Chapter 5
Secure Healthcare Data Sharing Using Federated Learning, Blockchain, and Quantum Cryptography

M. Srivarshini
https://orcid.org/0009-0009-1621-1172
Avinashilingam Institute for Home Science and Higher Education for Women, India

R. Vanithamani
https://orcid.org/0009-0006-2767-3629
Avinashilingam Institute of Home Science and Higher Education for Women, India

ABSTRACT

Secure exchange of patient healthcare data is vital due to the rise of AI in the medical field. However, this advancement introduces challenges such as data breaches, privacy violations, and regulatory demands. Traditional centralized systems store all data in one location, increasing cyberattack risks. This study proposes a secure framework integrating Federated Learning, Blockchain, and Quantum Cryptography. Federated Learning enables decentralized model training without sharing raw data, preserving patient privacy. Blockchain ensures data integrity using an immutable distributed ledger. Quantum Key Distribution (QKD) and AES-256 encryption protect data during transmission and storage. Files are stored in the InterPlanetary File System (IPFS), and their unique Content Identifiers (CIDs) are recorded on the blockchain for tamper-proof verification. Only users with valid quantum-generated keys can decrypt and access the data, ensuring strong privacy and security.

DOI: 10.4018/979-8-3373-3551-3.ch005

1 INTRODUCTION

In today's digital world, the healthcare industry generates and manages an enormous amount of data every day. These data were obtained from various sources, including hospitals, clinics, laboratories, pharmacies, insurance companies, and wearable health devices. This includes patient demographics, medical histories, prescriptions, diagnostic test results, treatment records, and even real-time monitoring data from devices like fitness bands or heart rate monitors. Managing such a large volume of sensitive and varied information is not easy. This requires secure storage, efficient processing, and reliable sharing mechanisms so that doctors, nurses, and other medical professionals can access the right information at the right time. The traditional centralized systems used to store and share patient data pose multiple risks. When data is stored on a single server or location, they are vulnerable to breach, unauthorized access, and potential manipulation. Moreover, sharing data across institutions often necessitates the transfer of raw patient information, which can lead to privacy violations and legal issues, particularly in light of stringent regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the United States Congress in 1996. It primarily addresses the protection of sensitive patient information and the standardization of healthcare data formats. HIPAA applies to healthcare providers, insurance companies, and any third-party vendors or business associates that handle protected health information (PHI). One of the core components of HIPAA is the Privacy Rule, which establishes a framework for how PHI may be used and disclosed. It provides patients with the right to access their medical records and request amendments if inaccuracies are found. The Security Rule under HIPAA mandates the implementation of physical, administrative, and technical safeguards to ensure that patient data remains confidential and protected from breaches. For example, encryption, access control mechanisms, authentication systems, and activity logs are part of the required safeguards. Another critical aspect of HIPAA is the Breach Notification Rule. This regulation obligates covered entities to notify individuals, the Department of Health and Human Services (HHS), and sometimes the media, in the event of a data breach involving unsecured PHI. Failure to comply with HIPAA regulations can lead to significant fines, penalties, and reputational damage. From the perspective of modern healthcare technology, HIPAA compliance plays a major role in the design and implementation of AI-driven systems. For instance, Federated Learning is an approach that supports HIPAA's privacy goals because it trains machine learning models on decentralized data located at various institu-

Geo Spatial Query System Using Quantum NLP