions, patient-specific treatment, remote patient monitoring, and efficient hospital operations. Moreover, cloud computing enhances the capabilities of healthcare analytics with the ability to store and process vast amounts of data efficiently and collaboratively share medical information [2]. But the move to the cloud poses significant privacy issues regarding privacy and confidentiality, unauthorized access, data leakage, model inversion, cyber-attacks and regulatory compliance. Most of the current security systems are based on public-key classical cryptographic methods such as RSA, elliptic curve cryptography [3] etc. These algorithms are threatened by the advent of quantum computing, for if powerful enough quantum computers could solve the mathematical problems they are based on efficiently, they would be able to do so [4]. Data encrypted today can be collected and later decrypted through “harvest-now, decrypt-later” attacks as the information often needs to be kept confidential for longer periods of time. The risk makes it imperative to secure quantum computers before they hit the mass market in a way that is secure against quantum attackers [5]. This study aims at designing an AI-powered healthcare analytics system with privacy in post-quantum cloud computing era. The framework brings together the following technologies: post-quantum cryptography, federated learning, differential privacy, secure aggregation, access control, and explainable artificial intelligence [6]. The Post-quantum algorithms safeguard the exchange of data, authentication, and key management, and Federated learning allows hospitals to collectively train models without sharing patient data. Differential privacy and secure aggregation minimize the risk of re-constructing the individual information from model updates. Explainable AI enhances analytical results' transparency and clinical acceptability [7].

The research checks the framework in multiple aspects such as predictive accuracy, encryption cost, processing latency, communication overhead, protection against classical and quantum attacks, and privacy protection [8]. It made its biggest claim with an integrated security architecture that was designed to be both analytical and patient privacy friendly, computationally efficient, and secure for future collaboration in healthcare services via cloud. It also helps to ensure compliance to regulations in distributed and heterogeneous institutions.

Identify threats and develop a system model. Identify threats and create a system model.

The proposed system assumes a distributed health care environment where patient data from heterogeneous sources, such as hospitals, diagnostic centres, laboratories, wearable devices and IOTM (Internet of Medical Things) devices are produced. These data can consist of electronic health records, medical images, lab reports, physiological data, prescriptions and demographic information [9]. Every participating healthcare institution stores its own data in the local infrastructure, and shares it with a post-quantum cloud platform to collaborate on developing AI models.

2. System Model and Threat Analysis

The proposed system considers a distributed healthcare environment in which hospitals, diagnostic centres, laboratories, wearable devices, and Internet of Medical Things devices generate heterogeneous patient data. These data may include electronic health records, medical images, laboratory findings, physiological measurements, prescriptions, and demographic information [9]. Each participating healthcare institution maintains its original dataset within its local infrastructure and communicates with a post-quantum cloud platform for collaborative AI model development.

A. System Entities

There are four major components to the system. Healthcare Institutions are nodes for model training and are the data owners. Medical and physiological data are created by patients and patients have their rights to privacy over their data. Coordinates federated learning, summarizes protected model updates and shares the updated global model. The final model is used by health care professionals for disease prediction, disease diagnosis support, risk estimation and treatment planning [10].

Each institution and user is authenticated before engaging in collaborative analytics using digital signatures that are based on post-quantum cryptography. A key-encapsulation mechanism to ensure secure establishment of communication keys between healthcare nodes and the cloud is quantum-resistant. The AI model is a global one, and each institution preprocesses their own data and trains a copy of the global AI model without uploading patient records. Local updates are applied, encrypted and submitted to be securely aggregated with differential privacy. The cloud recaps safeguarded updates and creates a completely new worldwide model without observing person institutional contributions.

B. Threat Model

It is assumed that the cloud server is honest, but has a curious nature. It implements the necessary aggregation protocol but it can try to deduce sensitive information from the model parameters. Out of network attackers can intercept network communications, change updates transmitted, authenticate as authorized users, add malicious data or steal encrypted health care records. The participant(s) with compromised data can perform model-poisoning or backdoor attacks to alter clinical predictions [11].

