International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 2, 2026

Federated Healthcare Recommendation System

Dr K.Ashok Kumar[1], Loukhya Reddy[2],Mokshitha[3],Soumya[4]

[1]associate Professor;Department Of Computer Science And Engineering (AI&Ml) Bhoj Reddy Engineering College For Women Hyderabad India

[2,3,4]b.Tech Students;Department Of Computer Science And Engineering (AI&Ml) Bhoj Reddy Engineering College For Women Hyderabad India

Mail Id;loukhyareddy@gmail.com[2],mokshitha.varimadugu@gmail.com[3],Soumyagaddala1@gmail.com[4]

Abstract

The rapid digitalization of healthcare has generated vast amounts of sensitive patient data through Electronic Health Records (EHRs), wearable sensors, and connected medical devices. However, conventional centralized healthcare recommendation systems often face serious challenges related to privacy breaches, unauthorized access, limited transparency, and poor interoperability among institutions. To address these concerns, this paper proposes a Federated Healthcare Recommendation System (FHRS) that combines Federated Learning (FL), Differential Privacy (DP), and Explainable Artificial Intelligence (XAI) for secure and intelligent clinical decision support.The proposed framework enables multiple hospitals and healthcare centers to collaboratively train machine learning models without sharing raw patient data. Instead, only encrypted model parameters are exchanged, preserving data confidentiality and regulatory compliance. Differential Privacy is integrated into local model updates to prevent reconstruction attacks and identity leakage during training. Furthermore, Explainable AI techniques such as SHAP and LIME are incorporated to generate transparent and interpretable recommendations, thereby improving trust among clinicians and patients.The system supports multimodal healthcare data including laboratory reports, imaging summaries, prescription history, wearable sensor data, and demographic records. It provides personalized treatment recommendations, disease risk prediction, and real-time monitoring insights. Experimental evaluation indicates that the proposed framework achieves high recommendation accuracy while significantly reducing privacy risks compared with centralized approaches.The Federated Healthcare Recommendation System offers a scalable, ethical, and privacy-aware solution for next-generation digital healthcare ecosystems. By combining secure collaborative intelligence with transparent decision-making, the framework contributes to patient-centered care and reliable AI adoption in healthcare environments.

Keywords: *Federated Learning, Healthcare Recommendation System, Differential Privacy, Explainable AI, Electronic Health Records, Privacy Preservation, Clinical Decision Support, Secure Healthcare Analytics.*

Introduction

The increasing adoption of digital healthcare technologies has led to the generation and storage of enormous volumes of sensitive patient information across hospitals, clinics, diagnostic centers, and laboratories. Although digital transformation has improved healthcare accessibility and operational efficiency, many institutions continue to depend on centralized data storage architectures. These traditional systems are highly susceptible to cybersecurity threats, unauthorized access, single-point failures, and inconsistent data governance practices. In addition, poor interoperability among healthcare providers often delays information exchange, reduces diagnostic efficiency, and negatively impacts patient outcomes. To overcome these limitations, the proposed HealthFed system introduces a privacy-preserving and intelligent healthcare recommendation framework by integrating Federated Learning, Differential Privacy, and Explainable Artificial Intelligence.The proposed framework eliminates the need to transfer raw patient records to a centralized repository. Instead, machine learning models are trained locally within participating hospitals, where only encrypted model updates are shared for aggregation. This distributed learning strategy preserves confidentiality while enabling collaborative intelligence across multiple healthcare institutions. Differential Privacy further strengthens security by introducing controlled noise into training updates, reducing the possibility of identity disclosure. Explainable AI techniques provide transparent and interpretable recommendations, helping doctors and patients understand the reasoning behind predictions. The system contains dedicated modules for administrators, medical staff, patients, insurance providers, and research analysts, thereby creating a complete ecosystem for secure healthcare operations. Through trusted data sharing, enhanced interoperability, and patient-centric control mechanisms, HealthFed supports the future of ethical and scalable digital healthcare.

Literature Survey

Healthcare prediction systems have evolved rapidly with the application of machine learning, deep

learning, federated intelligence, and explainable analytics. Earlier studies mainly relied on centralized machine learning approaches for disease prediction using structured clinical datasets. These methods demonstrated promising performance but introduced serious privacy concerns because all patient records were required to be stored in a single repository.

