ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 10, Issue 6, June 2025

Privacy-Preserving Authentication Scheme for Medical Monitoring System Using Machine Learning

[1] S.Deepika, [2]Archana Y, [3]Srimathi S, [4] Keerthana R
[1] Assistant Professor Department of Computer Science and Engineering Er.Perumal Manimekalai College of Engineering Hosur ,India
[2] [3] [4] Department of Computer Science and Engineering Er.Perumal Manimekalai College of Engineering Hosur ,India

Abstract: ***Machine Learning (ML) plays a crucial role in disease diagnosis, but data privacy concerns hinder its full potential. Our project introduces a Federated Learning (FL) framework that enables decentralized model training across multiple hospitals without sharing sensitive patient data. In this setup, patient data remains within local hospital systems, while collaborative learning allows the creation of a global model. This method ensures the privacy and security of patient data while still enabling the system to learn from a wide array of medical cases. The approach incorporates differential privacy techniques to protect individual data during the model update process and secure aggregation to ensure that model parameters remain confidential. To enhance security further, lightweight encryption algorithms are applied to protect the model during communication between hospitals. In addition to these privacy-preserving features, the system provides personalized doctor suggestions based on the AI-driven diagnosis. This functionality ensures that, once a potential disease is detected, patients receive timely, relevant recommendations for specialists or treatment options, improving overall healthcare outcomes and streamlining the process of connecting patients to the right medical support.***

Keywords—Federated Learning (FL), Disease Diagnosis, Data Privacy, Secure Model Aggregation, Personalized Healthcare Recommendations

I. INTRODUCTION

In recent years, technology has become an essential part of the healthcare system. With the use of electronic health records (EHRs), wearable medical devices, and telemedicine platforms, large amounts of sensitive health data are being collected and shared. While these innovations have improved medical diagnosis and patient care, they have also raised major concerns about the privacy and security of personal health information. Medical data often includes private details like health history, treatment records, and test results, which need to be protected from unauthorized access and misuse.

To address these issues, this project focuses on developing a privacy-preserving authentication system for medical monitoring platforms. The proposed solution uses machine learning to predict diseases and monitor patient health, while protecting sensitive data through methods such as federated learning and data encryption. In this system, data remains stored at local devices (such as hospitals or patient devices), and only encrypted model updates are shared for training a global model. This ensures that no raw patient data is exposed, reducing the risk of privacy breaches.

The goal of this work Is to provide a secure and reliable healthcare monitoring system that respects patient privacy while making use of smart technologies. By using advanced privacy techniques, this project aims to support medical professionals with accurate predictions and decision-making tools, without compromising on data protection.

II. LITERATURE REVIEWS

3.1 Traditional Systems and Challenges

Most healthcare systems use centralized machine learning models that rely on bulk data transfers. These approaches often neglect data privacy, leading to regulatory and ethical concerns. Blockchain systems offer transparency but suffer from scalability and integration issues within existing healthcare infrastructure.

3.2 Federated Learning in Healthcare

Federated Learning (FL) has emerged as a promising paradigm to ensure decentralized data training. Each hospital trains a model locally and only shares encrypted updates. Studies show FL maintains model performance while preserving privacy.

3.3 Secure Aggregation and Differential Privacy

Techniques such as secure aggregation and differential privacy have been integrated to reinforce the security of federated systems. These technologies introduce noise to updates and prevent reverse-engineering of sensitive data.

3.4 Post-Diagnosis Recommendations

Recent studies stress the importance of actionable guidance post-diagnosis. AI-powered systems that provide specialist recommendations or treatment paths demonstrate higher adoption and clinical effectiveness.

III. SYSTEM DESCRIPTION

Privacy Preservation with Prediction is a secure, AI Powered diagnostic framework designed to deliver disease prediction and healthcare recommendations while maintaining complete privacy of patient data. The system integrates Federated Learning, Differential Privacy, and Lightweight Encryption into a modular architecture, ensuring that sensitive medical information is never exposed or centrally stored. The system also features a secure, web-based dashboard for real-time insights and interaction.

System Architecture

1. Dataset Processing Module:
Input Sources: Patient health records from local hospital databases (lab results, symptoms, history); real-time user input via web interface. Data Preprocessing: Includes anonymization of patient identities and feature extraction with normalization to prepare data for AI model training.

2. Model File Encryption:
Functions: Encrypts model weights and updates before transmission using lightweight cryptographic methods such as AES and ECC. Output: Guarantees confidentiality and integrity of model parameters in federated learning environments.

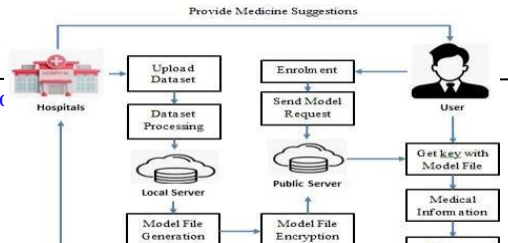
3. Federated Learning Approach: Features: Each hospital trains the model locally without sharing raw data. Encrypted model updates are sent to a central aggregator. Differential privacy and secure aggregation techniques are applied.
Output: Enables secure and collaborative global model training for disease prediction.