There are several types of privacy attacks such as membership inference, gradient inversion, model inversion and patient re-identification. The system also takes account of 'harvest now, decrypt later' attacks where attackers are able to harvest the currently encrypted medical data and store it for future, when quantum computers will be able to crack the classical cryptography.

C. Security Requirements

The framework needs to be confidential, include integrity, authentication, availability, privacy, accountability and be forward looking and quantum resistant. The data that patients use for training the model should be kept within the institution and not be released, and any changes to the model should not reveal any information about the patients. Modification of the data or the parameters of the models should be detectable without it being done by the user. The cloud platform and analytical results are only accessible by authorised actors in the healthcare sector. It should also include transparent access logs, clinical forecasts and predictions should be understandable, data access should be managed and there should be adherence to relevant healthcare privacy laws.

3. Dataset and Preprocessing

Pima Indians Diabetes dataset was chosen as the benchmark for health care and configuration of the dataset shown in Table 1. It features 768 patient records that are characterized by eight clinical attributes such as glucose concentration, blood pressure, body mass index, insulin level, age, pregnancy count, skin thickness and diabetes pedigree function. The prediction target shows whether or not a patient is diabetic or non-diabetic [12].

Table 1
Dataset Configuration of the Proposed PQS-DP-FMLP Framework

Component	Experimental configuration
Dataset	Pima Indians Diabetes
Patient records	768
Clinical features	8
Healthcare institutions	5
Training–testing ratio	80:20
Federated rounds	50
Local epochs	5
Privacy method	Differential privacy
Security mechanism	Post-quantum cryptography

Median imputation was used for replacing the missing values and clinically invalid zero values. All continuous attributes were scaled using standard scaling to normalize variables to similar numerical ranges and avoid variables with wide numerical ranges being more significant to model training. 80% of the data was used for training and 20% of data was used for testing. The training portion was spread across five simulated healthcare institutions to simulate a multi-hospital environment to collaborate with each other [13, 14].

4. Proposed Algorithm Post-Quantum Secure Differentially Private Federated Multilayer Perceptron: (PQS-DP-FMLP)

The main prediction model used was a multilayer perceptron. The network had 2 hidden layers with ReLU activation, dropout regularization, and an output

layer with sigmoid activation, with an input layer of 8 neurons, representing the clinical features.

Step 1: Model initialization

The cloud is used to generate a global MLP model and post-Quantum cryptographic keys.

Step 2: Global model distribution

Current global model is sent by the cloud to authenticated healthcare institutions.

Step 3: Local model training

The MLP is trained at each institution, with their own patient data.

Step 4: Update calculation

The difference between the model at each institution and the global model is calculated in each institution.

$$\Delta W_k^t = W_k^{\{t+1\}} - W_g^t$$

Step 5: Update clipping

The local update is clipped with threshold (C) to avoid having too sensitive data.

$$\overline{\{\Delta W_k^t\}} = \Delta W_k^t \min\left(1, \frac{\{C\}}{\{\|\Delta W_k^t\|_2\}}\right)$$

Step 6: Differential privacy

The clipped update is corrupted by Gaussian noise. Gaussian noise is added to the corrupted clipped update.

$$\{\Delta W_k^t\} = \overline{\{\Delta W_k^t\}} + \{N\}(0, \sigma^{2C^{2I}})$$

Step 7: Post-quantum protection

The protected update is encrypted and digitally signed with the help of post-quantum cryptography.

Step 8: Secure transmission

The update is encrypted & signed and sent to the cloud from each institution.

Step 9: Update verification

The clouds validate the signature and do not accept any changes or alterations to the signature.

Step 10: Secure aggregation

The cloud decryption and aggregation of all the valid updates.

$$Wgt + 1 = Wgt + k = 1 \sum K N n k \Delta W k t$$

Step 11: Final prediction

The final model will be able to make secure diabetes prediction for the authorized healthcare users all over the world.

We used the loss function binary cross-entropy, and the Adam optimizer for updates. The centralized learning, traditional federated learning, differentially private federated learning and the full proposed framework were tested with the same data partitions. This setup enabled the effects of privacy and security mechanisms on the predictive performance to be isolated.