Smith and Lee (2021) analyzed traditional predictive models such as Logistic Regression, Decision Trees, and Random Forest algorithms for disease diagnosis. Their findings showed that these algorithms could achieve acceptable prediction accuracy for several healthcare datasets. However, the centralized architecture created vulnerabilities related to unauthorized data access and security breaches. Similarly, Gupta et al. (2022) investigated deep learning methods for multi-disease prediction and found that neural networks effectively captured hidden patterns in clinical information, improving prediction performance for diseases such as diabetes and heart disorders. Despite this advantage, deep models were often criticized for poor interpretability, making it difficult for clinicians to trust automated decisions.With increasing privacy concerns, researchers began exploring federated learning for healthcare systems. Verma and Kulkarni (2023) proposed a federated learning framework where hospitals collaboratively trained models without exchanging raw records. Their work demonstrated improved privacy preservation and institutional collaboration. However, they also reported challenges related to communication cost, synchronization delays, and model convergence. In another study, Chen and Wang (2023) focused on Explainable Artificial Intelligence using SHAP and LIME techniques to interpret medical predictions. Their results indicated that explanation mechanisms significantly improved transparency and confidence among healthcare professionals.Further developments were presented by Reddy et al. (2024), who designed a multi-disease prediction platform using specialized machine learning models for heart, lung, and liver disorders. While their disease-specific architecture improved classification performance, it remained limited by centralized deployment and lacked unified interpretability. Sharma et al. (2024) later combined federated learning with explainable analytics for healthcare applications, proving that privacy-preserving and interpretable AI solutions are more practical for real-world environments. However, usability and deployment simplicity were still insufficient.From the reviewed studies, it is clear that current systems often sacrifice one critical aspect for another, such as privacy, transparency, scalability, or usability. To address these persistent gaps, the proposed Federated Explainable Multi-Disease Prediction System combines federated learning for privacy-preserving collaboration, advanced machine learning for disease prediction, SHAP and LIME for interpretability, and a user-friendly web interface for real-time access. This integrated framework is designed to improve trust, efficiency, and clinical decision support in modern healthcare environments.

Methodology

The proposed system is designed as a distributed healthcare intelligence platform that securely connects hospitals, patients, insurance agencies, and research entities. It uses federated learning to train predictive models locally at each healthcare institution while maintaining data ownership and privacy. Each participating node trains the model using internal records, after which only encrypted parameters are transmitted to a central aggregator. The global model is updated and redistributed for the next training cycle. This process ensures privacy-preserving collaboration without exposing sensitive patient information.The system includes multiple functional modules. The Admin Module manages user accounts, controls hospital nodes, monitors training processes, and reviews system logs. The Medical Staff Module enables doctors and healthcare workers to register, log in, view patient histories, upload reports, update treatments, and access AI-generated recommendations. The Patient Module allows users to create accounts, view medical records, monitor treatment progress, and grant consent for the use of anonymized data in federated training. The Research and Analytics Module supports secure analysis, report generation, and submission of healthcare findings without direct access to raw private records. The Insurance Module verifies policies, reviews authorized patient information, validates claims, and updates payment decisions.

To ensure reliable performance, the platform is developed with strong non-functional characteristics. It provides real-time responses with low latency, scalable operation for multiple hospitals and users, responsive user interfaces, stable connectivity, encrypted communication, and simplified maintenance. Compatibility across desktop and mobile browsers improves accessibility for all stakeholders.The software environment consists of Windows 10, Flask for backend development, HTML/CSS/JavaScript for frontend design, MongoDB for database storage, and OpenStack for cloud deployment. Machine learning tasks are implemented using PyTorch or TensorFlow Federated frameworks, while SHAP and LIME are used for explainability analysis. Recommended hardware includes an Intel Core i5 processor or higher, 8 GB RAM, 256 GB storage, and reliable broadband connectivity for cloud communication.By combining secure distributed learning, interpretable predictions, and multi-stakeholder access control, the methodology creates

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

an effective framework for privacy-aware disease prediction and healthcare recommendation services.

Design

Architecture

The proposed Federated Explainable Multi-Disease Prediction System is designed using a modular and scalable architecture that combines distributed intelligence, privacy preservation, and user-centric healthcare services. The architecture enables secure interaction among hospitals, patients, administrators, insurance providers, and research entities while maintaining confidentiality of sensitive medical records. It is divided into software architecture and technical architecture to simplify implementation and ensure efficient coordination among all components.

