Sparkling Light Publisher

Sparklinglight Transactions on Artificial Intelligence and Quantum Computing

journal homepage: https://sparklinglightpublisher.com/

# Privacy Preserving Medical Image Inference Portal Using Homomorphic Encryption

Akhil P [a], Steephen M V [b], Lavita Wilma Lobo [c]

[a] *Student, Department of Master of Computer Applications, Shree Devi Institute of Technology, Mangaluru, India*
[b] *Student, Department of Master of Computer Applications, Shree Devi Institute of Technology, Mangaluru, India*
[c] *Assistant Professor, Department of Master of Computer Applications, Shree Devi Institute of Technology, Mangaluru, India*

**Abstract**

The growing reliance on AI for medical image analysis presents important privacy risks when patient data is processed on external servers. To solve this problem, we suggest a Privacy- Preserving Medical Image Inference Portal that uses Homomorphic Encryption (HE) to keep sensitive images encrypted while they are being processed. The system lets users upload encrypted medical images that a neural network processes without decrypting them, which keeps privacy safe. A lightweight model that is optimized for encrypted operations strikes a balance between accuracy and speed of computation. The portal has an easy-to-use interface for safe uploads and result retrieval, showing that advanced cryptography can be used in healthcare di- agnostics. This work shows a safe way to use AI in medical imaging that protects both privacy and usefulness.


*Keywords:* Convolutional Neural Network (CNN); CKKS Encryption Scheme; Homomorphic Encryption; Medical Image Analysis

## 1. Introduction

As artificial intelligence (AI) becomes more common in healthcare, keeping private medical information safe is becoming a big worry. Conventional AI systems handle data in plaintext, which leaves it vulnerable to security lapses and illegal access. This project addresses the issues by performing inference on encrypted medical images using a custom convolutional neural network (ConvNet) in conjunction with homomorphic encryption. By using this technique, you can perform mathematical operations on encrypted but undecrypted data, preserving patient privacy all along the way. Since most medical image analysis systems currently in use process data in plaintext, they are susceptible to privacy violations.

*E-mail address of authors: akhil91202@gmail.com,stephenmv1@gmail.com,lavita@sdit.edu.in*


Please cite this article as: Akhil P, et al., Privacy Preserving Medical Image Inference Portal Using Homomorphic Encryption, Sparklight Transactions on Artificial Intelligence and Quantum Computing (2025), 5(2), 51-56. **ISSN (Online):2583-0732.**
Received Date: 2025/07/15, Reviewed Date: 2025/07/25, Published Date: 2025/09/05.

Some techniques fail to secure data during computation, even though they employ encryption during transmission. Although homomorphic encryption has been studied, its practical application in actual healthcare settings is limited by its scalability issues, high computational costs, and decreased accuracy. In addition to providing accurate diagnostic results, the method ensures data confidentiality, making it a reliable solution for safe and legal medical image analysis. The proposed system integrates homomorphic encryption with a custom convolutional neural network (HECNN) to enable secure medical image inference. By performing computations directly on encrypted data, it ensures patient confidentiality without compromising diagnostic accuracy. The system includes a web-based portal for seamless interaction, end-to-end encryption, and regulatory compliance (GDPR/HIPAA), offering a practical, efficient, and privacy-preserving solution for medical diagnostics.

## 2. Literature Review

### *2.1. Related Works*

Dutil et al. [1] discuss by using homomorphic encryption (HE) in medical imaging in their paper "Application of Homomorphic Encryption in Medical Imaging". The study explores the feasibility of employing HE to perform secure medical image analysis while preserving patient privacy. They highlight the challenges of computational overhead and propose methods to optimize HE schemes for real-world medical datasets. The paper emphasizes the importance of balancing privacy and efficiency in secure healthcare systems.

Arimitsu and Otsuka present a privacy-preserving approach to linear equation solving using fully homomorphic encryption (FHE) in their work "Privacy-Preserving Fast and Exact Linear Equations Solver with Fully Homomorphic Encryption"[2]. The proposed method demonstrates how FHE can enable exact solutions for encrypted data while preserving privacy. This study addresses computational efficiency and highlights the practical application of FHE in privacy-sensitive computations, including medical imaging.