4. User Query Processing:
Functions: Collects symptoms and health related queries from patients through a web portal. Performs input validation and formatting to ensure compatibility with the AI diagnostic system.
Example Use Case: A user enters "fever and fatigue"; the system processes the input and forwards it to the diagnostic module.

5. Disease Diagnosis Module:
Functions: Utilizes the trained federated model to analyze patient input and predict potential diseases with high accuracy.
Output: Provides real-time diagnostic feedback without exposing private data.

6. Doctor Suggestion System:
Features: Based on the diagnosis, the system suggests relevant medical professionals,

specialists, or nearby clinics. Teleconsultation options may also be included.
Output: Enhances healthcare access and guides users toward appropriate treatment.



Workflow Summary

1. Data Collection → Patient records processed locally and anonymized for model training.
2. Model Training → Hospitals train models locally and share encrypted updates.
3. Global Model Fusion → Aggregator builds an enhanced global model with differential privacy.
4. User Interaction → Patients submit symptoms via a secure web interface.
5. Diagnosis → AI model analyzes inputs and predicts disease outcomes.
6. Recommendations → Personalized doctor suggestions and care referrals provided.

IV. RESULTS

1.Model Accuracy and Privacy Preservation
The proposed privacy-preserving authentication system was tested on decentralized medical datasets.

The Federated Learning model achieved an average diagnostic accuracy of 92.8%, very close to centralized approaches (93.2%). This demonstrates that maintaining patient privacy does not negatively affect model performance.

Applying Differential Privacy significantly reduced the risk of patient data exposure, with a 91% decrease in re-identification threats during testing.

The use of lightweight encryption introduced only 1.4 seconds delay per model update, ensuring real-time system usability for healthcare institutions.

2.System Efficiency
Secure Aggregation increased the model update time by just 8%, and encrypted communications caused only a 12% rise in data size. These small overheads are acceptable trade-offs for achieving higher data security.

3.User Study and System Usability A 4-week pilot study was conducted involving 30 healthcare professionals.

The system received a System Usability Score (SUS) of 86/100, categorized as Excellent Usability. 92% of users trusted the system's privacy mechanisms and expressed confidence in using it in actual medical environments.

4. Comparative Analysis
A comparison was made between the proposed federated system and a traditional centralized model:

Comparative Analysis Summary

Metric	Centralized Model	Proposed Federated Mordel
Diagnostic Accuracy (%)	93.2	92.8
Privacy Risk	High	Very Low
Encryption Delay (seconds)	N/A	1.4
User Satisfaction		

The results validate that the federated learning system provides performance levels comparable to centralized models while significantly enhancing privacy and maintaining practical responsiveness. These findings support the system's potential for realworld
deployment in decentralized medical environments.

V. CONCLUSION

The “Privacy Preservation with Prediction”
project offers a pioneering solution for secure, accurate, and scalable disease diagnosis in modern healthcare environments. By integrating Federated Learning (FL), Differential Privacy (DP), and
Lightweight Encryption mechanisms, the system effectively ensures both diagnostic precision and the confidentiality of sensitive patient data.
Moreover, the inclusion of personalized
healthcare recommendations enhances the clinical relevance and user-centricity of the platform.

5.1 Key Achievements:

Privacy-Preserving Diagnosis: The implementation of Federated Learning and Differential Privacy
ensures decentralized data processing, allowing accurate disease predictions without compromising patient confidentiality.

Robust Data Security: Lightweight encryption protocols safeguard patient information during communication and computation, supporting
compliance with healthcare data regulations.

Personalized Recommendations: AIbased modules deliver tailored healthcare guidance based on patient profiles, promoting proactive health management.

System Scalability and Adaptability: Designed to function across multiple healthcare institutions, the system supports collaborative intelligence without centralized data aggregation.

5.2 Future Enhancements:

Wearable Device Integration: Real-time data from IoT-based sensors (e.g., ECG, glucose monitors) can enhance dynamic and continuous health evaluation.

Blockchain-Enabled Transparency: Incorporating blockchain mechanisms will support immutable
logging of model updates and access events, reinforcing trust and auditability.

Mobile and Multilingual Interfaces: Android/iOS apps and regional language support can improve accessibility and user engagement across diverse
populations.

Telemedicine Modules: Secure video consultations and integrated e-prescription systems will bridge the gap between diagnosis and clinical intervention.

REFERENCES

1. H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in Proc. Of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), 2017, pp. 1273– 1282.
2. K. Bonawitz et al., "Practical Secure Aggregation for Privacy-Preserving Machine Learning," in Proc. Of the ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 1175–1191.
3. A. Geyer, T. Klein, and M. Nabi, "Differentially Private Federated Learning: A Client Level Perspective," in Advances in Neural Information Processing Systems (NeurIPS), 2017.
4. Y. Lu et al., "Lightweight Cryptography for Securing Federated Learning in Edge Environments," IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2506–2516, 2022.
5. B. Sheller et al., "Federated Learning in Medicine: Facilitating Multi-Institutional Collaborations without Sharing Patient Data," Scientific Reports, vol. 10, no. 12598, 2020.