Software Architecture

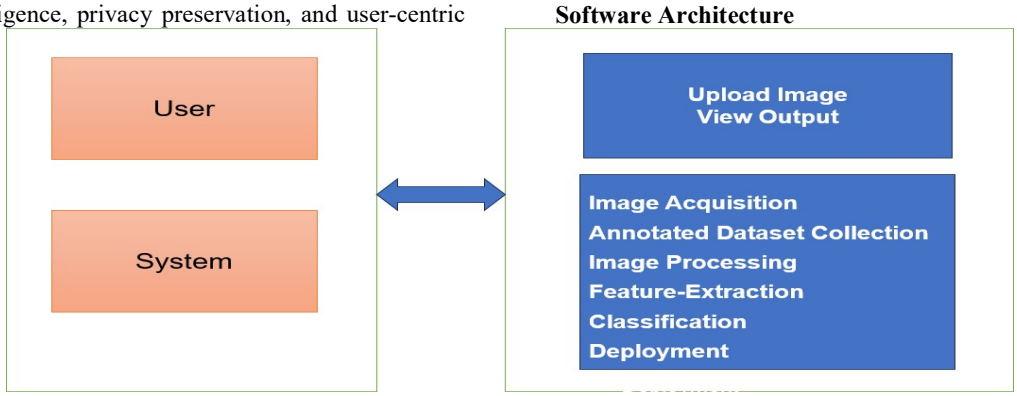

Figure-1 Software Architecture

The software architecture follows a layered design model consisting of presentation, application, intelligence, and data layers. The presentation layer includes web-based dashboards for administrators, doctors, patients, insurers, and researchers. These interfaces provide secure login, data access, prediction services, reports, and consent management. The application layer manages workflows such as user authentication, patient record handling, model requests, treatment recommendations, and claim verification.The intelligence layer contains machine learning and federated learning modules responsible for disease prediction, model training, and recommendation generation. Explainable AI tools such as SHAP and LIME are integrated into this layer to interpret outputs in a transparent manner. The data layer stores hospital records, patient profiles, wearable data, diagnostic reports, and encrypted model parameters in secure databases. This structured design ensures maintainability, extensibility, and efficient performance.

Technical Architecture

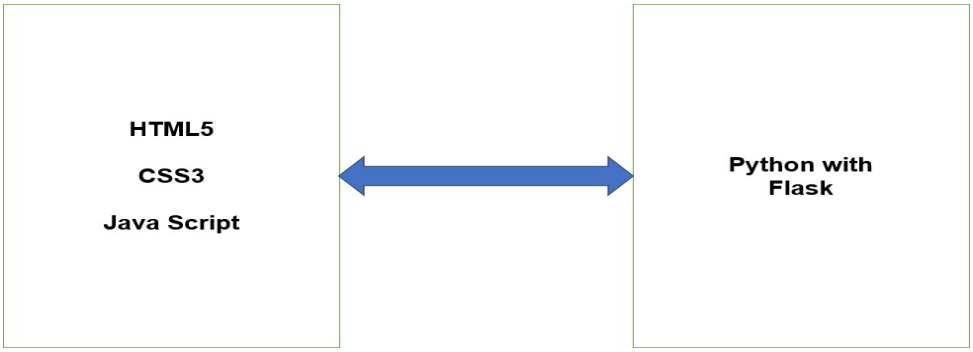

Figure-2 Technical Architecture

The technical architecture is based on distributed hospital nodes connected through a secure federated server. Each hospital node contains local patient data and independently trains disease prediction models. Instead of sending raw records, only encrypted model parameters are transmitted to the central aggregation server. The server combines updates from multiple nodes using federated averaging techniques and redistributes the improved global model.The frontend is developed using HTML, CSS, JavaScript, and Streamlit for interactive healthcare dashboards. Flask is used as the backend framework for API services and workflow management. MongoDB serves as the cloud database platform for structured and semi-structured medical data. PyTorch or TensorFlow Federated supports decentralized model training, while SHAP and LIME generate explanations for predictions. Secure communication is maintained through encryption protocols, role-based access control, and audit logging mechanisms.