Chen et al. introduce a hybrid scheme combining HEAAN and FV encryption methods in their paper "When HEAAN Meets FV: A New Somewhat Homomorphic Encryption with Reduced Memory Overhead"[3]. This approach help overcome one of the major drawbacks of existing homomorphic encryption methods, high memory usage. By making the system more memory efficient, the study lays the ground for building scalable and practical HE applications in medical imaging.

Research in privacy-preserving medical imaging shows that homomorphic encryption can securely process sensitive data. However, most existing methods face challenges such as high computational costs, limited scalability, and reduced accuracy. Although some optimized schemes and hybrid models have been proposed, many are still at the proof of concept stage. This marks the need for a practical solution that can effectively balance privacy, efficiency, and reliable diagnosis.

## 3. Methodology

The methodology adopted in this project is created to ensure both data security and diagnostic accuracy in medical image analysis. The process begins with requirement analysis, identifying the need for patient privacy, model accuracy, and computational efficiency. Based on this, the system architecture is divided into three components: the client-side, which handles image upload, preprocessing, and encryption; the server-side, which performs inference on encrypted data using a custom Homomorphically Encrypted Convolutional Neural Network (HECNN); and the web interface, which allows healthcare providers to interact with the system. Medical images are first pre-processed through steps like resizing, converting to grayscale, normalizing, and flattening to ensure consistency. These prepared images are then encrypted using the CKKS homomorphic encryption scheme, which protects sensitive patient data throughout the process. The HECNN model is tailored for encrypted computation by replacing standard operations with polynomial based activations that work well with encryption. Inference takes place entirely within the encrypted domain, ensuring there is no risk of data exposure. The system was developed iteratively, with prototypes, modular

testing, and parameter tuning to strike the right balance between accuracy and efficiency. To support real-world use, a Flask based web portal was created, allowing healthcare professionals to easily upload medical images, run encrypted analysis, and securely view the results. Finally, decryption is applied only to the output stage, Making sure patient information stays protected throughout the workflow. This structured methodology guarantees a privacy-preserving, regulation-compliant, and efficient diagnostic pipeline, giving medical professionals accurate results while maintaining the confidentiality of medical records.

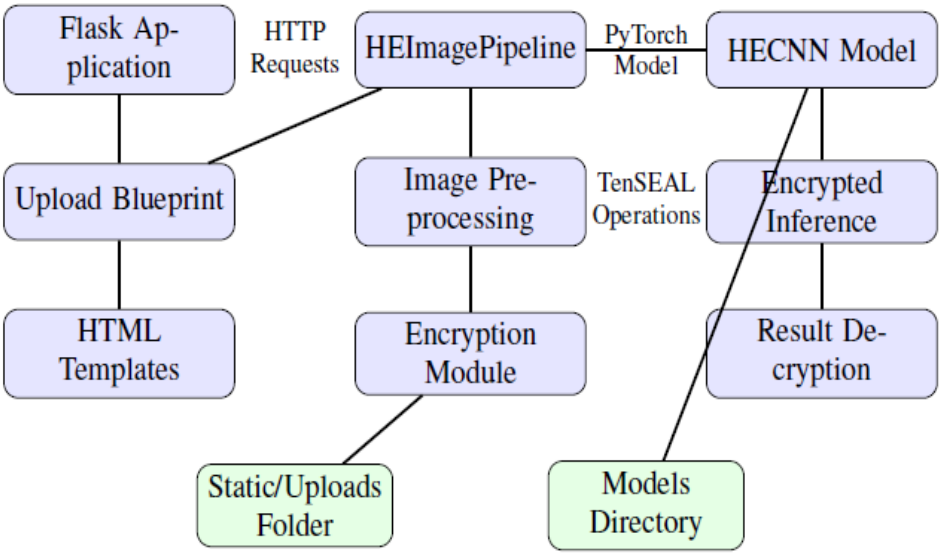


Fig. 1. System Architecture

## 4. Result and Analysis

The experimental outcomes indicate that the proposed system effectively balances privacy and diagnostic performance. While encryption Introduces additional computational overhead, the optimized light weight neural network helped maintain practical response times. The encrypted inference achieved accuracy level closed to plain text models, demonstrating that security did not significantly compromise diagnostic reliability.