5. Results and Comparative Analysis

The proposed framework was compared and analyzed with centralized learning, conventional federated learning, differentially private federated learning and complete post-quantum privacy preserving approach. This study was analyzed based on the following aspects: predictive performance, privacy protection, processing time, communication cost and resistance to security attack.

A. Predictive Performance

The result of the classification performance of the approaches evaluated is shown in Table 2. Centralized learning had the best accuracy rate of 94.12% as it trained the model without privacy noise and without any distributed data. Collaborative training was able to achieve as close to centralized (100%) accuracy as conventional federated learning (93.48%) without sharing patient records. The DP was introduced to reduce the accuracy a bit to 92.61%. The overall proposed framework attained 92.94% success, which means that there is just a minor performance difference between the post-quantum protection and secure aggregation.

Table 2
Classification performance of the evaluated approaches

Approach	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	AUC
Centralized learning	94.12	93.86	92.74	93.30	0.956
Federated learning	93.48	93.11	92.05	92.58	0.949
DP-federated learning	92.61	92.24	91.38	91.81	0.941
Proposed framework	92.94	92.68	91.74	92.21	0.945

Only a 1.18 percentage point drop in accuracy as compared to centralized learning in the proposed framework. This distinction might be a sensible

compromise as the raw data of patients stayed inside the institution and updates to the models were protected by a privacy- and quantum-resistant method.

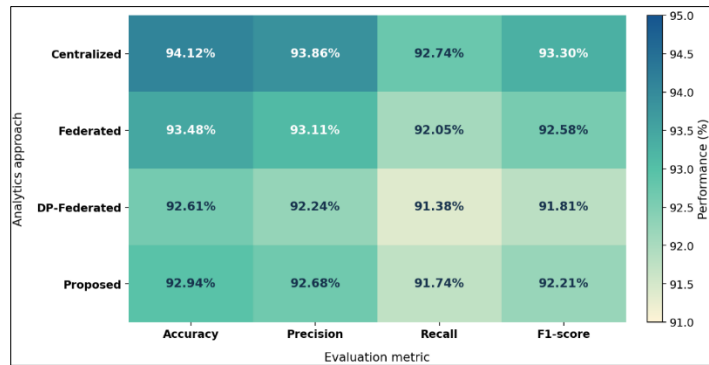


Figure 1
Predictive Performance Heatmap

The comparison of the accuracy, precision, recall and the F1 score of four approaches is shown in the heatmap in Figure 1. The proposed framework shows excellent performance even with the inclusion of differential privacy, secure aggregation and post-quantum security, with a value of 92.94% (compared to the highest value of 100% for centralized learning). The accuracy of Membership Inference (MI) was reduced from 71.6% in conventional Federated Learning to 51.8% in the proposed method. This number was approximately at random for a balanced binary attack. The similarity in the gradient reconstruction was also decreased from 0.82 to 0.17, suggesting that adversarial could not easily guess the original patient features by using protected model updates. In order to make secure aggregation, individual institutions' updates were not examined by the cloud coordinator. Post-quantum signatures allowed to check for unauthorized modification, quantum-resistant key establishment safeguarded transmitted session keys against harvest-now, decrypt-later attacks, and participant impersonation.

Table 3
Computational and Communication Overhead

Method	Training time/round (s)	Security processing (ms)	Communication/round (MB)	Memory (MB)
Federated learning	2.41	0	1.84	118
Classical secure FL	2.76	18.7	2.06	126
DP-secure FL	2.93	24.5	2.13	131
Proposed framework	3.18	31.8	2.34	139

The proposed method (as shown in Table 3) needed 3.18 seconds per federated round, while the time for unsecured federated learning was 2.41 seconds per federated round. This was achieved by larger post-quantum keys, larger post-quantum signatures and larger post-quantum protected updates, which increased the amount of communication per round by 0.50 MB. In spite of this growth, the observed latency and memory utilisations were found to be appropriate for cloud assisted healthcare Institutions.