Implementation

Technologies

The implementation of the proposed healthcare prediction platform combines modern web technologies, artificial intelligence frameworks, privacy-preserving mechanisms, and cloud infrastructure. The system environment is first configured to support distributed hospital nodes and secure communication channels. Hospital nodes are registered and connected to the federated server, where each institution maintains its own local data repository.A structured patient data schema is designed to manage Electronic Health Records, wearable sensor information, and laboratory results. Federated learning clients are deployed at hospital nodes to perform local model training using internal datasets. Differential Privacy techniques are incorporated during parameter updates to protect user identity and reduce leakage risks. A secure aggregation mechanism combines local model weights to create an improved global model.Version control is applied to maintain multiple global model releases and enable rollback if required. Explainable AI libraries such as SHAP and LIME are integrated to provide transparent outputs for doctors and patients. Consent-based workflows ensure that patient data participation occurs only after authorization. APIs are developed for doctors, insurers, patients, and administrators to support secure transactions.

Authentication and authorization are managed through role-based access control mechanisms. Data encryption protects information during storage and transmission. Dedicated dashboards are developed for administrators, clinicians, and patients to access predictions, logs, and reports. Real-time inference pipelines generate rapid disease risk assessments. Monitoring tools supervise federated rounds, system health, and communication failures. Backup strategies protect models and logs, while periodic retraining ensures model relevance. Future extensions may include telemedicine support, IoT integration, and multi-modal diagnostics.

Pseudo Code Description

The prototype implementation is developed using Streamlit for the user interface and Python-based machine learning libraries for backend analytics. After user login validation, the system loads dashboards and displays disease prediction modules for Diabetes, Heart Disease, Lung Disease, and Liver Disease. Users enter medical parameters through forms, after which the corresponding trained model is loaded.The selected model predicts disease presence and calculates risk probability scores. Results are displayed visually using progress bars, metrics, and status indicators such as low, moderate, or high risk. Input summaries are shown for user verification. SHAP explanations are generated to identify which clinical factors contributed most strongly to the decision. LIME is used to provide local explanations for individual cases. Finally, the system displays possible symptoms and healthcare recommendations based on predicted outcomes. This workflow combines usability, prediction intelligence, and interpretability in one platform.

Testing

Software testing is a critical process used to validate whether an application performs according to expected requirements while maintaining reliability, performance, and security. In healthcare applications, testing becomes especially important because users may rely on predictions and recommendations for health-related decisions. Any errors in prediction logic, input handling, or explanation outputs could reduce trust and lead to incorrect interpretations.In this project, testing is performed across all disease modules including Diabetes, Heart, Lung, and Liver prediction systems. Validation includes correctness of preprocessing steps, prediction outputs, federated learning workflows, and explainability mechanisms using SHAP and LIME. Security testing also ensures confidentiality of sensitive medical information in distributed environments.

Stages of Testing

Unit testing is performed on individual components such as preprocessing scripts, model loaders, and explanation generators. Integration testing evaluates communication among interfaces, backend APIs, prediction engines, and visualization modules. System testing examines the complete application in a realistic environment, ensuring that all modules work together correctly. Acceptance testing is conducted with end users to confirm usability, reliability, clarity of explanations, and readiness for deployment.

Types of Testing

Black box testing is used to validate outputs against supplied inputs without examining internal code logic. It confirms whether disease predictions and recommendations match expected behavior. White box testing is applied to internal logic, code paths, conditional branches, and algorithm pipelines to ensure correctness and coverage. Both methods complement each other in building a dependable healthcare application.

Test Cases

Representative test cases include verifying successful login for authorized users, checking validation messages for incomplete inputs, confirming correct disease predictions for known medical samples, ensuring explanation charts are generated after predictions, testing secure logout behavior, and validating performance under multiple concurrent requests. These test cases demonstrate functional correctness, robustness, and practical usability of the proposed system.