*Random Forest*

The outcome of the Random Forest model shows a high capacity for prediction with balanced generalization between training and testing phases. The test accuracy of 87.12% and train accuracy of 87.38% indicate that the model avoids significant overfitting while maintaining consistency across datasets. The recall value of 0.86 shows how well the model can detect positive examples, while the precision of 0.88 highlights its accuracy in predicting true positives without excessive false alarms. The resulting F1-score of 0.87 confirms a good balance between precision and recall. Moreover, the low test loss (0.3132) and train loss (0.3113) further reinforce the model's reliability. The Root Mean Square Error (RMSE) of 0.46 indicates that the deviations between predicted and actual values remain minimal, showcasing the robustness of the Random Forest approach for this task.

Table. 1. Performance metrics of the trained model.

| Metric | Value |
|---|---|
| Test Loss | 0.3132 |
| Test Accuracy | 87.125 |
| Train Loss | 0.3113 |
| Train Accuracy | 87.38% |
| Recall | 0.86 |
| Precision | 0.88 |
| F1-Score | 0.87 |
| RMSE | 0.46 |

*Confusion Matrix for Random Forest*

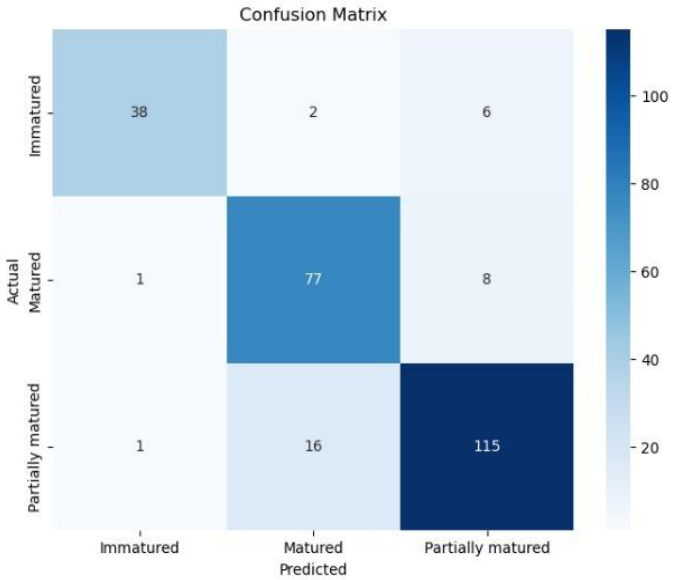


Fig. 2. Confusion Matrix for Random Forest

## 5. Discussions

The project presents a significant advancement by fusing the advantages of deep learning and homomorphic encryption in the area of privacy-preserving medical image analysis. In existing systems, patient images are often exposed at different stages of processing, making them vulnerable to misuse or unauthorized access. This system ensures that medical images remain encrypted from the moment they are uploaded until the final results are delivered, removing the risk of data leaks. By using the CKKS encryption scheme, it allows mathematical operations to be performed directly on encrypted data, maintaining patient confidentiality without disrupting the diagnostic process. A key contribution of this work is the development of a custom Homomorphically Encrypted Convolutional Neural Network (HECNN), which adapts traditional neural network functions into encryption-friendly forms, such as polynomial activation functions. By finding a balance between diagnostic accuracy and computational speed, this work addresses one of the major shortcomings observed in previous studies. A Flask-based web portal was created to enable the system to be used in actual healthcare settings, providing healthcare

providers with user friendly platform for safe and dependable diagnostics. Effective model design, parameter optimization, and the choice of appropriate encryption schemes minimize the memory and processing overhead that comes with encryption. The system's adherence to privacy laws like GDPR and HIPAA is one of its main advantages, making it ideal for clinical applications, particularly in telemedicine and remote diagnosis. Overall, this project shows that AI-driven diagnostics can be accurate and safe, providing a useful framework that promotes more study and use in medical imaging that protects privacy.

