Chapter 7
Enhancing Machine Learning Efficiency Through Secure Medical Image Sharing

M. Rajkumar
Vellore Institute of Technology, India

Niladri Maiti
https://orcid.org/0000-0001-8014-0342
School of Dentistry, Central Asian University, Tashkent, Uzbekistan

Riddhi Chawla
School of Dentistry, Central Asian University, Tashkent, Uzbekistan

Ripal Ranpara
https://orcid.org/0000-0002-5823-5406
Faculty of Computer Application, Marwadi University, India

R. Yogitha
https://orcid.org/0000-0001-9880-8750
Sathyabama Institute of Science and Technology, India

Pallavi Sagar Deshpande
https://orcid.org/0000-0002-2203-5867
Bharati Vidyapeeth, India

Aakifa Shahul
SRM Medical College, India

ABSTRACT

The development of machine learning applications in the healthcare industry depends on safe medical image sharing. Protecting patient privacy is more difficult but necessary as medical imaging data grows. This paper investigates how to integrate encryption techniques and secure data-sharing methods, like blockchain, to facilitate cross-organizational collaboration while maintaining data privacy. Sensitive patient data is kept in local systems thanks to collaborative models like federated learning,

DOI: 10.4018/979-8-3693-9821-0.ch007

which enable institutions to train machine learning algorithms on decentralized datasets. This strategy makes use of the variety of data available across healthcare facilities while protecting the privacy of medical records. The creation of machine learning models for diagnosis and treatment planning that are more reliable and accurate is made possible by the safe interchange of medical images.

INTRODUCTION

Machine learning models are being used more and more in medical image analysis to diagnose diseases and plan treatments. However, access to sizable, varied datasets is necessary for these models to function well and be accurate (Pandey, B. K., & Pandey, D., 2025). Strict privacy laws pertaining to medical data, like HIPAA and GDPR, which restrict the sharing of patient information, including medical images, present a significant obstacle to the creation of such datasets. Beyond these constraints, secure medical image sharing is critical to improving machine learning effectiveness. Encryption techniques, which safeguard patient privacy and guarantee that only authorized parties can access medical images, are among the main solutions for safe sharing. Federated learning is a newer method that allows collaboration without direct data sharing by training machine learning models locally at different healthcare facilities. This decentralized setup (Khadka, M. et al., 2025) preserves privacy while still allowing institutions to benefit from larger datasets because only model updates rather than the actual data are shared between them. Artificial neural network (Pandey, B. K., & Pandey, D., 2023) based blockchain technology also provides a means of guaranteeing traceable, transparent, and safe image sharing amongst healthcare systems. Data integrity is maintained by recording any modifications or access to medical images on blockchain's immutable ledger. Another method that enables multiple institutions to work together on machine learning model training while maintaining the privacy of their data is secure multi-party computation (MPC) (Sheela, M. S. et al., 2025). Secure medical image sharing improves the performance of machine learning models by providing access to larger datasets. This is essential for developing more generalized models that are capable of identifying illnesses in a range of demographics. A greater variety of data sources improves convergence and model accuracy, increasing the overall effectiveness of machine learning (Satheesh, N. et al., 2025) in medical diagnostics. In the end, safe medical image sharing will spur advancements in artificial intelligence in healthcare, guaranteeing improved patient outcomes and more precise diagnostic instruments