Results

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

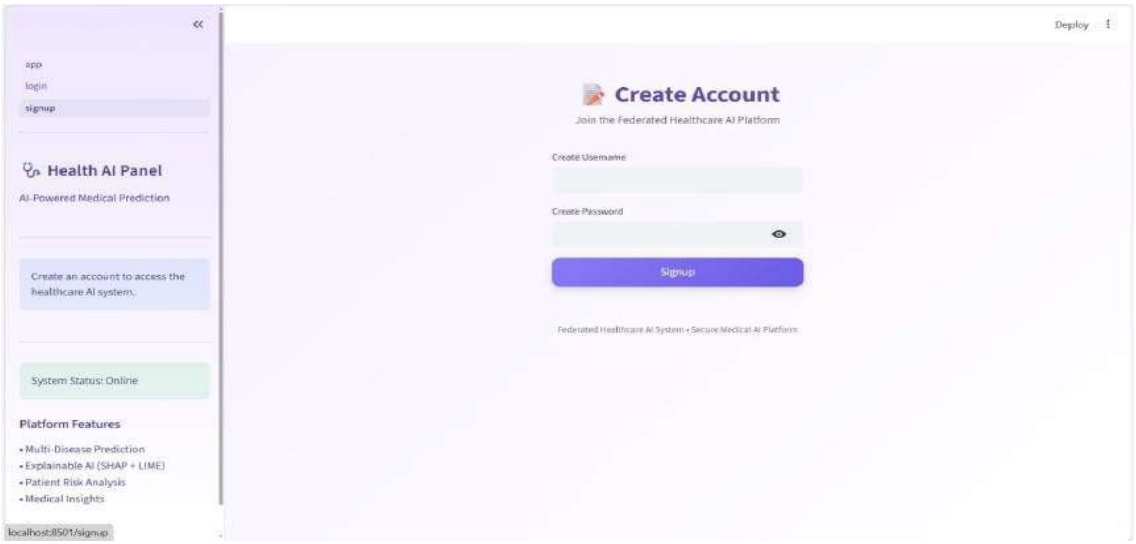

Figure-1 Home Page

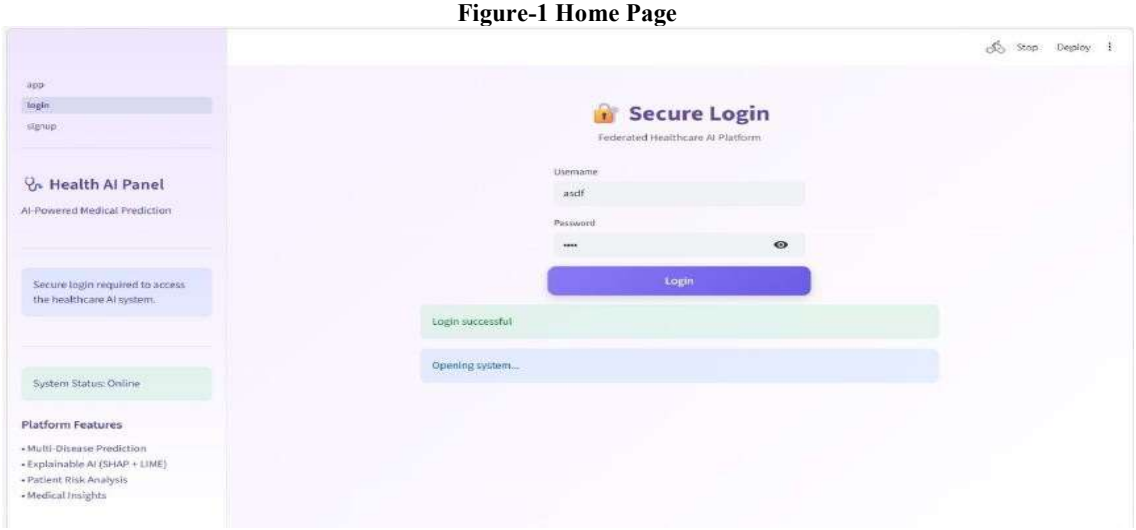

Figure-2 Home Page

Figure-3 AI Health Panel

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

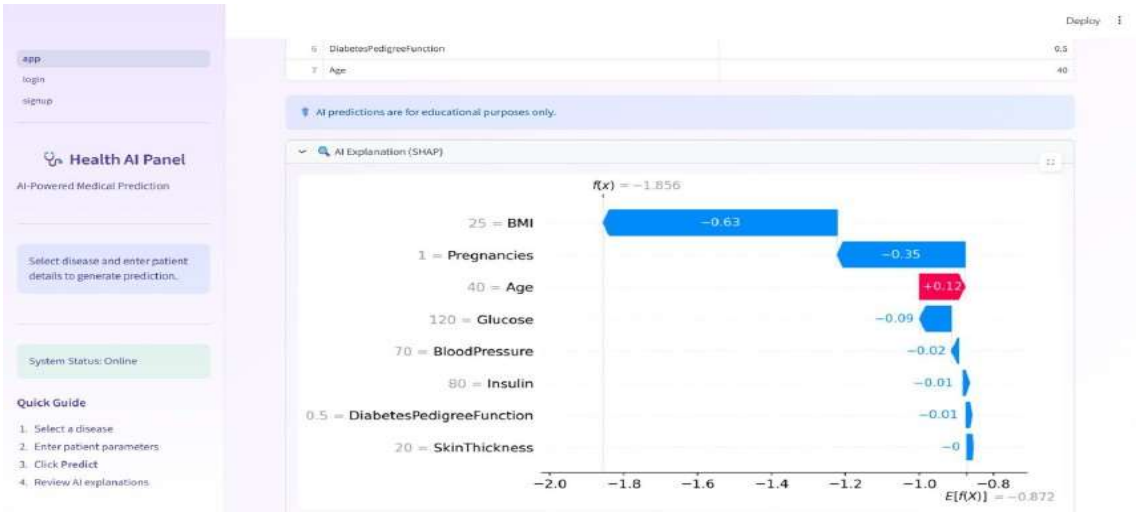

Figure-4 AI Health Panel

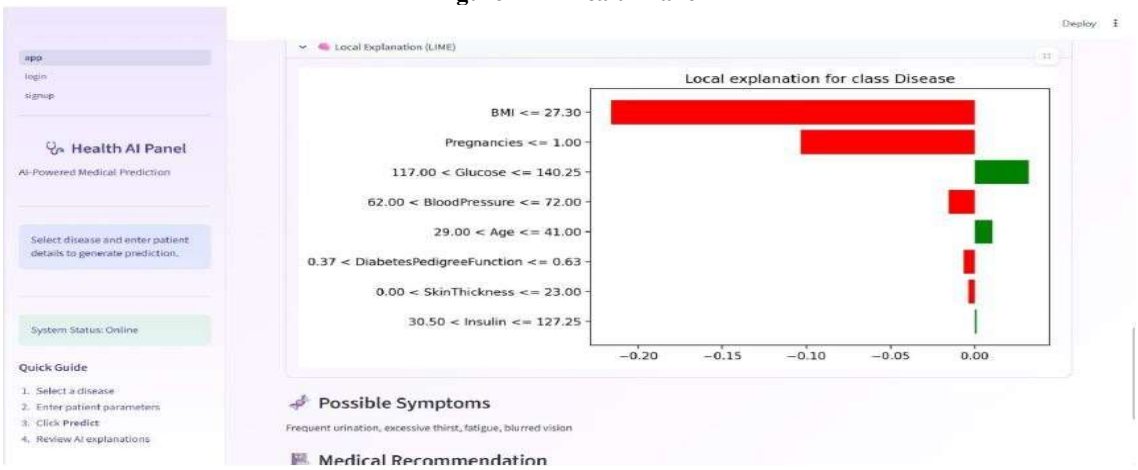

Figure-7.5 Output

Conclusion

The proposed Federated Healthcare Recommendation System presents an efficient and privacy-aware solution for modern digital healthcare environments. Traditional healthcare analytics often depend on centralized data storage models, which increase the risk of cyberattacks, unauthorized access, and regulatory non-compliance. The developed framework overcomes these limitations by adopting Federated Learning, where patient records remain within hospitals or healthcare institutions while only model parameters are exchanged for collaborative training. This decentralized strategy significantly strengthens data protection and supports secure cooperation among multiple medical organizations.The system also improves healthcare intelligence by generating personalized recommendations related to treatments, specialist consultation, disease prevention, and health monitoring. Since learning is performed from distributed datasets, the recommendation engine benefits from broader knowledge patterns without compromising confidentiality. The inclusion of Differential Privacy mechanisms further enhances security by preventing sensitive information leakage during parameter sharing. In addition, Explainable Artificial Intelligence methods improve transparency by clarifying the reasons behind system recommendations, thereby increasing trust among doctors and patients.Another important contribution of the framework is its scalability and adaptability. The system can operate across multiple hospitals, clinics, laboratories, and connected devices while maintaining consistent performance. It also supports interoperability between institutions, helping to reduce delays in diagnosis and treatment planning. By combining privacy preservation, intelligent analytics, and transparent decision support, the Federated Healthcare Recommendation System demonstrates a reliable pathway toward secure patient-centered healthcare services. Overall, the framework successfully balances data utility, trustworthiness, and operational efficiency, making it highly suitable for future healthcare ecosystems.