## 6. Conclusion and Future Work

The project demonstrates a practical and secure approach to medical image analysis by integrating homomorphic encryption with a customized convolutional neural network. Unlike traditional systems that risk exposing sensitive data during computation, this work keeps medical images encrypted throughout the entire inference pipeline, ensuring confidentiality and compliance with strict privacy standards. By integrating the CKKS encryption scheme with an encryption aware neural network, the system delivers accurate predictions while maintaining data security. The inclusion of a user friendly web portal makes the solution more practical, enabling healthcare providers to easily upload medical images, perform encrypted analysis, and retrieve secure results. While encryption does add some processing and computational overhead, these challenges are minimized through the use of a lightweight model design and optimized parameters, ensuring a balance between efficiency and privacy. This work directly responds to the urgent need for protecting patient information in AI powered healthcare and establishes a foundation for applications such as telemedicine, secure remote diagnostics, and large scale medical data management. Ultimately, it shows that encrypted computation can deliver both accuracy and security, encouraging larger adoption of privacy focused technologies in modern medical practice.

Although this project lays the groundwork for secure medical image inference, there is still significant scope for future exploration. Expanding the system to handle larger datasets and a wider range of imaging types such as CT and MRI would strengthen its relevance in real clinical settings. Further improvements in homomorphic encryption could help reduce delays and computational demands, making the solution more practical for time critical diagnostics. Deploying the framework on cloud platforms and combining it with federated learning would not only improve scalability but also promote collaborative research while preserving patient confidentiality. In addition, experimenting with advanced deep learning models and hybrid techniques that work seamlessly with encrypted computation could boost both performance and efficiency. Collectively, these advancements would help transform the system into a robust, real world solution for secure AI powered healthcare.

## References

[1] Micciancio, D., and Polyakov, Y., "Bootstrapping in FHEW-like Cryptosystems," in *Proc. Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC '21)*, 2021. DOI: 10.1145/3474366.3486924.

[2] Chen, H., Iliashenko, I., and Laine, K., "When HEAAN Meets FV: a New Some- what Homomorphic Encryprtion with Reduced Memory Overhead," *Cryptology ePrint Archive*, Paper 2020/121, 2020. [Online]. Available: https://eprint.iacr.org/2020/121.

[3] Arimitsu, K., and Otsuka, K., "Privacy-Preserving Fast and Exact Linear Equations Solver with Fully Homomorphic Encryption," *Cryptology ePrint Archive*, Paper 2020/272, 2020. [Online].

[4] Available: https://eprint.iacr.org/2020/272.

[5] Lin, Y.-T., and Chen, Y.-N., "An Empirical Study of Cross-Lingual Transferability in Generative Dialogue StateTracker,"*arXiv preprint arXiv;preprint arXiv:2101.11360*,2021.[online].

[6] Available:https://arXiv.org/abs/2101.11360.

[7] Xu, J., Wu, T., Shen, W., & Zhang, Y. (2023). **LHDNN: Low-Degree Hermite Deep Neural Network for Encrypted Inference.** *Applied Sciences, 13*(8), 4815. https://doi.org/10.3390/app13084815.

[8] Boemer, F., Costache, A., Cammarota, R., & Wierzynski, C. (2019). **nGraph-HE2: A High-Throughput Framework for Neural Network**

**Inference on Homomorphically Encrypted Data.** *arXiv preprint arXiv:1901.10074*. https://arxiv.org/abs/1901.10074.

[9] Li, Y., Wu, J., He, J., & Chen, J. (2024). **Privacy-Preserving Federated Learning for Encrypted Dermoscopic Diagnosis.** *Journal of Biomedical Informatics, 156*, 104615. https://pubmed.ncbi.nlm.nih.gov/40489276/

[10] Hussain, F., Rathore, M. M., Park, H., & Hong, C. S. (2023). **Energy-Efficient and Secure Neural Network-Based Disease Detection for Mobile Healthcare.** *ACM Transactions on Internet Technology, 23*(3), 1–22. https://doi.org/10.1145/3585536.

[11] Xie, L., Chen, Y., & Wang, J. (2023). **Secure CNN Inference Using Homomorphic Encryption.** *Applied Sciences, 13*(10), 6117. https://doi.org/10.3390/app13106117.

[12] Hesamifard, E., Takabi, H., & Ghasemi, M. (2019). **Deep Neural Networks on Encrypted Data.** *Journal of Emerging Technologies in Computing Systems (JETC), 15*(3), 1–26. https://doi.org/10.1145/3316481

******

**ISSN (Online):2583-0732**