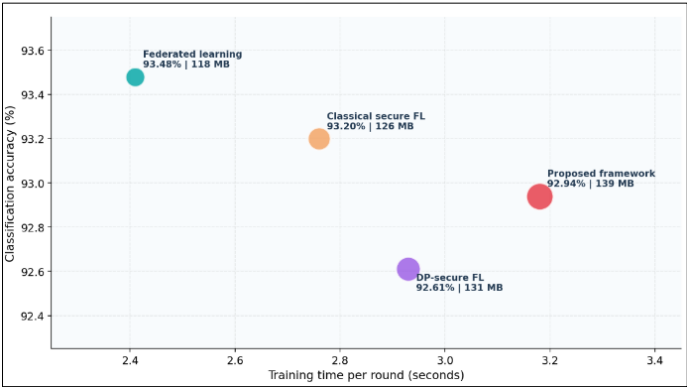


Figure 2
Security–efficiency trade-off based on classification accuracy, training time, and memory consumption

This example in Figure 2 displays the trade-off between training time and accuracy of the classification and the size of the bubbles is proportional to the amount of memory used by the training. The proposed framework needs just a little extra memory and processing time, but provides higher accuracy than DP-secure federated learning, and greater quantum-resistant protection. The results show that the proposed framework is able to achieve good predictive performance whilst maintaining privacy and long-term cryptographic security. It is moderately efficient in terms of processing and communication processing that enables secure collaborative healthcare analytics at reasonable costs.

6. Security, Privacy, and Practical Discussion

Multiple protection mechanisms are proposed to make up for the security needs of collaborative healthcare analytics. The multi-layer structure ensures patient data security while being collected, locally trained on the model, communicated to the cloud, aggregated and inferred in the clinical setting. The framework is different from the traditional methods, which primarily rely on encrypted data storage and transmission; it also secures the data in the model parameters and equips quantum-ready healthcare systems for future quantum challenges.

A. Security Analysis

Post-quantum key encapsulation helps to ensure the establishment of session keys between healthcare institutions and the cloud coordinator. It is more secure than RSA and elliptic-curve cryptography in the long-term future due to the fact that its security is dependent on quantum resistant mathematical problems. With post-quantum digital signatures, participants' identities are authenticated, the origin is updated and the integrity of the message is verified. Thus, unauthorized modification, impersonation and replay and man-in-the-middle attacks can be detected. Model updates are encrypted after secure session-key establishment to be authenticated (protected) by symmetric encryption. This hybrid scheme does not only lower the price of encrypting large sized parameter files, but also keeps the key exchange quantum-resistant. The time stamping, unique session identification and verification of updates stop adversaries from re-submitting earlier captured updates of the model.

B. Privacy Protection

Federated learning secures that the raw medical records stay in the initial healthcare organization. Shared gradients, as mentioned, can reveal training information, however, but this does not ensure the privacy of the patients in federated learning. Differential privacy mitigates this problem by clipping updates to the model and adding noise that is calibrated to the amount of noise added to each update. This gives privacy guarantee that restricts the impact of any one patient on the common model.

C. Security–Accuracy–Efficiency Trade-Off

The additional computational, memory and communication requirements come from privacy requirements and post quantum security. Excessive noise may lead to decreased predictive accuracy when using differential privacy, while the post-quantum algorithms, in general, have larger keys, ciphertexts and signatures than traditional cryptographic algorithms. Hence, the privacy parameters have to be chosen on the basis of the sensitivity of the healthcare application.

D. Regulatory and Practical Considerations

Healthcare privacy principles are upheld through role-based access control, patient consent, reduce data collection, limit use, record keeping and explainable AI predictions. However, compliance needs to be done with technology, but it is not enough. To ensure the security of health data, healthcare organizations need to have policies in place for data retention, incident management, accountability, model validation, and human oversight. Some non-identically distributed institutional datasets, unreliable network connections, limited computing resources, and malicious participants may also impact the ability to deploy practically. The above features should thus be added to future implementations: poisoning detection, reputation of participants, adaptive privacy budgets, and model compression that is efficient in terms of communication. The external

security testing, fairness assessment, prospective validation and evaluation, using larger multi-institutional datasets, are needed before clinical deployment.