Future Scope

Although the proposed system provides a strong foundation for secure healthcare recommendations, several enhancements can further improve its real-world impact. One promising direction is the integration of wearable devices and Internet of Things healthcare sensors for continuous monitoring of patient vitals such as heart rate, glucose level, oxygen saturation, and physical activity. Real-time federated updates from such devices would enable dynamic recommendations and early disease detection.Future versions may also incorporate advanced deep learning architectures capable of processing multimodal medical data, including radiology images, clinical notes, genomic records, and sensor streams. These models can improve prediction accuracy for complex diseases and support personalized treatment planning. Stronger privacy technologies such as Homomorphic Encryption and Secure Multi-Party Computation can be integrated to protect data even during model computation and aggregation stages.Another major opportunity lies in expanding the framework for cross-border healthcare collaboration, where hospitals in different countries can jointly train models while complying with regional laws and international data governance standards. Blockchain technology may also be adopted to maintain immutable audit logs, consent records, and trusted data-sharing transactions. Further development of Explainable AI dashboards with visual reasoning tools can help clinicians better interpret recommendations and improve acceptance of AI systems in medical practice.In addition, future research can focus on adaptive federated optimization methods that reduce communication cost, manage non-identical hospital datasets, and improve convergence speed. Telemedicine integration, multilingual support, and mobile healthcare applications are also valuable directions for increasing accessibility. With these advancements, the Federated Healthcare Recommendation System can evolve into a globally deployable, intelligent, and fully trusted digital healthcare platform.

References

[1] McMahan, B., Moore, E., Ramage, D., Hampson, S., and Aguera y Arcas, B., "Communication-Efficient Learning of Deep Networks from Decentralized Data," AISTATS, 2017.
[2] Abadi, M., Chu, A., Goodfellow, I., et al., "Deep Learning with Differential Privacy," ACM CCS, 2016.
[3] Lundberg, S. M., and Lee, S. I., "A Unified Approach to Interpreting Model Predictions," NeurIPS, 2017.
[4] Ribeiro, M. T., Singh, S., and Guestrin, C., "Why Should I Trust You? Explaining the Predictions of Any Classifier," KDD, 2016.
[5] Kairouz, P., McMahan, B., Avent, B., et al., "Advances and Open Problems in Federated Learning," Foundations and Trends in Machine Learning, 2021.
[6] Rieke, N., Hancox, J., Li, W., et al., "The Future of Digital Health with Federated Learning," NPJ Digital Medicine, 2020.
[7] Sheller, M. J., Reina, G. A., Edwards, B., et al., "Federated Learning in Medicine: Facilitating Multi-Institutional Collaborations," Scientific Reports, 2020.
[8] Li, T., Sahu, A. K., Talwalkar, A., and Smith, V., "Federated Learning: Challenges, Methods, and Future Directions," IEEE Signal Processing Magazine, 2020.
[9] Bonawitz, K., Ivanov, V., Kreuter, B., et al., "Practical Secure Aggregation for Privacy-Preserving Machine Learning," ACM CCS, 2017.
[10] Dwork, C., and Roth, A., "The Algorithmic Foundations of Differential Privacy," Foundations and Trends in Theoretical Computer Science, 2014.
[11] Tjoa, E., and Guan, C., "A Survey on Explainable Artificial Intelligence in Healthcare," IEEE Transactions on Neural Networks and Learning Systems, 2020.
[12] Esteva, A., Robicquet, A., Ramsundar, B., et al., "A Guide to Deep Learning in Healthcare," Nature Medicine, 2019.
[13] Miotto, R., Wang, F., Wang, S., Jiang, X., and Dudley, J., "Deep Learning for Healthcare: Review, Opportunities and Challenges," Briefings in Bioinformatics, 2018.
[14] Google AI, "Federated Learning: Collaborative Machine Learning without Centralized Data," Technical Report, 2017.
[15] Sheller, M. J., Edwards, B., Reina, G., et al., "Multi-Institutional Deep Learning Modeling without Sharing Patient Data," BrainLes Workshop, 2019.