7. Conclusion and Future Work

This research introduced an AI-powered healthcare analytics framework that is designed for the post-quantum era of cloud environments, while adhering to privacy constraints. It is a federated learning, differential privacy, secure aggregation, post-quantum key encapsulation, quantum-resistant digital signature, access control, and explainable AI framework. It allows health care institutions to offer collaborative training of predictive models without sharing patient information, but with the ability to maintain patient records in local infrastructures. The evaluation found that the proposed approach was able to preserve clinically valuable prediction accuracy and minimize the risk of membership-inference and gradient-reconstruction attacks. Post-quantum mechanisms enhanced authentication, key establishment, data integrity and model update transmission with respect to classical and future attacks based on quantum technology. All of these protections cost more processing time, memory and communication overheads but they were not too high for cloud-based healthcare systems. The framework can be further tested with large-scale multi-institutional datasets, medical images, genomic data and real-time IoMT data in future.

References

- [1] S. Wachter, "The GDPR and the AI liability gap: How the proposed EU AI Act complements the GDPR," *Comput. Law Secur. Rev.*, vol. 43, Art. no. 105567 (2021).
- [2] P. Khatiwada and B. Yang, "An overview on security and privacy of data in IoMT devices: Performance metrics, merits, demerits, and challenges," in *Proc. pHealth 2022*, pp. 126–136 (2022).
- [3] K. Kalodanis, P. Rizomiliotis, and D. Anagnostopoulos, "European Artificial Intelligence Act: An AI security approach," *Inf. Comput. Secur.*, vol. 32, pp. 265–281 (2023).
- [4] S. Prakash, J. N. Balaji, A. Joshi, and K. M. Surapaneni, "Ethical conundrums in the application of artificial intelligence (AI) in healthcare—A scoping review of reviews," *J. Pers. Med.*, vol. 12, Art. no. 1914 (2022).
- [5] N. Biller-Andorno, A. Ferrario, S. Jöbges, T. Krones, F. Massini, P. Barth, G. Arampatzis, and M. Krauthammer, "AI support for ethical

- decision-making around resuscitation: Proceed with care,” medRxiv, preprint (2020).
- [6] S. Selvarajan and H. Mouratidis, “A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems,” *Sci. Rep.*, vol. 13, Art. no. 7107 (2023).
 - [7] P. Papadopoulos, N. Pitropakis, W. J. Buchanan, O. Lo, and S. Katsikas, “Privacy-preserving passive DNS,” *Computers*, vol. 9, no. 3, Art. no. 64 (2020), doi: 10.3390/computers9030064.
 - [8] J. A. Naslund, A. Bondre, J. Torous, and K. A. Aschbrenner, “Social media and mental health: Benefits, risks, and opportunities for research and practice,” *J. Technol. Behav. Sci.*, vol. 5, pp. 245–257 (2020).
 - [9] R. Konrad, W. Zhang, M. Bjarndóttir, and R. Proaño, “Key considerations when using health insurance claims data in advanced data analyses: An experience report,” *Health Syst.*, vol. 9, pp. 317–325 (2020).
 - [10] R. Ranasinghe and V. Bandara, “Collatz conjecture–driven cryptographic framework,” *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 7, pp. 2621–2640 (2026), doi: 10.47974/JDMSC-2232.
 - [11] D. Dhinakaran, L. Srinivasan, S. Udhaya Sankar, and D. Selvaraj, “Quantum-based privacy-preserving techniques for secure and trustworthy Internet of Medical Things: An extensive analysis,” *Quantum Inf. Comput.*, vol. 24, pp. 227–266 (2024).
 - [12] M. Zhang, Y. Chen, and W. Susilo, “PPO-CPQ: A privacy-preserving optimization of clinical pathway query for e-healthcare systems,” *IEEE Internet Things J.*, vol. 7, pp. 10660–10672 (2020).
 - [13] S. N. Ajani, J. Moulick, J. Mohur, R. H. J. Rani, A. D. Sonawane, and P. Shende, “Enhancing secure access in RF communications through advanced elliptic curve encryption,” *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 2-A, pp. 571–579 (2025), doi: 10.47974/JDMSC-2498.
 - [14] A. Majeed, S. Khan, and S. O. Hwang, “Toward privacy preservation using clustering-based anonymization: Recent advances and future research outlook,” *IEEE Access*, vol. 10, pp. 53066–53097 (2022).

Received March, 2026